Wireless Communications and Mobile Computing

Internet of Things, Artificial Intelligence and Machine Learning: Architecture, Algorithms, and Applications

Lead Guest Editor: Shafiq Ahmad
Guest Editors: Md. Shamsul Huda and Muhammad Imran

Internet of Things, Artificial Intelligence and Machine Learning: Architecture, Algorithms, and Applications

Wireless Communications and Mobile Computing

Internet of Things, Artificial Intelligence and Machine Learning: Architecture, Algorithms, and Applications

Lead Guest Editor: Shafiq Ahmad
Guest Editors: Md. Shamsul Huda and Muhammad Imran

Chief Editor

Associate Editors

Academic Editors

Contents

Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 1005813, 17 pages
https://doi.org/10.1155/2022/1005813

Research Article

Application of Industrial Internet of Things (IIoT) in Crude Oil Production Optimization Using Pump Efficiency Control

Ali S. Allahloh,[1] **Mohammad Sarfraz**,[1] **Mejdal Alqahtani**,[2] **Shafiq Ahmad**,[2] **and Shamsul Huda**[3]

[1]*Department of Electrical Engineering, Aligarh Muslim University, Aligarh, India*
[2]*Industrial Engineering Department, College of Engineering, King Saud University, P.O. Box 800, Riyadh 11421, Saudi Arabia*
[3]*School of Information Technology, Deakin University, Australia*

Correspondence should be addressed to Mohammad Sarfraz; msarfraz@zhcet.ac.in

Received 22 February 2022; Accepted 8 August 2022; Published 7 October 2022

Academic Editor: SK Hafizul Islam

The collapse of oil prices in mid-2014 and early 2016 was the biggest in modern history that witnessed more than a 70% drop in the price to around $40 barrel. It prompted companies to think seriously to maintain profitability. Most companies were able to survive partly by simplifying their operations. Price recovery in 2021 is only 70% of its peak value. Companies are focusing on reducing the cost of operations, increasing production simultaneously, and finding new and different strategies to survive. The current scenario is witnessing strong research focusing on the development of process control for oil and gas upstream and downstream to improve the control and preventive maintenance to reduce operating costs and increase production. This paper presents the Industrial Internet of Things (IIoT) practical solution that improves the oil production rate from the well and increases the average pump efficiency (fillage) to 90%. This paper proposes a mechanism for collecting, storing, and analyzing all required parameters to build valuable charts. These charts' data help optimize the values and parameters for controller setpoints to prevent pump gas lock problems. An artificial lift is required to lift the oil from the well. In this paper, the sucker rod pump is driven by a gas engine fed by the well's gas. At the same time, SCADAPack 535E remote terminal unit collects all pump and well parameters such as hydraulic pressure, casing pressure, tubing pressure, and pump speed in stroke per minute (SPM). The remote terminal unit sends the data through a wireless network using a 5 GHz antenna to the main control room. The IIoT platform is designed using a visual basic programming language. Microsoft DDE (Dynamic Data Exchange) and Kepware OPC server were used to work on the received data to monitor, generate charts, and apply the controllers.

1. Introduction

Intelligent oil and gas production depends on understanding all crude oil well and pump parameters. Ensure the uniform increase of liquid production rate from the crude oil well and avoid problems such as gas lock. Field operators currently record these parameters two or three times a day, giving experts a fuzzy picture. Increasing guesswork due to the dynamic behavior of these parameters, which changes minute after minute, this paper introduces an approach to thoroughly understanding the surface and downhole parameters. Using Industrial Internet of Things technology (IIoT) gives users a clear picture. It reduces the guesswork and optimizes different parameters to maximize the production for the long-term in a stable situation. Over 90% of the wells in the United States are currently being artificially lifted. Beam pumping is the most commonly used method, accounting for over 85% of artificial lift installations. The beam pumping system is mechanically very simple. It consists of a surface unit that transmits the upstroke and downstroke motion to a bottom-hole pump through a sucker rod string (Figure 1). While the system is simple, a proper design requires many factors. Over the years, formulas developed to be used in the optimum pumping design. However, a good design still depends on experience as a key.

Energy from the crude oil pumping unit is transmitted to the bottom-hole pump through a sucker rod string. Sucker rod strings operate under cyclic load in erosive and corrosive

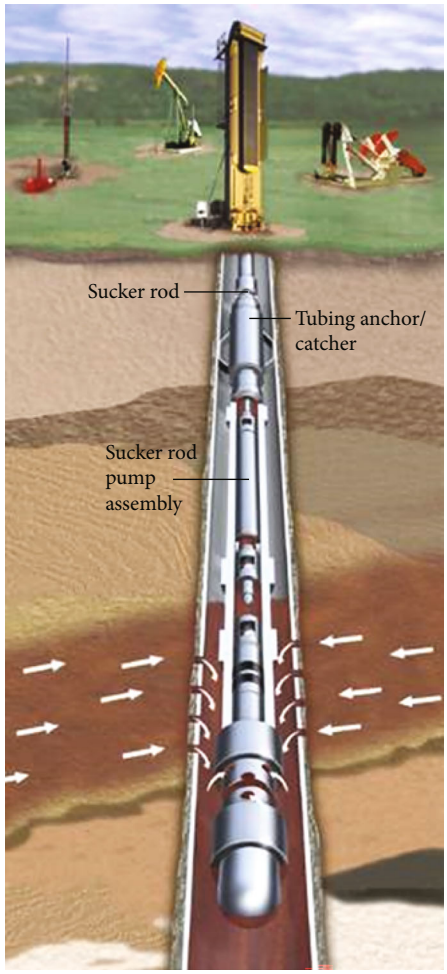


Figure 1: Sucker rod pump.

environments. At the same time, the target is a good sucker rod design is the most critical part of a successful sucker rod pumping system. It will decrease the pulling cost and increase production. The next step is the surface unit. In this paper, the surface unit is the gas engine that feeds by the well gas itself to reduce the cost. At the same time, the jack pump is driven by SCADAPack 535E remote terminal unit. It is an IIoT device to provide a local and remote controller to prevent the gas lock problem using an on-off controller and the oil well casing pressure, PID controller. It ensures the well's liquid level and pumps fillage at optimum values.

1.1. Literature Review. Our work proposes an IIoT-based strategy to control the smart sucker rod pump automatically and intelligently. The development of this strategy aims to ensure the optimization of oil well production using AI models that enable IIoT closed-loop process control. The Industrial Internet of Things found its way to the oil and gas industry via building online intelligent controllers, such as fuzzy logic or neurofuzzy, developing the management and control, centralizing the data, or digitalizing the production process for intelligent production purposes [1, 2]. The current research discussed control strategy, efficiency, optimization, multiphase, pump fillage calculation, pumping system simulation, and an expert system to develop the sucker rod pump system. On the other side, researchers focus on using the IIoT in oil and gas for management, health, and safety to reduce maintenance costs. Integrating optimization and process control with IIoT is still a gap in this field. Our work introduces the solution to integrate intelligent pump control with an IIoT system. The review of the current research discussed below:

In this work, authors describe the control strategy method for the sucker-rod pumping (SRP) system which is discussed; this method stands out for its simplicity and low cost in maintenance and investment, and it can be operated in a large range of flow rates with fluids of different compositions and viscosities. The sucker rod pump units require periodic maintenance and adjustments, whether preventive or corrective. Two common procedures are important for the sucker rod pump units: the first one is to adjust the counterbalancing of the pumping unit, while the second is to adjust the polished rod stroke length. Stopping oil well production is required to accomplish these procedures [3]. A special design for the sucker rod pumping unit using a given condition was studied and tested. A horizontal wellbore with a range of up to 90 degrees bore curvature operated by sucker rod pumping units was studied. The target was to increase the volume efficiency, reduce bottom hole pressure, and decrease the gas impact while increasing drainage speed for the best sucker rod pump efficiency. The gas impact increases in the drainage speed for the best sucker rod pump efficiency [4]. In this work, the author tunes the production potential and controls the oil well rate by understanding all parameters to face the challenge in unconventional reservoirs: the deliverability of the reservoir governing the rate changes with time. The complexity of understanding an artificial lift well's performance pushes the author to optimize the oil well production gains by changing the operating parameters and then finding the optimization and modeling approaches that affect well performance [5]. This paper discussed and developed a pragmatic and robust technique to design and apply a multiphase sucker rod pump in oil wells with high gas-oil ratios. More specifically, in the design of the sucker rod pump structure according to pump working mechanism in the presence of various liquid contents and high gas-oil ratios, effective solutions were enhancing oil production by enforcing gas evacuation. They designed a unique gas buffer to include both chamber gas and fluid inside and connected it through the slotted liner to prevent the pump from the gas lock. In addition, this gas buffer can be bypassed if the stroke is shortened as the traditional downhole pump [6]. This work shows an advanced approach to optimize the sucker rod pump. While most of the operators still depend on surface dynocards for sucker rod pump diagnostic, the author shows the value to use wave equation mathematical calculations as pump (calculated) dynocards to obtain production insights [7]. This paper shows the importance of knowing the correct value of pump fillage in the oil well control to represent the pump efficiency and optimize the production of a rod pumping well. The downhole card graphical representation is often used to know the pump fillage, which can

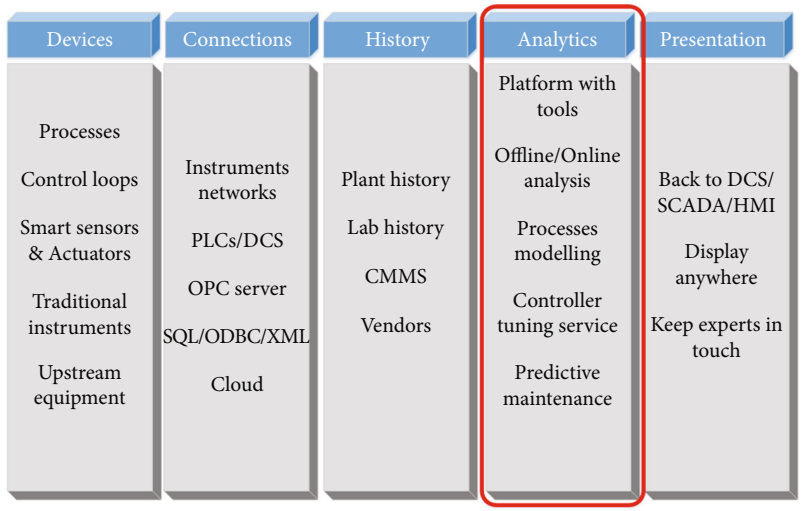


Figure 2: IIoT platform potential.

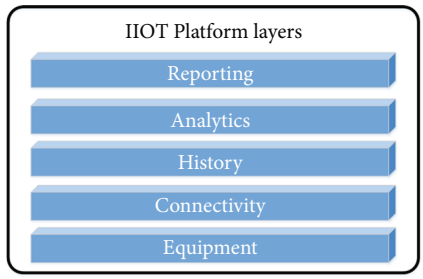


Figure 3: IIoT platform layers.

sometimes be inaccurate. The authors introduced a compute method that used the downhole position to calculate pump fillage. The pump fillage accurate calculation involves the correct location of the transfer point, and it is the point of transferring the load from the standing valve to the traveling valve: a method comprised of four algorithms to locate the transfer point introduced. Correct transfer point location extracted using a combination of these methods, the accurate value of the pump fillage optimizes well production. Application of the method over numerous data sets resulted in a wide coverage range of conditions for optimizing sucker rod pump well assets [8]. The authors discussed how a sucker rod pumped oil well increased the gas to liquid ratio, in addition to the unconventional reservoirs that have high gas to liquid ratio from the beginning of production. To improve the sucker rod pump, the gas production efficiency should be handled. Several methods are used to handle gas production, increasing the sucker rod pump efficiency. The authors focused on three areas, gas separator design, variable speed drives, and the backpressure valves [9]. This work discussed how advanced technologies could overcome many common problems in downhole and surface, such as unconventional oil wells production, high gas oil wells, and sandy oil wells. High-capacity sucker rod pumps with ultralong stroke length maximize the production from heavy crude wells with a high liquid rate with fewer problems of downhole equipment. This technology affects operation costs by reducing the OPEX maintenance and the number of operators required [10]. This paper discussed the most common artificial lift technology, a sucker rod pump, and focuses on the efficiency problems caused by incomplete pump fillage. This problem results from a pump capacity that exceeds the rate of production from the well or gas lock. High pump fillage means lower cost, and more efficient operations will result. The author also presents using the pump off the controller to control pump run time to keep the pump displacement in harmony with the wellbore volume to avoid shock loading problems that occur on 24 hours running well with pump capacity excess wellbore volume [11]. The problem of obtaining downhole data makes monitoring the hydraulic performance of the sucker rod pump difficult. These data, including gas interference, pump fillage, gas locking, sticking valves, fluid pound, equipment failure, rod downstroke compression loading, and reduced production, are difficult to diagnose from the surface. Currently, guesswork and component analysis are the base of root cause analysis. They also develop a sucker rod pump knowledge base [12]. They explained the expert technology and system applications to diagnose sucker rod pumps. This capture expert's knowledge approach is held by a few individuals and makes it available on PC to record it permanently to solve more difficult problems. The authors developed a rule-based expert system that gives users a clear picture to analyze the subsurface pump problems. The analysis information obtained by the presented system utilizes auxiliary programs available for users. The need for such a system means growth in production and reducing the maintenance cost, especially for the wells far away from the head office, to reduce the cost of delayed analysis [13]. The authors discuss the digital transformation and IIoT, and it is effective to keep the plant running, reduce the maintenance cost, and extend life time of equipment that led to increase the productivity. Also, review the IIoT-based project examples to reduce the human and equipment costs in the oil and gas field [14, 15]. They discussed the impact of industry 4.0 and operations based on data centric on oil and gas production that led to discover various scenarios about

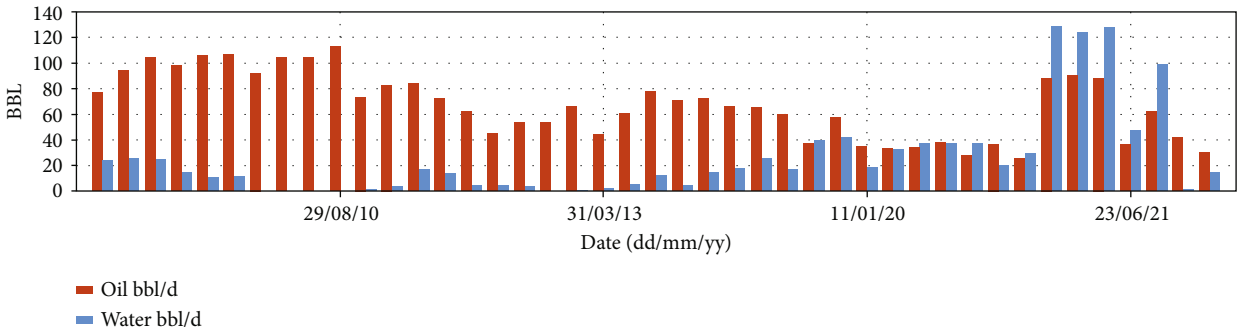


Figure 4: History of selected crude oil well tests with and water capacity.

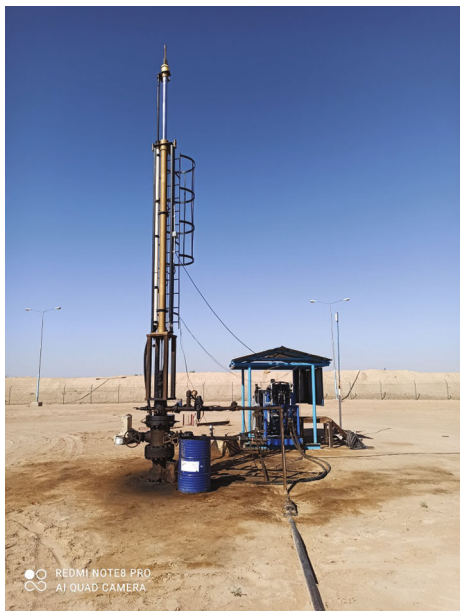


Figure 5: Crude oil pump surface unit.

the future of oil and gas industry [16, 17]. Authors discussed a cyber-physical system for an IoT-based industrial solution such as SCADA to monitor and control their critical infrastructure [18]. Data privacy and security in the Industrial Internet of Things application discussed by enabling user authentication with transfer learning empowered blockchain [19]. Authors discussed machine learning-based malware attack detection protocol in the IoT industrial multimedia environment [20]. New key management and remote user authentication scheme is proposed for securing 6G-enabled NIB deployed for industrial applications [21]. Novel blockchain-edge framework for industrial IoT networks was proposed. It ensures low latency services for industrial IoT applications and optimizes the network usage, the data integrity, trust, and security ensured by a decentralized way provided by blockchain [22].

2. IIoT in Process Control

Industrial IoT is the application of IoT in process control and manufacturing to ensure data exchange between various instrumentation and control equipment. Figure 2 shows the potential of the IIoT platform in the process control industry by providing the analysis tools for predictive maintenance through device health analysis and automated tuning recommendations for controllers through analyzing the interaction, error, variance, model, and knowing the tuning needs. Figure 3 shows the IIoT platform layers for the oil and gas plant. These layers are equipment, communications, history, analytics, and reporting.

The equipment layer includes the processes, control loops, smart sensing and actuating devices, and traditional sensing and actuating devices. In contrast, the communication or connection layer includes industrial wireless, Profinet, fieldbus, and OPC. The history layer includes all data collected from processes, maintenance management system, laboratory information system, and logistics system.

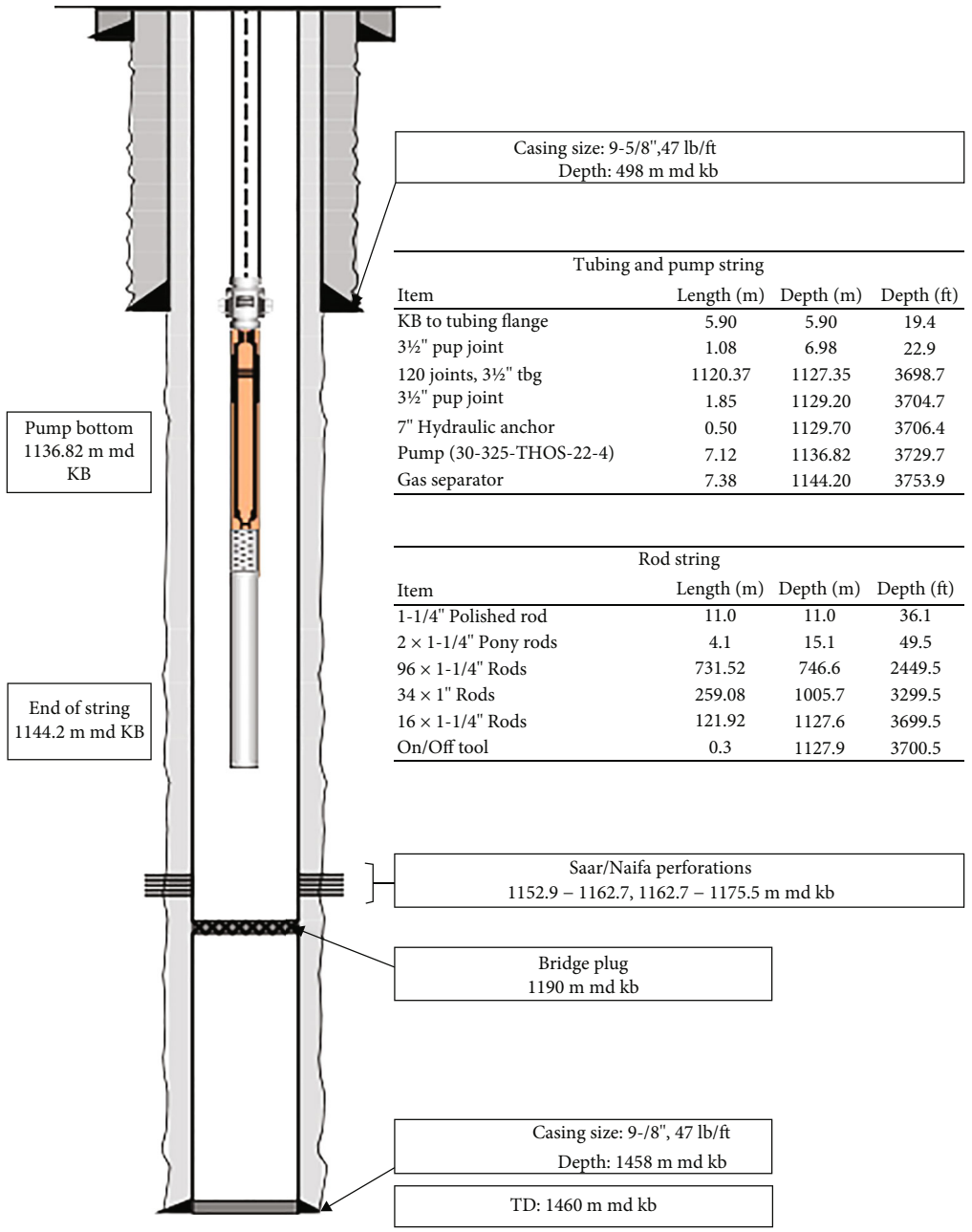
The analytic layer is the most important layer because it is the core of IIoT's strength. It gives the Industrial Internet of Things power to apply intelligent algorithms such as genetic algorithms, neural networks, fuzzy logic, and neuro-fuzzy to control the complex nonlinear and dynamic processes. The analytic layer affects the reporting layer and shows better results of production due to the smooth operation and high quality of process control and automation.

3. Crude Oil Well

This paper selected a crude oil well drilled in 2008 in Yemen for the study. We showed the effect of the Industrial Internet of Things by applying control algorithms or tuning parameters to ensure maximum production with the lowest cost.

3.1. Selected Crude Oil Well History. The oil field downstream facility has a small separator used to test every crude oil individually for 24 hours or more to know the crude oil production rate. Furthermore, it separates the oil, water, and gas from the crude oil. It measures the average daily production rate for oil, water, and gas. Figure 4 shows the crude oil well test history with 43 tests that indicate the maximum and minimum production of crude oil and water.

3.2. Crude Oil Pumping Control. The pump surface unit shown in Figure 5 includes all parts main prime mover (gas engine), and the hydraulic jack pump gives positive displacement to the pump. The SCADAPack 535E controller is used for the control unit. It links the wireless technology



Tubing and pump string

Item	Length (m)	Depth (m)	Depth (ft)
KB to tubing flange	5.90	5.90	19.4
3½" pup joint	1.08	6.98	22.9
120 joints, 3½" tbg	1120.37	1127.35	3698.7
3½" pup joint	1.85	1129.20	3704.7
7" Hydraulic anchor	0.50	1129.70	3706.4
Pump (30-325-THOS-22-4)	7.12	1136.82	3729.7
Gas separator	7.38	1144.20	3753.9

Rod string

Item	Length (m)	Depth (m)	Depth (ft)
1-1/4" Polished rod	11.0	11.0	36.1
2 × 1-1/4" Pony rods	4.1	15.1	49.5
96 × 1-1/4" Rods	731.52	746.6	2449.5
34 × 1" Rods	259.08	1005.7	3299.5
16 × 1-1/4" Rods	121.92	1127.6	3699.5
On/Off tool	0.3	1127.9	3700.5

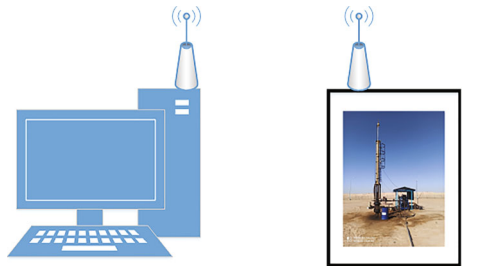
Figure 6: Crude oil pump downhole installation and well bore data.

through the 5 GHz nanostation to the main control room. The IIoT platform is installed to collect the data, monitor the whole operation, draw the charts, and apply the control algorithms.

Figure 6 shows the downhole pump installation, including all data such as casing size, depth, tubing and pump string, and rod string.

4. Design and Configuration of IIoT System

This paper purposes novel system hardware and software setup that includes IIoT device, communication network, data acquisition, data log, SCADA, control, and valuable charts.



IIoT platform and SCADA system

Sucker rod pump with IIoT device

Figure 7: Proposed hardware system.

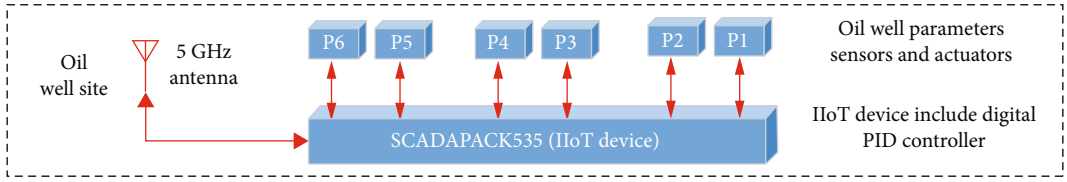


Figure 8: SCADAPack535E IIoT device.

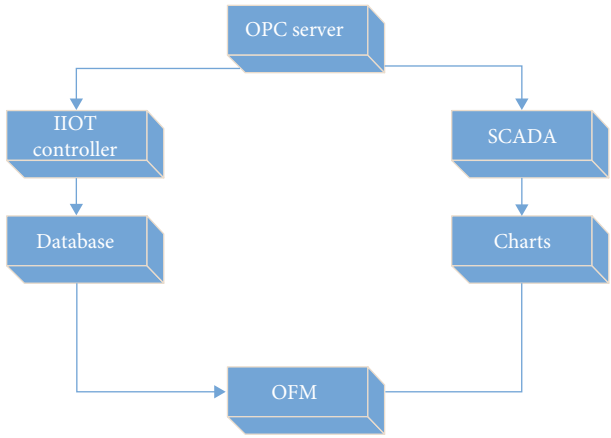


Figure 9: Proposed software system.

4.1. Proposed Hardware System. Figure 7 shows the purposed hardware system. It includes the sucker rod pump, SCADAPack 535E as IIoT device, a 5 GHz antenna, and a server in the control room that will include the IIoT platform and SCADA system. The difficult nature of the environment for oil and gas fields represents a real challenge, considering oil well scattered location and distance from the central processing facility which made the industrial wireless Ethernet the solution for data acquisition, especially nanostation M5 5 GHz antennas that provide a reliable connection for up to 10 km.

Figure 8 shows SCADAPack 535E remote terminal unit and automation controller from Schneider Electric; they are the perfect solution for IIoT applications that need high-speed time stamping and data capture. With an open standard programming environment, SCADAPack 535E supports standard industrial communication protocols such as Modbus RTU, Modbus TCP, and even DNP3 level 4 with security suit and data encryption. SCADAPack 535E works as an agent for the IIoT platform. It collects the data from engine sensors through Modbus RTU communication protocol. Also, it collects data from the rod pump and oil wellhead sensors using 4-20 ma I/O. Finally, SCADAPack 535E sends the data to the control room using Modbus TCP communication protocol through nanostation M5 5 GHz antenna.

4.2. Proposed Software System. Figure 9 shows the proposed software system; in this paper, the Kepware OPC server collects the crude oil well controller (SCADAPACK 535E) through a 5 GHz wireless link using TCP/IP network that passes it to two main branches, SCADA and IIoT platform.

The SCADA system monitors and generates valuable charts. At the same time, the IIoT platform uses these data for modeling, controlling and forecasting, and storing optimum parameters in the database. The two branches then send the data to the OFM (Oil Field Manager) software from Schlumberger, France. The visual basic programming language was used to build the SCADA system and IIoT platform. Figure 10 shows the proposed software implementation algorithm.

Figure 11 shows the proposed platform working flowchart. It clarifies the build of machine learning-based AI models that simulate the expert's responses. The proposed platform uses code to prepare training datasets by recording all expert's resonances that achieved the goals and increased pump efficiency. Machine learning builds the prediction models using training datasets.

4.3. Sucker Rod Pump Performance Calculation for Production Maximization. Because it is difficult to measure the crude oil level in the well continuously and stop the pump during the measuring process, the pump performance is needed to indicate the level and pump fillage. So, the dynamometer card is used to accomplish this job while the surface card displays the load on the polished rod over the pump cycle. The card result shape is a function of everything, such as speed in stroke per minute, PPU geometry, pump depth, and fluid load on the pump, while the wave equation mathematically models the elastic nature of the rod string (assuming a downhole friction factor) and uses the surface card data to represent what happens at the pump plunger.

A dynagraph card represents the forces acting on the pump plunger as it moves upward and downward in the well, capturing and releasing fluid with each stroke. Surface and downhole dynagraph cards measure the load on the polished rod, and this load is plotted with the polished rod position as the pump moves through each stroke cycle. A complete stroke cycle is one up and downstroke. The controller uses this data to create an x-y plot. By observing the graphs, information about the efficiency of the pump operation can be collected. Rather than being a plot of load vs. time, as shown below in Figure 12, a card is a plot of load vs. position, as shown in Figure 13. The ideal card, as shown above in Figure 13, demonstrates the instantaneous increase in load from $L_{\min}$ to $L_{\max}$. The pump plunger begins its upward stroke, and the load remains constant as it travels to the top. As soon as the pump plunger starts back down, the load instantly falls back to $L_{\min}$ where it remains constant as the pump travels to its bottom position again.

The card shown in Figure 14 shows a dynacard with an ideal upstroke and 30% pump fillage, demonstrating the effect of conditions such as fluid pound. If the traveling valve

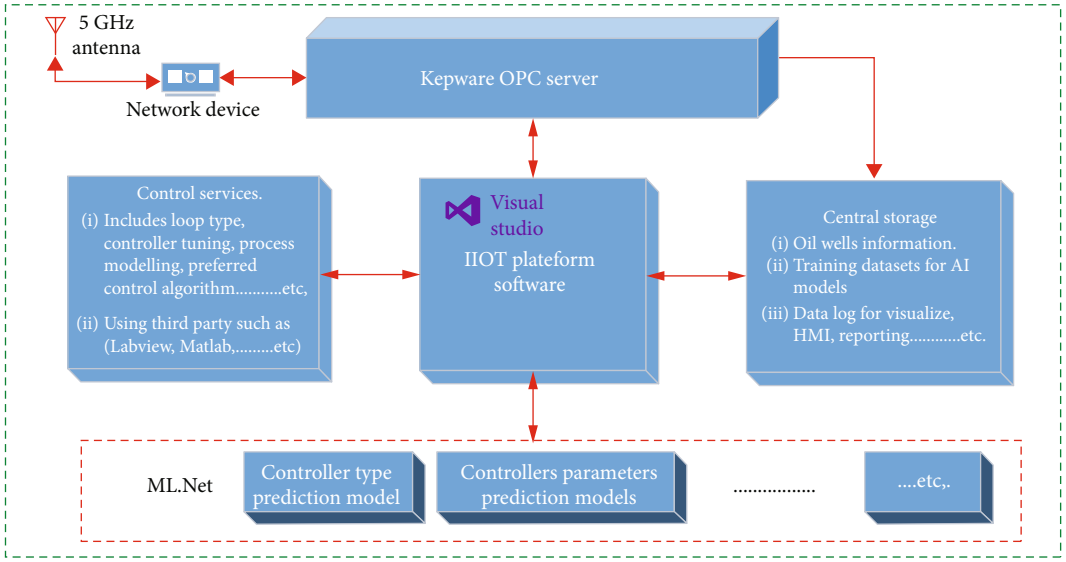


Figure 10: Proposed software implementation algorithm.

on the pump opens properly, the load falls instantly to $L_{\min}$ and remains constant for the entire downstroke (P_{top} to P_{bottom}), and the fluid is transferred from the pump to the tubing. When the pump plunger reaches the bottom, the barrel is empty.

The hydraulic pump begins to lift the entire fluid column to the top again, causing more fluid to be pulled in from the reservoir through the standing valve. However, when a condition such as low fluid level or trapped gas stops traveling valve from opening properly as the plunger starts downward, transfer of the contents of the pump; so, the tubing does not begin at the top of the stroke.

The fluid in the tubing descends with the traveling valve, maintaining the load at $L_{\max}$, until fluid is encountered or the gas compresses enough to open the traveling valve. Only when the plunger reimmerses in the fluid can it use the traveling valve open, and fluid transfer occurs through the travelling valve. The maximum and minimum load can be expressed as

$$L_{\text{Max}} = S_f(62.4)D\left(\frac{A_p - A_r}{144}\right) + \frac{\lambda_s DA_r}{144} + \frac{\lambda_s DA_r}{144}\left(\frac{SN^2M}{70471.2}\right), \tag{1}$$

$$L_{\text{Min}} = S_f(62.4)D\left(\frac{A_r}{144}\right) + \frac{\lambda_s DA_r}{144} - \frac{\lambda_s DA_r}{144}\left(\frac{SN^2M}{70471.2}\right). \tag{2}$$

The liquid flow rate Q can be expressed as

$$Q = 0.1484\left(\frac{A_p NS_p E_v}{B_o}\right). \tag{3}$$

The symbols listed in Table 1.

In this paper, surface load is calculated from the hydraulic pressure and the geometry of the hydraulic system. The position is represented by the position readings obtained by monitoring the hydraulic fluid flow.

5. Results and Experimental Setup

The most important parameter that indicates the status of the crude oil well is the fluid level. It must be ensured that this level is above the pump. We determine the casing pressure's critical value in the next stage, which pushes the level down under the pump. Therefore, the first part of the experiments in this paper is measuring the level. After that, the second part is activated, connecting the dedicated IIoT platform to the crude oil well controller and showing the results. These two parts are explained below.

5.1. Measuring Fluid Level in Wells Using Echometer Device. The most important parameter is the liquid level in the oil well. It is the process variable that needs to be maintained to ensure the fillage of the pump. This parameter is measured by an echometer device that uses an ultrasound gun to measure the number of tube joints to level.

The results of the echometer instrument can be read using Total Manager software to calculate the tubing joints liquid level in the oil well, as shown in Figure 15. Figure 16 shows the raw signal recorded by the echometer mic and displays the acoustic gunshot start, tubing joint reflection and fluid level kick (appears in zoom window). Low-pass filter is applied to the signal to make it easier for the operator to read and determine tube joints kick and fluid level kick as shown in Figure 17.

Depth determination screen is shown in Figure 18, where the joints can be counted easily, and zoom tools are used to show the kicks.

5.2. Performance Enhancement by the Proposed IIoT System. Once the system is installed and commissioned, the SCADA

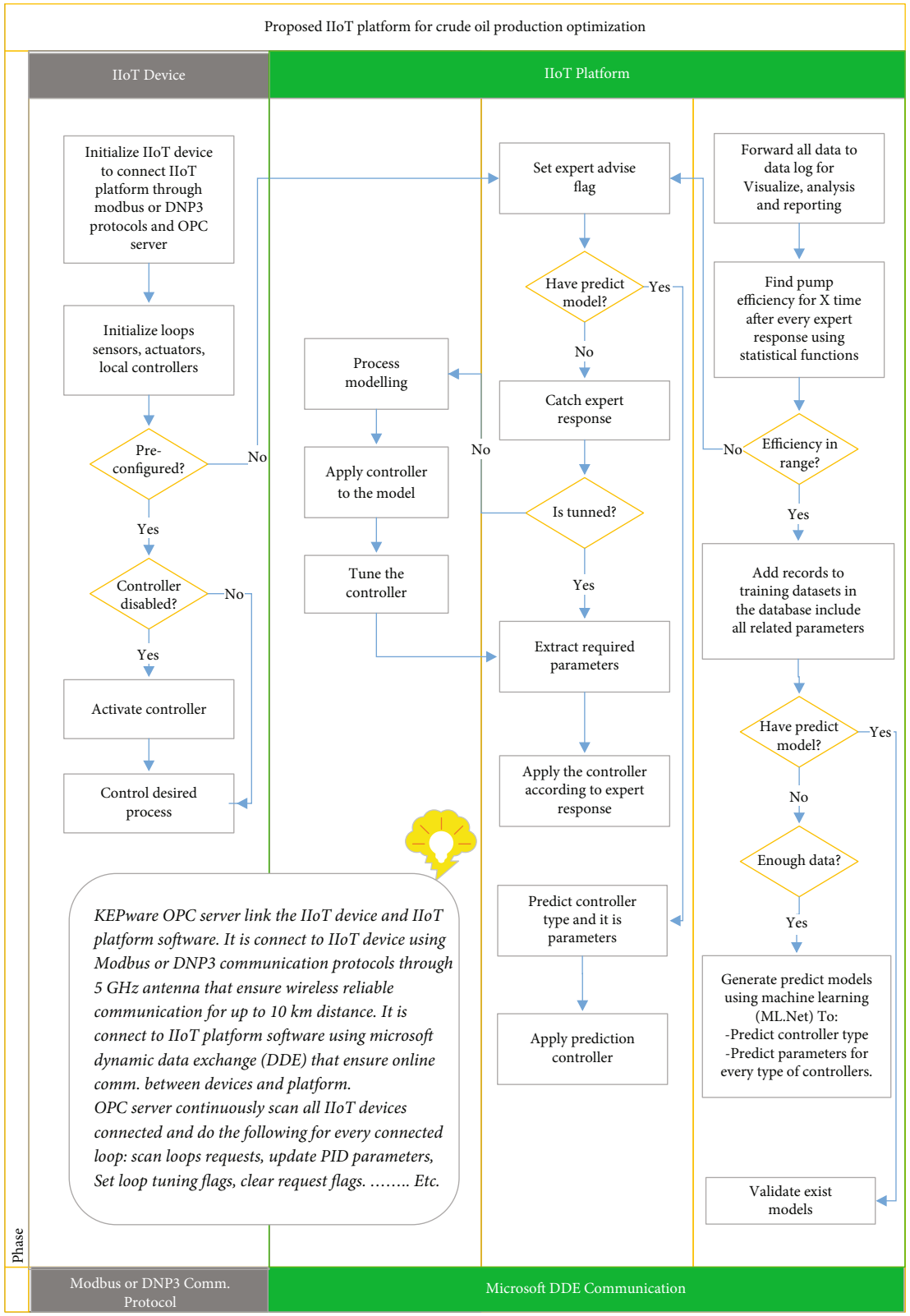


Figure 11: Proposed IIoT platform working flowchart.

system is built, and the IIoT platform is launched. The oil well chart includes fillage (pump efficiency), tubing pressure, jack pump hydraulic pressure, pump speed (stroke per minute), and casing pressure displayed. It depends on the data log recorded by the IIoT platform using a one-second scan rate stored in CSV files or ODBC database.

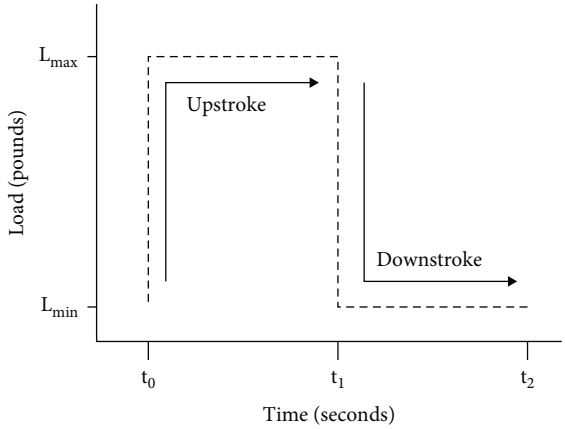


Figure 12: Load vs. time.

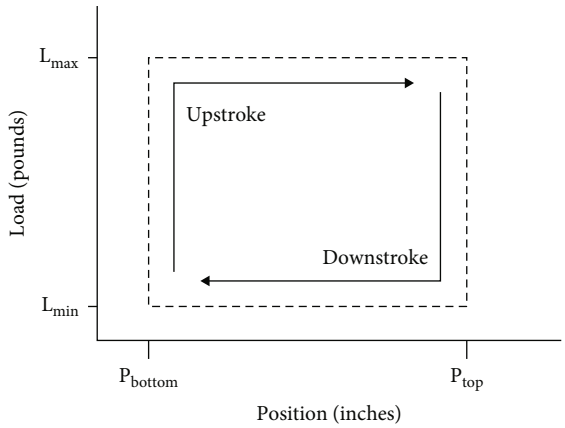


Figure 13: Load vs. position.

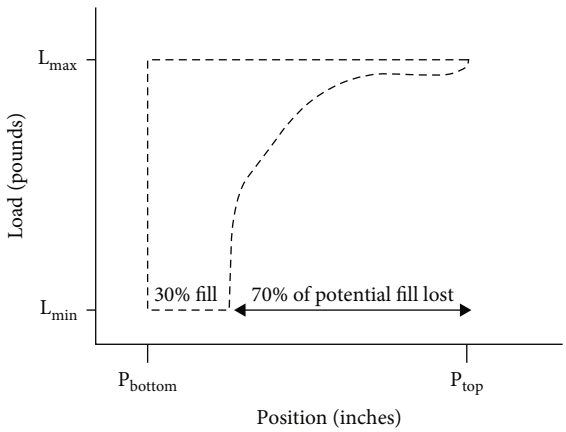


Figure 14: Load vs. position.

Figure 19 above shows the one-month oil well chart that indicates how the gas lock problem affects pump efficiency, which needs to be maintained. For best understanding, the higher resolution chart for 48 hours is shown in Figure 20. The pump fillage affected by gas lock without any control action is noticeable.

Table 1: Symbols.

Symbol	Remark
S_f	Liquid specific gravity
D	Sucker rod string length
A_p	Plunger area
A_r	Rod area
λ_s	Specific weight of steel
M	Machine factor
N	Pump speed stroke per minute
S_p	Stroke length
E_v	Pump fillage (efficiency)
B_o	Formation volume factor

Our proposed solution avoids the gas lock effect by stopping the pump for some time to give the reservoir a chance to build up again. It increases the liquid level in the crude oil well. Figure 21 shows the five-day well chart and how the on-off crude oil well pump controller affects pump efficiency.

With the proposed method for pump operation as discussed above, the pump fillage efficiency is stable at 90% as Figure 22 shows.

For a clearer picture, the higher resolution chart for 48 hours is shown in Figure 23 with continuous stability of pump fillage (efficiency) around 90% after stopping the pump for 6 hours.

The other solution to avoid the gas lock problem and maintain the oil well level is to control the casing pressure. The pressure controller maintains the casing pressure at a certain setpoint taken from the experts in real time via the IIoT platform.

Figure 24 shows the effect of casing pressure on the pump efficiency. This higher resolution chart for 48 hours is shown in Figure 25, while Figure 26 shows the higher resolution chart for 2 hours that gives a deep view of the behavior of all parameters with continuous stability of pump fillage (efficiency) under control via the IIoT platform.

With the effectiveness of our proposed system visible in the results, the oil well's production rate should be tested on other oil wells to ensure the solution's acclaim. The last three tests were done before applying the proposed technology in this paper. These tests showed a drop-in liquid production rate with unstable pump fillage after a short time from the last well workover, which means a well needs work over. The average liquid production rate was 43 BPD oil and 50 BPD water while the maximum expected is 100 BPD oil. The other test was done after applying the new IIoT system solution, especially when the pump fillage was stable at 90%, and the liquid production rate increased from 43 to 80 BPD oil. In contrast, the water increased from 50 to 110 BPD, and the increase in water rate is not an issue as it can be reinjected to a reservoir. The results have shown an improvement in the liquid production rate of the oil well, which means duplicating the production and decreasing the work over frequency with reducing work over cost and well-off

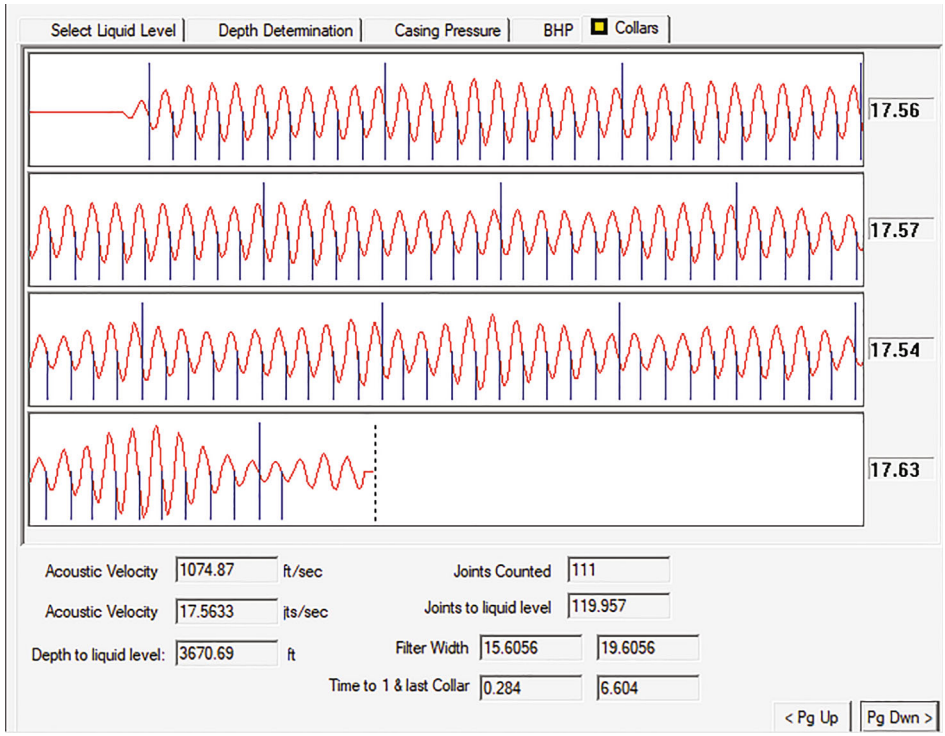


Figure 15: Echometer final ultrasound response to count the tube joints.

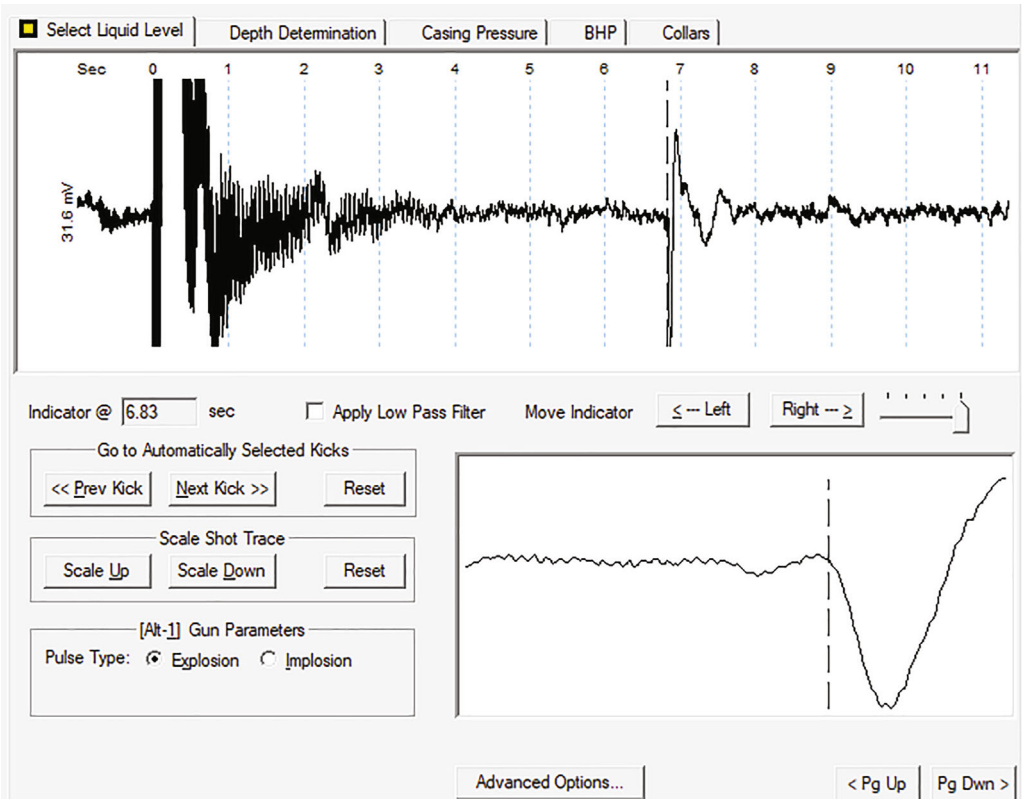


Figure 16: The raw signal recorded by echometer to count the tube joints.

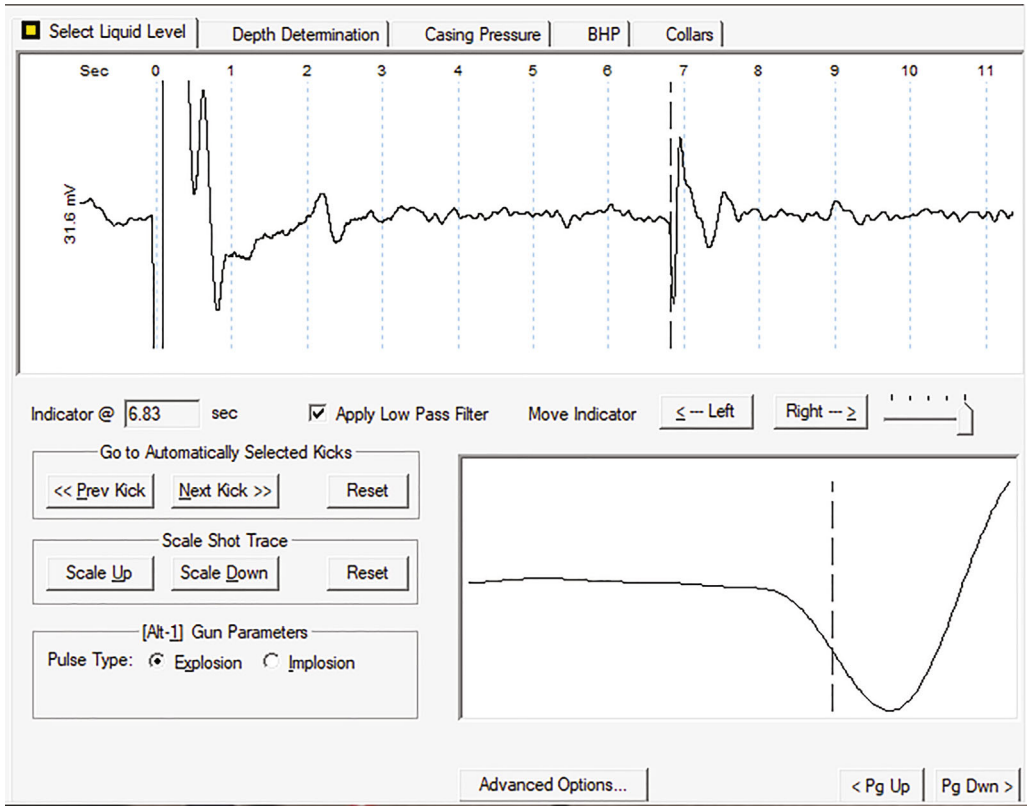


Figure 17: Number of tubing joint liquid level in crude oil well by applying low-pass filter to the signal.

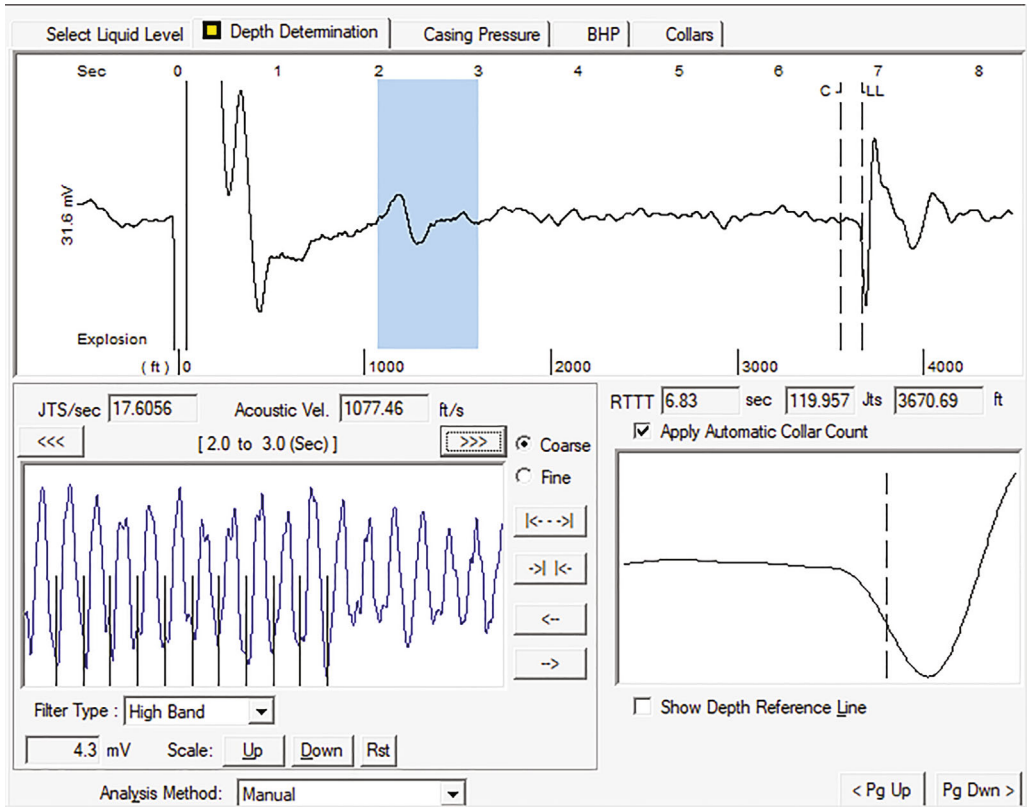


Figure 18: Depth determination screen.

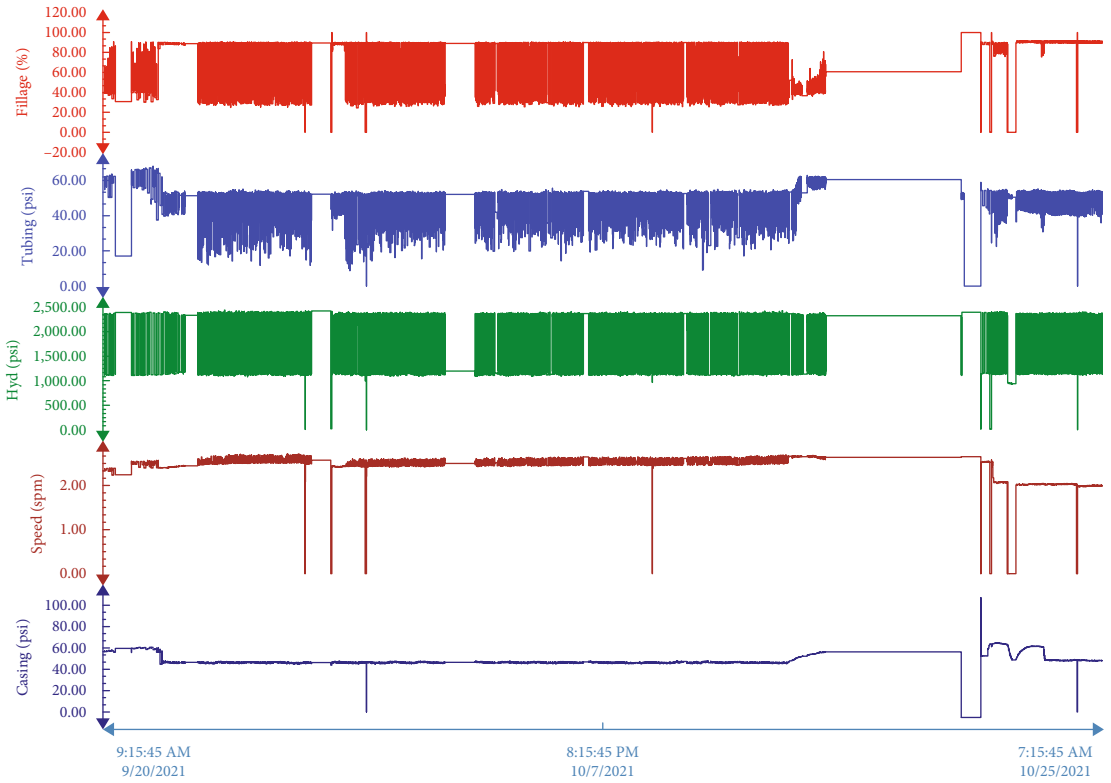


Figure 19: One month crude oil well chart showing essential parameters.

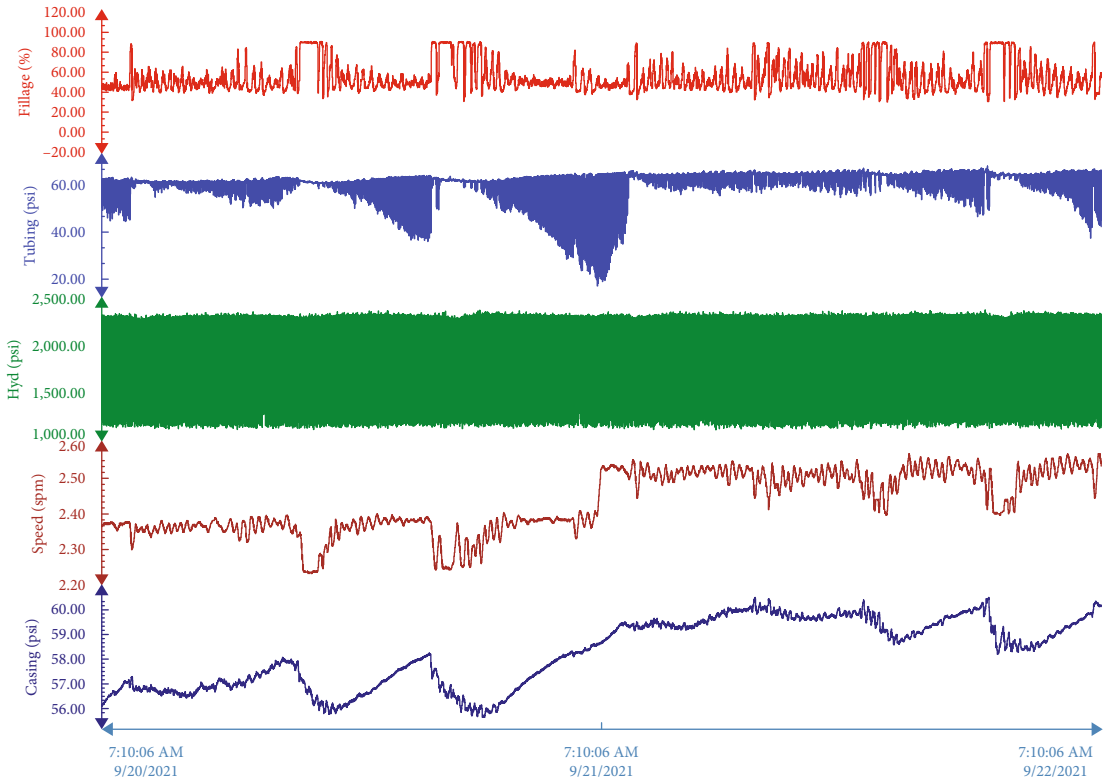


Figure 20: 48 hours oil well chart without control.

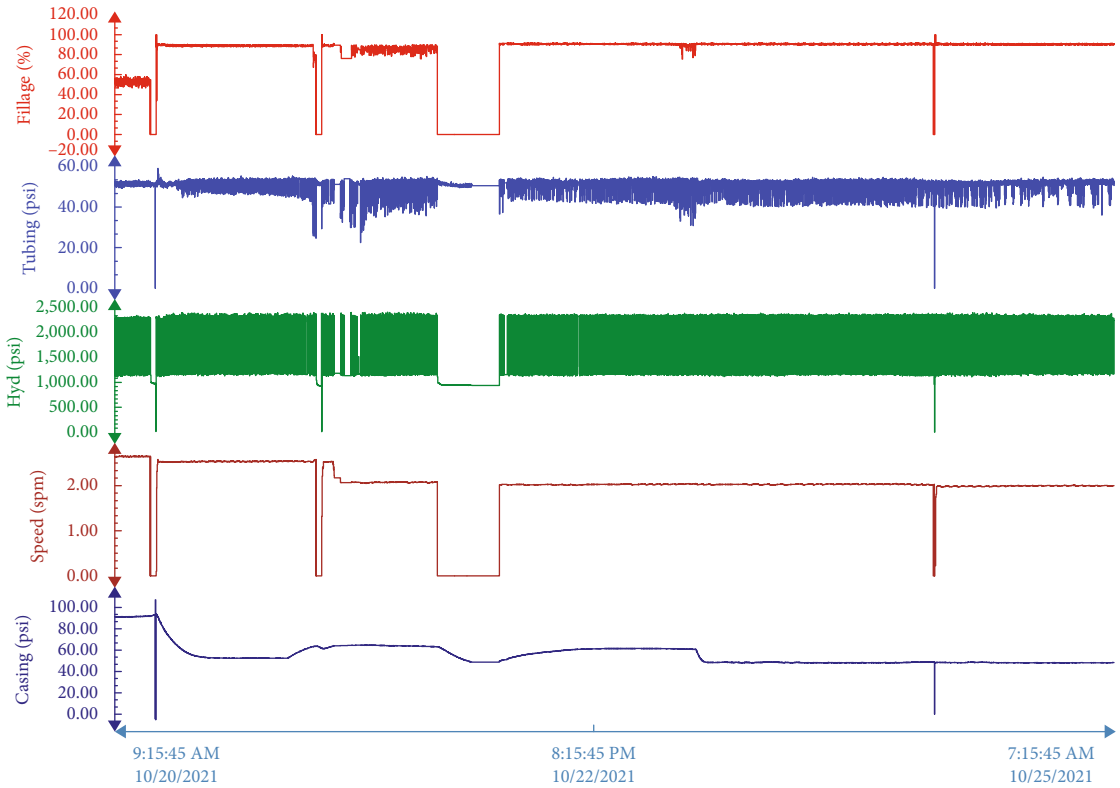


Figure 21: Five-day well chart with pump on-off control.

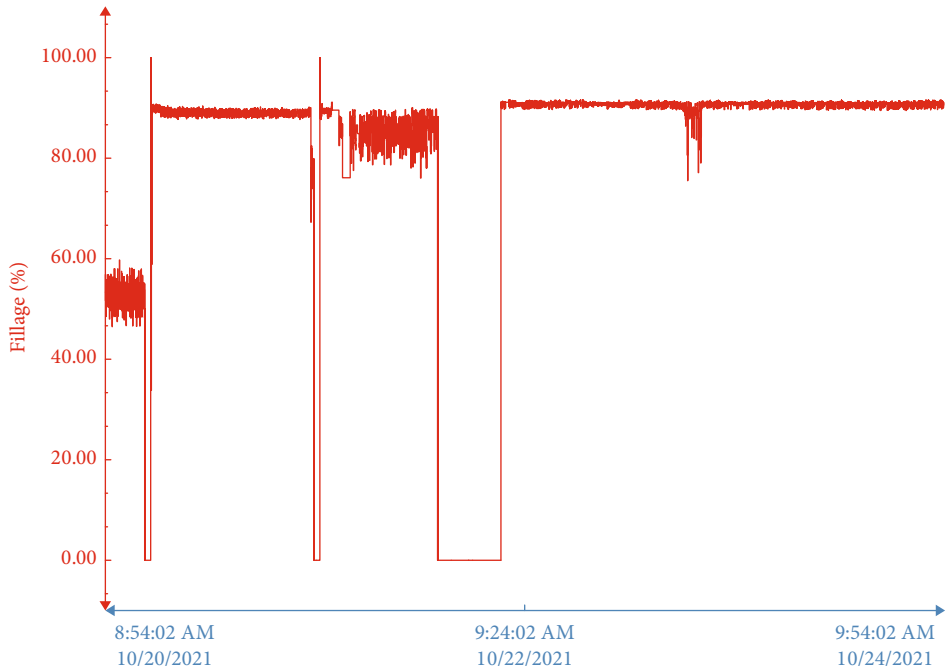


Figure 22: Five-day pump efficiency chart with pump on-off control.

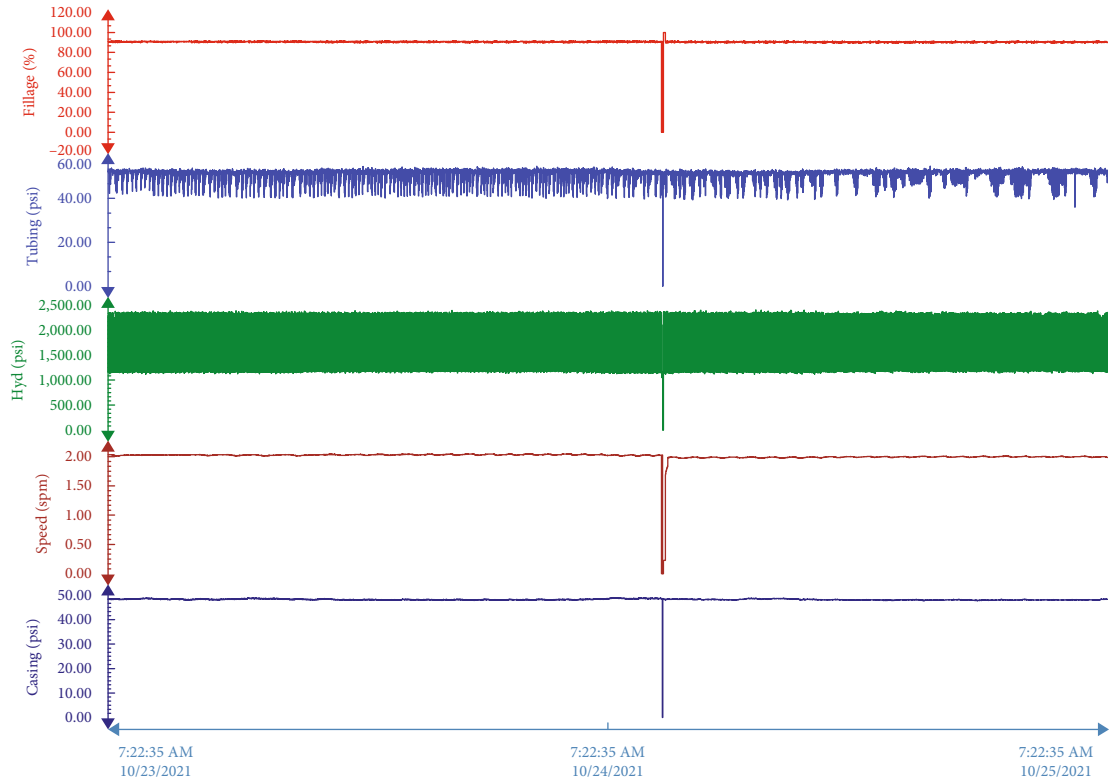


Figure 23: 48 hours oil well chart after 6 hours of shut-down.

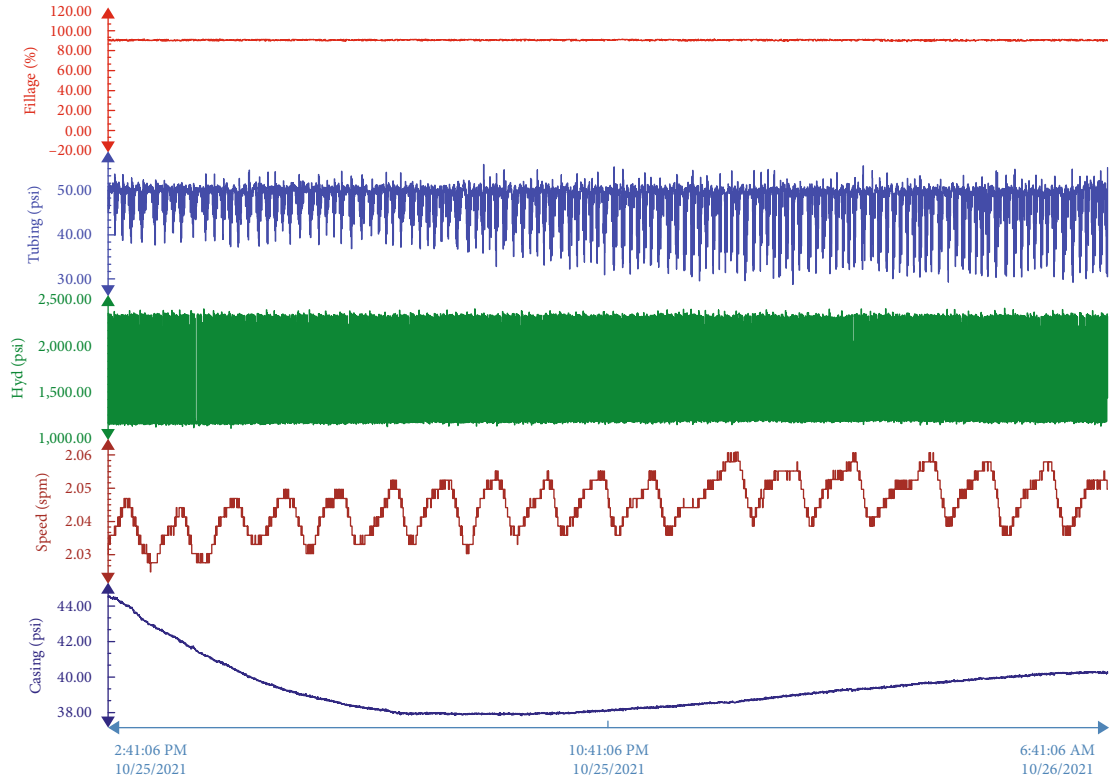


Figure 24: Effect of casing pressure controller.

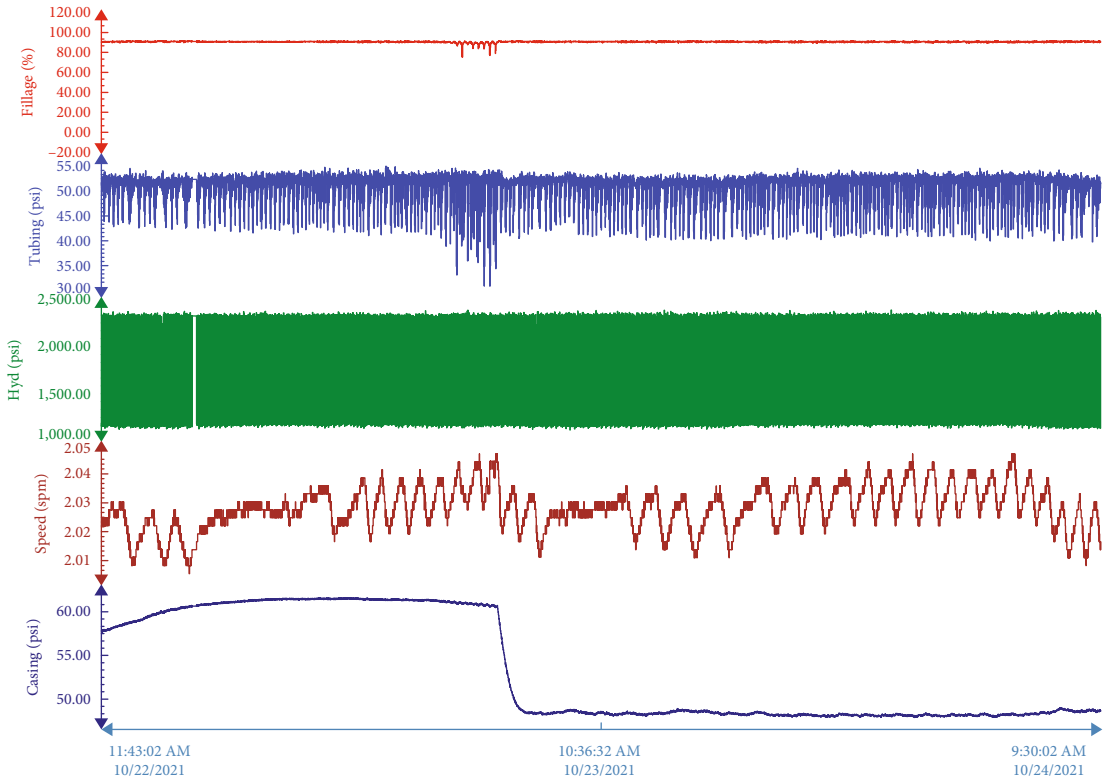


Figure 25: 48 hours oil well chart with casing pressure controller.

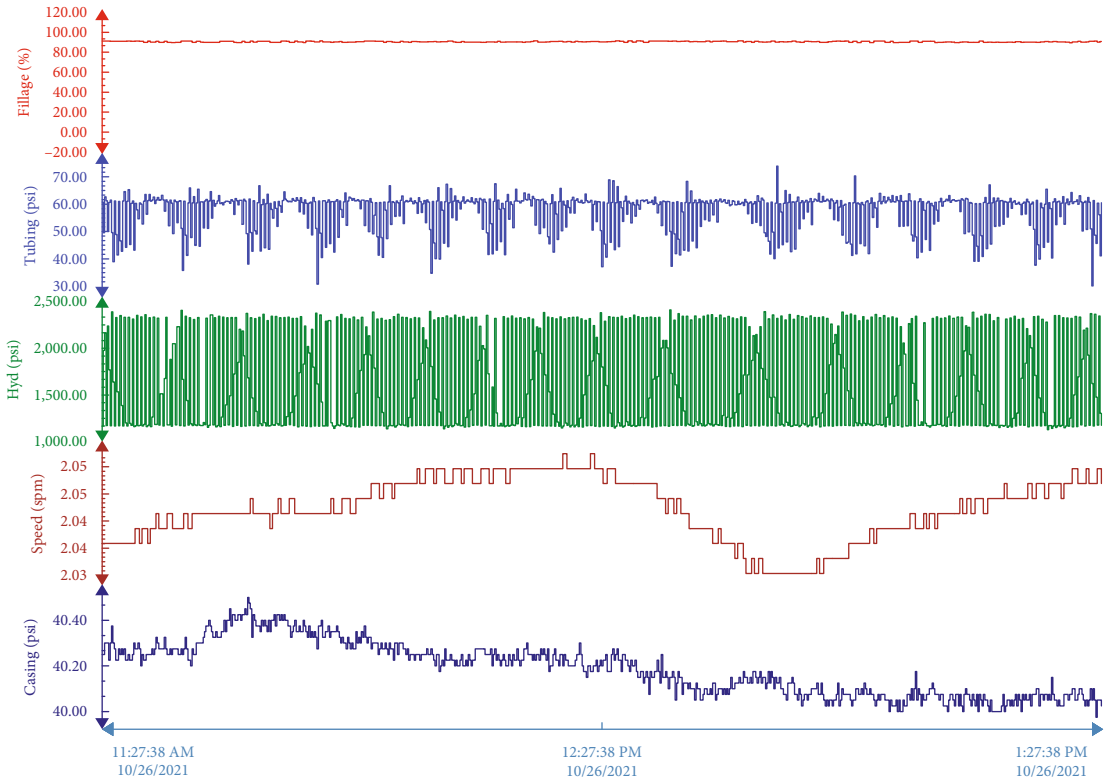


Figure 26: 2 hours oil well chart.

days. Furthermore, make the right decisions by reflecting the right picture of sucker rod pump behavior that helps experts.

6. Conclusion

Using the Industrial Internet of Things (IIoT) in the oil and gas industry means intelligent production and opening the door for a new level of optimization and cost-effective production. This paper shows how this technology successfully transferred a clear picture of the sucker rod pumping well. It introduces an approach to understand all the required parameters such as pump efficiency, pump fillage, tubing pressure, casing pressure, hydraulic pressure, and pump speed. The clear picture leads to the right expert's responses and transfers their experience to AI prediction models. The AI models predict the control parameters based on experts' responses. The production rate of the oil well studied in this paper has increased by 90% when applying this new technology. It prevents the gas lock problem by using an on-off pump controller. It maintains the liquid level in the well by controlling the case pressure using PID controller. At the same time, the experts determine the optimized setpoints for the controller and the lowest pump off-time. The future of oil and gas is the Industrial Internet of Things (IIoT) that will optimize the upstream and downstream to reduce maintenance costs, improve production, increase reliability, and more.

Data Availability

Data supporting Figures 2, 4, and 10–21 are not publicly available according to company policy. However, these datasets can be accessed on request from Mr Ali S. Allahloh, upon the completion of a Data Usage Agreement, according to policies from the Yemen Petroleum Exploration and Production Authority (PEPA).

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

The authors extend their appreciation to King Saud University, Riyadh, Saudi Arabia. for funding this work through Researchers Supporting Project number (RSP-2021/387).

References

[1] A. S. Allahloh and S. Mohammad, "Development of the intelligent oil field with management and control using iiot (industrial internet of things)," in *2018 2nd IEEE International Conference on Power Electronics, Intelligent Control and Energy Systems (ICPEICES)*, pp. 815–820, Delhi, India, 2018.

[2] A. S. Allahloh, S. Y. Sondkar, and S. Mohammad, "Implementation of online fuzzy controller for crude oil separator industry based on internet of things using labview and pic microcontroller," in *2018 International Conference on Computing, Power and Communication Technologies (GUCON)*, pp. 341–346, Greater Noida, India, 2018.

[3] G. B. Oliva, H. L. Galvão, R. E. Silva et al., "Development of a control strategy for a smart sucker rod pump," *SPE Production & Operations*, vol. 35, no. 3, pp. 481–496, 2020.

[4] I. Kitapov and R. Gilfanov, "Determination of operating efficiency of sucker-rod pumping units of different design in horizontal wells," in *SPE Russian Petroleum Technology Conference*, Moscow, Russia, 2018.

[5] E. Orji, J. Lissanon, and O. Omole, "Sucker rod lift system optimization of an unconventional well," in *SPE North America Artificial Lift Conference and Exhibition*, The Woodlands, Texas, USA, 2016.

[6] H. Wang, S. Zheng, and D. Yang, "Design and application of multiphase sucker-rod pumps in wells with high gas-oil ratios," in *SPE Artificial Lift Conference*, Latin America and Caribbean, Salvador, Bahia, Brazil, 2015.

[7] A. Sultabayev, "Advanced rod pump optimization approach – case study," in *SPE Annual Caspian Technical Conference, Virtual*, Astana, Kazakhstan, 2020.

[8] V. Ehimeakhe, "Calculating pump fillage for well control using transfer point location," in *SPE Eastern Regional Meeting*, Morgantown, West Virginia, USA, 2010.

[9] A. Samad, "Gas interference in sucker rod pump," *AIP Conference Proceedings*, vol. 298, pp. 274–281, 2010.

[10] B. Ordonez, A. Codas, U. F. Moreno, and A. Teixeira, "Sucker-rod pumping system: simulator and dynamic level control using bottom hole pressure," in *2008 IEEE International Conference on Emerging Technologies and Factory Automation*, pp. 282–289, Hamburg, Germany, 2008.

[11] J. N. McCoy, O. L. Rowlan, D. J. Becker, and A. L. Podio, *How to maintain high producing efficiency in sucker rod lift operationsSPE Production and Operations Symposium*, Oklahoma City, Oklahoma, 2003.

[12] A. L. Podio, A. J. Jaime Gomez, B. W. Mansure, and M. Mahoney, "Laboratory-instrumented sucker-rod pump," *SPE Production & Facilities*, vol. 18, no. 2, pp. 104–113, 2003.

[13] H. J. Derek, J. W. Jennings, and S. M. Morgan, "Sucker rod pumping unit diagnostics using an expert system," in *Permian Basin Oil and Gas Recovery Conference*, Midland, Texas, 1988.

[14] J. Berge, "Digital transformation and iiot for oil and gas production," in *Offshore Technology Conference*, Houston, Texas, USA, 2018.

[15] P. Flichy and C. Baudoin, "The industrial IoT in oil & gas: use cases," in *SPE Annual Technical Conference and Exhibition*, Dallas, Texas, USA, 2018.

[16] S. C. Christos and G. Christos, "Data-centric operations in oil & gas industry by the use of 5g mobile networks and Industrial Internet of Things (IIoT)," in *ICDT 2018: The Thirteenth International Conference on Digital Telecommunications*, p. 16, Athens, Greece, 2018.

[17] L. Hongfang, L. Guo, M. Azimi, and K. Huang, "Oil and gas 4.0 era: a systematic review and outlook," *Computers in Industry*, vol. 111, pp. 68–90, 2019.

[18] A. Sajid, H. Abbas, and K. Saleem, "Cloud-assisted iot-based scada systems security: a review of the state of the art and future challenges," *IEEE Access*, vol. 4, pp. 1375–1384, 2016.

[19] X. Wang, S. Garg, H. Lin, M. J. Piran, J. Hu, and M. S. Hossain, "Enabling secure authentication in industrial iot with transfer learning empowered blockchain," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 11, pp. 7725–7733, 2021.

[20] S. Pundir, M. S. Obaidat, M. Wazid, A. K. das, D. P. Singh, and J. J. P. C. Rodrigues, "MADP-IIME: malware attack detection

protocol in IoT-enabled industrial multimedia environment using machine learning approach," *Multimedia Systems*, vol. 27, pp. 1–13, 2021.

[21] M. Wazid, A. K. Das, N. Kumar, and M. Alazab, "Designing authenticated key management scheme in 6g-enabled network in a box deployed for industrial applications," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 10, pp. 7174–7184, 2021.

[22] T. Kumar, E. Harjula, M. Ejaz et al., "BlockEdge: blockchain-edge framework for industrial iot networks," *IEEE Access*, vol. 8, pp. 154166–154185, 2020.

Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 9654858, 12 pages
https://doi.org/10.1155/2022/9654858

Research Article

A Distributed Emergency Vehicle Transit System Using Artificial Intelligence of Things (DEVeTS-AIoT)

Umar Mahmud,[1] **Shariq Hussain**,[1] **Amber Sarwar**,[1] **and Ibrahima Kalil Toure**[2]

[1]*Department of Software Engineering, Foundation University Islamabad (FUI), Pakistan*
[2]*Department of Computer Science, Gamal Abdel Nasser University, Conakry, Guinea*

Correspondence should be addressed to Ibrahima Kalil Toure; ikalil@msn.com

Received 5 April 2022; Revised 4 August 2022; Accepted 11 August 2022; Published 30 August 2022

Academic Editor: Chi-Hua Chen

The advent of the 4th industrial revolution has realized smart environments composed of cloud and fog. These have been improved to enable intelligence at the fog, where numerous, inexpensive devices communicate with each other and provide computation capabilities to solve domain-specific problems in a distributed fashion. One of these domains is smart traffic flow with a focus on emergency vehicle (EV) transit. The increase in traffic congestion in third-world countries is a hindrance in EV transit to save human lives. This paper proposes an Artificial Intelligence of Things– (AIoT–) based, distributed, EV transit system developed on Raspberry PI as a rule-based system with minimal sensors. The sensors include an infrared sensor to detect emergency light and directional microphones to detect siren. The departure direction of the EV is shared with adjacent intersections to further reduce the transit time.

1. Introduction

The rapid urbanization of the modern world has created many challenges for developing nations. The high volume of vehicles moving about the city leads to traffic congestion. This not only burns precious fuel but also intoxicates the environment, leading to non-green cities [1]. Traffic congestion also creates an obstacle for emergency vehicles (EVs): including ambulances, fire tenders, and security vehicles, consequently wasting valuable time. In 2017, 20 percent of patient deaths were caused by traffic jams where ambulances either could not reach the patient in time or could not reach a trauma center [2]. This percentage is higher in the developing world where there are weak traffic monitoring and a lack of emergency lanes. However, an emergency lane is a partial solution since it may have to cross a busy intersection. The presence of traffic sergeants at different intersections improves the situation. In the absence of a traffic sergeant, the transit is dependent on the distributed intelligence of commuters.

Among many solutions is the use of cameras installed at all intersections monitored remotely by humans. This setup creates a large amount of data in the form of video feeds. A further improvement is the use of cloud for automatic EV detection and control of traffic signals. These systems are centrally controlled and dependent on the amount of bandwidth available for uploading video feeds. It is natural to note that a central traffic monitoring system is prone to single-point failure as has been highlighted in crime thriller movies like The Italian Job [3]. The traffic signal is connected with video cameras as well as microphones to detect the arrival of an EV [4]. This creates an Internet of Things (IoT) environment at a traffic intersection. IoT is the realization of the 4th industrial revolution which connects ordinary sensors seamlessly to provide better services as well as monitor activities [5]. IoT solutions have been developed for all walks of life including home automation, industrial automation, and smart cities [6]. IoT Analytics has reported 12.3 Billion connected devices worldwide with an industry worth $160 Billion by the end of 2021 [7].

Table 1: Comparison of evidences in literature for traffic management.

Reference	Technique	Basis	Low power	Scalable	Fog	EV transit	AIoT
[35]	SVM	ML and AI	×	×	×	×	×
[48]	Big data	Traffic density	×	✓	×	×	×
[39]	Prioritization of traffic signals, in emergency	Intelligent, autonomous UAV	×	×	×	✓	×
[38]	TABU search	Efficiency of traffic transit	×	×	✓	×	×
[44]	V2V	Distributed traffic monitoring	×	×	✓	✓	×
[41]	Reinforcement learning and fuzzy logic	Dynamic traffic light controlling system	×	×	✓	×	×
[45]	Rule-based	Traffic management	✓	×	✓	×	×
[43]	Rule-based	IoT-based real-time traffic monitoring	✓	×	✓	×	×
[47]	Rule-based	Smart traffic controlling	×	×	×	×	×
[46]	Rule-based	Dynamic traffic signal controlling system	✓	×	×	×	✓
[42]	Rule-based and V2V	Distributed, dynamic traffic density management	✓	×	✓	✓	×
[37]	VANET	Traffic density and emergencies	×	×	✓	✓	×
[36]	Object detection	Dynamic traffic density detection using video frames	×	×	✓	×	×
[40]	Game theory and	Intelligent traffic control	×	×	✓	×	×
DEVeTS-AIoT	Rule-based	AIoT	✓	✓	✓	✓	✓

Traditionally, IoTs are connected with a cloud interface to provide storage as well as computation capabilities. This arrangement is inherently centralized and is a combination of IoT-based edge components and service providing cloud components.

An IoT system when connected with legacy applications, remote services, and available appliances via the Internet gives birth to the concept of the Internet of Everything (IoE) [8]. An IoE system is a generalization of wireless sensor networks (WSN), focused on higher availability of services, ease of use, and seamless integration but at the cost of increased security vulnerabilities [9]. With the continuous evolution in technology and progressive development of 5G and 6G networks, IoT is transforming into IoE. IoE applications tend to offer an extensive assortment of interconnections of things and space applicability for various domains [10]. Smart wearable devices, smart cars, smartphones, and smart home appliances are interconnected making relevant information accessible and life intelligent [11]. The increasing need for self-sustainable systems and autonomous sensor services in smart environments had resulted in the amalgamation of AI coupled with highly available communication technologies termed as AIoT [12]. An AIoT system includes a cloud computational server that gathers, stores, processes, and analyzes the data that further control services as well as nano- and microsystems. Recent developments have combined Artificial Intelligence (AI) with IoT to evolve IoT into autonomous and futuristic architectures characterized by higher computation at the edge known as Artificial Intelligence of Things (AIoT), alternatively termed as fog computing [13, 14]. The presence of sensors, microcomputers, or system on a chip (SoC) machines and GSM, 5G, or Wi-Fi communication modules allow faster processing at the edge and reduce the communication overhead [15]. AIoT has been employed in all industrial domains including smart homes, healthcare, automation, education, and traffic congestion monitoring [16].

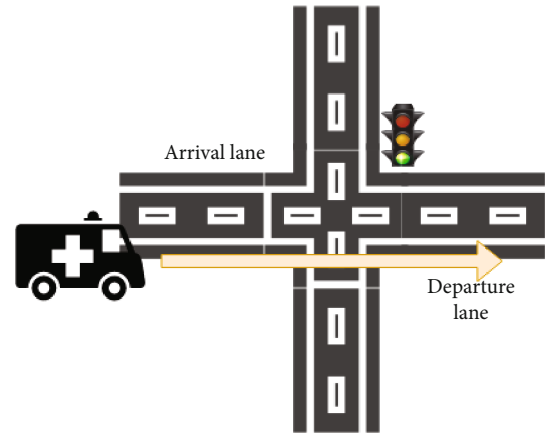


Figure 1: An EV at an Intersection.

DEVeTS-AIoT is an AIoT-based distributed EV transit system envisaged to deliver an open passage for an EV arriving at an intersection. The system detects the arrival of an EV by listening to the siren via microphones and detecting the emergency light (red) emitted by the EV using an Infrared (IR) sensor. After the departure of the EV from an intersection, the intended direction is transmitted to the next intersection using a communication module. This allows prior information to be considered by the next intersection for traffic signal

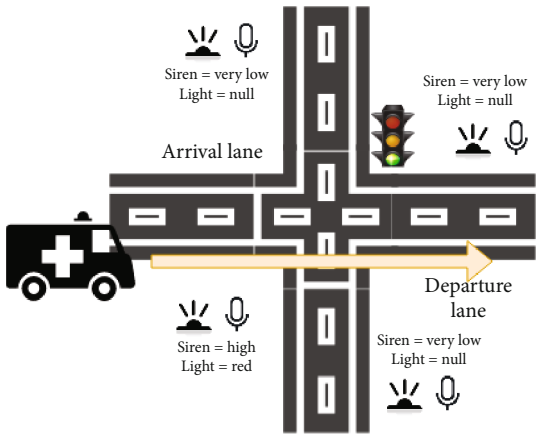


Figure 2: Arrival lane of EV and sensor values at the intersection.

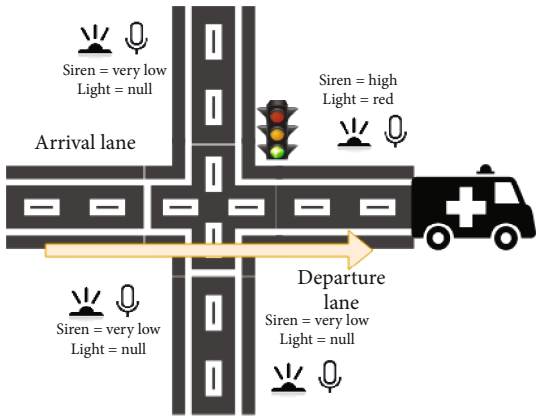


Figure 3: Departure lane of EV and sensor values at the intersection.

adjustment, thus establishing a distributed environment. The contribution of this research work is as follows:

(i) This article presents design and implementation details based on Raspberry Pi, for the traffic management system and EV transition through the intersections

(ii) EV detection is carried out using a microphone and an IR sensor that detects siren and red emergency light

(iii) EV transition through adjacent intersections is managed by using multiple rules in a distributed fashion

(iv) Departure lane information of EV is shared with the adjacent nodes through GSM/4G/5G as prior information for smooth transit

The rest of the paper is organized as follows. Section 2 presents related literature with a comparison highlighting the contribution. Section 3 presents the design and the process model using BPMN. Section 4 outlines the implementation details and the evaluation is carried out in Section 5. Section 6 concludes this research work.

2. Literature Review

With fast-growing trends and technology-embedded urbanization, multiple solutions have been proposed for making cities smart by overcoming traffic congestion. Cities are shifting towards smart concepts by offering optimal traffic management resulting in resource maximization and cost reductions. Similarly, new technologies and trends have also been embedded in cities to offer optimal solutions based on various technologies.

Elmrini and Amrani as well as Hilmani et al. propose solutions based on employing wireless sensor networks (WSN) [17, 18]. Pawłowicz et al. have developed a solution on radio frequency identification (RFID) [19].

Javaid et al. have proposed a smart traffic management system using IoT along with a decentralized approach to augment traffic using intelligent algorithms [20]. This system inputs sensor data from traffic density through digital image processing (DIP) and outputs signals operation management. Their work also predicts the traffic density which minimizes traffic bottlenecks. RFID tags are used to prioritize emergency vehicles.

The use of artificial neural network (ANN) has been reported by Brzozowska et al. [21]. ANN is a classification-based technique that suffers from large training times. Adaptations and adjustments can also result in high training times.

One of the commonly applied solutions for traffic management to support emergency vehicles is the application of IoT [22]. IoT provides a rational solution to the urban traffic congestion problem. This problem results in increased depression, higher carbon emissions, deterioration in health, wastage of fossil fuels, as well as unwanted delays in EV transit [23]. The architecture of IoT is composed of multiple interconnected equipment including sensors and smart devices via the Internet. IoT devices use global system for mobile communication (GSM), Bluetooth, Wi-Fi, etc.

Lalitha and Pounambal as well as Elkin and Vyatkin have used IoT as an enabler of smart traffic management systems [22, 24]. Bellini et al. have introduced IoE to the smart traffic management problem and proposed a full stack approach to realizing IoE [12]. Zafarullah et al. and Mondal and Rehena have recommended AIoT as the building block for smart traffic management systems [25, 26].

Soni and Saraswat have reviewed different methods for IoT-based traffic management and controlling system [27]. Lavanya has presented different IoT-based traffic control systems with their hardware and software implications as well as their pros and cons [28]. Wani et al. have proposed a hardware-based traffic management system designed for ambulances [29]. These techniques employ machine learning to optimize and reroute traffic, using both hardware and software components.

Juric and Madland have proposed an IoE solution based on semantics, stored for the environment, and generating reasoning suitable for the vehicles [30]. The proposed solution tuned conventional computational algorithms through

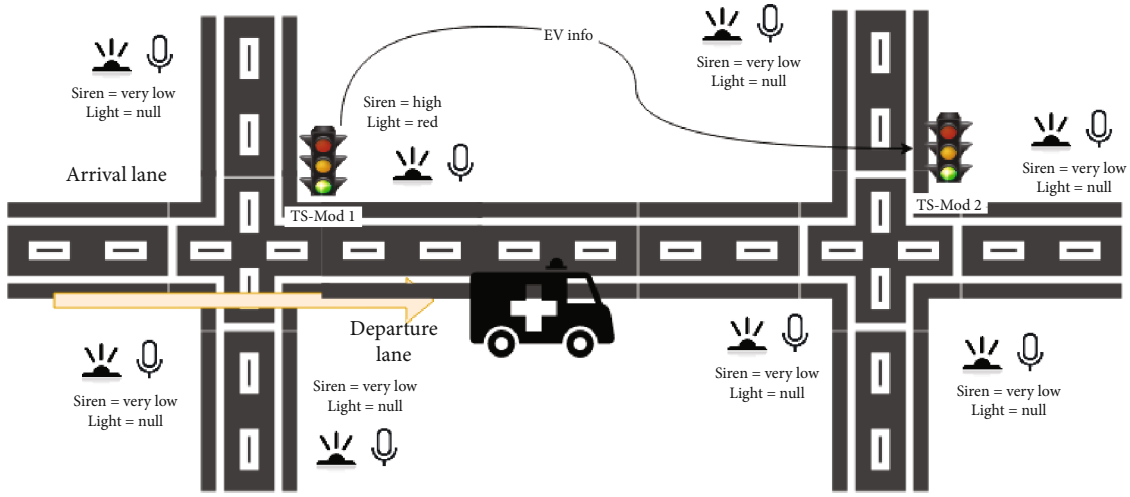


Figure 4: Interaction between adjacent TS-mod after departure of an EV.

the semantics of situations in urban traffic, thus facilitating the urban traffic decision-making process.

The amount of data generated in an IoT environment is large. The centralized solutions are limited and discard data that can be utilized for classification as well as prediction. To overcome the limitations of local storage, an efficient cloud computing solution is required that can process information [31].

Wang and Hsu have proposed an intelligent solution to enhance traffic quality, reduce carbon emission, and maximize energy saving through AIoT technology [32]. The authors used deep learning methods to resolve traffic scheduling and road safety issues, enabling the concept of a smart city vision. Wang has highlighted the concept of power awareness in smart traffic control. Power awareness is the ability of a smart machine to provide services while consuming less power and reducing carbon emissions [33].

Due to the amalgamation of AI in urban intelligent transportation, Guillen-Perez and Cano have proposed an innovative opportunity for a more viable urban transport agility [34]. The authors proposed a random early detection (RED) for dynamic behaviors of vehicles as a basis. The RED algorithm detects signaled intersections to proactively detect emerging congestion and models unknown traffic scenarios.

Ali et al. overcame the issue of traffic congestion and challenges by implementing a support vector machine–(SVM–) based model [35]. This model further optimized the configuration signal of high-traffic zones to medium or low-traffic zones.

Sharma et al. have developed a detection system, for traffic control, that provides input on basis of the patterns extracted from dynamic traffic density [36]. Using this technique, traffic signal switching is improved by the street limit thus saving voyaging time and preventing traffic congestion.

Sankar and Voorandoori have designed an intelligent traffic control systems using mobile ad-hoc networks (MANET), allowing communication among vehicles termed as vehicular ad hoc networks (VANETs) [37]. The authors have implemented a frequency and protocol-based solution for effective traffic management in the Indian context.

Cheng has designed a mathematical model for the efficient traffic of autonomous vehicular devices, based on a high traffic light [38]. The model calculated the traffic efficiency based on the time consumed by a certain vehicle passing over. In the case of emergency vehicles, the model utilized dynamic planning.

Beg et al. investigated the inadequacies of current traffic policing and handling emergency response systems [39]. The authors further proposed an autonomous and intelligent UAV-enabled solution. The proposed system prioritized the traffic signal for ground emergency response units, thus reducing the delays on congested traffic routes.

Wang et al. have proposed an intelligent traffic control and monitoring system based on the dynamic Level-k model and game theory [40]. The proposed system also studied the impact of multi-agent vehicle joint and achieved decision-making process through disturbance of group behavior on system state.

Kumar et al. have designed an intelligent and dynamic traffic light control system that inputs real-time traffic data and adjusts the traffic lights' duration dynamically [41]. A deep reinforcement learning model was also proposed for the switching of traffic lights and a fuzzy inference system was applied for traffic data inference.

Sadhukhan and Gazi have proposed an approach to measure the urban traffic density based on particular junctions by setting time-based signal functional and using ultrasonic proximity sensor (UPS) for dense traffic congestion [42]. The proposed approach is hardware based comprises microcontrollers, Wi-Fi module, signal LEDs, and ultrasonic sensors node (USN). The authors have implemented two modules, one monitored traffic density and the other managed the traffic congestion.

Masum et al. have designed an IoT-based smart traffic management system (TMS) in the context of Bangladesh [43]. The system is hardware based where the conventional traffic signal is controlled by utilizing Artificial Intelligence and sensors. The hardware components include Arduino mega controller, ultrasonic sensors, RFID module, Wi-Fi module, and signal LEDs.

Table 2: Description of submodules of TS-Mod.

Submodule	Description
TS-Mod engine	This is the heart of the TS-Mod. It is responsible for implementing the logic of TS-Mod. The EV detection module sends the arrival lane information once an EV is detected to the next TS-Mod installed at the next intersection A TS-Mod that receives the departure lane information from another TS-Mod increases the duration of the green signal on the arrival lane. This is carried out until the EV arrives and is detected on the arrival lane, after which the signal is turned green till the EV departs
Traffic signal controller unit	This module interfaces with the traffic lights and interrupts normal operation when an EV is detected. Once the EV has departed the normal operation is resumed.
Microphone	Microphones are used to detect the siren of an EV. A microphone is installed at each incoming lane. The detection of a siren and its intensity helps in identifying the transit of an EV. Once an EV transits an intersection, the intensity of the siren at the arrival lane decreases but at the same time, it increases on the microphone installed at the departure lane. This is then used to determine the departure lane.
IR sensor	IR sensor is installed with the microphone at each incoming lane. This is used to detect the red light emitted by an EV and confirm the presence of an EV at the arrival lane
EV detection	EV is detected in two steps. The detection of the siren as well as on emergency light ensures that an EV is detected correctly. This is a rule firing module with the following rule: $\text{if}(Siren == High \&\& Light == Red) \longrightarrow EVState = Arriving, ArrivalLane = CurrentMicrophoneLocation$ The following rule is used to determine the departure lane: $\text{if}(Siren == High \&\& Light == Red) \longrightarrow EVState = Departing, DepartureLane = CurrentMicrophoneLocation$ Figures 2 and 3 show the situation and the sensor values at arrival and departure lanes
Communication unit	This unit uses GSM/4G/5G to send and receive information with other TS-Mods installed at other intersections. The same information is sent to Cl-Mod for storage and data analytics as well. This case is shown in Figure 4

Harikumar et al. have designed a system supporting emergency vehicles in dense traffic congestions [44]. The system incorporates ZigBee for communication among vehicles and provides ambulance information as soon as the patient is boarded on the stretcher due to the pressure sensors. Information is transmitted resulting in clearing the heavy traffic congested lanes on the travel route.

Madisa and Joseph have designed a traffic control system for preventing and handling traffic congestion, resulting in delays in emergency vehicles for the urban transport system [45]. The system is based on android based hardware controller and cloud computing. Rani, et al. have developed an IoT-based TMS using a GSM module and infrared (IR) sensors [46]. This system is hardware based and uses cheap and easily accessible sensors.

Ramaprasad and Kumar have designed an intelligent traffic control system based on GSM technology at traffic junctions [47]. An IR sensor is deployed in signal junctions for the estimation of vehicles based on the traffic density across all the junctions. Avatefipour and Sadry have compared different TMS presented in the literature [48]. The comparison comprised of several traffic controller systems like RFID systems, green wave system, WSN systems, IR systems, and GSM systems applicability along with their merits and demerits.

Using WSN or radio frequency identification (RFID) requires hardware installation on all vehicles. This is not suitable for third-world counters, where the sheer number of vehicles makes it an impractical solution [49]. Using IoT/IoE or AIoT to overcome the deployment cost of WSN or RFID can connect with the cloud to enhance services and provide high computation capability while employing the low-power device, in the fog. The evidences in the literature address traffic management and traffic flow with no focus on EV transit. Since the scope is smooth traffic flow, the solutions are complex and require large hardware resources. There is a need to develop low powered, smart, inexpensive, fast, scalable, fog-oriented, and simple system to ensure EV transit. Table 1 compares the evidences in literature for traffic management systems and the technique employed. The comparison is based on low-power, scalability, fog-oriented distributed intelligence, EV transit, and the use of AIoT. The use of IoT is recommended for low-power setup. Scalability refers to cost-effective deployment. Fog-oriented distributed intelligence refers to real-time localized solutions with less dependency on centralized cloud-based setups. Fog can be provided through both IoT as well as vehicle-2-vehicle (V2V) communication.

3. DESIGN of DEVeTS-AIoT

An intersection is characterized by multiple lanes going in different directions, where a lane is a unique road converging at an intersection. There could be many lanes in an intersection but a 4-way intersection is usually found in cities. The lane at which an EV arrives is termed as the arrival lane, while the lane on which the EV departs is termed as departure lane. This is shown in Figure 1. The state of the intersection when an EV arrives is shown in Figure 2 and 3. The arrival and departure lane information of an incoming EV is communicated with adjacent intersection as shown in Figure 4.

3.1. Components of DEVeTS-AIoT. DEVeTS-AIoT is designed using a structured approach composed of two distinct modules communicating with each other over the Internet. These are traffic signal module (TS-Mod) and cloud module (Cl-Mod).

3.1.1. TS-Mod. TS-Mod is a Raspberry Pi-based SoC installed as an add-on black box at a traffic signal. A Raspberry Pi is suitable for TS-Mod as it is a SoC and provides more computing power as well as parallel processing than an Arduino device. As compared with FPGA-based devices, Raspberry Pi is a low-powered device. TS-Mod has directional microphones as well as IR sensors to detect the arrival and exit of an EV. The prime task of TS-Mod is to identify the arrival lane as well as the departure lane of an EV using directional microphones that matches the siren. In addition, to confirm the detection the light emitted by an EV is also detected using an IR sensor. A Raspberry Pi SoC is used to connect the sensors and to implement the software program. A TS-Mod has an interface that allows it to connect with the traffic lights installed at an intersection. The TS-Mod changes the traffic signal of the arrival lane of an EV to green until the EV has successfully crossed the intersection. After the transit, the departure direction of the EV can be determined by the increase in sound detected by a microphone on the departure lane. The departure lane as well as the type information is used by a TS-Mod to inform the next TS-Mod installed at the next intersection in the direction of the EV's route. The next TS-Mod can then adjust the signal to green before the arrival of EV on the expected lane. This ensures a green signal throughout the route of the EV. However, a guard timer is set within which the EV is expected to arrive. This allows resuming normal operation if the EV does not arrive at the next intersection. The details of each submodule are given in Table 2.

3.1.2. Cl-Mod. The second component is Cl-Mod which gathers data from all TS-Mods installed on a road network. The Cl-Mod provides a dashboard for an admin that plots the latest situation on a digitized map of a road network. Information shared by a TS-Mod to its neighbor is also shared with the Cl-Mod. The Cl-Mod provides long-term data storage as well as analytics that can be drawn using history. Since the major computation is performed by TS-Mod, the information is shared directly with the next neighbors creates a distributed solution based on AIoT. Figure 5 shows the concept diagram of DEVeTS-AIoT.

3.2. Process Model of DEVeTS-AIoT. DEVeTS-AIoT is developed as a structured system using business process model and notation (BPMN) following BPMN 2.0 standard [50, 51]. BPMN is an abstract design method suitable for modeling flow and control information among participating objects. BPMN shows tasks, gateways, and events including parallel activities. BPMN is used to model business processes among participating entities. The tasks of the BPMN model of DEVeTS-AIoT are given in Table 3. Figure 6 shows the BPMN model of DEVeTS-AIoT.

The BPMN model of DEVeTS-AIoT has two participating objects that are shown as the swim lanes. These participants are the interacting modules. The mechanism starts with TS-Mod operating normally and executing three simultaneously threads. Its job is to detect an EV arriving at the intersection. In addition to this, it can also receive information about a departing EV at an adjacent intersection. Once an EV is detected using a microphone and IR sensor, the arrival lane is determined, and the signal is turned green for the arrival lane. The signal remains green until EV has successfully crossed an intersection. The departure lane is then determined by detecting the increased volume of the siren. The information is then shared with the adjacent node and TS-Mod resumes normal operation. It also uploads the information to the CL-Mod.

Cl-Mod then records history on the cloud and updates the map. This is used to track an EV transiting through city by city officials. The recorded history is also used to generate insights. The insights include asking how many EVs were detected correctly and how much time it took for an EV to safely transit over a month or year.

4. Implementation of DEVeTS-AIoT

In this section, the implementation details of the DEVeTS-AIoT system are being presented. The architecture of the DEVeTS-AIoT is presented in Figure 7. The system is divided into two main components as already mentioned in Section 3.

The TS-Mod component consists of sensory hardware and software solutions with a traffic control mechanism to prioritize traffic flow for EVs. The details of the hardware used in this work are presented in Table 4. The specifications include the power consumption of a TS-Mod. Overall, a single intersection consumes less than 2 Watts. Since, during a 24-hour day, traffic congestion mostly occurs during work hours, a sleep-scheduling policy can be implemented as a supplementary rule [54]. The sleep mode would let reduce power consumption over a 24-hour period. For an adaptive sleep-scheduling mechanism, a dataset must be compiled after deployment [55].

5. Evaluation

DEVeTS-AIoT is developed as a rule-based system. Rule-based systems are simple to implement and have the fastest rule-firing time [61], while classification-based systems have been developed that consider the context for activity recognition, thus making it a context-aware system [62]. A context-aware system is an overfit for DEVeTS-AIoT [63].

The input to DEVeTS-AIoT is primarily based on two sensors, i.e., light sensor and microphone, which is then further converted to two inputs, i.e., red light and siren. The red light and siren are the only two facets that describe the state or more appropriately the context of an intersection [64]. The information of the departure lane can also be provided as prior information to an adjacent intersection. This means that there are no more than 3 input variables and has a single class outcome, i.e., if EV is detected or not. The size of a truth table is no more than 8 for each arrival lane. These rules are used to determine the state of an individual intersection among three options that are normal, caution, and emergency. In a caution state, an EV is expected though it

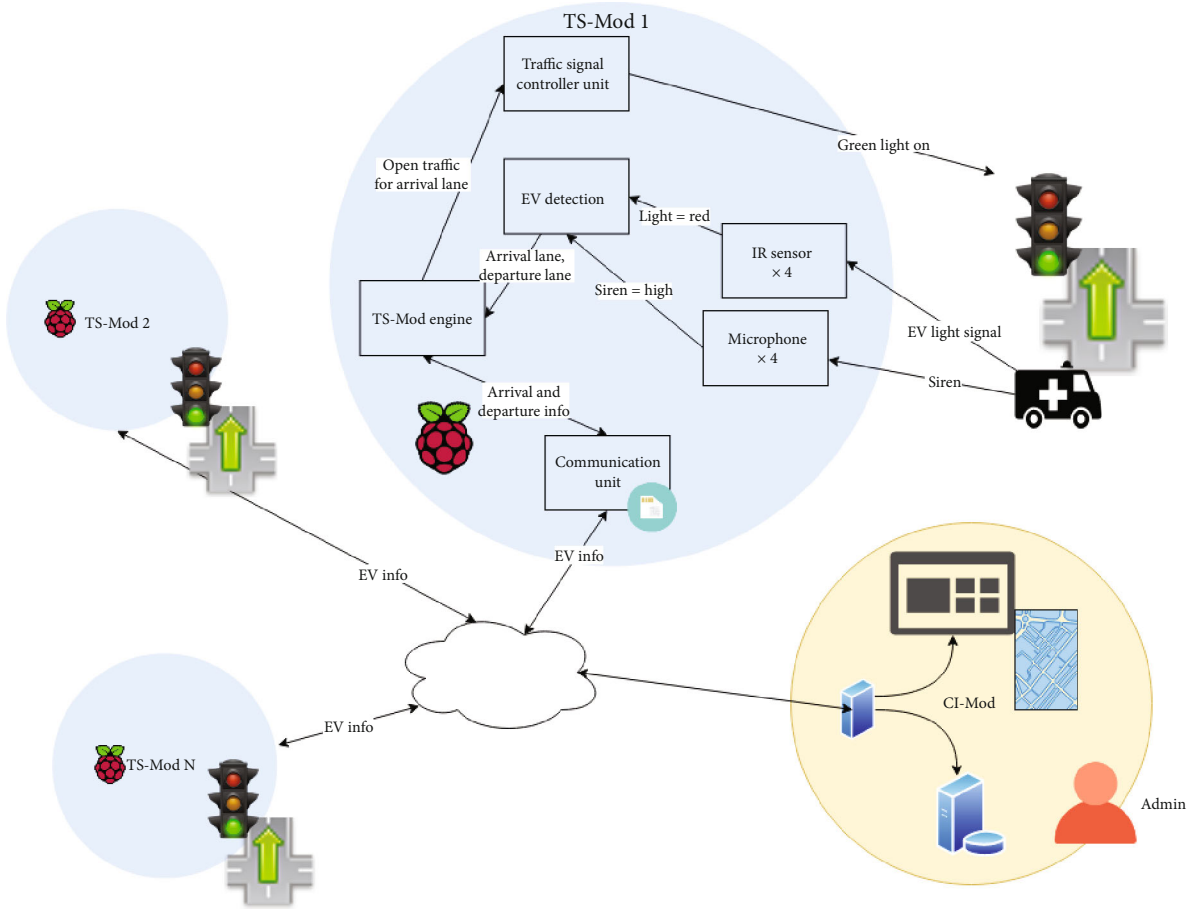


Figure 5: Concept diagram of DEVeTS-AIoT.

Table 3: Description of tasks in BPMN of DEVeTS-AIoT.

Task	Description	Component
Detect EV siren	The siren is detected using microphones	TS-Mod
Detect EV light	The emergency light is detected using an IR sensor	
Receive EV arrival info from adjacent TS-mod	Prior information is received using the GSM module. This information is then subject to a counter within which the EV should be detected. If the EV is not detected, this information is then discarded. The counter is similar to the metric of age of information (AoI) [52]. Since the distance is known, the Peak AoI (PAoI) is hard coded to the system [53]. There is no need for a classification system here as the nodes are fixed and the maximum time to travel to an adjacent node would be a constant	
Control traffic signal	The traffic signal is turned green until the time EV has successfully transited from the intersection. The signal is kept green until the departure lane is determined	
Determine departure lane	The departure lane is determined by detecting the increase in volume using a microphone. Normal operation resumes after the departure lane is determined	
Send EV departure info to adjacent TS-Mod	The information is shared with the adjacent node. This information is shared with the adjacent TS-Mod on the departure lane	
Upload history	The interaction information is uploaded as history	Cl-Mod
Update map	A street map is generated at the admin screen. The formation from TS-Mods is plotted on the map. This allows the admin to oversee the state	
Record history	History is kept in a data store. This includes TS-Mod ID, EV arrival time, EV departure time, arrival and departure lane, as well as total transit time	
Generate insights	This task generates insights and allows an admin to generate reports and monitor and plot data to uncover patterns and acumens	

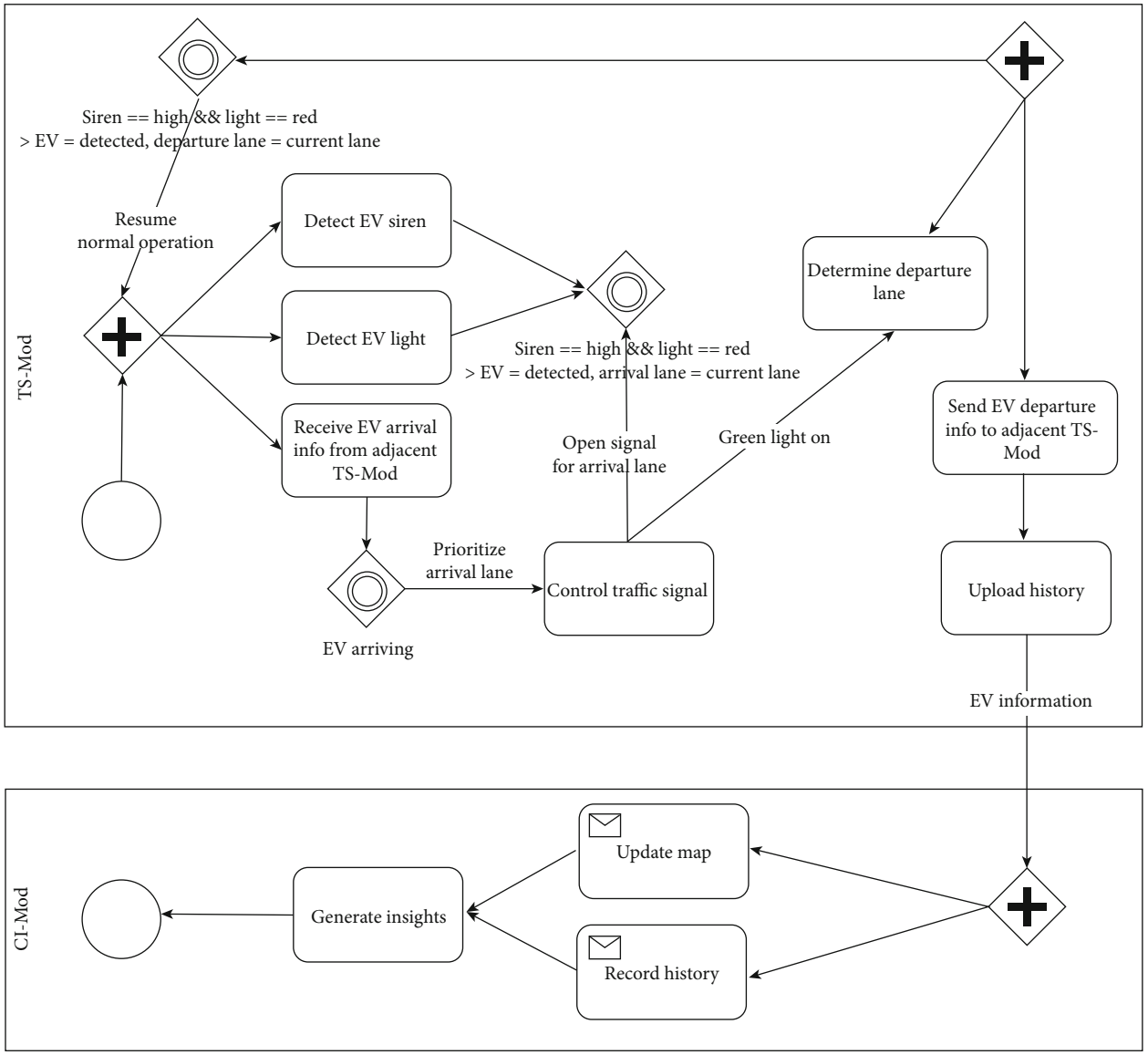


Figure 6: BPMN model of DEVeTS-AIoT.

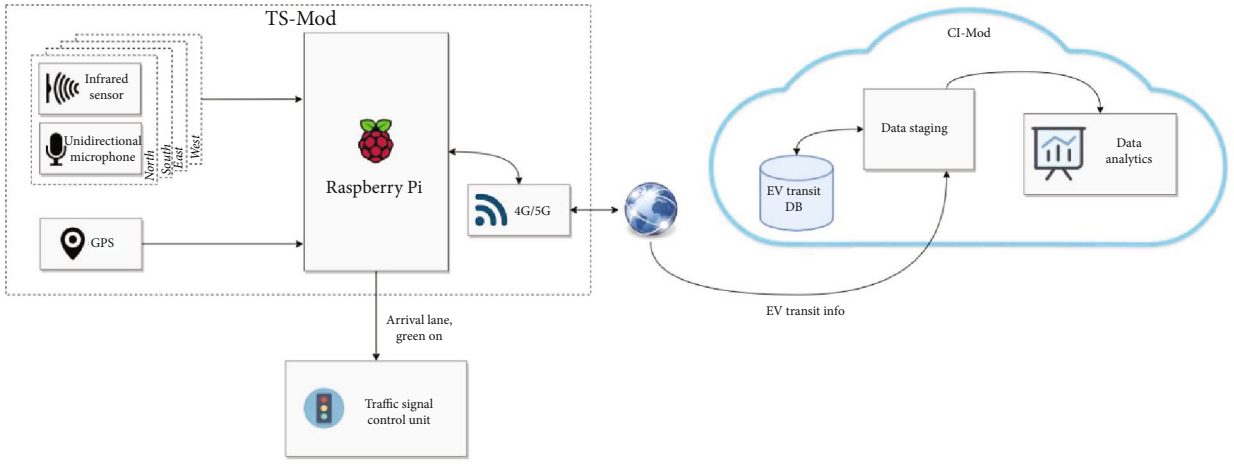


Figure 7: Architecture of DEVeTS-AIoT.

Table 4: Specifications of hardware components and their power consumption.

Component	Power	Connectivity	Other specs
Raspberry Pi 3 model B (Raspberry [56])	1.3-1.4 (W)	(i) Wireless LAN (ii) Bluetooth low energy (BLE) (iii) 100 base Ethernet (iv) 4 USB 2 ports	(i) Quadcore 1.2GHz (ii) 64-bit (iii) 1 GB RAM (iv) 4 pole stereo output (v) Full-size HDMI (vi) CSI camera port (vii) DSI display (viii) Micro SD port
GPS module NEO-M8N [57]	36-75 (mW)	(i) UART (ii) USB	(i) Baud rate 9600 (ii) Precision 2.5 meter
SIM7600E-H 4G HAT [58]	0.25 (W)	(i) 2G–4G (ii) 85.6 kbps–50 Mbps	(i) LTE (ii) WCDMA (iii) TD-SCDMA (iv) CDMA 2000 (v) EDGE (vi) GSM (vii) GPRS
SunFounder Infrared Sensitive IR Receiver Sensor [59]	3 (mW)	(i) 1838b highly sensitive IR receiver	(i) Low cost, wide-angle, and long-distance receiving (ii) Output levels compatible with TTL and CMOS
Ultramic 384 K EVO [60]	90 (mW)	(i) USB 2.0 (ii) Bluetooth	(i) High performance (ii) Omnidirectional audio and ultrasonic receiver (iii) 4 level sensitivity

Table 5: Truth table for detection of EV in DEVeTS-AIoT.

Input			Output		
Light == red	Siren == high	EV arriving	EV detected	Description	State of intersection
0	0	0	0	No EV	Normal
0	0	1	0	EV at the adjacent intersection, however, has not arrived yet	Caution
0	1	0	0	Siren but no red light, not EV	Normal
0	1	1	0	EV at the adjacent intersection, however, has not arrived yet	Caution
1	0	0	0	Red light but no siren, not EV	Normal
1	0	1	0	EV at the adjacent intersection, however, has not arrived yet	Caution
1	1	0	1	EV detected	Emergency
1	1	1	1	EV arriving and has been detected now	Emergency

needs to be confirmed that it will arrive at the intersection. In the emergency state, an EV has arrived and should transit quickly. Table 5 shows the truth table that is used to construct the rules for DEVeTS-AIoT. Since the space is small, there is no need to employ a classification-based approach.

The recommended mechanism is to increase the green time on an expected arrival lane to ensure a faster transit. However, an associated timer is necessary to revert to a normal state if the EV does not arrive at all. There are two cases when an intersection is in an emergency state and three cases when it is in a caution state. The caution state increases successful EV transit from 25% to 62.5%.

6. Conclusion

Traffic management in developing countries is a challenging issue. Traffic management systems as well as human resources are utilized to manage the traffic flow. Traffic congestion results in resource wastage in the form of fossil fuel, pollutes the urban environment, and creates annoying delays. These delays hamper quick EV transit through traffic intersections which can end in a fatal outcome. This work proposes a distributed AIoT-based EV transit system, built on Raspberry PI with minimal sensors including infrared sensors for detecting emergency lights and directional

microphones for detecting sirens. This system makes decisions based on rules to ensure that an EV moves smoothly through crossings. Once an EV is detected on an incoming lane, the traffic signal is turned to green until the time the EV has successfully passed through the intersection. The departure lane is detected, and this information is shared with adjacent intersections to further reduce the transit time. As a result of the system, successful EV transit has increased from 25% to 62.5 percent.

Data Availability

The authors confirm that the data generated or analyzed and supporting the findings of this study are available within the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

The authors acknowledge the support of Mr. Asad Zaman and Ms. Zahra Qaisar, students of Foundation University Islamabad, in implementing a prototype.

References

[1] A. Boukerche and J. Wang, "Machine learning-based traffic prediction models for intelligent transportation systems," *Computer Networks*, vol. 181, p. 107530, 2020.

[2] T. Nation, *Percent of Emergency Patient Deaths Blamed on Traffic Jam Delays*, The Nation Thailand, 2017, https://www.nationthailand.com/in-focus/30304268.

[3] P. Collinson, *The Italian Job [Motion Picture]*, Oakhurst Productions, 1969.

[4] W.-H. Lee and C.-Y. Chiu, "Design and implementation of a smart traffic signal control system for smart city applications," *Sensors*, vol. 20, no. 2, 2020.

[5] S. Hussain, U. Mahmud, and S. Yang, "Car e-talk: an IoT-enabled cloud-assisted smart fleet maintenance system," *IEEE Internet of Things Journal*, vol. 1-1, 2021.

[6] J. D. Esquicha-Tejada and J. C. Copa-Pineda, "Low-cost and energy-efficient alternatives for home automation using IoT," *International Journal of Interactive Mobile Technologies*, vol. 16, no. 5, pp. 153–168, 2022.

[7] K. L. Lueth, "IoT analytics," 2022, IoT Analytics: https://iot-analytics.com/iot-2021-in-review/.

[8] U. Mahmud, S. Hussain, A. J. Malik, S. Farooqui, and N. A. Malik, "Realizing IoE for smart service delivery: case of museum tour guide," in *Smart Systems Design, Applications, and Challenges*, J. M. Rodrigues, P. J. Cardoso, J. Monteiro, and C. M. Ramos, Eds., IGI Global, 2020.

[9] L. G. Nikolov, "Wireless network vulnerabilities estimation," *Security & Future*, vol. 2, no. 2, pp. 80–82, 2018, https://stumejournals.com/journals/confsec/2018/2/80.

[10] Z. Lv and N. Kumar, "Software defined solutions for sensors in 6G/IoE," *Computer Communications*, vol. 153, pp. 42–47, 2020.

[11] M. Masoud, Y. Jaradat, A. Manasrah, and I. Jannoud, "Sensors of smart devices in the Internet of Everything (IoE) era: big opportunities and massive doubts," *Journal of Sensors*, vol. 2019, 26 pages, 2019.

[12] E. Bellini, P. Bellini, D. Cenni et al., "An IoE and big multimedia data approach for urban transport system resilience management in smart cities," *Sensors*, vol. 21, no. 2, p. 435, 2021.

[13] T. Guo, K. Yu, M. Aloqaily, and S. Wan, "Constructing a prior-dependent graph for data clustering and dimension reduction in the edge of AIoT," *Future Generation Computer Systems*, vol. 128, pp. 381–394, 2022.

[14] M. A. Jan, M. Zakarya, M. Khan et al., "An AI-enabled lightweight data fusion and load optimization approach for internet of things," *Future Generation Computer Systems*, vol. 122, pp. 40–51, 2021.

[15] Y. Liao, N. Yu, G. Zhou, Y. Wu, and C. Wang, "A wireless multi-channel low-cost lab-on-chip algae culture monitor AIoT system for algae farm," *Computers and Electronics in Agriculture*, vol. 193, p. 106647, 2022.

[16] S. Y. Siddiqui, I. Ahmad, M. A. Khan et al., "AIoT enabled traffic congestion control system using deep neural network," *EAI Endorsed Transactions on Scalable Information Systems*, vol. 8, no. 33, pp. 1–7, 2021.

[17] A. Elmrini and A. G. Amrani, "Wireless sensors network for traffic surveillance and management in smart cities," in *2018 IEEE 5th International Congress on Information Science and Technology (CiSt)*, pp. 562–566, Marrakech, Morocco, 2018.

[18] A. Hilmani, A. Maizate, and L. Hassouni, "Automated real-time intelligent traffic control system for smart cities using wireless sensor networks," *Wireless Communications and Mobile Computing*, vol. 2020, Article ID 8841893, 28 pages, 2020.

[19] B. Pawłowicz, B. Trybus, M. Salach, and P. Jankowski-Mihułowicz, "Dynamic RFID identification in urban traffic management systems," *Sensors*, vol. 20, no. 15, p. 4225, 2020.

[20] S. Javaid, A. Sufian, S. Pervaiz, and M. Tanveer, "Smart traffic management system using Internet of Things," in *2018 20th International Conference on Advanced Communication Technology (ICACT)*, Chuncheon, Korea (South), 2018.

[21] A. Brzozowska, D. Bubel, and A. Kalinichenko, "Analysis of the road traffic management system in the neural network development perspective," *Eastern-European Journal of Enterprise Technologies*, vol. 2, no. 3 (98), pp. 16–24, 2019.

[22] D. Elkin and V. Vyatkin, *IoT in Traffic Management: Review of Existing Methods of Road Traffic Regulation*, A. I. Systems and R. Silhavy, Eds., Springer, Cham, 2020.

[23] J. C. Falcocchio and H. S. Levinson, "The costs and other consequences of traffic congestion," in *Road Traffic Congestion: A Concise Guide*, J. C. Falcocchio and H. S. Levinson, Eds., Springer, Cham, 2015.

[24] K. Lalitha and M. Pounambal, "IoT-based traffic management," in *Emerging Research in Data Engineering Systems and Computer Communications*, P. V. Krishna and M. S. Obaidat, Eds., Springer, Singapore, 2020.

[25] M. A. Mondal and Z. Rehena, "An IoT-based congestion control framework for intelligent traffic management system," in *Advances in Artificial Intelligence and Data Engineering*, N. N. Chiplunkar and T. Fukao, Eds., Springer, Singapore, 2021.

[26] Z. Ullah, F. Al-Turjmanb, L. Mostarda, and R. Gagliardia, "Applications of artificial intelligence and machine learning in smart cities," *Computer Communications*, vol. 154, pp. 313–323, 2020.

[27] N. B. Soni and J. Saraswat, "A review of IoT devices for traffic management system," in *2017 International Conference on Intelligent Sustainable Systems*, pp. 1052–1055, Palladam, India, 2017.

[28] N. R. Lavanya and S. V. Pancham, "A review on Iot based traffic management system," *International Journal of Engineering Applied Sciences and Technology*, vol. 5, no. 1, pp. 612–615, 2020, https://www.ijeast.com/papers/612-615,Tesma501,IJEAST.pdf.

[29] M. M. Wani, S. Khan, and M. Alam, "IoT based traffic management system for ambulances," 2020, https://arxiv.org/abs/2005.07596.

[30] R. Juric and O. Madland, "Semantic framework for creating an instance of the IoE in urban transport: a study of traffic management with driverless vehicles," in *2020 IEEE International Conference on Human-Machine Systems (ICHMS)*, pp. 1–8, Rome, Italy, 2020.

[31] H. Rajab and T. Cinkelr, "IoT based smart cities," in *2018 International Symposium on Networks, Computers and Communications (ISNCC)*, pp. 1–4, Rome, Italy, 2018.

[32] W.-H. Wang and Y.-T. Hsu, "Action research on development and application of AIoT traffic solution," in *CEB 2018 Proceedings*, p. 92, Guilin, China, 2018, https://aisel.aisnet.org/iceb2018/92.

[33] U. Mahmud, S. Hussain, and S. Yang, "Power profiling of context aware systems: a contemporary analysis and framework for power conservation," *Wireless Communications and Mobile Computing*, vol. 2018, 15 pages, 2018.

[34] A. Guillen-Perez and M.-D. Cano, "Intelligent IoT systems for traffic management: a practical application," *IET Intelligent Transport Systems*, vol. 15, no. 2, pp. 273–285, 2021.

[35] M. Ali, G. L. Devi, and R. Neelapu, "Intelligent traffic signal control system using machine learning techniques," in *Microelectronics, Electromagnetics and Telecommunications*, Springer, Singapore, 2021, https://www.springerprofessional.de/en/intelligent-traffic-signal-control-system-using-machine-learning/18113312.

[36] M. Sharma, A. Bansal, V. Kashyap, P. Goyal, and T. H. Sheikh, "Intelligent traffic light control system based on traffic environment using deep learning," in *1st international conference on computational research and data analytics (ICCRDA 2020)*, p. 1022, Rajpura, India, 2020.

[37] P. Sankar and G. Voorandoori, "Intelligent transportation systems and its necessity in various traffic conditions in Indian scenarios," in *Internet of Vehicles and Its Applications in Autonomous Driving*, N. Gupta, A. Prakash, and R. Tripathi, Eds., Springer, Cham, 2021.

[38] B. Cheng, "Intelligent traffic strategy based on 5G auto autonomous driving," in *The 2nd International Seminar on Computer Science and Engineering Technology (SCSET)*, p. 1732, Shanghai, China, 2021.

[39] A. Beg, A. R. Qureshi, T. Sheltami, and A. Yasar, "UAV-enabled intelligent traffic policing and emergency response handling system for the smart city," *Personal and Ubiquitous Computing*, vol. 25, no. 1, pp. 33–50, 2021.

[40] H. Wang, Y. Li, and H. V. Zhao, "Research on intelligent traffic control methods at intersections based on game theory," 2020, http://arxiv.org/abs/2009.05216.

[41] N. Kumar, S. S. Rahman, and N. Dhakad, "Fuzzy inference enabled deep reinforcement learning-based traffic light control for intelligent transportation system," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 8, pp. 4919–4928, 2021.

[42] P. Sadhukhan and F. Gazi, "An IoT based intelligent traffic congestion control system for road crossings," in *2018 International Conference on Communication, Computing and Internet of Things (IC3IoT)*, Chennai, India, 2018.

[43] A. M. Masum, M. K. Chy, I. Rahman, M. N. Uddin, and K. I. Azam, "An Internet of Things (IoT) based smart traffic management system: a context of Bangladesh," in *2018 International Conference on Innovations in Science, Engineering and Technology (ICISET)*, pp. 418–422, Kumira, Chittagong, 2018.

[44] M. E. Harikumar, M. Reguram, and P. Nayar, "Low cost traffic control system for emergency vehicles using ZigBee," in *2018 3rd International Conference on Communication and Electronics Systems (ICCES)*, pp. 308–311, Coimbatore, India, 2018.

[45] M. K. Madisa and M. K. Joseph, "Android and Cloud based traffic control system," in *2018 International Conference on Advances in Big Data, Computing and Data Communication Systems (icABCD)*, pp. 1–4, Durban, South Africa, 2018.

[46] L. P. Rani, M. K. Kumar, K. S. Naresh, and S. Vignesh, "Dynamic traffic management system using infrared (IR) and Internet of Things (IoT)," in *2017 Third International Conference on Science Technology Engineering & Management (ICONSTEM)*, pp. 353–357, Chennai, India, 2017.

[47] S. S. Ramaprasad and K. N. Kumar, "Intelligent traffic control system using GSM technology," in *2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI)*, pp. 830–834, Chennai, India, 2017.

[48] O. Avatefipour and F. Sadry, "Traffic management system using IoT technology - a comparative review," in *2018 IEEE International Conference on Electro/Information Technology (EIT)*, pp. 1041–1047, Rochester, MI, USA, 2018.

[49] Ceic, *Number of Registered Vehicles by Country*, CEIC, 2019, https://www.ceicdata.com/datapage/en/basket?basketId=62321cc5a1aad000204e1319.

[50] J. Fuehrer and J. Butchko, *Learning BPMN 2.0: A Practical Guide for Today's Adult Learners*, Indie Books International, 2018.

[51] R. Shapiro, S. A. White, C. Bock et al., *BPMN 2.0 Handbook Second Edition: Methods, Concepts, Case Studies and Standards in Business Process Modeling Notation (BPMN)*, Future Strategies, Incorporated, 2011.

[52] R. D. Yates and S. K. Kaul, "The age of information: real-time status updating by multiple sources," *IEEE Transactions on Information Theory*, vol. 65, no. 3, pp. 1807–1827, 2019.

[53] Z. Fang, J. Wang, C. Jiang, X. Wang, and Y. Ren, "Average peak age of information in underwater information collection with sleep-scheduling," *IEEE Transactions on Vehicular Technology*, p. 1, 2022.

[54] Z. Fang, J. Wang, Y. Ren, Z. Han, H. V. Poor, and L. Hanzo, "Age of information in energy harvesting aided massive multiple access networks," *IEEE Journal on Selected Areas in Communications*, vol. 40, no. 5, pp. 1441–1456, 2022.

[55] U. Mahmud, S. Hussain, and I. K. Toure, "Gathering contextual data with power information using smartphones in Internet of Everything," *Wireless Communications and Mobile Computing*, vol. 2022, 14 pages, 2022.

[56] R. Pi, "Raspberry Pi 3 Model B," 2016, https://www.raspberrypi.org/products/raspberry-pi-3-model-b/.

[57] ublox, "NEO-M8N," 2021, https://www.u-blox.com/en/product/neo-m8-series.

[58] waveshare, "SIM7600 E-H," 2021, https://www.waveshare.com/wiki/SIM7600E-H_4G_HAT.

[59] SunFounder, 2018, https://www.sunfounder.com/products/infrared-receiver-module.

[60] Dodotronic, 2021, https://www.dodotronic.com/product/ultramic-384k-evo/?v=2a47ad90f2ae.

[61] N. A. Malik, U. Mahmud, and M. Y. Javed, *Future challenges in context aware computing*, Villa Real, 2007.

[62] U. Mahmud, N. Iltaf, A. Rehman, and F. Kamran, *Context-Aware Paradigm for a Pervasive Computing Environment (CAPP)*, Villa Real, Portugal, 2007.

[63] U. Mahmud and M. Y. Javed, "Context inference engine (CiE): classifying activity of context using Minkowski distance and standard deviation-based ranks," in *Systems and Software Development, Modeling, and Analysis: New Perspectives and Methodologies*, IGI Global, 2014.

[64] U. Mahmud and M. Y. Javed, "Context inference engine (CiE)," *International Journal of Advanced Pervasive and Ubiquitous Computing*, vol. 4, no. 3, pp. 13–41, 2012.

Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 6916048, 17 pages
https://doi.org/10.1155/2022/6916048

Review Article

Systematic Analysis of Risk Associated with Supply Chain Operations Using Blockchain Technology

Habib Ullah Khan, Muhammad Zain Malik, and Sulaiman Khan

Department of Accounting and Information Systems, College of Business and Economics, Qatar University, Doha, Qatar

Correspondence should be addressed to Habib Ullah Khan; habib.khan@qu.edu.qa
and Muhammad Zain Malik; zainmalik59@hotmail.com

Received 30 May 2022; Revised 29 June 2022; Accepted 20 July 2022; Published 26 August 2022

Academic Editor: Muhammad Imran

Advancements in information and communication technologies (ICT), big data analytics, and artificial intelligence- (AI-) based techniques brought a dramatic revolution in diverse research domains, including healthcare, IoT, and networking. Blockchain technologies are gaining traction from both private and government organizations at an incredible rate. Emerging technologies have different levels of technological complexities and commercial ramifications. This technology is playing an essential role in the financial revolution of banking and regulatory sectors. Blockchain has piqued the interest of many academics, organizations, and businesses, particularly in using bitcoin. To grasp the significance of this revolution, a comprehensive assessment is performed to bridge the gaps in the targeted blockchain-driven domain with different perspectives. For this systematic review process, a set of four distinct research questions were formulated to accumulate the most relevant research trends. In private and public organizations, it is a securing technology to deliver trustworthy and protected services to users because of its decentralized, controlled aspect. Financial services, real estate, supply chain management, healthcare, academics, and other industries benefit significantly from this evolutionary technology. These application cases are diverse and far-reaching, ranging from smart contracts to blockchain-encrypted educational certificates. This systematic analysis has investigated a total of 113 relevant articles and concluded with the features and functions in an economic setting and briefed how these variables can balance players' incentives, define core blockchain-related features, and present new research ideas to solve the proposed risk.

1. Introduction

Technology has changed administration departments in the organizations to observe the positive influences of the technology [1]. Recently, our civilization has witnessed introducing an inventive trend of disruptive technologies across several industries dubbed Industry 4.0 [2]. The Internet of Things (IoT) [3] and its emerging concepts are increasingly coming together to achieve a common goal: enabling intelligent objects to interconnect nearby and over the Internet to gather comprehensive data that provide modified automation services with minimum deliberate human interlinkage [4]. IoT has multiplied due to the continual advancement and development of sensor technology, wireless network data transfer, embedded technology, and computer control technology. The IoT is deliberated the 3rd world information industry wave after computers and the Internet, quickly expanding [5]. The IoT intends to ease the collecting of dispersed data in the worldwide manufacturing industry [6] and the sharing and processing of knowledge and information thru many cooperating associates through the use of suitable information system design [10].

In this modern technological age, the Internet of Things- (IoT-) based application and blockchain technology-based smart systems can process data to retrieve information by ensuring high privacy and data security. It is building a global information network made of many interlinked "Things," which is a vital enhancing technology for contemporary manufacturing [7]. Data is the key to quickly gauging educational performance. However, data and education are

locked and segregated among centralized systems, resulting in knowledge gaps and errors [8]. With constant improvements in computation studies, ranging from high-speed calculations to smart autonomous systems, there has been a significant influence on other related subjects such as aerospace engineering, biomedical engineering, and robotics. As a contemporary trend and key multidisciplinary topic in the scientific world, robotics has embraced different technical assets from multiple fields [9]. Collaboration between companies is vital for achieving larger, shared goals. Consider a supply chain, where the cooperation of several firms results in a product via the various processes from manufacture to distribution [10].

Blockchain technology has just expanded much attention from industry and academics [11]. It is being employed in cryptocurrencies or electronic cash and other areas such as healthcare, financial transactions, manufacturing, insurance [12], education, and IoT, with the capacity of increased skills and durability [13]. Due to high security and credibility, it has changed the way accounts are kept in recent years. Its implementation has been spread to various other industries, such as financial sectors, banking, intellectual property protection, securities, and electronic currency [14]. Blockchain has several valuable qualities, including the ability to reduce trust assumptions. It is a technology that improves transparency by allowing users to get data and verify its integrity locally [15]. Bitcoin [16] and other cryptocurrencies are enabled by blockchain technology, which is a secure decentralized computer ledger [17].

Blockchain is a decentralized ledger for securely storing peer-to-peer network data transactions. Further, it ensures that transactions are verifiable and transparent. The primary goal of blockchain technology is to enable dual parties to perform secure transactions without the interference of a moderator [18]. Data is public and cannot be redacted in the classic blockchain system. With the advancement of blockchain technology, the problem of data immutability will become more important once it has been written on the chain [19]. Recently, the blockchain technology has fascinated well-known attention due to its valuable features, e.g., transparency [20, 21], traceability [20], decentralization [22], and immutability [23]. A blockchain contains data in blocks, which create a linked list in the order determined by a distributed consensus process [24]. Blockchain technologies are still in their early phases, and recent advancements in blockchain technology may influence findings. The created tool might provide decision-makers with a basic picture of the advantages of using blockchain technology before deciding whether or not to integrate it into their existing system [2].

The blockchain architecture facilitates information collection, management, preservation, storage, and delivery. As a result, it may be used in various industries, including health record management, digital voting, IoT data, academia, and research publishing [25]. The blockchain is a new technology that accesses many people to agree on a shared state without trusted middlemen [26]. Blockchain has recently piqued the interest of many industries and academics. By making a trustworthy and secure solution, the participants in the network share the same ledger in a distributed setting with no centralized authority. Traditional blockchain protocols have a relatively poor throughput, and researchers have proposed many strategies to increase it. Bitcoin is the first blockchain system that organizes blocks in a linear chain. Bitcoin miners will do their best to solve random cryptographic problems, a process is known as proof-of-work, to keep the chain alive. In conjunction with blockchain technology that processes network data, high privacy, and security issues, data regulations may be applied to software artefacts and data, as with the IoT [27].

2. Background Study

The economy is essential in building a resilient community, and publicly traded enterprises play a crucial role in the native economy. The challenge posed by global environmental developments has converted a severe impediment to long-term humanoid progress, and long-term process development has grown considerably more complex [28]. Corporate governance has been formed to control and direct the company by its shareholders. According to the agency theory, there will always be a mismatch between shareholders' and the organization's management's aims [29]. Corporate governance is explained by the board of directors and audit committee characteristics, and corporate debt is calculated by debt ratios, short-term debt ratios, and long-term debt ratios. The situation of corporate governance has been a significant factor that affects corporate development and even regular economic running [30].

The so-called internal management and control system's internal governance structure comprises three components or methods by the board of directors, the managers, and the shareholders. The management operations of the control system on the external market through competition are referred to as the outer governance structure or external control mechanism such as market manager, capital markets [31], product markets [32], market control, the government management system [33], accounting standards [34], legal, market manager, social media [35]. They give company performance statistics and analyze corporate conduct and operational performance [36]. The state of corporate governance has been a critical factor influencing business development and even routine economic operation [37]. The form of ownership in a corporate is an essential component of appropriate regulation of significant enterprises' activities in the market environment at the micro and macro levels allowing all parties to the relationship to reflect their interests [38].

Artificial intelligence (AI), a subfield of computer science, underpins the theory, technique, technology, and applications for mimicking, extending, and enhancing human intellect [23]. The notion of a smart city relates to improving the city's quality of life by utilizing full use of idle resources via sharing. Because of technical limitations, most modern resource distribution systems use centralized data storage [39]. In 2008, bitcoin was the first suggested cryptocurrency, presenting the blockchain as a distributed infrastructure platform. It enables the transfer of decentralized peer-to-peer Internet currency known as "bitcoins" from

one party to another without needing a banking sectors [40]. In various digital contexts, the big data age is undermining consumer privacy. By analyzing, correlating, collecting, and managing huge volumes of personal data, large third parties gain from managing their users' data. These organizations and their services are vulnerable to security breaches and exploitation of customer data, which influence compromise their operations consumers' privacy, even if they are not aware of it [41].

Blockchain was established in January 2009 as the core technology of bitcoin, combining significant accomplishments in disciplines such as contemporary cryptography and distributed networks. Since the advent of bitcoin, the blockchain network has increasingly handled huge transfer transactions in a distributed way [19]. A blockchain is an advanced data structure comprising a growing list of immutable documents called blocks that are connected using cryptographic algorithms. Each block in a blockchain covers a cryptographic hash of the transactional data, the previous block, and a timestamp. In another way, a blockchain may alternatively be thought of as a distributed data structure or a distributed ledger that operates logically over a network with several nodes connected in a peer-to-peer function [42]. With the fast growth of emerging technologies such as the big data, cloud computing, and Internet of Things (IoT), the underlying technology, blockchain, is becoming the driving force behind research and technology [43]. In the last several years, blockchain has gained a lot of interest. This enormous popularity has prompted several issues, one of which is the scalability of blockchain networks [44].

A blockchain is a precise structure used to store all types of essential data in an unforgeable manner. Blockchain is a new technology that promises to solve unmanageable trust concerns by enabling safe and verified systems in various areas. It is a series of blocks interlinked together as a chain that includes proof of information. This blockchain is first used to timestamp documents to eliminate backdating. The most crucial aspect is that it cannot be modified once the data is captured. Each block is made up of information, a hash, and a hash of the preceding block [45]. After having developed as the technology behind cryptocurrencies, smart contract-enabled blockchains are increasingly implemented in the application of spirited within the organizational information systems [46]. The fundamental technology of bitcoin is blockchain, and its initial purpose is driven from economic incentives. Blockchain is a new technology encompassing several domains, including distributed systems and the Internet of Things (IoT) [47].

Following the Internet as another disruptive technical invention, blockchain has led to developing a distributed accounting system that is tamper-resistant, traceable, highly trustworthy, and decentralized. It can increase the security of grid system data and aid in developing a dependable, effective, and reliable distributed smart grid system [48]. A hybrid of blockchain and IoT seems promising, even though blockchain demands real-time data application and IoT provides mechanisms for safely and efficiently storing and managing information overloads. The technology is vital to the manufacturing industry, undergoing a digital revolution by merging equipment, advances, and data, resulting in the Industrial IoT (IIoT). A combination of IIoT and blockchain is called Blockchain Industrial Internet of Things (BIIoT) [49]. By recording and verifying permitted access to confidential medical records, blockchain can ensure the security of sensitive data. Blockchain is used to protect medical records from manipulation by acting as a distributed database [50].

3. Research Protocol

A systematic literature review (SLR) evaluates and identifies a topic of interest based on specific formulated most relevant research questions. The research questions act as a cornerstone in the SLR process. SLR seeks to provide a balanced assessment of a study topic by employing a rigorous, reliable, and traceable approach [51]. SLR is carried out by many researchers in various fields, e.g., networking [52] and healthcare systems [53]. This research examined and analyzed the most recent studies on the usage of blockchain technology for identification and solving technics of various risk factors. The following are the objectives of this SLR:

(i) To analyze the current research work, four different research questions have been formulated. These questions aim to outline the models and to guarantee high security within the organizations, various kinds of threats that generally faced by the employees in the organizations, various types of tools suggested to help the organizations during unwanted situations to overcome the security risks, and various implications of the blockchain to tackle many research problems within the regulatory organizations

(ii) The aim of SLR is to identify the critical problems within the available solutions and suggest exploited research directions and fulfil the research gaps within the available resolutions. These new research directions will ultimately assist the organizations and employees in ensuring high authenticity for their security means and will have no information leakage and combat intruder's attacks

(iii) This SLR work selected one hundred thirteen most relevant research articles from four different available online libraries. This selection is made on the relevant pertinent research papers that will allow the researchers to identify the most relevant research articles within the blockchain field and assessment details

This SLR work is being carried out in accordance with the established parameters presented by Keele and Kitchenham et al. [54, 55] which is considered in this proposed SLR process. The review procedure for this SLR is shown in Figure 1. It includes eight essential steps: (1) choosing of research domain; (2) formulation research questions; (3) keyword identification and query formulation; (4) digital library selection for article accumulation; (5) filtering the

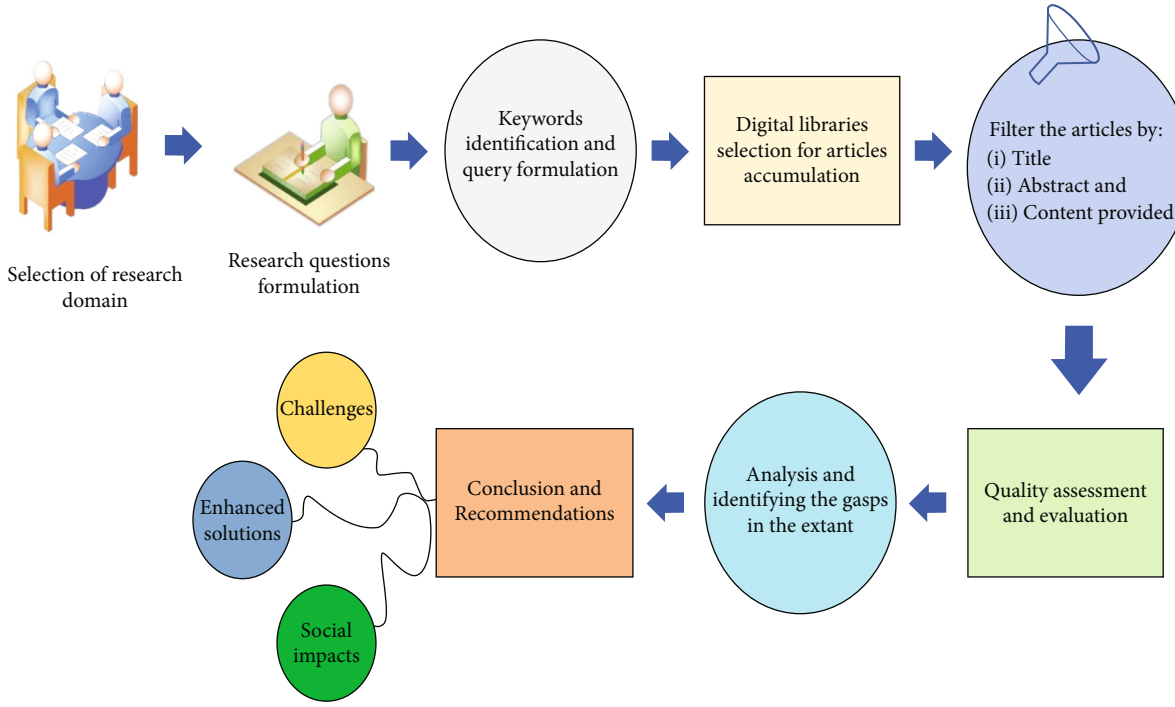


Figure 1: Research methodology for a proposed systemic literature review.

Table 1: Formulations of research questions.

S. no	Research questions	Description
RQ1.	What are the key elements that must be considered for developing a blockchain-based solution for a certain research problem?	Organizations have to face many security issues, i.e., reliability, privacy, and protection. So, the main objective of this research question is to analyze the key elements and develop a blockchain-based solution for the certain research problems.
RQ2.	What are the different applications of blockchain-based solution in our daily life?	Blockchain plays an essential role in the financial industry, and the core objective of this question presents the significance of blockchain-based solution in our daily life.
RQ3.	What are the key challenges that are currently faced in blockchain-driven application?	This research question emphasizes on categorising different types of challenges currently faced in the blockchain implementation.
RQ4.	How block-based solution have revolutionized the banking and financial industry?	Based on the literature, this research question purposes to revolution of the blockchain technology and provide solution to the financial sector and banking.

articles by their titles, abstract, and content provided; (6) quality assessment and evaluation; (7) analysis and identifying the gaps in the extant; and (8) conclusion and recommendations. In Figure 1, each of these steps is fully described.

3.1. Selection of Research Domain. Research papers from different online digital libraries were systematically studied to identify the concept of blockchain, discover the problem linked to the selected domain, and find out the solutions of various problems so far that what the researchers have examined.

3.2. Research Question Formulation. SLR is another method for critically assessing a given situation. Several features exist for AI-based platforms to be examined critically. Most relevant papers, book chapters, conference proceedings, and journals were deliberated at the primary stage that clearly defined blockchain application. Our initial study identified the problem faced in the selected domain. To bring out the research result, the proposed research emphasizes some research questions given below that are extracted based and helps the assessment from various papers and articles to make this SLR an effective search.

3.3. Research Questions. The research questions (RQ) are an essential part for every SLR work. Identifying the most suitable and relevant questions ensures the accuracy and relevancy of the SLR work. To explore the most relevant questions, we have formulated a set of four questions to conduct this SLR work in the proposed area from various aspects. The aims of the research questions are described in detailed in Table 1.

Table 2: Article selection process and development of the final database.

Online library	Filter articles on title bases	Filter articles on abstract bases	Articles selected on contents provided bases
IEEE Xplore	337	134	48
ScienceDirect	112	42	11
Hindawi	213	67	23
Springer Link	311	59	31
Total			113

3.4. Keyword Identification. After finalizing the set of RQs, the next step is to formulate the most relevant keywords that exploit relevant paper from the online libraries. The completed best relevant articles retrieved are as follows: "BLOCKCHAIN, BITCOIN, DIGITAL CURRENCY, CRYPTOCURRENCY, SECURITY THREATHS, CROWD FUNDING, CHALLENGES, ISSUES, DILEMMAS". The finalized keywords are used to develop a set of query related to the required database and modified further for the best outcomes (for obtaining most relevant results from the suitable articles).

3.5. Query Selection. To find out the best outcomes from the articles, an accumulation process is selected from the online libraries; the formulated queries are ("BLOCKCHAIN" OR "CRYPTOCURRENCY" OR "BITCOIN" OR "DIGITAL CURRENCY") AND ("SECURITY" OR "SAFETY") AND ("CROWD FUNDING" OR "FINANCING") AND ("CHALLENGES" OR "ISSUES" OR "DILEMMAS"). These queries are further changed based on required results and the selected online libraries. Based on the title, substance, and abstract of the research article, the most relevant 113 articles and research publications are preferred. The full description of the accumulated research articles is defined in the following subsection.

3.6. Digital Library Selection for Article Accumulation. To gather the most pertinent research articles for the proposed SLR work, we chose four of the most popular peer-reviewed online libraries including ScienceDirect, IEEE, Hindawi, and Springer Link. Overall, the most relevant 113 research articles are selected for evaluation and assessment expect. The description regarding final database infrastructure and suitable articles chosen is described in Table 2.

A total of 113 articles are selected for the analyzing and assessment purposes. The total finalized articles have contributed in this last pool from the various online peer-reviewed repositories shown in Figure 2.

Figure 3 represents the overall impact of the selected online libraries in the finalized suitable research articles. After assessing the proportion contribution, it was concluded that IEEE Xplore and Springer Link contributed the most, which shows the interest of researchers to publish their work in these repositories.

With the increase in the technology, blockchain has become an emerging and attractive domain for the research around the world. The researchers extensively exploited blockchain and cryptocurrency in various domains including banking, financial sectors, healthcare, education, IoT and smart contracts, and Internet security and privacy, to ensure the business profitability of the organization and industries. Keeping in mind about these applications, the researchers exploited these models in banking, financial sectors, and many others to ensure high integrity, privacy, decentralization, and security of the organizations. Figure 4 explains the annual contribution of various research articles in the proposed domain based on the selected research questions.

After assessing the results as shown in Figure 4, it is identified that the number of research articles tremendously increases showing that the research community keenly explores the proposed domain. The trend shows that after 2019, the number of articles exponentially increased that indicates the interest of the different organizations to ensure high privacy and security for its assets.

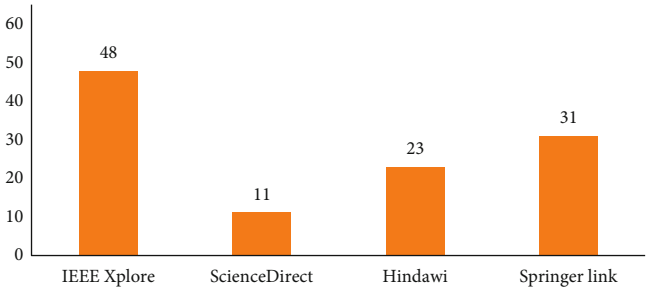


Figure 2: Number of publications from online database.

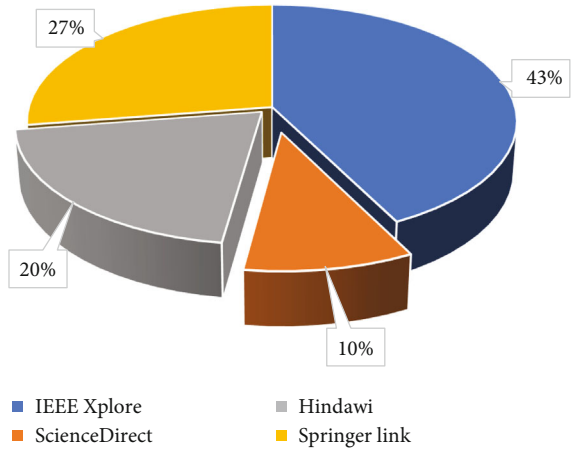


Figure 3: Percentage contribution of each library.

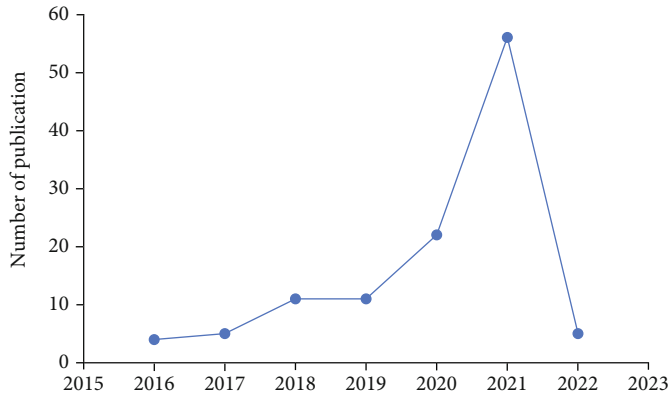


Figure 4: Year-wise sorting results.

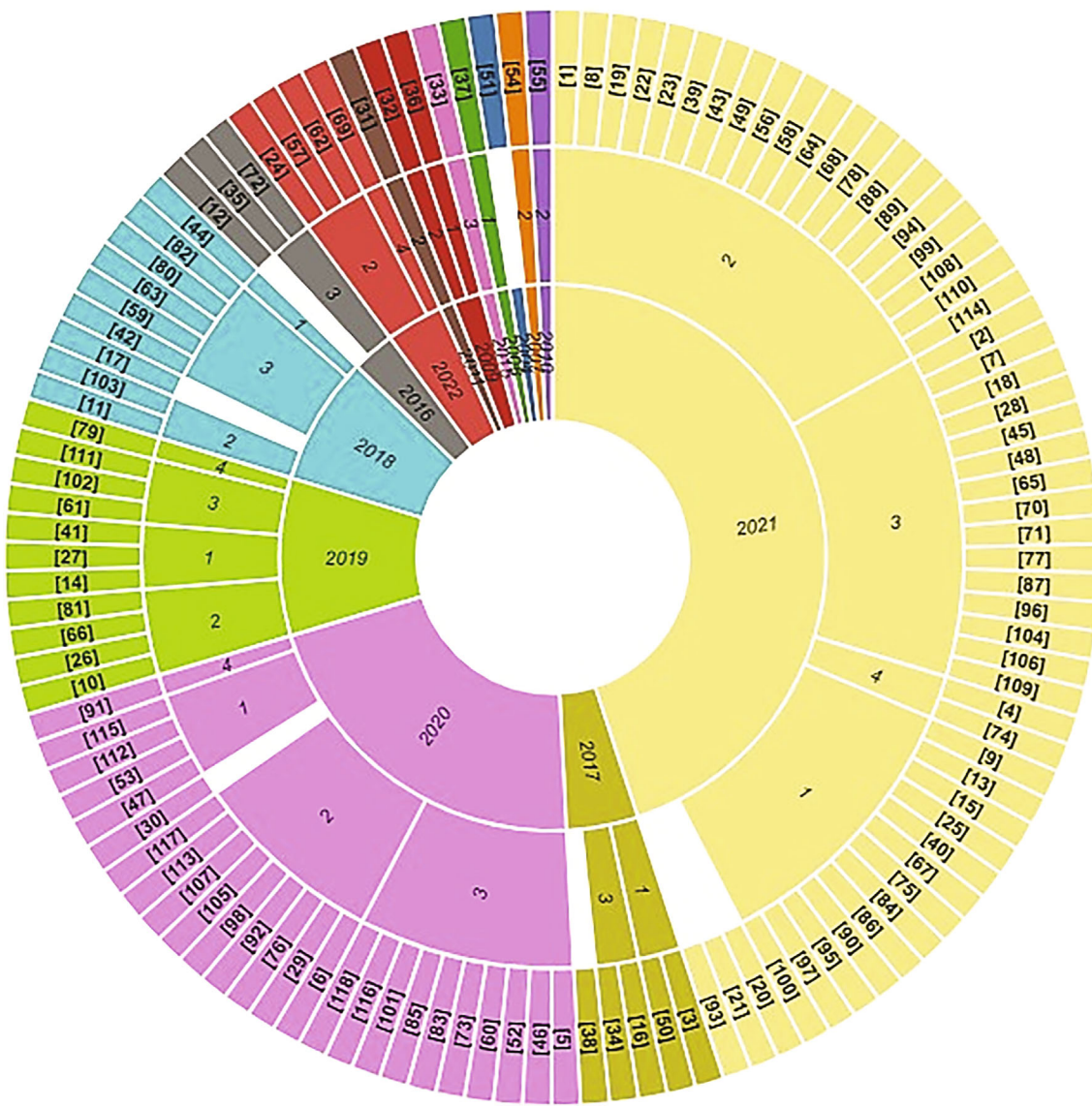


Figure 5: Quality assessment and evaluation representation of the final pool.

Table 3: List of key elements in the literature.

S. no	Key elements	Description	References
1.	Privacy	The purposes of this paper in terms of security and privacy of telecare medicine information systems and e-health were also analyzed and appraised.	[18, 19, 41, 57–59]
2.	Sharding	In this article, researchers examine how Ethereum, a well-known blockchain system, will response to sharding.	[44]
3.	Information management system	This study proposes and constructs a blockchain-based intelligent power material storage information management system.	[60]
4.	Efficiency	This study offered interesting undeveloped blockchain solutions, including those for blockchain efficiency, security, creditworthiness, performance, supervision, privacy, and online-to-offline integration.	[61]
5.	Conceptualization	In this paper, author presents perspectives from a heterogeneous collection of practitioners at the cutting edge of blockchain conceptualization, deployment, and development.	[62]
6.	Interledger technique	Study focuses the interledger methods, which are critical for allowing large-scale blockchain networks and ensuring scalable interconnection across different, distributed ledgers.	[63]
7.	Solidity programming language	The paper suggests that the smart contracts are written in the solidity programming language. A private Ethereum network hosts this blockchain and intelligent contract-based platform.	[64]
8.	Structural optimization factor model	This research proposes an intelligent contract structural optimization factor model. The gas optimization theory is used to optimize the structure of blockchain intelligent contracts by modifying the order, limiting the usage of expensive EVM data fields, eliminating duplicate fields, and optimizing intelligent contract algorithms.	[39]
9.	Bibliometric method	This study intends to investigate using the bibliometric technique, research trends, and collaboration in the field of blockchain IoT. According to the findings, the number of publications in this sector has grown dramatically.	[65]
10.	Artificial intelligence	In this article, researchers provide a thorough examination of how blockchain might improve artificial intelligence in these four areas.	[23, 66]
11.	Cryptography	Based on this paper with previous research, the application of material circulation under the emergency condition is investigated and enhances the blockchain with smart contract technology and cryptography.	[67]
12.	5G networks	The authors go on to look at the possibilities of blockchain in 5G networks and beyond artificial intelligence, as well as open up new research areas for upcoming blockchain-enabled SAG-IoT systems.	[68]
13.	Distributed systems	In this paper, researchers begin by dissecting the main components of blockchain technology and demonstrating the features of each of these components in the context of distributed systems.	[69]
14.	Traceability	The paper has proposed that it requires traceability implementation to solve existing issues of information asymmetry and low visibility is the textile and garment industry.	[70, 71]
15.	Transparency	In the article, author discusses the data, supply chain, feasibility, transparency, traceability, application, integrity, automobile, privacy, and manufacturing.	[71]
16.	Decentralized	This paper delivers to use blockchain to enable decentralized AI applications, such as safe data sharing, data privacy preservation, and providing trustworthy AI decision.	[24, 72–74]
17.	Practical scalability and applicability	In this paper, researchers offer a realistic scalability and applicability evaluation of the Quorum blockchain and its consensus algorithms.	[75]
18.	Symmetric encryption and ring signature	The study covers to safeguard transaction data and users' identities, symmetric encryption, and ring signature which are utilized. To demonstrate the validity of data redaction, the transaction sender might expose the names and transaction data of the invalid users in an anonymous environment.	[19]
19.	Intelligent contract	The authors propose and elaborate three application scenarios for blockchain-based intelligent contract technology in the supply chain factoring business, focusing on the division and transfer of creditor's rights certificates, upstream supplier factoring financing, and core enterprise due payment, as well as their implementation processes.	[76]

Table 3: Continued.

S. no	Key elements	Description	References
20.	Reliability	This research examines the reliability and significance of blockchain in smart cities of the future.	[77]
21.	Data integrity	The paper offers a blockchain technique for securing the network slice (NS) administration layer. This process assures the NS settings' data integrity and dependability.	[78]
22.	Protection	The paper describes a privacy protection structure for blockchain that implement in the multiasset model and account.	[79]
23.	Verifiability	The study enables to remove particular blocks while keeping the blockchain's verifiability.	[15]
24.	Scalability	The prospects of success of some generalized blockchain models, such as network effect scalability and future client-side use, are weighed in this article.	[80]
25.	Crowdsensing systems	In this study, the researchers build on the original research effort by looking at a new design point for bridging public blockchain with crowdsensing systems and offer a paradigm for developing blockchain-enabled crowdsensing systems that are resilient, verifiable, and private.	[81]
26.	Measuring instruments	In this paper, writers examine how blockchain might aid in the resolution of such issues and also compare to the traditional measuring instruments and distributed measuring models discussed and provide a conceptual model for implementing measuring instruments in a distributed blockchain-based architecture.	[82]
27.	SWOT analysis	The study explains the strengths, weaknesses, opportunities, and threats (SWOT) analysis in the construction supply chain by using blockchain technology.	[83]

3.7. Quality Assessment and Evaluation. After defining a set of final some relevant and suitable articles, the next main point is to evaluate all the relevant articles based on precise measures defined [56]. A quality criterion has been proposed for the SRL work for assessment purposes as given below:

(i) 1 if an article is satisfying the research question

(ii) Meanwhile 0 if an article dissatisfy to research question

The overall information regarding the set of relevant articles is detailed in Figure 5. It contains the information about the references, publication year, and so on. The outer shell in Figure 5 depicts the relevant article accumulated for the assessment process. The second last shell represents the average weighted value. A higher weighted value represents the relevancy of a certain articles with the targeted research problem.

The last shell represents the year-wise publication of the most relevant articles. In Figure 5, the trend shows that since 2019, the publication number increases in the domain, and 2021 reflects that the researchers have high contribution in the maturity of this field.

4. Results and Analysis

This portion of the paper analyzes the outcome of this SLR work. The suitable articles and their highlighted explanation against each research query are described in detail as below.

What are the key elements that must be considered for developing a blockchain-based solution for a certain research problem?

This research question has outlined key elements to develop a blockchain-based solution for the research difficulties. In this technological age, security is a prime concern for many departments including both government and nongovernment organizations. The ever-growing advancements in technology have emerged security concerns for these organizations. The main objective of this research question is to summarize different factors described in the extant and figure out what type of new elements are available to insure and protect to the blockchain technology. Table 3 depicts the list of various types of key elements for research problem.

What are the different applications of blockchain-based solution in our daily life?

Blockchain has various impacts on our lives and has offered numerous state-of-the-art applications in various fields. It secures the human privacy by introducing automated applications in many research fields such as banking, financial industry, network security, and healthcare. Table 4 shows the list of application of blockchain-based solution in our daily life.

What are the key challenges that are currently faced in blockchain-driven applications?

This research question has suggested different challenges of blockchain to secure the systems by using blockchain capabilities. The prime objective of this research question is to outline the currently challenges of blockchain-driven applications. Table 5 shows the list of different challenges proposed in the research.

How block-based solutions have revolutionized the banking and financial industry?

Table 4: List of impact of blockchain in the literature.

S. no	Application in daily life	Description	References
1.	Education	The aim of this study is to provide blockchain technology that never-before-seen precision, dependability, and immutability. This foundation of clear, verifiable data will be utilized to fuel blockchain-based apps in the future. As a consequence of our effort at a varied, comprehensive, and decentralized perspective of educational performance, we assure the best e-learning outcomes for both students and teachers.	[8, 40, 84]
2.	Tradeoffs	This article covers several existing and future merged mining, scalability, network effect, fragmentation, and generalized blockchain techniques, as well as tradeoffs in the strategy and applications of blockchain systems that aim to give universal functionality.	[80]
3.	Power material logistics	The logistics information collecting device is created and implemented in the logistics information system of power firms to get information in real time.	[85]
4.	Multiasset model	The paper proposes asset transmission and double-spending detection methods, as well as the anonymous addresses, anonymous asset information, and transaction structure in blockchain system which implement in accounts and multiasset model.	[79]
5.	Tourism industry	The use of innovation in the IT technologies in the tourism industry has been proposed by focusing the blockchain-based technology in destination management organizations (DMOs).	[86]
6.	Drug production	This study enlisted the help of pharmaceutical businesses to provide feedback on blockchain technology for medication manufacturing records. The resulting technology known as blockchain can be utilized to track medication manufacture.	[87, 88]
7.	Space-air-ground	This study provides a thorough examination of the use of blockchain technology to secure space-air-ground IoT applications.	[68]
8.	Diamond industry	The study explains the implementation of blockchain in diamond industry, as well as the benefits and drawbacks of this integration.	
9.	Construction supply	The research demonstrates the needs for, and stages toward, a blockchain-enabled construction supply structure.	[83]
10.	System architecture	In this research, author presents a novel architecture known as the dual-channel parallel broadcast (DCPB) model, which might solve such an issue to a higher degree by utilizing three methods: parallel pipeline processing, block broadcast approach, and dual communication channels.	[14]
11.	E-health	The network slicing idea is proposed to provide a solution for nonpublic networks (NPNs) in e-health contexts that meets quality of service (QoS) and privacy criteria across slices. In addition, a blockchain technique for securing the network slices (NS) administration layer.	[59, 78]
12.	Distributed computing systems	The study proposes a novel blockchain-based mechanism for delegating rights inside distributed computing systems that is devoid of the flaws seen in prior methods.	[89]
13.	Business process	Researchers demonstrate how to develop and conduct interorganizational business processes utilizing blockchain. Further, they demonstrate the ideas and reasoning of the model-driven approach to business process automation on blockchain in particular and then report on recent achievements in the field.	[10, 26]
14.	Project management	In this article, the researcher first examines the most recent blockchain applications in project management to disclose the present level of blockchain research and suggests blockchain implementation in the areas of project management. Secondly, it offers a framework to advice implementers and researchers on blockchain privacy, design decisions concerning blockchain type, transparency, platform considerations, and decentralization that are distinctive to a certain project management field.	[90]
15.	Business sector	The primary goal of this research is to present and explain the idea of blockchain in the business sector, its existing commercial applications, and the different dangers and security challenges associated with blockchain technology.	[45]
16.	Society	The study aims to demonstrate how blockchain might restore promised qualities of the previous two waves of digitalization and traits that were lost due to centralization tendencies caused by business models that are independent of the underlying technology and also discusses the technology's decentralization and the issues it brings to organizations and individuals.	[91]

Table 4: Continued.

S. no	Application in daily life	Description	References
17.	Data quality assessment	This paper sets the stage for future study by contextualizing the issue of data quality in blockchain, exploring ways to extend or modify blockchain technology to facilitate data quality evaluation, and highlighting a set of obstacles.	[46]
18.	Academic entrepreneurship	According to the research, the economic service function of colleges and universities to regional economic and social development is becoming more prominent, resulting in a scale effect; pure technical efficiency, academic entrepreneurship efficiency, and scale of universities and colleges in various regions are all improving, with an upward trend; academic entrepreneurship activities of universities and colleges in various regions.	[65, 92]
19.	Industrial Internet of Things	The article provides a comprehensive overview of Blockchain Industrial IoT and analyzes all pertinent features of this innovative idea.	[49]
20.	Smart grid	This study investigates the structure and implementation of blockchain-based technology in smart grids in order to integrate it with smart grids and develop a sustainable supply chain.	[48]
21.	Smart cities	This research demonstrates the reviews and relevance of blockchain in smart cities of the future. Due to their powerful qualities such as reliability, decentralization, transparency, and authentication, it can help smart cities thrive.	[39, 77]
22.	Aviation industry	The paper presents the key factors offered by blockchain technology in the aviation industry and also highlights layer-by-layer services and interface among aviation system mechanisms.	[93]
23.	Insurance contract	This article proposes a framework for using smart contracts for insurance agreements and storing them on the blockchain. If the claim occurs, all of the determined requirements are satisfied, and the transaction occurs; then, it is disregarded.	[64]
24.	Auto insurance	This article suggests to enhance the present vehicle insurance claim system, a blockchain-based vehicle insurance data sharing scheme. The plan is comprised of four primary bodies: the owner of car, insurer, 4S workshop, and the government body.	[94]
25.	Vehicle industry	Study examines the state of blockchain in the vehicle industry and discusses hot themes.	[71]
26.	Manufacturing industry	This article primarily highlights common patterns in blockchain-based IoT technology concentrating on essential themes and by comprehending the integration of IoT and blockchain technology.	[7]
27.	Healthcare	The motive for using of blockchain technology in the healthcare business has been proposed. The application of blockchain technology in healthcare is rapidly expanding, and it is having a massive influence on the healthcare business. Stakeholders, hospitals, clinics, patients, and other medical may exchange data and promote interoperability by using blockchain to manage and distribute electronic health and medical records.	[18, 50, 62, 95–97]
28.	Textile and clothing industry	This paper explores and offers a blockchain-based traceability framework in multitier textile and garment supply chains in this setting. On organizational level, it intellectualises the interaction of supply chain partners, as well as associated network architecture, at the operational level.	[70]
29.	Supply chain management system	In this study, seven main issues have been identified in SCM's basic operational aspects, such as logistics, distribution, supplier, manufacturer, and customer.	[98]
30.	Food supply chain	The suggested approach discusses the food supply chain management systems and leverages Ethereum smart contracts, which eliminates fabricating data, external threats, and corrupting databases.	[99]
31.	Vehicle maintenance	The study shows the use of blockchain technology in the vehicle spare part maintenance to provide benefits and carry out the automobile industry.	[100]
32.	Internet of vehicles	The paper expedites the blockchain-based system for privacy and protection of Internet of vehicles.	[101]
33.	Energy systems	This article discusses prominent energy blockchain application scenarios, evaluates generic blockchain limits and their implications on energy systems, and investigates alternative solutions to these limitations for future blockchain-based energy systems.	[24]

Table 4: Continued.

S. no	Application in daily life	Description	References
34.	Internet of Things (IoT)	The use of blockchain technology to the Internet of Things (IoT) remains a significant problem. A lightweight and high-throughput consensus method paired with blockchain technology to satisfy the actual demands of IoT.	[4, 5, 19, 58, 65, 66, 102, 103]
35.	Power trading system	The paper describes the AdaBoost algorithm which is used to forecast power trading node supply and demand gaps.	[104]
36.	Integrated project delivery	The study's findings used in a favourable external environment would facilitate IPD uptake and utilization across the architecture, engineering, and construction (AEC) sector by giving a feasible answer to present financial constraints. The results broaden the scope of future study into blockchain's ability to address problems similar to those afflicting the AEC sector.	[105]
37.	Game theory	In this study, researchers emphasize the intersection of blockchain and game theory, including game-theoretic assaults, rational mining tactics, and rational smart contracts.	[47, 106]
38.	Medical imaging	In this study, the ideas and principles behind medical imaging technology and applications are examined.	[107]
39.	Supply chain	This study examines the relationship between blockchain technology and the supply chain factoring sector.	
40.	Editorial management system	This study presents TimedChain, a functional blockchain-based editorial management system, for handling the peer-reviewed process and submission to publication.	[25]
41.	Smart contracts	The research examines how rational actors engaged in blockchain select their methods based on economic incentives to maximize their utility and provide benefit and significance of the smart contracts.	[47, 66, 108]
42.	Internet	The paper explores the factor of blockchain's compatibility with other upcoming Internet technologies and the influence of blockchain on those technologies.	[69, 74]
43.	Patents	The research focuses on patent publishing patterns, descriptive analysis and important technological categories for the data, and citation analytics for top patents and companies.	[109]
44.	Music industry	In this article, authors create smart contracts on public-permission-less blockchain to defend the music industry from the repercussions of illegally downloading copyrighted music files and provide a decentralized music file sharing network where the owner of music file may post music files and music lover can download the required music.	[110]
45.	Measuring instruments	The paper suggests a conceptual model for implementing measuring instruments in a distributed blockchain-based architecture, and it has been compared to traditional measuring instruments with the current distributed estimating models.	[82, 111]

The Industry 4.0 revolution includes a wide range of technologies such as 3D printing, cyberphysical systems (CPS), Internet of Things (IoT), cloud computing, and blockchain and artificial intelligence (AI). The benefit of these disruptive technologies is their capacity to self-learn, to be secure, and to forecast in dynamic environments [2]. The immutability of data recorded on the ledger is ensured by the architecture of blockchain technology, which assures that no single corporate entity may edit, remove, or even append any record to the log without the consent of other network members [63]. A good bank is not merely the society's financial heart, but it is also obligated to help the familiar people better their economic situations in every way feasible. Blockchain technology is a distributed, decentralized ledger that keeps track of all transactions. Blockchain technology and distributed ledger have advanced significantly to provide best solutions for a wide range of industries, particularly the financial sector. Banks, as the country's financial cornerstone, are obligated to improve society's overall economic status. The study seeks to investigate existing methods and governance structure weaknesses, and it gives insight into how blockchain might reorganize governance in banks [114]. Blockchain applications also encourage the development of "multicentre, weakly intermediated" scenarios, which will improve the banking industry's efficiency [72]. With the emergence of blockchain technology and advanced technological approaches, the Central Bank Digital Currency (CBDC) is focusing on technology empowerment, interests of financial consumers under new business models, and planning for protecting the rights; building data transaction, strengthening data governance, and privacy protection mechanisms; actively innovating regulatory approaches and deepening international cooperation to meet upcoming challenges; focusing on technology empowerment; and developing the system for protecting the interests and rights of financial customers under new business models. Wholesale CBDC and retail CBDC are two types of central bank

Table 5: List of challenges reported in the literature.

S. no	Challenges	Description	References
1.	Security	This study investigates the privacy, security, and policy challenges raised by this hybrid architecture to grasp the convergence and comprehend the integration of IoT and blockchain technologies.	[7, 18, 45, 59, 65, 82, 94, 111]
2.	Confidentiality	This study examines blockchain-based solutions for a variety of security services. Services include confidentiality, access control, privacy, authentication, integrity assurance, and data and source provenance.	[11]
3.	Access control	The paper analyzes the information security problem from data protection and access control to implementation with the emerging blockchain technology.	[43]
4.	Spam attacks	In this paper, a "spam attack" approach for parties with enough bitcoin holdings to delay a statistically significant share of transactions made to the Ethereum network.	[103]
5.	Scalability	The paper outlines the critical technological difficulties that must be addressed before it can reach its full potential, such as performance, cross-chain interoperability, and scalability.	[69]
6.	Integrating	The article discusses the real-time challenge of integrating blockchain in the diamond industry.	[112]
7.	Recommender systems	This article explains a comprehensive outline of blockchain-based recommender systems, including problems, unresolved concerns, and solutions.	[57]
8.	Applications	This paper delivers and describes the implementation of the blockchain in the business sectors to secure the business activity.	[45]
9.	Robotics	The study begins by delving into the major criteria and technological obstacles that robots face in general. Following that, it gives a full understanding of blockchain technology in an instructional format.	[9]
10.	Safety	The study covers the combination of blockchain technology with Internet of vehicles system and to provide an efficient and safe two-way authentication method.	[13, 101]
11.	Algorithms	The paper analyzes the consensus algorithms, which are critical components for blockchain decentralization. Researchers identify three major consensus algorithms, including PoP, Paxos, and PoAH, that are better suited for establishing consensus on such a massive scale blockchain-enabled Internet architecture.	[74, 113]
12.	Adoption	Researchers recognize and discuss significant research challenges impeding blockchain adoption in the healthcare industry.	[95]
13.	IoT system	The study discusses the many problems that an IoT system faces and summarizes the benefits of incorporating blockchain into IoT infrastructure. The study also explains the specially interest in demonstrating blockchain applications in IoT with better capabilities and security.	[102]
14.	Acceptance	The paper gives a more in-depth look at the key features of the blockchain, as well as the prospects for application in the management of big data in healthcare and the barriers to its acceptance in the healthcare perspective.	[96]
15.	Integration	This article attempts to map the requirements and features of both systems and point out the critical coexistence difficulties and technology options for more seamless combination of IoT and blockchain.	[4]
16.	Threats	The paper discusses the architecture, features, and security threats of space-air-ground- (SAP-) IoT systems and focus on the capable blockchain-based solutions for SAG-IoT security.	[68]
17.	Implementations	In the article, the core challenge is to implement issues such as public vs. private key access, distributed ledger size restrictions, speed, complexity, and security risks.	[13, 107]

digital currency. When compared to the wholesale CBDC, existing payment system offers benefits such as speedier delivery and some anonymity and provides cheaper transaction costs, which give help to improve cross-border payment efficiency [115].

First, there is blockchain 1.0 technology. It primarily reflects to programmable currency, which is extensively utilized in electronic currency, payment and settlement, and so on. Second, there is blockchain 2.0 technology. It is an abbreviation for programmable finance. It is typically utilized in financial transactions, such as financial derivatives, private equity, and stocks [69]. The application of blockchain technology in the process of accounts receivable processing, information integration, information supervision and convenience, credit transmission process, chattel pledge management, financial financing process, service platform operation, and other links drives the expansion trend of blockchain technology in supply chain finance [116].

Blockchain technology began as distributed ledgers for bitcoin and has now evolved into a financial technology (FinTech). For a while, it was overshadowed by the bitcoin craze, but in several years, it has begun to gather lot of attention and is quickly becoming a vital technology in the FinTech family. Many professionals and academic scholars have recognized that the effect of blockchain technology extends beyond the financial industry and even bitcoin to drive change in a wide range of sectors [117]. Currently, blockchain is a topic that is receiving a lot of interest in financial technology (FinTech). It incorporates several computer technologies like point-to-point transmission, distributed data storage, encryption methods, and consensus procedures [72]. With the advent and expansion of bitcoin and Ethereum over the last decade, an increasing number of firms, from FinTech to retail, have shown an interest in incorporating blockchain-based solutions into their application portfolios [75]. Trust may lead to successful enterprises via financial tools and tactics. A trustable platform is an essential component of the financial system used to determine whether or not a user can be trusted. FinTech (Financial Technology) is the combination of finance and technology. FinTech and blockchain are popular topics among financial technology executives today. The FinTech-assisted applications and blockchain technology-based data encryption have revolutionized the regulatory organizations with a full spectrum [118].

Decentralized financing assists in identifying the possible difficulties, current business models, and other security constraints. It is considered as a new era of financial technology that has the potential to transform and modernize the traditional financial structures by providing a new canvas for entrepreneurship and creativity. Blockchain technology enables decentralized financial services in the financial sector, which are more inventive, interoperable, decentralized, transparent, and borderless [73].

5. Conclusions

Blockchain is a new technology that deserves more research. It has exposed emerging capabilities in various domains, specifically in banking, financial, and other regulatory sectors. The paper assesses a systematic literature review, develops a classification of blockchain application domains, and identifies key contributions in risk solution by using the blockchain-based technology. The analysis shows that blockchain's unique and innovative qualities provide a significant potential for creating trust, lowering disputes and claims, enhancing communications, and precluding fraud in the financial industry. However, the advantages and qualities of blockchain for a specific application, on the other hand, are determined by technical decisions. The aim of this paper was to give a thorough examination of blockchain applications in our daily life. Our review of existing work assists us in identifying the benefits and limitations of using blockchain technology into different sectors especially in the financial and banking industry. Although this technology is still in its early phases of development and must undergo testing, it has the potential to more innovation in the future. Based on the findings of this systematic mapping, new research directions are suggested to ensure high privacy, transparency, and reliability in the blockchain-based systems.

Blockchain has changed the decision tactics of organizations. By using the capabilities of blockchain in various industries, the data can be secured and decentralized. The suggested framework can help researcher and implementers make technical design decisions in the creation of blockchain systems for a certain domain, such as privacy, decentralization, platform selection, blockchain type, and transparency. The study's key contribution is a complete review and classification of relevant research publications on blockchain and their integration into various trends and applications, as well as the identification of specific literary trends. The blockchain platform enables the creation of a decentralized application in which the pattern of data exchanges is not influenced by any third party. The data transactions of the entities are recorded in a decentralized database in a verifiable, secure, immutable, and transparent way, complete with time stamps and other necessary information. During the initial phases of development and design, many studies have suggested solutions that have the potential to boost operating efficiency and data transparency. However, the privacy scalability and security of blockchain-based technology will demand further research before large-scale commercial implementation. As a result, a review of current blockchain research in our field of financial services and banking is required to identify specific research gaps that must be addressed in future studies.

6. Implications

This paper has many implications in our daily life especially in the banking and financial sectors. By exploiting the capabilities of blockchain technology in different fields, the effectiveness of various activities will be boosted. Organizations can be protected with the help of blockchain and hybrid technologies and protocols. The blockchain technology implementation to different industry should be made a strong policy choice that guaranteed security, efficiency, and privacy.

Data Availability

The data used to support the findings of this study are included from peer-reviewed online repositories, and all the articles are mentioned with full references.

Disclosure

The results obtained herein are solely the obligation of the writers.

Conflicts of Interest

The authors declare that there is no conflict of interest regarding the publication of this paper.

Acknowledgments

The Qatar University Internal Grant No. QUHI-CBE-21/22-1 funded this publication.

References

[1] A. Čižmešija and N. Vrček, "Organizational challenges of blockchain adoption: an exploratory literature review," in *2021 IEEE Technology & Engineering Management Conference-Europe (TEMSCON-EUR)*, pp. 1–6, 2021.

[2] P. Garg, B. Gupta, A. K. Chauhan, U. Sivarajah, S. Gupta, and S. Modgil, "Measuring the perceived benefits of implementing blockchain technology in the banking sector," *Technological Forecasting and Social Change*, vol. 163, article 120407, 2021.

[3] J. Y. Jo, "Editorial note: empirical multimedia service and its applications for IoT," *Multimedia Tools and Applications*, vol. 76, no. 17, p. 17613, 2017.

[4] I. Romashkova, M. Komarov, and A. Ometov, "Demystifying blockchain technology for resource-constrained IoT devices: parameters, challenges and future perspective," *IEEE Access*, vol. 9, pp. 129264–129277, 2021.

[5] Y. Wu, L. Song, L. Liu, J. Li, X. Li, and L. Zhou, "Consensus mechanism of IoT based on blockchain technology," *Shock and Vibration*, vol. 2020, Article ID 8846429, 9 pages, 2020.

[6] H. Xiao, B. Muthu, and S. N. Kadry, "Artificial intelligence with robotics for advanced manufacturing industry using robot-assisted mixed-integer programming model," *Intelligent Service Robotics*, 2020.

[7] K. Pal, "Privacy, security and policies: a review of problems and solutions with blockchain-based Internet of Things applications in manufacturing industry," *Procedia Computer Science*, vol. 191, pp. 176–183, 2021.

[8] R. Manoj, S. Joshi, U. Dabholkar et al., "Blockchain ecosystem for credit transfer in education," *Mathematical Problems in Engineering*, vol. 2021, Article ID 8526456, 12 pages, 2021.

[9] U. S. Aditya, R. Singh, P. K. Singh, and A. Kalla, "A survey on blockchain in robotics: issues, opportunities, challenges and future directions," *Journal of Network and Computer Applications*, vol. 196, article 103245, 2021.

[10] C. Di Ciccio, A. Cecconi, M. Dumas et al., "Blockchain support for collaborative business processes," *Computer Science Spectrum*, vol. 42, no. 3, pp. 182–190, 2019.

[11] T. Salman, M. Zolanvari, A. Erbad, R. Jain, and M. Samaka, "Security services using blockchains: a state of the art survey," *IEEE Communications Surveys & Tutorials*, vol. 21, pp. 858–880, 2019.

[12] I. Nath, "Data exchange platform to fight insurance fraud on blockchain," in *2016 IEEE 16th International Conference on Data Mining Workshops (ICDMW)*, pp. 821–825, 2016.

[13] M. R. Islam, M. M. Rahman, M. Mahmud, M. A. Rahman, and M. H. S. Mohamad, "A review on blockchain security issues and challenges," in *2021 IEEE 12th Control and System Graduate Research Colloquium (ICSGRC)*, pp. 227–232, 2021.

[14] L. Feng, H. Zhang, W.-T. Tsai, and S. Sun, "System architecture for high-performance permissioned blockchains," *Frontiers of Computer Science*, vol. 13, no. 6, pp. 1151–1165, 2019.

[15] E. Daniel and F. Tschorsch, "Poster: towards verifiable mutability for blockchains," in *2021 IEEE European Symposium on Security and Privacy (Euro S&P)*, pp. 722–724, 2021.

[16] S. Nadarajah and J. Chu, "On the inefficiency of bitcoin," *Economics Letters*, vol. 150, pp. 6–9, 2017.

[17] C. Berger, B. Penzenstadler, and O. Drögehorn, "On using blockchains for safety-critical systems," in *Proceedings of the 4th International Workshop on Software Engineering for Smart Cyber-Physical Systems*, pp. 30–36, 2018.

[18] H. M. Hussien, S. M. Yasin, N. I. Udzir, M. I. H. Ninggal, and S. Salman, "Blockchain technology in the healthcare industry: trends and opportunities," *Journal of Industrial Information Integration*, vol. 22, article 100217, 2021.

[19] Y. Ren, X. Cai, and M. Hu, "Privacy-preserving redactable blockchain for Internet of Things," *Security and Communication Networks*, vol. 2021, Article ID 4485311, 12 pages, 2021.

[20] K. Zhang, Y. Li, and L. Lu, "Privacy-preserving attribute-based keyword search with traceability and revocation for cloud-assisted IoT," *security and communication Networks*, vol. 2021, Article ID 9929663, 13 pages, 2021.

[21] Z. Qiu and Y. Zhu, "A novel structure of blockchain applied in vaccine quality control: double- chain structured blockchain system for vaccine anticounterfeiting and traceability," *Journal of Healthcare Engineering*, vol. 2021, Article ID 6660102, 10 pages, 2021.

[22] Y. Zhang, W. Liu, Z. Xia et al., "Blockchain-based DNS root zone management decentralization for Internet of Things," *Wireless Communications and Mobile Computing*, vol. 2021, Article ID 6620236, 20 pages, 2021.

[23] R. Wang, M. Luo, Y. Wen, L. Wang, K.-K. Raymond Choo, and D. He, "The applications of blockchain in artificial intelligence," *Security and Communication Networks*, vol. 2021, Article ID 6126247, 16 pages, 2021.

[24] T. Wang, H. Hua, Z. Wei, and J. Cao, "Challenges of blockchain in new generation energy systems and future outlooks," *International Journal of Electrical Power & Energy Systems*, vol. 135, article 107499, 2022.

[25] E.-Y. Daraghmi, M. Abu Helou, and Y.-A. Daraghmi, "A blockchain-based editorial management system," *Security and Communication Networks*, vol. 2021, Article ID 9927640, 17 pages, 2021.

[26] G. Falazi, M. Hahn, U. Breitenbücher, and F. Leymann, "Modeling and execution of blockchain-aware business processes," *SICS Software-Intensive Cyber-Physical Systems*, vol. 34, no. 2-3, pp. 105–116, 2019.

[27] S. Yang, Z. Chen, L. Cui, M. Xu, Z. Ming, and K. Xu, "CoDAG: an efficient and compacted DAG-based blockchain protocol," in *2019 IEEE International Conference on Blockchain (Blockchain)*, pp. 314–318, 2019.

[28] S. Li, D. Gao, and X. Hui, "Corporate governance, agency costs, and corporate sustainable development: a mediating effect analysis," *Discrete Dynamics in Nature and Society*, vol. 2021, Article ID 5558175, 15 pages, 2021.

[29] M. Almulla and O. I. Juhmani, "Corporate governance mechanisms and firms' dividend payout policies: evidence from Bahrain," in *2020 International Conference on Decision Aid Sciences and Application (DASA)*, pp. 49–53, 2020.

[30] Z. Husain and O. I. Juhmani, "Corporate governance mechanisms and corporate debt: a study on non-financial firms listed in GCC stock exchanges," in *2020 Second International Sustainability and Resilience Conference: Technology and Innovation in Building Designs (51154)*, pp. 1–6, 2020.

[31] W. Kuang, H. Zhou, and Y. Zhang, "The linkage of real estate market and capital market," in *MSIE 2011*, pp. 508–511, 2011.

[32] M. Ishioka and K. Yasuda, "A study on market oriented product innovation strategies for technology product market," in *2009 16th International Conference on Industrial Engineering and Engineering Management*, pp. 959–963, 2009.

[33] H. Qiyuan, "Government Management Information System Based on J2EE," in *2015 International Conference on Intelligent Transportation, Big Data and Smart City*, pp. 442–445, 2015.

[34] G. Han, W. Chen, and D. Li, "Research on XBRL's improvement of quality of accounting information in the new accounting standards," in *2017 29th Chinese Control And Decision Conference (CCDC)*, pp. 5295–5298, 2017.

[35] Z. Wang, C. S. Chong, L. Lan, Y. Yang, S. B. Ho, and J. C. Tong, "Fine-grained sentiment analysis of social media with emotion sensing," in *2016 Future Technologies Conference (FTC)*, pp. 1361–1364, 2016.

[36] X. Wenwu and C. Biao, "Impacts of corporate governance on companies' behaviors: in view of corporate social responsibility," in *2009 Fourth International Conference on Computer Sciences and Convergence Information Technology*, pp. 598–601, 2009.

[37] Y. Wang, L. Shen, and J. Zhu, "A conceptual action model of reputation mechanism and corporate governance," in *2008 International Symposium on Intelligent Information Technology Application Workshops*, pp. 620–623, 2008.

[38] N. Tereshina and A. Sorokina, "Corporate governance quality assessment based on a balanced system of indicators," in *2017 Tenth International Conference Management of Large-Scale System Development (MLSD)*, pp. 1–4, 2017.

[39] T. Huang, "Resource sharing of smart city based on blockchain," *Wireless Communications and Mobile Computing*, vol. 2021, Article ID 5886024, 11 pages, 2021.

[40] F. Loukil, M. Abed, and K. Boukadi, *Blockchain Adoption in Education: A Systematic Literature Review*, vol. 26, no. 5, 2021Education and Information Technologies, 2021.

[41] J. B. Bernabe, J. L. Canovas, J. L. Hernandez-Ramos, R. T. Moreno, and A. Skarmeta, "Privacy-preserving solutions for blockchain: review and challenges," *IEEE Access*, vol. 7, pp. 164908–164940, 2019.

[42] B. Shah, N. Shah, S. Shakhla, and V. Sawant, "Remodeling the healthcare industry by employing blockchain technology," in *2018 international conference on circuits and systems in digital enterprise technology (ICCSDET)*, pp. 1–5, 2018.

[43] S. Liu, B. Tang, and Y. Zhang, "The key technology of blockchain and its research in the field of information security," in *2021 IEEE 4th Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC)*, pp. 673–677, 2021.

[44] E. Fynn and F. Pedone, "Challenges and pitfalls of partitioning blockchains," in *2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W)*, pp. 128–133, 2018.

[45] S. Gomathi, M. Soni, G. Dhiman, R. Govindaraj, and P. Kumar, "A survey on applications and security issues of blockchain technology in business sectors," in *Materials Today: Proceedings*, 2021.

[46] M. Comuzzi, C. Cappiello, and G. Meroni, "On the need for data quality assessment in blockchains," *IEEE Internet Computing*, vol. 25, no. 3, pp. 71–78, 2021.

[47] T. Li, Y. Chen, Y. Wang et al., "Rational protocols and attacks in blockchain system," *Security and Communication Networks*, vol. 2020, Article ID 8839047, 11 pages, 2020.

[48] X. Du, Y. Qi, B. Chen, B. Shan, and X. Liu, "The integration of blockchain technology and smart grid: framework and application," *Mathematical Problems in Engineering*, vol. 2021, Article ID 9956385, 12 pages, 2021.

[49] R. L. Kumar, F. Khan, S. Kadry, and S. Rho, "A survey on blockchain for industrial Internet of Things," *Alexandria Engineering Journal*, vol. 61, no. 8, pp. 6001–6022, 2022.

[50] Z. Alhadhrami, S. Alghfeli, M. Alghfeli, J. A. Abedlla, and K. Shuaib, "Introducing blockchains for healthcare," in *2017 international conference on electrical and computing technologies and applications (ICECTA)*, pp. 1–4, 2017.

[51] B. Kitchenham, "Procedures for performing systematic reviews," *Keele, UK, Keele University*, vol. 33, pp. 1–26, 2004.

[52] A. Hussain, S. Nazir, S. Khan, and A. Ullah, "Analysis of PMIPv6 extensions for identifying and assessing the efforts made for solving the issues in the PMIPv6 domain: a systematic review," *Computer Networks*, vol. 179, article 107366, 2020.

[53] K. Immonen, A. M. Tuomikoski, M. Kääriäinen et al., "Evidence-based healthcare competence of social and healthcare educators: a systematic review of mixed methods," *Nurse Education Today*, vol. 108, article 105190, 2022.

[54] S. Keele, *Guidelines for Performing Systematic Literature Reviews in Software Engineering*, Citeseer, 2007.

[55] B. Kitchenham, R. Pretorius, D. Budgen et al., "Systematic literature reviews in software engineering - a tertiary study," *Information and Software Technology*, vol. 52, no. 8, pp. 792–805, 2010.

[56] Y. Zhen, A. Khan, S. Nazir, Z. Huiqi, A. Alharbi, and S. Khan, "Crowdsourcing usage, task assignment methods, and crowdsourcing platforms: a systematic literature review," *Journal of Software: Evolution and Process*, vol. 33, no. 8, 2021.

[57] Y. Himeur, A. Sayed, A. Alsalemi et al., "Blockchain-based recommender systems: applications, challenges and future opportunities," *Computer Science Review*, vol. 43, article 100439, 2022.

[58] M. A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian, "A survey on the adoption of blockchain in IoT: challenges and solutions," *Blockchain: Research and Applications*, vol. 2, no. 2, article 100006, 2021.

[59] A. Zhang and X. Lin, "Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain," *Journal of Medical Systems*, vol. 42, no. 8, pp. 1–18, 2018.

[60] M. Zhou, Y. Huang, K. Li, Z. Li, and J. Wei, "Design of intelligent power material storage information management system based on blockchain technology," in *2020 13th International Conference on Intelligent Computation Technology and Automation (ICICTA)*, pp. 479–485, 2020.

[61] Y. Li, *Emerging Blockchain-Based Applications and Techniques*, vol. 13, Springer, 2019.

[62] T. K. Mackey, T.-T. Kuo, B. Gummadi et al., "Fit-for-purpose?—challenges and opportunities for applications of blockchain technology in the future of healthcare," in *Advances in Clinical Immunology, Medical Microbiology, COVID-19, and Big Data*, pp. 583–609, Jenny Stanford Publishing, 2022.

[63] H. T. Vo, Z. Wang, D. Karunamoorthy, J. Wagner, E. Abebe, and M. Mohania, "Internet of blockchains: techniques and challenges ahead," in *2018 IEEE international conference on internet of things (iThings) and IEEE green computing and communications (GreenCom) and IEEE cyber, physical and social computing (CPSCom) and IEEE smart data (SmartData)*, pp. 1574–1581, 2018.

[64] A. Hassan, M. Ali, R. Ahammed, M. M. Khan, N. Alsufyani, and A. Alsufyani, "Secured insurance framework using blockchain and smart contract," *Scientific Programming*, vol. 2021, Article ID 6787406, 11 pages, 2021.

[65] R. Duan and L. Guo, "Application of blockchain for Internet of Things: a bibliometric analysis," *Mathematical Problems in Engineering*, vol. 2021, Article ID 5547530, 16 pages, 2021.

[66] F. Golatowski, B. Butzin, T. Brockmann et al., "Challenges and research directions for blockchains in the Internet of Things," in *2019 IEEE International Conference on Industrial Cyber Physical Systems (ICPS)*, pp. 712–717, 2019.

[67] B. Li, T. Zhu, and W. Gong, "Study on intelligent response of emergency logistics under magnitude outburst public health events based on new generation information technology intelligent facilities and equipment," in *2021 International Conference on E-Commerce and E-Management (ICECEM)*, pp. 34–37, 2021.

[68] Y. Wang, Z. Su, J. Ni, N. Zhang, and X. Shen, "Blockchain-empowered space-air-ground integrated networks: opportunities, challenges, and solutions," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 1, pp. 160–209, 2022.

[69] H. Jin and J. Xiao, "Towards trustworthy blockchain systems in the era of "Internet of value": development, challenges, and future trends," *SCIENCE CHINA Information Sciences*, vol. 65, no. 5, pp. 1–11, 2022.

[70] T. K. Agrawal, V. Kumar, R. Pal, L. Wang, and Y. Chen, "Blockchain-based framework for supply chain traceability: a case example of textile and clothing industry," *Computers & Industrial Engineering*, vol. 154, article 107130, 2021.

[71] M. Meyliana, E. Fernando, H. A. E. Widjaja, C. Cassandra, and A. Tan, "bibliometric study and systematic literature review of blockchain technology in vehicle industry," in *2021 International Conference on Information Management and Technology (ICIMTech)*, pp. 171–176, 2021.

[72] Y. Guo and C. Liang, "Blockchain application and outlook in the banking industry," *Financial Innovation*, vol. 2, no. 1, pp. 1–12, 2016.

[73] Y. Chen and C. Bellavitis, "Blockchain disruption and decentralized finance: the rise of decentralized business models," *Journal of Business Venturing Insights*, vol. 13, article e00151, 2020.

[74] J. Zarrin, H. W. Phang, L. B. Saheer, and B. Zarrin, "Blockchain for decentralization of Internet: prospects, trends, and challenges," *Cluster Computing*, vol. 24, no. 4, pp. 2841–2866, 2021.

[75] M. Mazzoni, A. Corradi, and V. Di Nicola, "Performance evaluation of permissioned blockchains for financial applications: the ConsenSys Quorum case study," *Blockchain: Research and Applications*, vol. 3, article 100026, 2021.

[76] K. Zheng, Z. Zhang, and J. Gauthier, "RETRACTED ARTICLE: Blockchain-based intelligent contract for factoring business in supply chains," *Annals of Operations Research*, vol. 308, no. 1-2, pp. 777–797, 2022.

[77] T. Alam, "Blockchain cities: the futuristic cities driven by blockchain, big data and Internet of Things," *GeoJournal*, 2021.

[78] J. P. de Brito Gonçalves, H. C. de Resende, R. da Silva Villaca, E. Municio, C. B. Both, and J. M. Marquez-Barja, "Distributed network slicing management using blockchains in E-health environments," *Mobile Networks and Applications*, vol. 26, no. 5, pp. 2111–2122, 2021.

[79] D. Ding, K. Li, L. Jia, Z. Li, J. Li, and Y. Sun, "Privacy protection for blockchains with account and multi-asset model," *China Communications*, vol. 16, no. 6, pp. 69–79, 2019.

[80] C. Worley and A. Skjellum, "Blockchain tradeoffs and challenges for current and emerging applications: generalization, fragmentation, sidechains, and scalability," in *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, pp. 1582–1587, 2018.

[81] C. Cai, Y. Zheng, Y. Du, Z. Qin, and C. Wang, "Towards private, robust, and verifiable crowdsensing systems via public blockchains," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 4, pp. 1893–1907, 2019.

[82] W. Melo, L. F. Carmo, A. Bessani, N. Neves, and A. Santin, "How blockchains can improve measuring instruments regulation and control," in *2018 IEEE International Instrumentation and Measurement Technology Conference (I2MTC)*, pp. 1–6, 2018.

[83] A. Tezel, E. Papadonikolaki, I. Yitmen, and P. Hilletofth, "Preparing construction supply chains for blockchain technology: an investigation of its potential and future directions," *Frontiers of Engineering Management*, vol. 7, no. 4, pp. 547–563, 2020.

[84] E. V. Odisho and D. Truong, "Applying machine learning to enhance runway safety through runway excursion risk mitigation," in *2021 Integrated Communications Navigation and Surveillance Conference (ICNS)*, pp. 1–10, 2021.

[85] B. Xu, F. Yang, D. Zhang, L. Tang, and T. Xia, "Security sharing model of power material logistics information based on blockchain technology," in *2020 13th International Conference on Intelligent Computation Technology and Automation (ICICTA)*, pp. 539–544, 2020.

[86] F. Caddeo and A. Pinna, "Opportunities and challenges of blockchain-oriented systems in the tourism industry," in *2021 IEEE/ACM 4th International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB)*, pp. 9–16, 2021.

[87] E. Fernando and C. Cassandra, "Medicine information record based on blockchain technology," in *2021 2nd International Conference on Innovative and Creative Information Technology (ICITech)*, pp. 169–173, 2021.

[88] E. Fernando, "The business process of good manufacturing practice based on blockchain technology in the pharmaceutical ndustry," in *2021 Fifth International Conference on Information Retrieval and Knowledge Management (CAMP)*, pp. 91–95, 2021.

[89] A. Demichev, A. Kryukov, and N. Prikhod'ko, "Business process engineering for data storing and processing in a collaborative distributed environment based on provenance metadata, smart contracts and blockchain technology," *Journal of Grid Computing*, vol. 19, no. 1, pp. 1–30, 2021.

[90] R. Sonmez, F. Ö. Sönmez, and S. Ahmadisheykhsarmast, "Blockchain in project management: a systematic review of use cases and a design decision framework," *Journal of Ambient Intelligence and Humanized Computing*, 2021.

[91] T. Caradonna, "Blockchain and society," *Computer Science Spectrum*, vol. 43, no. 1, pp. 40–52, 2020.

[92] J. Zhao and Z. Ge, "Analysis of influencing factors of academic entrepreneurship based on blockchain," *Wireless Communications and Mobile Computing*, vol. 2020, Article ID 8825318, 9 pages, 2020.

[93] R. W. Ahmad, K. Salah, R. Jayaraman, H. R. Hasan, I. Yaqoob, and M. Omar, "The role of blockchain technology in aviation industry," *IEEE Aerospace and Electronic Systems Magazine*, vol. 36, no. 3, pp. 4–15, 2021.

[94] X. Liu, H. Yang, G. Li, H. Dong, and Z. Wang, "A blockchain-based auto insurance data sharing scheme," *Wireless Communications and Mobile Computing*, vol. 2021, Article ID 3707906, 11 pages, 2021.

[95] I. Yaqoob, K. Salah, R. Jayaraman, and Y. Al-Hammadi, "Blockchain for healthcare data management: opportunities, challenges, and future recommendations," *Neural Computing and Applications*, pp. 1–16, 2022.

[96] M. A. Bazel, F. Mohammed, and M. Ahmed, "Blockchain technology in healthcare big data management: benefits, applications and challenges," in *2021 1st International Conference on Emerging Smart Technologies and Applications (eSmarTA)*, pp. 1–8, 2021.

[97] A. A. Sathio, M. A. Dootio, A. Lakhan, M. u. Rehman, A. O. Pnhwar, and M. A. Sahito, "Pervasive futuristic healthcare and blockchain enabled digital identities-challenges and future intensions," in *2021 International Conference on Computing, Electronics & Communications Engineering (iCCECE)*, pp. 30–35, 2021.

[98] H. L. H. S. Warnars and E. Abdurachman, "Blockchain technology open problems and impact to supply chain management in automotive component industry," in *2020 6th International Conference on Computing Engineering and Design (ICCED)*, pp. 1–4, 2020.

[99] D. Sathya, S. Nithyaroopa, D. Jagadeesan, and I. J. Jacob, "Block-chain technology for food supply chains," in *2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV)*, pp. 212–219, 2021.

[100] E. Fernando, H. A. E. Widjaja, C. Cassandra, A. Tan, M. Carolina, and M. Carolina, "Blockchain technology for vehicle maintenance registration," in *2021 International Conference on Information Management and Technology (ICIMTech)*, pp. 608–613, 2021.

[101] T. Su, S. Shao, S. Guo, and M. Lei, "Blockchain-based Internet of vehicles privacy protection system," *Wireless Communications and Mobile Computing*, vol. 2020, Article ID 8870438, 10 pages, 2020.

[102] P. Cui, U. Guin, A. Skjellum, and D. Umphress, "Blockchain in IoT: current trends, challenges, and future roadmap," *Journal of Hardware and Systems Security*, vol. 3, no. 4, pp. 338–364, 2019.

[103] S. Paavolainen, T. Elo, and P. Nikander, "Risks from spam attacks on blockchains for intemet-of-things devices," in *2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, pp. 314–320, 2018.

[104] S. Chen, W. Ding, Z. Xiang, and Y. Liu, "Distributed power trading system based on blockchain technology," *Complexity*, vol. 2021, Article ID 5538195, 12 pages, 2021.

[105] F. Elghaish, S. Abrishami, and M. R. Hosseini, "Integrated project delivery with blockchain: an automated financial system," *Automation in Construction*, vol. 114, article 103182, 2020.

[106] S. Motepalli and H.-A. Jacobsen, "Reward mechanism for blockchains using evolutionary game theory," 2021, http://arxiv.org/abs/2104.05849.

[107] M. P. McBee and C. Wilcox, "Blockchain technology: principles and applications in medical imaging," *Journal of Digital Imaging*, vol. 33, no. 3, pp. 726–734, 2020.

[108] T. Hewa, M. Ylianttila, and M. Liyanage, "Survey on blockchain based smart contracts: applications, opportunities and challenges," *Journal of Network and Computer Applications*, vol. 177, article 102857, 2021.

[109] P. C. Bhatt, V. Kumar, and T.-C. Lu, "Identifying technology trends for blockchain applications in industry 4.0 domain: a patent perspective," in *2021 IEEE International Conference on Social Sciences and Intelligent Management (SSIM)*, pp. 1–5, 2021.

[110] M. N. Halgamuge and D. Guruge, "Fair rewarding mechanism in music industry using smart contracts on public-permissionless blockchain," *Multimedia Tools and Applications*, vol. 81, no. 2, pp. 1523–1544, 2022.

[111] W. S. Melo, A. Bessani, N. Neves, A. O. Santin, and L. F. R. C. Carmo, "Using blockchains to implement distributed measuring systems," *IEEE Transactions on Instrumentation and Measurement*, vol. 68, no. 5, pp. 1503–1514, 2019.

[112] U. Thakker, R. Patel, S. Tanwar, N. Kumar, and H. Song, "Blockchain for diamond industry: opportunities and challenges," *IEEE Internet of Things Journal*, vol. 8, no. 11, pp. 8747–8773, 2020.

[113] F. Shu, S. Chen, F. Li, J. Zhang, and J. Chen, "Research and implementation of network attack and defense countermeasure technology based on artificial intelligence technology," in *2020 IEEE 5th Information Technology and Mechatronics Engineering Conference (ITOEC)*, pp. 475–478, 2020.

[114] R. Kashyap and V. Saurav, "Blockchain technology: road to transform the Indian banking sector," in *Materials Today: Proceedings*, 2021.

[115] X. Zhang, "Opportunities, challenges and promotion countermeasures of central bank digital currency," in *2020 Management Science Informatization and Economic Innovation Development Conference (MSIEID)*, pp. 343–346, 2020.

[116] C. Jiang and C. Ru, "Application of blockchain technology in supply chain finance," in *2020 5th international conference on mechanical, Control and Computer Engineering (ICMCCE)*, pp. 1342–1345, 2020.

[117] O. Ali, M. Ally, and Y. Dwivedi, "The state of play of blockchain technology in the financial services sector: a systematic literature review," *International Journal of Information Management*, vol. 54, article 102199, 2020.

[118] V. Chang, P. Baudier, H. Zhang, Q. Xu, J. Zhang, and M. Arami, "How blockchain can impact financial services - the overview, challenges and recommendations from expert interviewees," *Technological Forecasting and Social Change*, vol. 158, article 120166, 2020.

Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 5108331, 21 pages
https://doi.org/10.1155/2022/5108331

Research Article

A Novel Machine Learning Technique for Selecting Suitable Image Encryption Algorithms for IoT Applications

Arslan Shafique,[1] **Abid Mehmood**,[2] **Moatsum Alawida**,[2] **Abdul Nasir Khan**,[3] **and Atta Ur Rehman Khan**[4]

[1]*Riphah International University, Islamabad, Pakistan*
[2]*Department of Computer Sciences, Abu Dhabi University, UAE*
[3]*COMSATS University Islamabad, Abbottabad Campus, Pakistan*
[4]*College of Engineering and Information Technology, Ajman University, UAE*

Correspondence should be addressed to Abdul Nasir Khan; anasir@cuiatd.edu.pk

Received 7 March 2022; Revised 16 May 2022; Accepted 14 June 2022; Published 5 July 2022

Academic Editor: Muhammad Imran

The Internet of Things connects billions of intelligent devices that can interact with one another without human intervention, and during communication, a large amount of data is exchanged between the devices. As a result, it is critical to secure digital data using an encryption technique that provides a suitable degree of security. Numerous existing encryption techniques do not offer sufficient security. Therefore, it is critical to figure out which encryption technique is most appropriate for a particular kind of data. When it comes to manually deciding which encryption technique to use, the process might take a long time. In this research, we present a novel technique for selecting Encryption Algorithms (EAs) based on a particular application using pattern recognition and machine learning techniques. To accomplish this goal, we also prepare a dataset. Several machine learning techniques, such as Support Vector Machines (SVMs), Linear Regression (LR), *K*-Nearest Neighbour (KNN), Naïve Bayes (NB), Decision Trees (DT), and Random Forests (RF), are evaluated. Based on the evaluation, the SVM has been chosen as the best option for the intended technique because its classification accuracy is 98.7%. The experimental results, including accuracy, precision, recall, and F1-score, are used to gauge the performance of the suggested technique. The proposed technique is also compared with the existing techniques to demonstrate its effectiveness.

1. Introduction

Nowadays, the Internet of Things IoTs is extensively used in a variety of industries and applications, including manufacturing, agriculture, e-health, home automation, and smart cities. According to Erickson, by 2022, the world will have around 28 billion linked smart devices. Additionally, about 15 billion devices make use of Machine-to-Machine (M2M) connectivity [1]. Additionally, according to a Cisco research, the internet will be connected to about 500 billion devices by 2030 [2]. In this way, it is easy to see why the IoT has attracted the interest of developers, and researchers have given the revolutionary changes it has brought to human existence. The IoT facilitates the sharing of multimedia data across a broad number of applications, including smart transportation, smart health, smart buildings, and industry [3]. As billions of network devices interact and share potentially sensitive data, the most essential concern in the IoT is data security and privacy [4–6]. Figure 1 shows the data transmission between the several linked devices.

Different types of Encryption Algorithms (EAs) are developed over the past few decades to secure digital images during transmission between multiple connected devices for IoT applications. One advantage of EAs is their efficiency in terms of computation time. However, insufficient

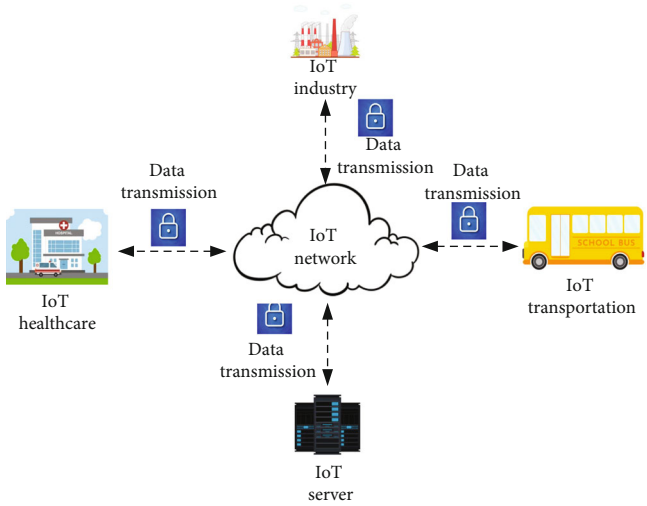


Figure 1: Data transmission between several connected devices.

encryption, as evidenced by patterns visible even after encryption, indicates a flaw in the EA [7, 8]. For proper concealment and a sufficient level of encryption of textual data, conventional Data Encryption Standard (DES) and Advanced Encryption Standard (AES) are well-known techniques [9, 10]. There are multiple rounds of encryption involved, making these classic image encryption techniques unsuitable for real-time applications. In the case of image encryption, traditional EAs are not suitable for real-time applications because they contain several encryption rounds. To overcome such issues, several cryptosystems have been proposed in recent years [11–13]. To break the correlation between the image pixels, permutation and substitution are the most widely used techniques to secure digital images [14, 15]. In [16], Shannon proposed a theory that any EA that contains confusion (referring to permutation) and diffusion (referring to substitution or any other process that can change the pixel value) may be considered a strong cryptosystem.

Generally, two things must be offered by the EA: (a) strong security (b) and computational efficiency. There will always be a trade-off between security and complexity in terms of time. At times, a strong security algorithm may take longer to execute due to the number of mathematical operations it contains [17]. Time-efficient encryption techniques are always required for real-time applications. Various forms of pixel transformations may be employed in image encryption, including permutation, substitution, the Discrete Wavelet Transform (DWT) [18], the Discrete Cosine Transform (DCT) [19], and the Discrete Fourier Transform (DFT) [20]. All of these approaches have been extensively utilised over the last several decades and proposed a variety of algorithms, some of which are resistant to various types of security attacks, including ciphertext-only attacks, brute force attacks, and plaintext-only attacks. A cryptosystem that is vulnerable to security attacks may have two fundamental problems: (a) it is unable to adequately encrypt the plaintext image due to the identical patterns included within it. Similar patterns also correlate to a high degree of correlation between image pixels; (b) it is computationally inefficient, making it unsuitable for low-profile applications such as data transmission from a drone to a base station, which needs high-speed encryption. On the other side, to propose a time-efficient technique, one may reduce the mathematical operations used in encryption schemes, compromising security and allowing the original image's patterns to be visible in the encrypted image. The plaintext images with the smooth patterns are shown in Figures 2(a)–2(h). This indicates that there is a significant degree of correlation between the pixels, whereas Figures 2(i)–2(p) depict the corresponding ciphertext images that have been encrypted using various existing encryption schemes [21–24].

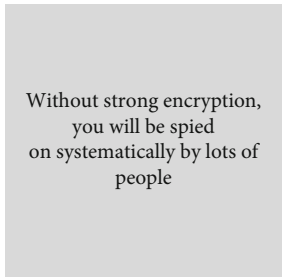
The patterns in Figures 2(i)–2(l) may be visualized, indicating that such images are encrypted using weak encryption techniques. While Figures 2(m)–2(p) are encrypted using secure encryption techniques, the plaintext image's patterns have been properly encrypted and are not visible, and the processing time required to encrypt the plaintext image is quite high.

For instance, if the image pixels have a low correlation, it is unnecessary to employ the majority of the resources available to encrypt the data included in the image. Generally, an encryption technique that employs a large number of mathematical operations is considered inefficient but extremely secure [28, 30]. Similarly, reducing the number of mathematical operations in an EA makes it more time-efficient, but it may compromise its security level [31]. In the proposed technique, EAs are categorized on the basis of computational complexity. For instance, EAs with processing times of [0.001, 1.00], [1.001, 2.000], and [2.001, ∞] are referred to as low-processing-time encryption (ELPT), moderate-processing-time encryption (EMPT), and high-processing-time encryption (EHPT), respectively.

Several metrics such as entropy, correlation, contrast, and energy [32] are evaluated in the suggested study to assess the patterns in the image, whether they are smooth or rough. After evaluating the patterns in the image, the appropriate encryption technique for that specific data may be chosen. The security parameter values may also be determined manually, but it may take a lot of time. As a result, a machine learning-based method is designed to examine the patterns in the plaintext image and suggest a suitable encryption technique, whether the image should be encrypted using a strong EA or concealed using a faster EA. The suggested approach is applicable to images in both colour and grayscale. When a colour image is used, it must be decomposed into three grayscale components, such as red, green, and blue.

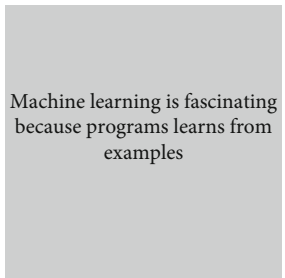
1.1. Contributions. The major contributions of this work are as follows:

(i) A machine learning model is proposed for pattern recognition-based selection of an appropriate encryption technique

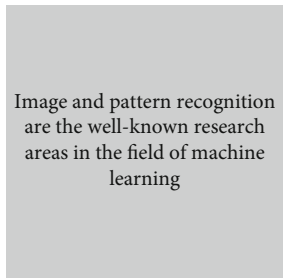


(a) Plaintext image

(b) Plaintext image

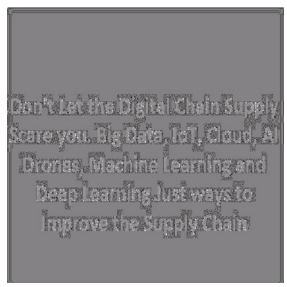


(c) Plaintext image

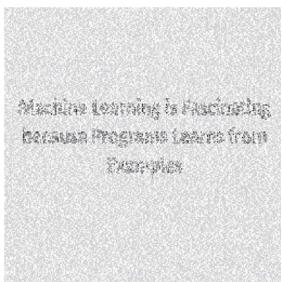


(d) Plaintext image

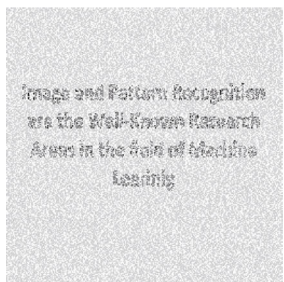
(e) Encryption using the scheme proposed in [21]



(f) Encryption using the scheme proposed in [25]



(g) Encryption using the scheme proposed in [26]



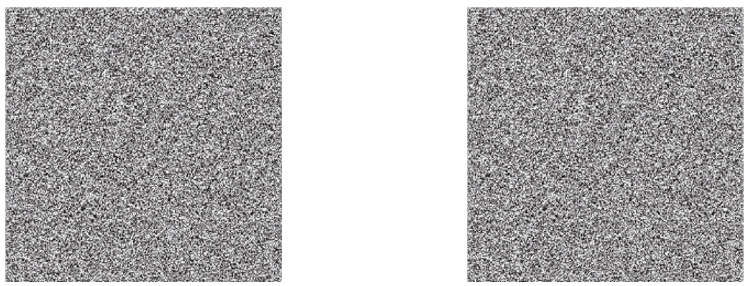
(h) Encryption using the scheme proposed in [27]

(i) Plaintext image

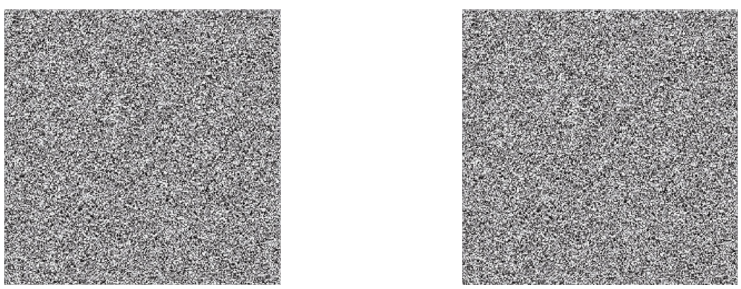
(j) Plaintext image

Figure 2: Continued.

(k) Plaintext image (l) Plaintext image



(m) Encryption using the scheme proposed in [23] (n) Encryption using the scheme proposed in [24]



(o) Encryption using the scheme proposed in [28] (p) Encryption using the scheme proposed in [29]

Figure 2: Plaintext images and their corresponding ciphertext images encrypted with the existing schemes [21, 23–29].

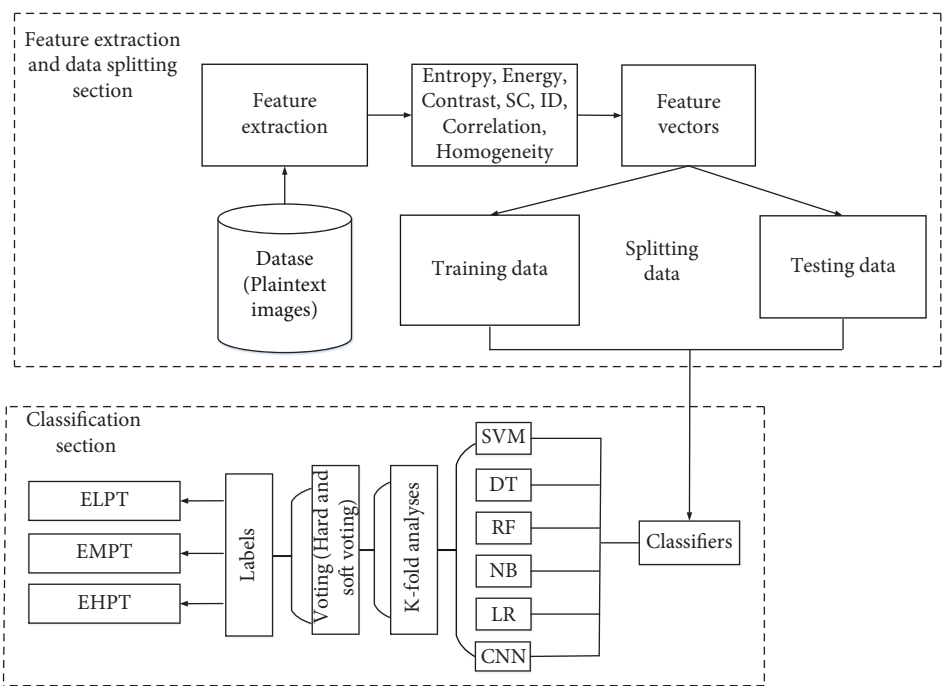


Figure 3: Proposed model for the selection of the suitable EA.

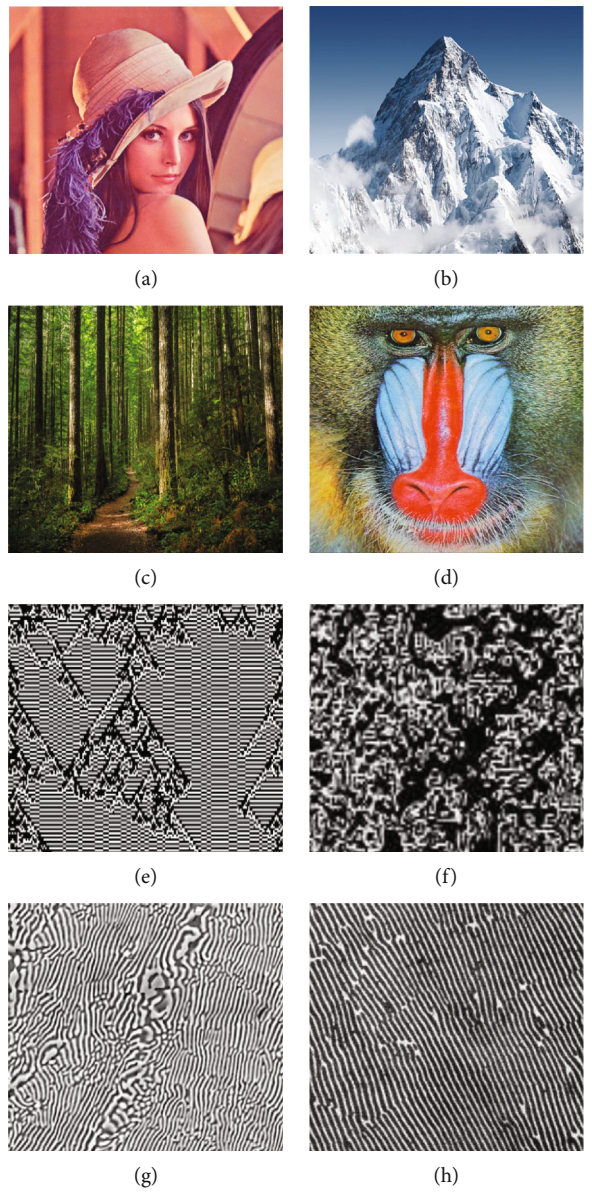


Figure 4: Information in the plaintext images (a–d) is more than the information in the plaintext images (e–h).

Table 1: Values of security parameters corresponding to Figures 4(a)–4(h).

Images	Entropy	Energy	Correlation	I_D	$(\text{Hist})^2$	Contrast	Homogeneity
Figure 4(a)	7.2416	0.7986	0.6798	250365	299.6898	8.9896	0.3367
Figure 4(b)	7.7998	0.6798	0.5710	256970	298.6410	8.6696	0.4697
Figure 4(c)	7.1720	0.6798	0.3367	256971	299.6401	8.9764	0.6798
Figure 4(d)	7.6477	0.5678	0.3665	256300	300.9963	8.6879	0.5556
Figure 4(e)	7.8099	0.0698	0.0167	240120	294.6544	9.8778	0.1352
Figure 4(f)	7.7007	0.0522	0.0331	231687	294.3330	9.9865	0.1001
Figure 4(g)	7.7556	0.0698	0.0130	246120	294.6660	9.7789	0.1336
Figure 4(h)	7.5996	0.0699	0.1978	246987	293.0299	9.7868	0.0157

(ii) The security parameters are used to identify the patterns in the plaintext image and set the appropriate intervals for each security parameter to achieve the desired task

(iii) Various machine learning algorithms are evaluated on the proposed work to find the best one

(iv) To improve the overall accuracy of the proposed model, K-fold analysis is performed to develop several models for the proposed work. The developed models are called K-models

(v) Voting mechanisms such as hard and soft voting are used to choose the final model from the several K-models

(vi) To gauge the performance of the proposed work, several tests and analyses such as accuracy, precision, F1-score, and recall are incorporated

The rest of the paper is as follows: Section 2 is dedicated to a review of the available schemes in the spatial and frequency domains. Section 3 contains preliminaries to the proposed research, including an explanation of SVM and DT. Section 4 discusses the proposed model for selecting an appropriate EA. Section 5 contains an assessment and comparison of the proposed work to previously published work. Finally, Section 6 finishes the proposed work.

2. Related Work

For secure communication, data encryption is necessary before transmission. To overcome the security issues, data can be encrypted either in the spatial domain or in the frequency domain. In the spatial domain, one can directly manipulate the pixel values. While in frequency domain encryption, first, pixels convert into their frequency domain and then further process. For instance, if a DWT is applied to the image pixels, it will convert into four different frequency subbands. Once the pixels are converted into their frequency subbands, the mathematical operations can be applied to them for further encryption. EAs can be used according to the applications and patterns existing in the plaintext image. The patterns having high correlation always required strong security EAs, whereas, in drone applications, a fast encryption speed is also required with strong security. Therefore, it is necessary to observe and analyze the patterns present in the image to select the right EA. There are several EAs that have been proposed in the last few decades which are based on either spatial domain or frequency domain.

2.1. Image Encryption in Spatial Domain. Spatial domain encryption has advanced significantly since incorporating chaos theory to secure digital images [18]. In the past few decades, chaos has been widely used in image encryption due to its several tremendous properties, such as sensitivity to initial conditions, nonperiodicity, and ability to generate pseudorandom numbers.

In [21], Anees et al. proposed an image encryption scheme comprised of two major components. One is a chaotic map, and the second is multiple substitution boxes (S-boxes). Both the components are used to break the high correlation between the image pixels. Moreover, several drawbacks of using a single S-box are addressed. To overcome the vulnerabilities that exist in using a single S-box, multiple S-boxes are used. The S-boxes are selected based on the random sequence generated using the chaotic logistic map. Using statistical analysis, it is proved that the multiple S-box scheme can perform better than the single S-box encryption scheme. However, the patterns of the plaintext image can be visualized. In [33], Ahmad and Hwang made a few improvements to the scheme proposed in [21] by adding noise in the plaintext image prior to the conversion of the noisy image into blocks. To manipulate each block of pixels, a Xor operation is performed that gives the final encrypted image.

In the encryption schemes, nonlinear components such as S-boxes also play a vital role in securing digital images. Therefore, it is crucial to use an S-box that exhibits strong cryptographic properties. In [34], Shafique et al. proposed a new methodology to construct an S-box based on a cubic logistic map, which has been given the name C-logo S-box. The purpose of proposing the S-box is to strengthen the overall EA so that the pixels of the plaintext image can be properly concealed. Several tests and analyses, such as Strict Avalanche Criterion (SAC), Bit Independent Criterion (BIC), and nonlinearity, are carried out to show the strength of the proposed S-box. A comparison reveals that the C-logo S-box performs significantly better than the other S-boxes that are present in the literature [35, 36].

In [37], Li and Yang introduced an image encryption technique based on chaos and discrete Fractional Wavelet Transforms (FWT). Confusion and diffusion operations are implemented independently, which results in a slight increase in the processing time required for encryption. Additionally, numerous cryptographic components, such as

Table 2: Defined intervals for entropy.

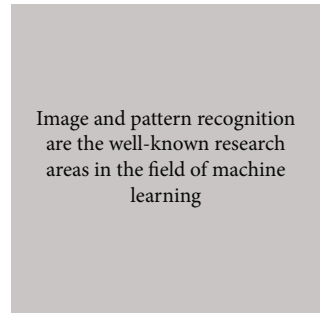
[07.999 07.900] ⟶ encryption with less processing time (ELPT)
[07.293 06.449] ⟶ encryption with moderate processing time (EMPT)
[06.423 06.001] ⟶ encryption with high processing time (EHPT)

Table 3: Defined intervals for contrast.

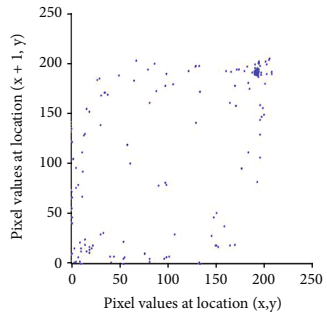
[10.5000 9.5000] ⟶ (ELPT)
[09.2500 8.7500] ⟶ (EMPT)
[08.5000 7.5000] ⟶ (EHPT)

Table 4: Defined intervals for energy.

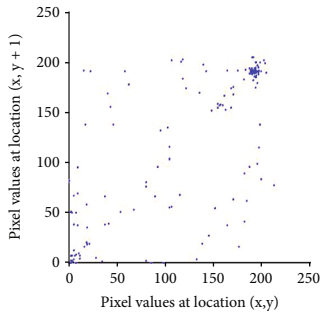
[0.01005 0.01505] ⟶ ELPT
[0.01510 0.02010] ⟶ EMPT
[0.02015 0.03495] ⟶ EHPT



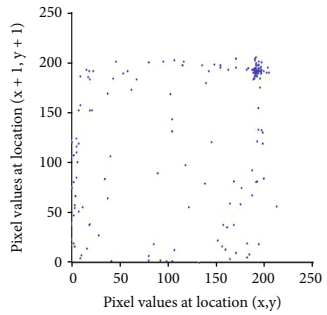
(a) Plain image with high correlation



(b) Horizontal correlation

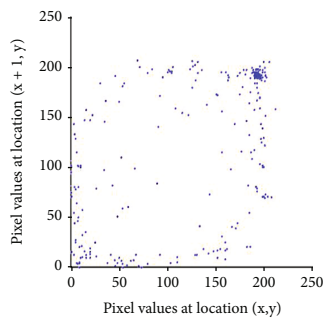


(c) Vertical correlation

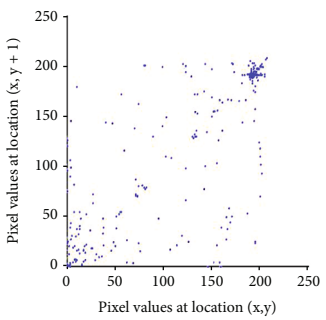


(d) Diagonal correlation

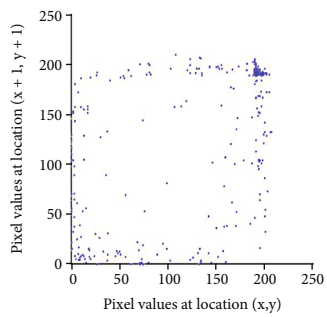
(e) Plain image with high correlation



(f) Horizontal correlation



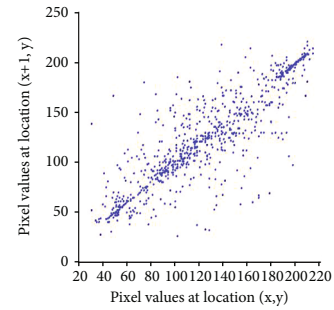
(g) Vertical correlation



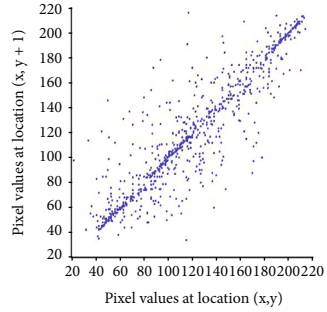
(h) Diagonal correlation

Figure 5: Continued.

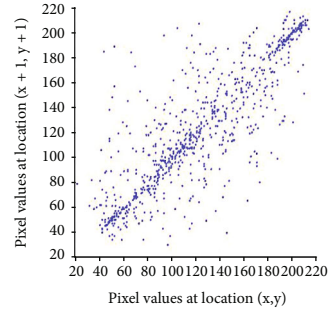
(i) Plain image with comparatively low correlation



(j) Horizontal correlation

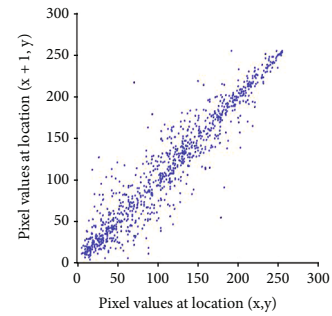


(k) Vertical correlation

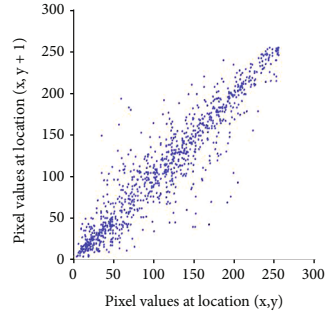


(l) Diagonal correlation

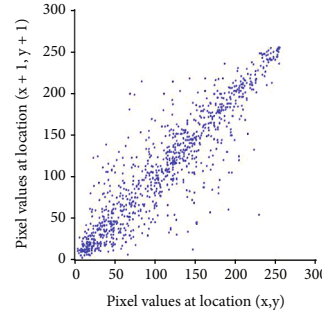
(m) Plain image with comparatively low correlation



(n) Horizontal correlation



(o) Vertical correlation



(p) Diagonal correlation

Figure 5: Plaintext images and their corresponding scattered diagrams to show the correlation between the image pixel in horizontal, vertical, and diagonal directions.

Table 5: Defined intervals for correlation.

$[-0.0012\ 0.0308] \longrightarrow$ ELPT
$[0.0001\ 0.0011] \longrightarrow$ EMPT
$[0.0000\ 0.4500] \longrightarrow$ EHPT

FWT, chaos, and quantum theory, are employed to increase the security of digital images. While using many encryption components sequentially may result in higher security, the processing time required for encryption may increase. Lin et al. [38] proposed a novel method for secure communication based on chaos theory in which mathematical operations to convert the plaintext picture to the ciphertext image are performed sequentially rather than concurrently.

Liu et al. [39] proposed a four-dimensional chaotic map-based encryption system with two encryption rounds and one hashing round. Multiple round encryption techniques often perform much better in terms of security but are not suited for real-time applications due to their increased computing time requirements. The encryption presented in [40] encountered computational complexity concerns because of the method's one-by-one encryption of the HSV components of colour images. Time complexity may be reduced by encrypting the HSV components in parallel. To make the chaos-based encryption scheme more robust, Lidong et al. [41] and Lu et al. [26] used S-box in their proposed cryptosystems. In [41], image compression is also incorporated, followed by encryption to reduce the encryption computational time. Moreover, the scrambling process is applied to the compressed image to break the correlation between the image pixels. To satisfy the criteria of confusion-diffusion proposed by Shannon [16], S-box is applied to create the diffusion in the scrambled image. A single S-box is not enough to secure the image against the deferential attack, specifically, when the image contains smooth patterns. In [26], a new chaotic map called the Logistic-sine System (LSS) is proposed, which has a wider chaotic range. The LSS is then used with the S-box in the proposed encryption scheme, which makes it comparatively more robust than the scheme proposed in [41].

2.2. Image Encryption in Frequency Domain. Apart from spatial domain encryption, frequency domain cryptosystems are also frequently used to secure the images from adversaries. Both of these types of encryption are useful to disturb the patterns of the pixels present in the image. Without a specific pattern in the image, it is difficult to read the information. Therefore, it is necessary to disturb the pixel patterns so that no one can read the information present in the image.

In [42], Rehman et al. proposed a cryptosystem in which both spatial and frequency domain sections are included. For spatial domain encryption, multiple chaotic maps used are known as chaotic logistic amp and chaotic sine map. These chaotic maps are used to generate random sequences for permutation purposes. Moreover, a chaotic sine map is also used to generate random images for diffusion purposes which are achieved using XOR operation performed on the precipher image with the random image. It is not always required to use a forward operation of any frequency transform such as DWT; one can also use its reverse operation Inverse Discrete Wavelet Transform (IDWT) to secure the digital images [43]. In [18], Shafique et al. proposed a DWT-based cryptosystem in which chaos and bit-plane extraction are the major parts. The whole scheme is consisting of three sections; the first and last sections are dependent on the spatial domain encryption while the middle section is devoted to the frequency domain section. The proposed is designed specially for those images that consist of a large number of the same patterns. As a lot of mathematical operations are included in the proposed scheme, it is somehow slower than the other existing schemes [13, 44–46]. Therefore, the scheme proposed in [18] is not suitable for real-time applications. The image encryption schemes presented in this section are based on chaos theory, bit-plane extraction, frequency transformation, and spatial domain transformation. Some of them can be used for specific purposes. For instance, the scheme proposed in [47] is useful to encrypt the image properly that can resist several security attacks, but it is not suitable for low-profile or real-time applications. Therefore, using the encryption scheme proposed in [47] is not the right choice when anyone wants to encrypt the image faster. Here, it can be noted that the orthodox selection of EA is very important for the particular kind of data. Therefore, a machine learning-based model is proposed to learn the image pattern for the selection of suitable EA.

Table 6: Defined intervals for homogeneity.

[0.4122 0.4418] ⟶ ELPT
[0.4521 0.4821] ⟶ EMPT
[0.5367 0.6125] ⟶ HLPT

3. Preliminaries

In the proposed work, several machine learning algorithms such as Decision Tree (DT), Support Vector Machine (SVM), Random Forest, *K*-Nearest Neighbour, and Logistic Regression (LR) are evaluated in which SVM and DT exhibit approximately comparable accuracy and precision. As a result, the preliminary section includes a discussion of SVM and DT. Moreover, among DT and SVM, the final selected ML algorithm is SVM as its accuracy is better than DT and other comparable ML algorithms.

3.1. Support Vector Machine. SVM implementation requires training on training data, since it is a supervised learning algorithm that takes training data as an input and predicts the label of the output based on training [48]. The training and testing datasets may or may not vary in size. The whole dataset's dimension is determined by the number of features employed. For instance, if the dataset has fourteen features, it will be fourteen-dimensional [49]. The general form of the dimension of the dataset is given below:

$$Y = X_1, X_2, X_3, \cdots, \mathrm{X}_n, \tag{1}$$

where Y is the dependent output label and X_i represents the number of independent features. The number of features may vary depending upon the output. A line that is a support vector is necessary to separate the data with maximum margins in the two-dimensional dataset. In the case of a higher-dimensional dataset, on the other hand, a plane is utilised to divide the data points rather than a line.

The proposed work makes use of an eight-dimensional dataset. As a result, it is required to determine the optimal plane for separating the data points in order to properly classify the unseen sample. The categorization function may be defined as follows:

$$\sigma(x) = T \cdot X + K, \tag{2}$$

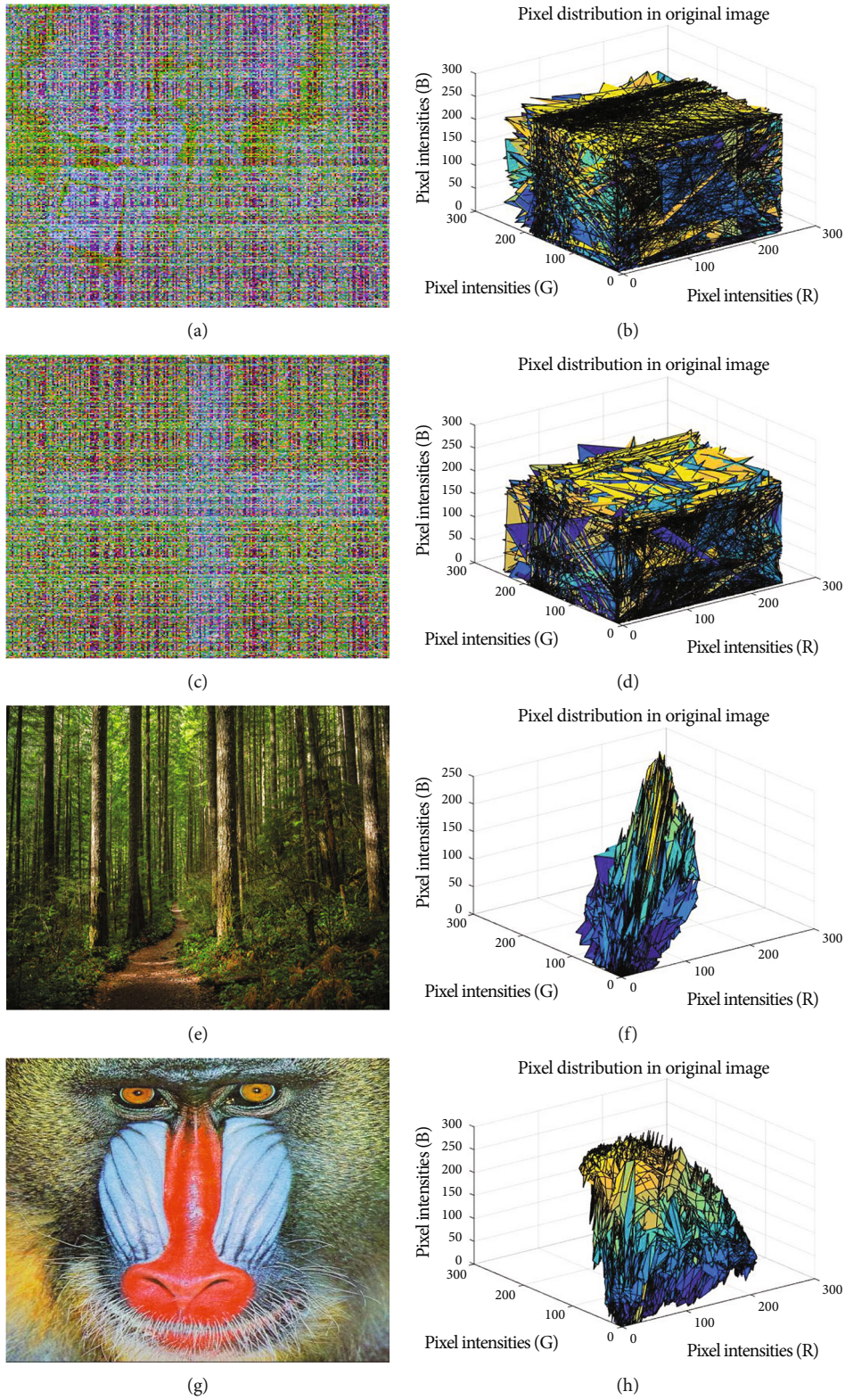


Figure 6: Pixel distribution in original and encrypted images.

where T and K are the weight vector and the intercept, respectively. However, T can be calculated as

$$T = \frac{xn - xm}{yn - ym}. \tag{3}$$

3.2. Decision Tree. DT is also a supervised learning technique to classify the data into specific classes. The growth of the tree may depend on the number of attributes used in the dataset. For determining the computational cost and classification performance, the heuristic plays a vital role in tree-growing [50]. Mostly, decision trees use an impurity-based heuristic which computes the purity of the resulting subset once the splitting attribute is applied to split the training data [51]. To build the tree for the classification purpose, a root node must be selected, which can be determined by calculating the Information Gain (IG), and the one with the highest IG will be selected as the splitting feature [52]. IG can be calculated as

$$\mathrm{IG}(X, Y) = \mathrm{Entropy}(X) - \sum_{y} \frac{|X_y|}{|X|} \mathrm{Entropy}(X_y), \tag{4}$$

where X represents the training events or feature vectors, Y represents the feature and y represents its value, X_y represents the subset of X containing occurrences with $Y = y$, and entropy (X) may be determined as follows:

$$\mathrm{Entropy}(X) - \sum_{j=1}^{|B|} T_X(b_j) \log T_X(b_j), \tag{5}$$

where $T_X(b_j)$ can be evaluated as the probability of the events belonging to b_j in X and $|B|$ is the number of labels present in the dataset.

4. Proposed Model

Numerous encryption techniques have been proposed in recent years, including chaos and transformation-based algorithms. Analyzing the statistical results of EAs indicates that some of them are insecure and do not provide enough protection [53–56].

In this article, a machine learning model that incorporates SVM is developed to determine the optimal encryption technique for the data in the form of images. The proposed work is shown schematically in Figure 3. The process for constructing the proposed model is as follows:

(i) Take a large collection of plaintext images (I) having size $M \times N$ ($[I_{ij}]_{MXN} \longrightarrow M$ and $N \in \mathbb{Z}$) in which a different amount of information is present. For instance, a few images from the dataset are shown in Figure 4 in which a significant amount of information lies in Figures 4(a)–4(d) as compared to the information present in Figures 4(e)–4(h)

Table 7: Defined intervals for histogram analysis.

[3000 4000] ⟶ ELPT
[4500 6000] ⟶ MLPT
[6500 7000] ⟶ HLPT

Table 8: Defined intervals for I_D.

[248800 247000] ⟶ EHPT
[250700 248900] ⟶ EMPT
[252600 250800] ⟶ ELPT

4.1. Features Used in the Proposed Work. Security parameters such as entropy, energy, contrast, correlation, homogeneity, histogram uniformity, and irregular deviation are considered features to select which plaintext image contains the highest, lowest, and moderate amount of information. On the other hand, peak signal to noise ratio and mean square error, both of which are security metrics, need at least two images, such as plaintext and ciphertext, in order to quantify the difference between the two. In our case, only plaintext images are considered in the proposed work.

4.1.1. Entropy. Entropy is used to find the randomness in an image. Furthermore, the entropy value corresponds to the high randomness [57]. The relation between entropy and randomness is given below:

$$\text{Entropy} \propto \text{randomness}. \tag{6}$$

The maximum entropy value for every image is determined by its bit count. For example, the maximum entropy values for an eight-bit and binary image are 8 and 2, respectively. Entropy may be stated mathematically as

$$\text{Entropy} = \sum_{x=1}^{A \times B} p(s_w) \log_2(p(s_w)), \tag{7}$$

where $p(\mathrm{s}_w)$ is the probability of occurrence of message s_w and $A \times B$ represent the number of pixels present in plaintext image.

The entropy value of an image increases in proportion to the complexity of the patterns contained inside. As seen in Figures 4(a)–4(d), the patterns are visible, indicating that the entropy value for such images is low. Similarly, the entropy values for the images shown in Figures 4(e)–4(h) will be rather high, as indicated in Table 1.

To classify the plaintext images to be encrypted either with fast, moderate, or slow processing EA, three intervals are defined in Table 2.

4.1.2. Contrast. Contrast analysis of an image allows the observer to identify the objects in the image [57]. Mathematically, it can be calculated as

$$\text{Contrast} = \sum_{c,d} |c - d|^2 p(c, d), \tag{8}$$

Table 9: Feature summary.

Features	Mathematical equations	Relationship with strong security (S.S)	Variable explanation
Energy	$\text{En} = \sum_{T=1}^{M} P(c,d)$	$\text{Energy} \propto \frac{1}{\text{S.S}}$	$P(a,b)$ is an original image
Histogram	$(\text{Hist})^2 = \sum_{k=0}^{255} \frac{g_i - t}{t}$		$t = M \times N/256$ g_i: number of gray levels
Entropy	$\text{Ent} = \sum_{x=1}^{A\times B} p(s_w)\log_2(p(s_w))$	$\text{Ent} \propto \text{S.S}$	$p(s_w)$: probability occurrence $A \times B$: no. of pixels
Contrast	$\text{Cont} = \sum_{c,d} \lvert c-d\rvert^2 p(c,d)$	$\text{Con} \propto \text{S.S}$	$p(c,d)$ is gray-level cooccurrence matrix
Homogeneity	$\text{Hom} = \sum_x \sum_y \frac{I(x,y)}{1+\lvert x+y\rvert}$	$\text{Hom} \propto \frac{1}{\text{S.S}}$	—
Correlation	$\text{Corr}_{qp} = \text{cov}\,(q,p)/\sqrt{T(q)}\sqrt{T(p)}$ $\text{Cov}(q,p) = 1/M\sum_{r=1}^{M}(q_r - G(q))(p_r - G(p))$ $T(q) = 1/M\sum_{r=1}^{M}(q_r - G(q))^2$ $T(p) = 1/M\sum_{r=1}^{M}(p_r - G(p))^2$ $G(q) = 1/M\sum_{r=1}^{M} q_r$ $G(p) = 1/M\sum_{r=1}^{M} p_r$	$\text{Correlation} \propto \frac{1}{\text{S.S}}$	Corr_{qp}: pixel correlation
Irregular deviation	$I_D = \sum_{j=0}^{255} \lvert X_i - X_h\rvert$	$I_D \propto \frac{1}{\text{S.S}}$	X_i, X_h: histogram deviations

where c and d represent the number of rows and columns of the image. $P(c,d)$ represents the number of gray levels in the occurrence matrices. The value of contrast reflects that the image contains less information. The relationship between the image pattern and contrast values is given in

$$\text{Image patterns} \propto \text{Less contrast value}. \tag{9}$$

As demonstrated in Table 1, the contrast values for the images in Figures 4(a)–4(d) are smaller than those in Figures 4(e)–4(h). This implies that the images (Figures 4(a)–4(d)) must use a robust encryption scheme to preserve the image's patterns. Using additional resources to encrypt the images (Figures 4(e)–4(h)) is not a viable option. It may be encrypted using a faster-processing encryption technique with a moderate level of security. The following intervals are given in Table 3 for the categorization of images that may be encrypted using either category of encryption methods.

4.1.3. Energy. Energy values reflect the amount of information present in the image. The higher the values of energy, the greater amount of information is present in the image [58]. Energy can be calculated using Equation (10), whereas the relationship between the amount of information and energy is given in Equation (11).

$$\text{Energy} = \sum_{T=1}^{M} P(c,d), \tag{10}$$

where M shows the total number of pixels in an image ($P(c,d)$):

$$\text{Information} \propto \text{Energy}. \tag{11}$$

Table 1 contains several energy values for various images, and it can be seen that the energy values for the images (Figures 4(a)–4(d)) are higher than the images shown in Figures 4(e)–4(h), implying that the images (Figures 4(a)–4(d)) require strong security algorithms to secure the patterns of the plaintext images. Table 4 shows the intervals for the classification of different EAs.

4.1.4. Correlation. Correlation indicates the similarity of two or more objects, i.e., correlation between the whole image or a subset of its pixels. Correlation coefficients increase as the object's similarity increases [59]. In digital images, a gradient pattern has a higher degree of correlation between the pixels than texture patterns, which indicates that images with more gradient patterns will have a higher correlation value, necessitating the use of a powerful encryption technique to break the correlation. In comparison, texture patterns in digital images have less correlation between pixels, which is very simple to eliminate even with a moderate or poor security level encryption techniques. Correlations between image pixels may be calculated using

$$\text{Corr}_{qp} = \frac{\text{cov}\,(q,p)}{\sqrt{T(q)}\sqrt{T(p)}}, \tag{12}$$

Table 10: Some portion of the dataset.

F.V no.	Images	Entropy	Energy	Contrast	Correlation	Homogeneity	I_D	Hist^2	EA
1	Plaintext-1	8	0.01	10.75	-0.5	0.392	247000	292.697	ELPT
2	Plaintext-2	7.9999	0.01005	10.745	-0.495	0.3921	247100	292.687	ELPT
3	Plaintext-3	7.9998	0.0101	10.74	-0.49	0.3922	247200 0	292.996	ELPT
4	Plaintext-4	7.9997	0.01015	10.735	-0.485	0.3923	247300	292.666	ELPT
5	Plaintext-5	7.9996	0.0102	10.73	-0.48	0.3924	247400	292.697	ELPT
6	Plaintext-6	7.9995	0.01025	10.725	-0.475	0.3925	247500	292.698	ELPT
7	Plaintext-7	7.9994	0.0103	10.72	-0.47	0.3926	247600	292.341	ELPT
8	Plaintext-38	7.9993	0.01035	10.715	-0.465	0.3927	247700	292.101	ELPT
9	Plaintext-9	7.9992	0.0104	10.71	-0.46	0.3928	247800	292.198	ELPT
10	Plaintext-10	7.9991	0.01045	10.705	-0.455	0.3929	247900	292.699	ELPT
11	Plaintext-11	7.999	0.0105	10.7	-0.45	0.393	248000	292.987	ELPT
12	Plaintext-12	7.9989	0.01055	10.695	-0.445	0.3931	248100	292.310	ELPT
13	Plaintext-13	7.9988	0.0106	10.69	-0.44	0.3932	248200	292.112	ELPT
14	Plaintext-14	7.9987	0.01065	10.685	-0.435	0.3933	248300	292.874	ELPT
15	Plaintext-15	7.9986	0.0107	10.68	-0.43	0.3934	248400	292.311	ELPT
16	Plaintext-16	7.9985	0.01075	10.675	-0.425	0.3935	248500	292.336	ELPT
17	Plaintext-17	7.9984	0.0108	10.67	-0.42	0.3936	248600	292.156	ELPT
18	Plaintext-18	7.9983	0.01085	10.665	-0.415	0.3937	248700	292.667	ELPT
19	Plaintext-19	7.9982	0.0109	10.66	-0.41	0.3938	248800	292.122	ELPT
20	Plaintext-20	7.9981	0.01095	10.655	-0.405	0.3939	248800	292.966	ELPT
21	Plaintext-21	7.293	0.01505	10.245	0.0001	0.4021	248900	294.334	EMPT
22	Plaintext-22	7.292	0.0151	10.24	0.00011	0.4022	249000	294.669	EMPT
23	Plaintext-23	7.291	0.01515	10.235	0.00012	0.4023	249100	294.110	EMPT
24	Plaintext-24	7.290	0.0152	10.23	0.00013	0.4024	249200	294.987	EMPT
25	Plaintext-25	7.289	0.01525	10.225	0.00014	0.4025	249300	294.001	EMPT
26	Plaintext-26	7.288	0.0153	10.22	0.00015	0.4026	249400	294.312	EMPT
27	Plaintext-27	7.287	0.01535	10.215	0.00016	0.4027	249500	294.900	EMPT
28	Plaintext-28	7.286	0.0154	10.21	0.00017	0.4028	249600	294.001	EMPT
29	Plaintext-28	7.285	0.01545	10.205	0.00018	0.4029	249700	294.361	EMPT
30	Plaintext-29	7.284	0.0155	10.2	0.00019	0.403	249800	294.936	EMPT
31	Plaintext-30	7.283	0.01555	10.195	0.0002	0.4031	249900	294.887	EMPT
32	Plaintext-31	7.282	0.0156	10.19	0.00021	0.4032	250000	294.474	EMPT
33	Plaintext-32	7.281	0.01565	10.185	0.00022	0.4033	250100	294.101	EMPT
34	Plaintext-33	7.280	0.0157	10.18	0.00023	0.4034	250200	294.031	EMPT
35	Plaintext-34	7.279	0.01575	10.175	0.00024	0.4035	250300	294.351	EMPT
36	Plaintext-35	7.278	0.0158	10.17	0.00025	0.4036	250400	294.333	EMPT
37	Plaintext-36	7.277	0.01585	10.165	0.00026	0.4037	250500	294.110	EMPT
38	Plaintext-37	7.276	0.0159	10.16	0.00027	0.4038	250600	294.669	EMPT
39	Plaintext-38	7.275	0.01595	10.155	0.00028	0.4039	250600	294.110	EMPT
40	Plaintext-40	7.274	0.016	10.15	0.00029	0.404	250700	294.311	EMPT
41	Plaintext-31	6.389	0.0201	9.74	0.0012	0.4122	250800	296.003	EHPT
42	Plaintext-42	6.388	0.02015	9.735	0.0013	0.4123	250900	297.963	EHPT
43	Plaintext-43	6.387	0.0202	9.73	0.0014	0.4124	251000	295.221	EHPT
44	Plaintext-44	6.386	0.02025	9.725	0.0015	0.4125	251100	298.733	EHPT
45	Plaintext-45	6.385	0.0203	9.72	0.0016	0.4126	251200	296.331	EHPT
46	Plaintext-46	6.384	0.02035	9.715	0.0017	0.4127	251200	297.301	EHPT
47	Plaintext-47	6.383	0.0204	9.71	0.0018	0.4128	251300	297.332	EHPT
48	Plaintext-48	6.382	0.02045	9.705	0.0019	0.4129	251400	297.301	EHPT

Table 10: Continued.

F.V no.	Images	Entropy	Energy	Contrast	Correlation	Homogeneity	I_D	Hist^2	EA
49	Plaintext-49	6.381	0.0205	9.7	0.002	0.413	251500	296.36	EHPT
50	Plaintext-50	6.380	0.02055	9.695	0.0021	0.4131	251600	298.36	EHPT
51	Plaintext-51	6.379	0.0206	9.69	0.0022	0.4132	251700	297.651	EHPT
52	Plaintext-52	6.378	0.02065	9.685	0.0023	0.4133	251800	297.660	EHPT
53	Plaintext-53	6.377	0.0207	9.68	0.0024	0.4134	251900	297.633	EHPT
54	Plaintext-54	6.376	0.02075	9.675	0.0025	0.4135	252000	297.336	EHPT
55	Plaintext-55	6.375	0.0208	9.67	0.0026	0.4136	252100	297.631	EHPT
56	Plaintext-56	6.374	0.02085	9.665	0.0027	0.4137	252200	297.310	EHPT
57	Plaintext-57	6.373	0.0209	9.66	0.0028	0.4138	252300	296.120	EHPT
58	Plaintext-58	6.372	0.02095	9.655	0.0029	0.4139	252400	296.999	EHPT
59	Plaintext-59	6.371	0.021	9.65	0.003	0.414	252500	297.613	EHPT
60	Plaintext-60	6.370	0.02105	9.645	0.0031	0.4141	252600	297.643	EHPT

Table 11: EA classification based on the information present in the plaintext images.

Plain images	Contrast	Entropy	Energy	Correlation	Homogeneity	I_D	$(\text{Hist})^2$	EA
Plain image$_1$	9.9971	7.97608	0.0183	0.00059	0.4092	24763	294.664	EMPT
Plain image$_2$	8.9651	7.9283	0.02334	0.0061	0.4192	24770	294.210	EMPT
Plain image$_3$	8.4131	7.8633	0.02452	0.0066	0.4027	248706	296.331	ELPT
Plain image$_4$	10.3574	7.9937	0.0159	-0.1351	0.3932	24993	292.665	EHPT
Plain image$_5$	11.3585	7.9982	0.0151	-0.0951	0.3984	247830	291.336	EHPT
Plain image$_6$	10.9875	7.99313	0.1682	-0.0651	0.3994	246378	292.346	EHPT
Plain image$_7$	9.6381	7.9832	0.0175	0.00063	0.4071	249763	291.032	EHPT
Plain image$_8$	10.8934	6 7.9931	0.0145	-0.044	0.3931	248610	291.336	EHPT

$$\text{Cov}(q,p) = \frac{1}{M}\sum_{r=1}^{M}(q_r - G(q))(p_r - G(p)), \tag{13}$$

$$T(q) = \frac{1}{M}\sum_{r=1}^{M}(q_r - G(q))^2, \tag{14}$$

$$T(p) = \frac{1}{M}\sum_{r=1}^{M}(p_r - G(p))^2, \tag{15}$$

$$G(q) = \frac{1}{M}\sum_{r=1}^{M} q_r, \tag{16}$$

$$G(p) = \frac{1}{M}\sum_{r=1}^{M} p_r, \tag{17}$$

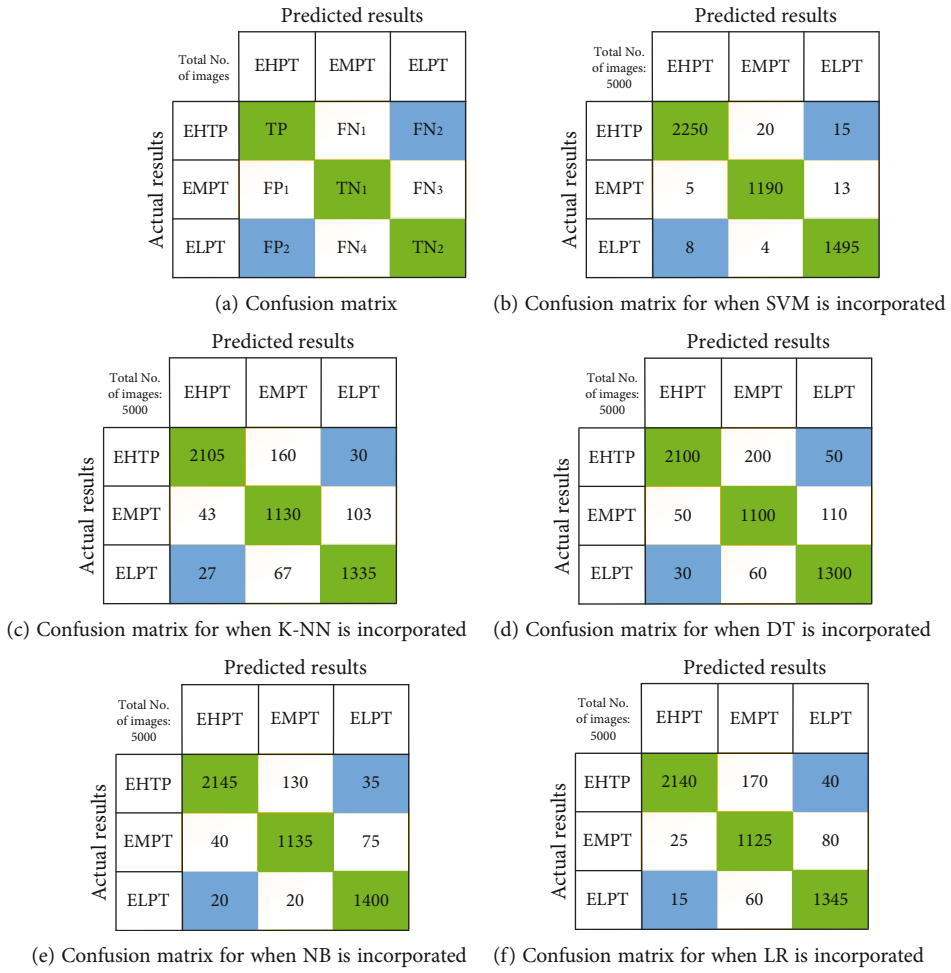
where q and p denote neighbouring pixel values, respectively, and Corr_{qp} denotes pixel correlation. Correlation coefficients are in the range of $[-1\ 1]$. $\text{Corr}_{qp} \longrightarrow -1$ and $\text{Corr}_{qp} \longrightarrow +1$ denoted the correlation between neighbouring pixels' lowest and maximum values, respectively. The 2500 pixel pairs are taken from the plaintext image in three distinct directions: horizontal, vertical, and diagonal. Figures 5(b)–5(d) and 5(f)–5(h) illustrate the horizontal, vertical, and diagonal correlations of image pixels, respectively. As can be observed, the pixels are closer together, indicating a significant correlation. In comparison, the distribution of pixels in Figures 5(j)–5(l) and 5(n)–5(p) is relatively random, indicating a weaker correlation. Thus, images with a low correlation may be easily secured using a simple, mathematically structured encryption approach. Digital image encryption is classified according to the intervals specified in Table 5.

4.1.5. Homogeneity. The Grey-level Co-occurrence Matrix (GLCM) illustrates the brightness of pixels. Those images that contain high information have higher homogeneity values. This means that encrypting images with high homogeneity values is difficult and requires a strong encryption scheme. Homogeneity can be calculated as

$$\sum_x \sum_y \frac{I(x,y)}{1+|x+y|}, \tag{18}$$

where $I(x,y)$ is plaintext image and x,y shows the pixel position. Table 6 contains the intervals used to classify encryption schemes. If the plaintext image's homogeneity values fall within the range $[0.4122\ 0.4418]$, it may be encrypted using a strategy that requires less mathematical operations and requires less processing time.

4.1.6. Histogram Analysis. Histogram analysis is often used in image encryption to determine the security of ciphertext



(a) Confusion matrix

(b) Confusion matrix for when SVM is incorporated

(c) Confusion matrix for when K-NN is incorporated

(d) Confusion matrix for when DT is incorporated

(e) Confusion matrix for when NB is incorporated

(f) Confusion matrix for when LR is incorporated

Figure 7: Confusion matrices for CNN, transfer learning, and fine tuning based on the proposed model.

Table 12: Performance measuring parameters and their statistical values.

Parameters	Mathematical equations
Accuracy (Acc_y)	$\frac{\Gamma P + \Gamma N_1 + \Gamma N_2}{\Gamma P + \Gamma N_1 + \Gamma N_2 + \sqsubseteq N_1 + \sqsubseteq N_2 + \sqsubseteq P_1 + \sqsubseteq N_3 + + \sqsubseteq P_2 + \sqsubseteq N_4} \times 100 = 98.7\%$ $\frac{2250 + 1190 + 1495}{2250 + 20 + 15 + 5 + 1190 + 13 + 8 + 4 + 1495} \times 100 = 98.7\%$
Specificity (Spec_y)/precision (Prec_y)	$\frac{\Gamma P}{\Gamma P + \sqsubseteq N_1 + \sqsubseteq N_2 + \sqsubseteq N_3 + \sqsubseteq N_4}$ $\frac{2250}{2250 + 20 + 15 + 13 + 4} = 0.97$
Sensitivity (Sen_y)/recall	$\frac{\Gamma N_1 + \Gamma N_2}{\Gamma N_1 + \Gamma N_2 + \sqsubseteq P_1 + \sqsubseteq P_2}$ $\frac{1190 + 1495}{1190 + 1495 + 5 + 8} = 0.99$
F1-score	$2 \times \left[\frac{\text{Sen}_y \times \text{Spec}_y}{\text{Sen}_y + \text{Spec}_y}\right] = 0.97$

images. To offer effective encryption, the encrypting images' pixel distribution must be constant, which means that the histogram must be flat, which corresponds to the image pixels being properly concealed. Plaintext images contain more information than encrypted images, indicating a less uniform pixel distribution. The histograms of multiple plaintext images are provided in Figure 6, along with the pixel distribution.

The relationship between the information present in the plaintext image and uniformity of the histogram is given as

$$\text{Plaintext information} \propto \frac{1}{\text{Histogram uniformity}}. \quad (19)$$

According to Equation (19), less uniformity in the histogram indicates that the corresponding image has a greater

quantity of information. This implies that images with flat histograms are simple to encrypt and can be made secure by using an encryption strategy with less mathematical operations and processing time. Equation (20) may be used to compute the statistical value of the histogram analysis:

$$(\text{Hist})^2 = \sum_{k=0}^{255} \frac{g_i - t}{t}, \tag{20}$$

where g_i represents the number of gray levels and $t = M \times N/256$. According to the existing work [60], $(\text{Hist})^2$ must be less than 293.24783 to achieve the uniformity in the histogram. $\text{Hist}^2 > 293.24783$ represents the variation in the peaks of the pixels. Based on the Hist^2 values, plaintext images are categorized into three intervals as shown in Table 7 for encryption purposes.

4.1.7. Irregular Deviation. The uniformity of the histogram also relates to the irregular deviation (I_D) in the image pixels. I_D may be used to determine image quality. The more information is present in the plaintext images, the higher the I_D value. It may be defined as the degree to which the histogram deviation distribution and the uniform distribution are similar. I_D can be calculated as

$$I_D = \sum_{j=0}^{255} |X_i - X_h|, \tag{21}$$

where X_i and X_h are the histogram deviations at the i^{th} and h positions, respectively, and the mean value. The less consistent the histograms, the lower the I_D value. The I_D interval is specified in Table 8 to classify encryption techniques for plaintext images. The summary of the features used in the proposed work is given in Table 9.

(i) A dataset is created using the security parameters as a feature and the intervals defined in Section 4.1. The collection is vast and includes the bulk of textual image categories that we see in everyday life, such as medical images and war images. As a consequence, this dataset is often referred to as the source domain for the proposed model training, validation, and construction. Table 10 includes a subset of the detailed data. The dataset is split into the training and test sets at a ratio of 0.8 : 0.2, as specified in

$$\begin{cases} \text{if} & \\ \text{Test dataset} & \text{Test} = N - \text{samples} \\ \text{Training dataset} & (\text{Total no.of samples}) - (N - \text{samples}) \end{cases} \tag{22}$$

(ii) After extracting statistical features from plaintext images, save feature values in an array to create unique vector streams (V.S), also referred to as feature vectors. Vector streams may be expressed as follows in terms of their features as given:

$$\text{Dataset} = \begin{pmatrix} \text{V.S}_1 = f.v_1, f.v_2, f.v_1, \cdots, f_7 \\ \text{V.S}_2 = f.v_1, f.v_2, f.v_1, \cdots, f_7 \\ \text{V.S}_3 = f.v_1, f.v_2, f.v_1, \cdots, f_7 \\ \text{V.S}_4 = f.v_1, f.v_2, f.v_1, \cdots, f_7 \\ \vdots \\ \text{V.S}_n = f.v_1, f.v_2, f.v_1, \cdots, f_7 \end{pmatrix}. \tag{23}$$

The feature values for each feature are $f.v_1, f.v_2, f.v_3, \cdots, f.v_7$. The provided dataset (22) is separated into two sections for the purpose of training the proposed model (training and testing). Each part is further separated into categories, such as X-train and Y-train for training purposes and X-test and Y-test for testing purposes. Train various machine learning algorithms on the training dataset to identify plaintext images based on the information contained in them. The purpose of comparing various machine learning algorithms is to determine which method outperforms the others

Table 13: K-fold analysis for accuracy.

Classifiers	SVM	NB	LR	K-NN	DT
$K = 5(M_1)$	98.5	91.6	93.9	93.8	93.8
$K = 10(M_2)$	98.6	90.5	92.2	94.2	92.3
$K = 20(M_3)$	98.8	92.3	92.7	93.9	92.9
$K = 25(M_4)$	98.7	91.6	93.3	93.4	93.8
$K = 50(M_5)$	98.4	92.8	93.1	94.7	93.6

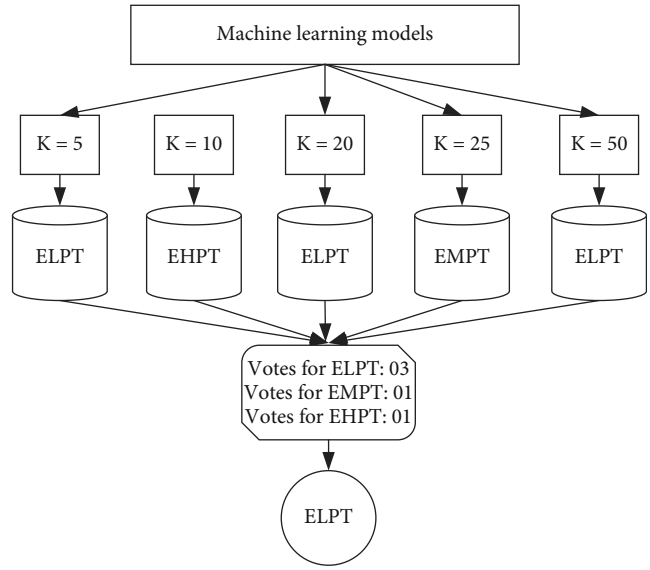


Figure 8: Hard voting-based classification

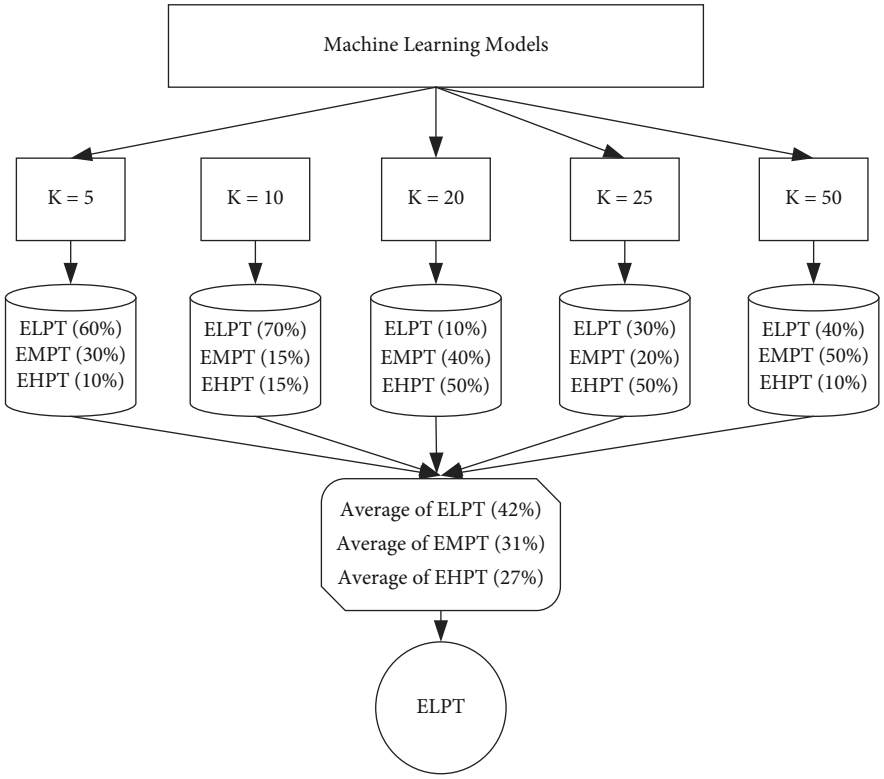


Figure 9: Hard voting-based classification

on the provided dataset. A few instances of categorization for numerous plaintext images are shown in Table 11.

5. Results and Discussion

Two distinct tools such as MATLAB 2014a and a Jupyter notebook (for Python, version 3.7) are used to construct the proposed model. Several characteristics including accuracy, precision, recall, and F-score are examined while evaluating the proposed model, and their values may be simply computed using the confusion matrix. This is a two-dimensional array that contains True Positive (TP), True Negative (TN), False Positive (FP), and False Negatives (FN). Figure 7 shows the generalised confusion matrix and the confusion matrices for the proposed work when DT, K-NN, RF, NB, and SVM are used.

The terms TP, TN, FP, and FN are defined below according to the proposed model.

(i) True positives (TP)

The proposed technique predicts that a strong EA (EHPT) is required to encrypt such a plaintext image that contains a bulk of information.

(ii) True negatives (TN)

The proposed technique predicts that such an EA is required that offers moderate security (EMPT) to encrypt a plaintext image that contains moderate amount of information, or the proposed technique predicts that such an EA is required that offers weak security (ELPT) to encrypt a plaintext image which contains less amount of information.

(iii) False positives (FP)

The proposed technique predicts that a strong EA (EHPT) is required to encrypt such a plaintext image that contains moderate or less amount of information.

(iv) False negatives (FN)

The proposed technique predicts that such an EA is required that offers moderate security (EMPT) to encrypt a plaintext image that contains a bulk of information, or the proposed technique predicts that such an EA is required that offers weak security (ELPT) to encrypt a plaintext image that contains a moderate amount of information.

The mathematical equations and corresponding values calculated using the proposed mode are shown in Table 12.

To enhance the overall accuracy of the proposed model, K-fold analysis is performed in which five different values of K ($K = 5, K = 10, K = 20, K = 25$, and $K = 50$) are selected to build five models (M_1, M_2, M_3, M_4, and M_5). For instance, if $K = 20$, a total of twenty iterations will be performed and take the average accuracy for M_1. The mathematical representation for calculating the average accuracy for M_3 (Avg_{acc}) is shown in Equations (24) and (25), whereas Av

Table 14: Performance comparison with existing models.

Schemes	SVM (sigmoid kernel)	SVM (linear kernel)	SVM (rbf kernel)	SVM (polynomial kernel)	NB	LR	DT	RF	K-NN
				Accuracy (Acc_y)					
Proposed	98.7	95.4	96.3	95.8	90.2	78.3	80.6	95.2	96.9
Reference [62]	91	81	89	90	90	92	91	84	86
Reference [63]	86	93	92	92	91	92	92	91	92
Reference [61]	95	75	77	79	73	74	82	84	86
Reference [64]	85	83	82	89	92	93	91	92	97
Reference [65]	92	86	82	92	92	94	91	92	93
				Precision ($Prec_y$)					
Proposed	0.97	0.98	0.98	0.89	0.99	0.32	0.35	0.99	0.97
Reference [62]	0.84	0.92	0.90	0.85	0.86	0.87	0.89	0.92	0.89
Reference [63]	0.92	0.95	0.93	0.96	0.93	0.93	0.95	0.98	0.99
Reference [61]	0.89	0.88	0.87	0.84	0.92	.97	0.98	0.97	0.98
Reference [64]	0.97	0.95	0.96	0.98	0.96	099	0.98	0.99	0.98
Reference [65]	0.89	0.88	0.87	0.84	0.92	.97	0.98	0.97	0.98
				Sensitivity (Sen_y)					
Proposed	0.97	0.98	0.99	0.96	0.80	0.15	0.87	0.92	0.85
Reference [62]	0.89	0.92	0.93	0.95	0.91	0.94	0.95	0.94	0.92
Reference [63]	0.92	0.94	0.91	0.90	0.98	0.94	0.95	0.92	0.91
Reference [61]	0.97	0.91	0.92	0.91	0.92	0.96	0.95	0.92	0.96
Reference [64]	0.91	0.92	0.90	0.89	0.96	0.92	0.93	0.91	0.92
Reference [65]	0.91	0.92	0.94	0.96	0.96	0.92	0.92	0.91	0.91
				F1-score					
Proposed	0.98	0.99	0.98	0.96	0.89	0.22	0.45	0.94	91
Reference [62]	0.86	0.92	0.81	0.88	0.85	0.97	0.93	0.94	0.92
Reference [63]	0.92	0.92	0.83	0.92	0.93	0.91	0.98	0.96	0.94
Reference [61]	0.91	0.90	0.92	0.93	0.92	0.91	0.95	0.96	0.99
Reference [64]	0.96	0.97	0.92	0.91	0.91	0.96	0.95	0.92	0.91
Reference [65]	0.91	0.90	0.92	0.93	0.92	0.91	0.95	0.96	0.99

g_{acc} for other classifiers at different values of K are displayed in Table 13:

$$\text{Avg}_{\text{acc}}(M_3) = \frac{\text{Acc}_{(K_1)} + \text{Acc}_{(K_2)} + \text{Acc}_{(K_3)} + \text{Acc}_{(K_4)} + \text{Acc}_{(K_5)}}{5} \times 100, \tag{24}$$

$$\text{Accuracy}(M_1) = \frac{98.8 + 98.7 + 98.9 + 98.9 + 98.8}{5} = 98.8\%. \tag{25}$$

Finally, voting techniques such as soft and hard voting are applied on the proposed M-models to classify the labels in a more sophisticated way.

5.1. Hard Voting. This technique works on the majority of votes. For instance, there are five models for the proposed work $(M_1, M-2, \cdots, M_5)$. Three of them classify the upcoming event as ELPT, one each is for classes EMPT and EHPT. Therefore, according to the hard voting technique, the new event will belong to class ELPT as shown in Figure 8.

5.2. Soft Voting. The probability-based classification can be performed using soft voting. In this technique, the probability of each class occurring is calculated separately, and then, the decision will be in favour of the class which has the highest probability value, as shown in Figure 9.

The probability of occurring in each class (ELPT, EMPT, and EHPT) using the generated M-models is calculated individually according to

$$\text{For class ELPT} = \frac{Po(\text{ELPT})_1 + Po(\text{ELPT})_2 + Po(\text{ELPT})_3 + \cdots + Po(\text{ELPT})_N}{N}, \tag{26}$$

$$\text{For class EMPT} = \frac{Po(\text{EMPT})_1 + Po(\text{EMPT})_2 + Po(\text{EMPT})_3 + \cdots + Po(\text{EMPT})_N}{N}, \tag{27}$$

$$\text{For class EHPT} = \frac{Po(\text{EHPT})_1 + Po(\text{EHPT})_2 + Po(\text{EHPT})_3 + \cdots + Po(\text{EHPT})_N}{N}, \tag{28}$$

where $Po(\text{ELPT})$, $Po(\text{EMPT})$, and $Po(\text{EHPT})$ is the probability of occurring in the events ELPT, EMPT, and EHPT, respectively. According to the calculated probabilities, Equations (29), (30), and (31) become

$$\text{For class ELPT} = \frac{60 + 70 + 10 + 30 + 40}{5} \times 100 = 42\%, \tag{29}$$

$$\text{For class EMPT} = \frac{30 + 15 + 40 + 20 + 50}{5} \times 100 = 31\%, \tag{30}$$

$$\text{For class EHPT} = \frac{10 + 15 + 50 + 50 + 10}{5} \times 100 = 27\%. \tag{31}$$

According to Equations (29), (30), and (31), the upcoming event will belong to class ELPT.

The statistical values of the performance metrics for the proposed and existing work are displayed in Table 14. Several machine learning algorithms, including SVM, NB, LR, DT, RF, and K-NN, are evaluated when comparing the proposed work to current models. Based on the comparative study, it is evident that, among the machine learning algorithms used in the proposed work, SVM offers the highest accuracy. Moreover, comparable schemes are significantly less accurate than the proposed approach. However, the technique suggested in [61] has a 95% accuracy rate, which is comparable to the accuracy offered by the proposed work.

6. Conclusions and Future Research Directions

The proposed research presents a pattern recognition-based machine learning technique for selecting the most appropriate encryption technique for a specific kind of data contained in digital images. Digital images are classified into three categories based on the amount of data present in them. Images containing highly correlated data which are transferred between the IoT devices should be encrypted through EHPT, while images containing textures should be encrypted through ELPT. Several machine learning algorithms are evaluated in the proposed study in order to determine the optimal ML algorithm to achieve the desired task. SVM outperforms all other machine learning methods in terms of accuracy, and it classifies the images with an accuracy of 98.7%. As a result, it is selected for the proposed technique. Moreover, a detailed comparison reveals that the proposed technique performs better than the existing ones.

In the future, we may use the proposed technique to secure digital images. Moreover, the dataset utilised in this research may be improved by incorporating more number of features.

Data Availability

The dataset generated and analyzed during this research study are available from the corresponding author on reasonable request.

Conflicts of Interest

The authors declare no conflict of interest.

References

[1] M. Condoluci, G. Araniti, T. Mahmoodi, and M. Dohler, "Enabling the iot machine age with 5g: machine-type multicast services for innovative real-time applications," *IEEE Access*, vol. 4, pp. 5555–5569, 2016.

[2] F. Ariani, R. Y. Endra, E. Erlangga, Y. Aprilinda, and A. R. Bahan, "Sistem monitoring suhu dan pencahayaan berbasis internet of thing (iot) untuk penetasan telur ayam," *EXPERT: Jurnal Manajemen Sistem Informasi dan Teknologi*, vol. 10, no. 2, pp. 36–41, 2020.

[3] Y. Harbi, Z. Aliouat, S. Harous, A. Bentaleb, and A. Refou, "A review of security in internet of things," *Wireless Personal Communications*, vol. 108, no. 1, pp. 325–344, 2019.

[4] A. Rashid, A. Masood, and A. R. Khan, "Zone of trust: blockchain assisted iot authentication to support cross-communication between bubbles of trusted IoTs," *Cluster Computing*, pp. 1–18, 2022.

[5] M. U. Rehman, A. Shafique, K. H. Khan et al., "Novel privacy preserving non-invasive sensing-based diagnoses of pneumonia disease leveraging deep network model," *Sensors*, vol. 22, no. 2, p. 461, 2022.

[6] S. Abbas, Q. Nasir, D. Nouichi et al., "Improving security of the internet of things via rf fingerprinting based device identification system," *Neural Computing and Applications*, vol. 33, no. 21, pp. 14753–14769, 2021.

[7] I. Hussain, F. Ahmed, U. M. Khokhar, and A. Anees, "Applied cryptography and noise resistant data security," *Security and Communication Networks*, vol. 2018, 2 pages, 2018.

[8] A. Shafique, A. Mehmood, and M. Elhadef, "Survey of security protocols and vulnerabilities in unmanned aerial vehicles," *IEEE Access*, vol. 9, pp. 46927–46948, 2021.

[9] A. M. Sagheer, S. S. Al-Rawi, and O. A. Dawood, "Proposing of developed advance encryption standard," in *2011 Developments in E-systems Engineering*, p. 197202, Dubai, United Arab Emirates, December 2011.

[10] D. Coppersmith, "The data encryption standard (des) and its strength against attacks," *IBM Journal of Research and Development*, vol. 38, no. 3, pp. 243–250, 1994.

[11] I. Hussain, A. Anees, T. A. Al-Maadeed, and M. Mustafa, "A novel encryption algorithm using multiple semield s-boxes based on permutation of symmetric group," 2020, http://arxiv.org/abs/2004.12264.

[12] A. Shafique, J. Ahmed, W. Boulila, H. Ghandorh, J. Ahmad, and M. U. Rehman, "Detecting the security level of various cryptosystems using machine learning models," *IEEE Access*, vol. 9, pp. 9383–9393, 2020.

[13] I. Hussain, A. Anees, M. Aslam, R. Ahmed, and N. Siddiqui, "A noise resistant symmetric key cryptosystem based on S8 S-boxes and chaotic maps," *The European Physical Journal Plus*, vol. 133, no. 4, pp. 1–23, 2018.

[14] T. S. Ali and R. Ali, "A new chaos based color image encryption algorithm using permutation substitution and Boolean operation," *Multimedia Tools and Applications*, vol. 79, no. 27, pp. 19853–19873, 2020.

[15] A. Shafique and F. Ahmed, "Image encryption using dynamic s-box substitution in the wavelet domain," *Wireless Personal Communications*, vol. 115, no. 3, pp. 2243–2268, 2020.

[16] C. E. Shannon, "Communication theory of secrecy systems," *The Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.

[17] S. S. Jamal, A. Anees, M. Ahmad, M. F. Khan, and I. Hussain, "Construction of cryptographic s-boxes based on mobius transformation and chaotic tent-sine system," *IEEE Access*, vol. 7, pp. 173273–173285, 2019.

[18] A. Shafique, J. Ahmed, M. U. Rehman, and M. M. Hazzazi, "Noise-resistant image encryption scheme for medical images in the chaos and wavelet domain," *IEEE Access*, vol. 9, pp. 59108–59130, 2021.

[19] A. Anees and Y.-P. P. Chen, "Discriminative binary feature learning and quantization in biometric key generation," *Pattern Recognition*, vol. 77, pp. 289–305, 2018.

[20] E. Salah, K. Amine, K. Redouane, and K. Fares, "A Fourier transform based audio watermarking algorithm," *Applied Acoustics*, vol. 172, p. 107652, 2021.

[21] A. Anees, A. M. Siddiqui, and F. Ahmed, "Chaotic substitution for highly autocorrelated data in encryption algorithm," *Communications in Nonlinear Science and Numerical Simulation*, vol. 19, no. 9, pp. 3106–3118, 2014.

[22] A. Shafique, A. Mehmood, and M. Elhadef, "Detecting signal spoofing attack in uavs using machine learning models," *IEEE Access*, vol. 9, pp. 93803–93815, 2021.

[23] I. Hussain, A. Anees, A. H. AlKhaldi, A. Algarni, and M. Aslam, "Construction of chaotic quantum magnets and matrix Lorenz systems S-boxes and their applications," *Chinese Journal of Physics*, vol. 56, no. 4, pp. 1609–1621, 2018.

[24] A. Anees and I. Hussain, "A novel method to identify initial values of chaotic maps in cybersecurity," *Symmetry*, vol. 11, no. 2, p. 140, 2019.

[25] J. Ahmad and F. Ahmed, "Efficiency analysis and security evaluation of image encryption schemes," *Computing*, vol. 23, p. 25, 2010.

[26] Q. Lu, C. Zhu, and X. Deng, "An efficient image encryption scheme based on the lss chaotic map and single s-box," *IEEE Access*, vol. 8, pp. 25664–25678, 2020.

[27] K. A. K. Patro, A. Soni, P. K. Netam, and B. Acharya, "Multiple grayscale image encryption using cross-coupled chaotic maps," *Journal of Information Security and Applications*, vol. 52, p. 102470, 2020.

[28] I. Hussain, A. Anees, A. H. Alkhaldi, M. Aslam, N. Siddiqui, and R. Ahmed, "Image encryption based on chebyshev chaotic map and s8 s-boxes," *Optica Applicata*, vol. 49, no. 2, 2019.

[29] A. Belazi, A. A. Abd El-Latif, R. Rhouma, and S. Belghith, "Selective image encryption scheme based on dwt, aes s-box and chaotic permutation," in *2015 International wireless communications and mobile computing conference (IWCMC)*, pp. 606–610, Dubrovnik, Croatia, August 2015.

[30] F. Masood, J. Ahmad, S. A. Shah, S. S. Jamal, and I. Hussain, "A novel hybrid secure image encryption based on julia set of fractals and 3d lorenz chaotic map," *Entropy*, vol. 22, no. 3, p. 274, 2020.

[31] M. Khan, A. S. Alanazi, L. S. Khan, and I. Hussain, "An efficient image encryption scheme based on fractal Tromino and Chebyshev polynomial," *Complex & Intelligent Systems*, vol. 7, no. 5, pp. 2751–2764, 2021.

[32] H. R. Alsanad, O. N. Ucan, M. Ilyas, A. U. R. Khan, and O. Bayat, "Real-time fuel truck detection algorithm based on deep convolutional neural network," *IEEE Access*, vol. 8, pp. 118808–118817, 2020.

[33] J. Ahmad and S. O. Hwang, "Chaos-based diffusion for highly autocorrelated data in encryption algorithms," *Nonlinear Dynamics*, vol. 82, no. 4, pp. 1839–1850, 2015.

[34] A. Shafique, "A new algorithm for the construction of substitution box by using chaotic map," *The European Physical Journal Plus*, vol. 135, no. 2, pp. 1–13, 2020.

[35] M. Khan and Z. Asghar, "A novel construction of substitution box for image encryption applications with gingerbreadman chaotic map and S8 permutation," *Neural Computing and Applications*, vol. 29, no. 4, pp. 993–999, 2018.

[36] A. Razaq, A. Yousaf, U. Shuaib, N. Siddiqui, A. Ullah, and A. Waheed, "A novel construction of substitution box involving coset diagram and a bijective map," *Security and Communication Networks, vol.*, vol. 2017, pp. 1–16, 2017.

[37] C. Li and X. Yang, "An image encryption algorithm based on discrete fractional wavelet transform and quantum chaos," *Optik*, vol. 260, p. 169042, 2022.

[38] C.-M. Lin, D.-H. Pham, and T.-T. Huynh, "Encryption and decryption of audio signal and image secure communications using chaotic system synchronization control by tsk fuzzy brain emotional learning controllers," *IEEE Transactions on Cybernetics*, pp. 1–15, 2021.

[39] J. Liu, Y. Wang, Q. Han, and J. Gao, "A sensitive image encryption algorithm based on a higher-dimensional chaotic map and steganography," *International Journal of Bifurcation and Chaos*, vol. 32, no. 1, p. 2250004, 2022.

[40] A. Shrivastava, J. B. Sharma, and S. D. Purohit, "Image encryption based on fractional wavelet transform, arnold transform with double random phases in the hsv color domain," *Recent Advances in Computer Science and Communications (Formerly: Recent Patents on Computer Science)*, vol. 15, no. 1, pp. 5–13, 2022.

[41] L. Lidong, D. Jiang, X. Wang, L. Zhang, and X. Rong, "A dynamic triple-image encryption scheme based on chaos, S-Box and image compressing," *IEEE Access*, vol. 8, pp. 210382–210399, 2020.

[42] M. U. Rehman, A. Shafique, S. Khalid, and I. Hussain, "Dynamic substitution and confusion-diffusion-based noise-resistive image encryption using multiple chaotic maps," *IEEE Access*, vol. 9, pp. 52277–52291, 2021.

[43] H. R. Shakir, "An image encryption method based on selective aes coding of wavelet transform and chaotic pixel shuffling," *Multimedia Tools and Applications*, vol. 78, no. 18, pp. 26073–26087, 2019.

[44] A. Shafique and J. Shahid, "Novel image encryption cryptosystem based on binary bit planes extraction and multiple chaotic maps," *The European Physical Journal Plus*, vol. 133, no. 8, pp. 1–16, 2018.

[45] A. Shafique and J. Ahmed, "Dynamic substitution based encryption algorithm for highly correlated data," *Multidimensional Systems and Signal Processing*, vol. 32, no. 1, pp. 91–114, 2021.

[46] A. Anees, I. Hussain, A. Algarni, and M. Aslam, "A robust watermarking scheme for online multimedia copyright protection using new chaotic map," *Security and Communication Networks, vol.*, vol. 2018, article 1840207, pp. 1–20, 2018.

[47] A. Shafique, M. M. Hazzazi, A. R. Alharbi, and I. Hussain, "Integration of spatial and frequency domain encryption for digital images," *IEEE Access*, vol. 9, pp. 149943–149954, 2021.

[48] S. K. Mishra and V. H. Deepthi, "Retracted article: brain image classification by the combination of different wavelet transforms and support vector machine classification," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 6, pp. 6741–6749, 2021.

[49] J. Cervantes, F. Garcia-Lamont, L. Rodrguez-Mazahua, and A. Lopez, "A comprehensive survey on support vector machine classification: applications, challenges and trends," *Neurocomputing*, vol. 408, pp. 189–215, 2020.

[50] T. Brázdil, K. Chatterjee, J. Křetínský, and V. Toman, "Strategy representation by decision trees in reactive synthesis," in *International Conference on Tools and Algorithms for the Construction and Analysis of Systems*, Lecture Notes in Computer Science, pp. 385–407, Springer, 2018.

[51] F. Avellaneda, "Efficient inference of optimal decision trees," *Proceedings of the AAAI Conference on Artificial Intelligence*, vol. 34, no. 4, pp. 3195–3202, 2020.

[52] M. U. Rehman, A. Shafique, S. Khalid, M. Driss, and S. Rubaiee, "Future forecasting of covid-19: a supervised learning approach," *Sensors*, vol. 21, no. 10, p. 3322, 2021.

[53] A. Anees and Y.-P. P. Chen, "Designing secure substitution boxes based on permutation of symmetric group," *Neural Computing and Applications*, vol. 32, no. 11, pp. 7045–7056, 2020.

[54] A. Khurshid, A. N. Khan, F. G. Khan, M. Ali, J. Shuja, and A. U. R. Khan, "Secure-CamFlow: a device-oriented security model to assist information flow control systems in cloud environments for IoTs," *Concurrency and Computation: Practice and Experience*, vol. 31, no. 8, p. e4729, 2019.

[55] F. Ahmed and A. Anees, "Hash-based authentication of digital images in noisy channels," in *Robust Image Authentication in the Presence of Noise*, pp. 1–42, Springer, Cham, 2015.

[56] M. F. Aziz, A. N. Khan, J. Shuja, I. A. Khan, F. G. Khan, and A. U. R. Khan, "A lightweight and compromise-resilient authentication scheme for IoTs," *Transactions on Emerging Telecommunications Technologies*, vol. 33, no. 3, p. e3813, 2022.

[57] I. Hussain, A. Anees, and A. Algarni, "A novel algorithm for thermal image encryption," *Journal of Integrative Neuroscience*, vol. 17, no. 3-4, pp. 447–461, 2018.

[58] A. Anees, W. A. Khan, M. A. Gondal, and I. Hussain, "Application of mean of absolute deviation method for the selection of best nonlinear component based on video encryption," *Zeitschrift für Naturforschung A*, vol. 68, no. 6-7, pp. 479–482, 2013.

[59] Y. Sang, J. Sang, and M. S. Alam, "Image encryption based on logistic chaotic systems and deep autoencoder," *Pattern Recognition Letters*, vol. 153, pp. 59–66, 2022.

[60] M. Guan, X. Yang, and W. Hu, "Chaotic image encryption algorithm using frequency-domain DNA encoding," *IET Image Processing*, vol. 13, no. 9, pp. 1535–1539, 2019.

[61] S. S. Vanjire and M. Lakshmi, "MDTA: a new approach of supervised machine learning for android malware detection and threat attribution using behavioral reports," in *Mobile Computing and Sustainable Informatics*, pp. 147–159, Springer, Singapore, 2022.

[62] S. Mishra and A. K. Tyagi, "The role of machine learning techniques in internet of things-based cloud applications," in *Artificial Intelligence-based Internet of Things Systems*, pp. 105–135, Springer, Cham, 2022.

[63] S. Sengan, O. I. Khalaf, D. K. Sharma, and A. A. Hamad, "Secured and privacy-based ids for healthcare systems on e-medical data using machine learning approach," *International Journal of Reliable and Quality E-Healthcare (IJRQEH)*, vol. 11, no. 3, pp. 1–11, 2022.

[64] M. U. Ilyas and S. A. Alharbi, "Machine learning approaches to network intrusion detection for contemporary internet traffic," *Computing*, vol. 104, no. 5, pp. 1061–1076, 2022.

[65] H. Li, C. Li, and Y. Liu, "Machine learning-based frequency security early warning considering uncertainty of renewable generation," *International Journal of Electrical Power & Energy Systems*, vol. 134, p. 107403, 2022.

Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 8290255, 13 pages
https://doi.org/10.1155/2022/8290255

Review Article

Imperative Role of Automation and Wireless Technologies in Aquaponics Farming

Kiran Kumari Gayam[1], **Anuj Jain**[1], **Anita Gehlot**[2], **Rajesh Singh**[2], **Shaik Vaseem Akram**[2], **Aman Singh**[3], **Divya Anand**[4,5] and **Irene Delgado Noya**[5,6]

[1]*School of Electronics & Electrical Engineering, Lovely Professional University, Punjab, 144411, India*
[2]*Division of Research & Innovation, UIT, Uttaranchal University, Uttarakhand, 248007, Dehradun, India*
[3]*Faculty of Engineering, Universidade Internacional do Cuanza, Estrada Nacional 250, Bairro Kaluapanda, Cuito-Bié, Angola*
[4]*Department of Computer Science and Engineering, Lovely Professional University, Phagwara 144411, India*
[5]*Higher Polytechnic School, Universidad Europea del Atlántico, C/Isabel Torres 21, 39011 Santander, Spain*
[6]*Department of Project Management, Universidad Internacional Iberoamericana, Campeche 24560, Mexico*

Correspondence should be addressed to Aman Singh; aman.singh@unic.co.ao

Received 25 March 2022; Revised 19 May 2022; Accepted 25 May 2022; Published 9 June 2022

Academic Editor: Shafiq Ahmad

Food and agriculture are significant aspects that can meet the food demand estimated by the Food Agriculture Organization (FAO) by 2050. In addition to this, the United Nations sustainable development goals recommended implementing sustainable practices to meet food demand to achieve sustainability. Currently, aquaponics is one of the sustainable practices that require less land and water and has a low environmental impact. Aquaponics is a closed-loop and soil-less method of farming, where it requires intensive monitoring, control, and management. The advancement of wireless sensors and communication protocols empowered to implementation of an Internet of Things- (IoT-) based system for real-time monitoring, control, and management in aquaponics. This study presents a review of the wireless technology implementation and progress in aquaponics. Based on the review, the study discusses the significant water and environmental parameters of aquaponics. Followed by this, the study presents the implementation of remote, IoT, and ML-based monitoring of aquaponics. Finally, the review presents the recommendations such as edge and fog-based vision nodes, machine learning models for prediction, LoRa-based sensor nodes, and gateway-based architecture that are beneficial for the enhancement of wireless aquaponics and also for real-time prediction in the future.

1. Introduction

According to the most recent United Nations forecasts, the world's population will expand from 6.8 billion now to 9.1 billion in 2050, representing a quarter more food is needed than there is today [1]. According to an FAO assessment, the primary problems for world agriculture in the future decades will be producing 70% more food for an additional 2.3 billion people while tackling hunger and poverty, utilizing finite natural resources more efficiently, and adjusting to climate change [2]. Globally, there are still adequate land resources available to feed the world's future population. However, FAO emphasized that much of the available acreage is only appropriate for cultivating a few commodities, and most of the unused land also suffers from chemical and physical restrictions, endemic diseases, and a lack of infrastructure, all of which are difficult to overcome. Healthy soils, land, and water are critical inputs in food production, and their scarcity in many parts of the world makes it critical to use and sustainably manage them [3]. The United Nations suggests that sensible water utilization through enhanced irrigation and storage technology, in conjunction with the creation of new drought-resistant crop types, can assist to sustain dryland output [4].

Aquaponics farming is a type of sustainable agriculture that involves a symbiotic link between fish and plants [5].

When the fish produce waste, it is cycled out of the fish tank into the grow bed, where bacteria convert ammonia into nitrates that plants require to grow (Figure 1). The water is subsequently purified and restored to the fish tank, contributing to the highly efficient, zero-waste process of cultivating fish and plants together [6]. When compared with the traditional farming method, it uses 80 to 95% less water, and also, the water usage efficiency can be increased; the use of pesticides and fertilizers can be reduced in this method [7]. Aquaponics is a closed-loop and soil-less method of farming, where it requires intensive monitoring, control, and management [8]. So, it is recommended to implement wireless technologies in aquaponics for effective monitoring, control, and management [9]. Currently, the advancement of wireless sensors and communication protocols empowered to implementation of an IoT-based system is continuously monitoring and analyzing the complete system to produce vegetables and plants that are needed for human use in a well-planned and well-maintained ecosystem with optimum use of water and minimum farmlands [10].

With motivation from the aspects, this study is aimed at providing a review of the significance and implementation of wireless and intelligent technologies in aquaponics farming. The study is drawn in such a way that it will provide a sequential way of understanding the various trends of wireless and intelligent technologies in aquaponics. The motive of this review is to bring various aspects that are specifically related to the effective real-time implementation of the aquaponics system. The major goals of this review paper are to identify (a) critical parameters that are suitable to monitor and control the growth of plants as well as fish; (b) to identify and discuss the growth of wireless technologies like IoT, edge, and fog computing implementation in an aquaponics system; and (c) evaluation of the progress of machine learning implementation in an aquaponics system that is used for real-time prediction of water quality identify suitably monitored and controlled parameters for effective growth of plants and fishes. This review also discusses the limitations of the previous studies and recommends a few suggestions such as edge and fog-based vision nodes, machine learning models for prediction, LoRa-based sensor nodes, and gateway-based architecture for the future enhancement in aquaponics. The contribution of the study is as follows:

(i) The environmental and water-based parameters that affect the growth of the organisms in aquaponics are discussed

(ii) The significance and function of the wireless-based systems for remote monitoring are discussed in this study with architecture

(iii) The significance of machine learning algorithms and edge and fog computing for real-time prediction in aquaponics are presented

The organization of the paper is as follows: Section 2 discusses the methodology of the review. Section 3 covers the parameters to be monitored in an aquaponics system. Section 4 covers the IoT systems and remote monitoring interfaces used. Section 5 covers the edge and fog-based architecture used. Section 6 covers the machine learning techniques that are used in aquaponics. Section 7 covers the recommendations and proposed architecture, and finally, the article concludes.

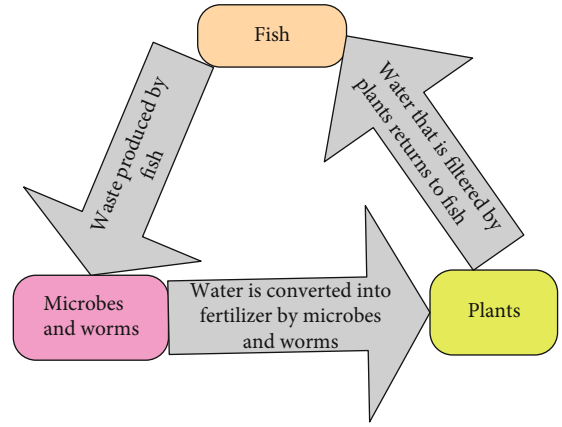


Figure 1: Aquaponics system cycle.

2. Methods

In this section, the discussion of methods and approaches are implemented for carrying out the review. The objective of this review is to discuss the significance of wireless technologies implemented by previous studies. In the field of an aquaponics system, there is a scarcity of quality articles from the reputed journals, so in this review, the conference articles are also included. The articles on aquaponics are obtained from the Web of Science, Scopus, ScienceDirect, IEEE Xplore, and Google Scholar. Initially, all studies related to the aquaponics are examined, and only those articles that satisfy the selection criterion such as the abstracts of studies that were available are selected but not the full text of the study not examined for review; research that proposes methodologies but does not conduct experiments or validation is not eligible for review; dissertation work and thesis completed at the postgraduate and graduate levels are not reviewed; non-peer-reviewed research articles are not considered for review, and book chapters, patent applications, and communications are not reviewed.

3. Significance of Water and Environmental Parameters

The aquaponics system is a combination of both aquaculture and hydroponics where plants and fish live in an integrated environment. The parameters related to both the water and the environment are to be monitored to ensure the proper growth and also to be healthy.

3.1. Water-Based Parameters. In an aquaponics system, the quality of water is the main factor that is to be considered [10]. Water is the medium through which nutrients are provided to the plants. Considering automation regard, water is

considered to be a complex factor as many parameters are dependent on one another. Aquaponics which is the integration of both aquaculture and hydroponics techniques is individually developed and adopted widely. For increasing the efficiency of water and sustainability, RAS design has been developed. But the ammonia present in the water begins to gather at the levels that are dangerous for the fish. So, for recirculating water, biofilters are being used. But the plants require nutrients and elements, which cannot be produced by water in the absence of fertilizers. But the use of fertilizers can lead to the disposal of water and replacement. The waste produced by fish can be used for the growing of plants. This process occurs indirectly and is called nitrification. To assure the standard quality in the solution of water, to make the process of nitrification favorable and growth of plants and keep fishes healthy at the same time, it is required to keep the right nutrient quantity, temperature, dissolved oxygen, pH, temperature, and salts during the complete process.

3.1.1. pH. Measurement of the concentration of hydrogen ions is known as pH. It is the alkalinity or acidity measurement of the solution. The rate at which nitrification occurs and the availability of nutrients to the plants are affected by the pH of water [11]. To measure the pH in a solution, a pH meter is used [12]. Manual electronic probes, test strips, and automatic probes in controllers are three different methods by which the measurement of pH values is obtained. The value that is acceptable for the pH of water in the aquaponics component can be from 6.5 to 9.5, and the acceptable value is 5.5 to 10, but this value may be varied slightly depending on the fish species. In slightly acidic solutions, the reproduction rate of fish may be decreased [13].

The optimum value is around 6.0 in the hydroponic component. Precipitation of Fe or Mn will occur if pH is more than 7.0, and root injury occurs if pH is less than 4.5 [14], and deficiency of nutrients is observed in plants [15]. The pH value is to be 7.0 to 9.0 for the nitrification process to occur. In an aquaponics system, the adjustment of pH values can be made by bases such as calcium and potassium because they act as a base for the nutrients [15, 16]. Minute changes in pH values (<0.3) in short time intervals can affect fish health very highly [15]. To the controller, the pH meter is connected to an automated system; the controller gets the change in output of the pH meter in millivolt and milliampere. The pH meter is then contacted with the controller and is tested in a solution to find the pH value. The value of output that is obtained is connected to the pH unit to the controller programming unit.

A pH meter named B&C Electronics-SZ 1093 gives a range of 0-13, a maximum temperature value of 80°C, and a maximum pressure of 7 bars [17]. The performance provided by a digital pH meter of 0.01 resolution and an ISFET ion-sensitive field-effect transistor is the same. A less percentage of error is provided by the Atlas EZO pH Sensor. Nonetheless, other options still exist [18]. An OMEGA PHE-45P pH sensor with lower maximum temperature resistance (60°C can be used in the aquaponics system [5]) and an Orion 3 Star meter from Thermo Fisher Scientific can be used to find the pH [11].

3.1.2. Dissolved Oxygen. The measure of the amount of oxygen that is dissolved in water which is available for living things in aquatics is dissolved oxygen. The organisms that share the environment of aquaponics are fish, bacteria, and plants for which dissolved oxygen is the most required parameter. The ability to support the life of aquatic organisms is determined by the oxygen amount present in water along with the level of water [19] At very low concentrations, oxygen is dissolved in water (in parts per million) and is considered to be the parameter that has an instant and extreme impact on the aquaponics [15]. Oxygen is made naturally in algae and green aquatic plants by photosynthesis. In every aquaponics system, it is mostly required to monitor the value of dissolved oxygen as its value changes sharply in small time intervals [19].

The temperature of the water and dissolved oxygen is strongly related to each other. Warm water has less oxygen. The intake of dissolved oxygen rises when fishes are taking food. For nitrifying bacteria, optimum levels are 4-8 milligrams/liter. Plants require dissolved oxygen of greater than 3 milligrams/liter [15]. If the oxygen is lowered, the fungus appears, and the roots of plants die. Dissolved oxygen of greater than 5 milligrams/liter is required by most species of fish. If the concentration of dissolved oxygen is low, the production of TAN will be perished [20].

The optical sensors detect the interaction of oxygen with particular luminous dyes. Because oxygen molecules interact with the dye when dissolved oxygen is present, the wavelengths that are returned are changed [21]. Galvanic and polarographic electromechanical options for measuring dissolved oxygen content exist. The existence of dissolved oxygen is determined by changing the electrical signal after applying a voltage to polarize or not polarize the system. Measurement systems for dissolved oxygen concentrations are costly. The data is transferred via a DO sensor coupled to a Modbus and TCP/IP technology [10]. In an aquaponics system, an Atlas DO probe with a capacity range of 0-100 milligrams/liter, maximum pressure of 3447 kPa, and 343 m of maximum depth is employed [18].

3.1.3. Temperature. In an aquaponics system, the temperature of the water is interconnected with many parameters that are related to water. The optimum value of temperature is in the range of 17-34°C for nitrification to take place. The nitrification process does not occur correctly, and bacteria productivity goes down if the temperature is below the value. A value of 18-30°C temperature is appropriate for the hydroponics component. A proper temperature value is to be maintained which decreases the disease risk in fish. Based on the type of fish, the suitable value of temperature changes. A temperature value of 22-32°C is favorable for tropical fish; for cold-water fish, the temperature to be maintained is 10-18°C. For other species, a temperature value in the 5-30°C range is favorable [15]. Calcium absorption is resisted in plants if the temperature of the water is high.

To measure the temperature of water, the method used is to examine the temperature range, tolerance of salinity, and resolution. The sensor resolution is the factor that is important in the selection because many of the water temperature

sensors have the required range covered. The sensor must not be waterproof only but should be designed to be submerged for a long time. A DS1820 temperature sensor along with an Arduino controller is used. The range of temperature in this sensor varies from -55°C to 125°C, and the resolution is about ±0.5°C. An IC named LM35 is used as temperature [18, 22, 23].

3.1.4. Ammonia. In surface and wastewaters, ammonia is present as a dissolved gas [13]. The protein that is given to the fish, only 10% of it is transformed into ammonia [24]. In an aquaponics system from the waste that is excreted by fish, ammonia is produced and acts as the main part as it is the main element for nutrients in the plants. For the fish, ammonia is very toxic, if present in small quantities. It is most noticeable when it changes as strongly acidic or alkaline. For fishes, the advisable range is 0 to 2 mg/L [13]. The optimum range of TAN is <3 mg/L for fish in warm water and 1 mg/L for fish in cold water. For bacteria that oxidizes ammonia and nitrite, the optimum range is <3 mg/L and <30mg/L [15].

Since ammonia is present in little quantities and does not have any color or odor, to know whether it is present or not, sensing it is required. The sensor has a wire electrode inside a filling solution. The solution is separated from the medium which has the sample by an ion-selective membrane, mixed with ammonium ions [25] The pH of water and water temperature is to be known necessarily to increase the accuracy of measurement of ammonia. The ammonia amount present in the water solution creates a data synthesis problem between ammonia sensors, temperature sensors, and pH sensors. Since the ammonia concentration before the biofilter is not considered, these sensors are to be placed in the water tank.

3.1.5. Nitrification. For plants, the main required nutrient inorganic is nitrogen. For the nitrification process to occur, ammonia is required which comes from the waste of the fish. It is in the form of ammonium and ammonia which is the function of pH, temperature, and salinity of water [26, 27]. Total ammonia-nitrogen concentration (TAN) is the sum of ammonium and ammonia [28]. Nitrification is the process in which the TAN is changed to nitrates [28]. With the help of ammonia-oxidizing bacteria, first TAN is oxidized into nitrite, and then, nitrate is converted into nitrates with nitrite-oxidizing bacteria [27]. So in an aquaponics system for nitrification, a biofilter is required. A hydroponic component, a biofilter for nitrification, and an aquaculture component are the constituents of an aquaponics system [29].

3.1.6. Nitrate. By nitrite-oxidizing bacteria, from ammonia, nitrate is obtained, the form in which plants can take the component of nitrogen that is required. For fish, nitrate is not dangerous. If the nitrate value is below 90 mg/L, it should not lead to health issues in fish [13], and the optimal range is 50-100 ppm. When designing a biofilter, this value is considered to be important. If the nitrates are present in large quantities, it means that it is dangerous to fish, and the biofilter is undersized [20]. To measure the nitrite concentration, the sensor that is used for knowing the ammonia concentration is used.

3.1.7. Nitrite. By ammonia-oxidizing bacteria, from ammonia, nitrite is obtained. For aquatic life, nitrite is considered to be dangerous [20]. The required value of nitrite in water for the bacteria, fish, and plants to survive is 0-1 mg/L [13]. For the proper growth of plants and the bacteria to survive the same value of nitrite is required. The nitrite that is present should not make a problem when it is provided in the optimum range. The mix of nitride-ionized electrodes and the element used for sensing are made of polyvinyl chloride membrane, works as an exchange of ions, and reference electrode forms nitrite concentration sensors. The sensor will develop electrical potential which is proportional to the nitrite ion concentration in solution and provides the concentration of nitrite in water.

3.1.8. Electroconductivity. Electroconductivity is a metric that measures a medium's ability to conduct electric current (EC), and in aquaponics, this is related to salinity [5, 30]. If the electrical conductivity changes, the fish are affected. The death of fish may occur if the level of electroconductivity is high, and this indicates that the water is polluted. To have a balance, there should be minimum content of salt. For fishes, the range of optimum level is 100-2000 mS/cm. The range of 30-500 mS/cm is also accepted [13].

A method was proposed for controlling the nutrient solution in the hydroponics system by monitoring the electrical conductivity [14]. Enshi-shoho nutrient solution was used to provide control over EC, as it has a known EC of 2400 mS/cm. These electroconductivity meters generally use a potentiometric method and four platinum electrodes. The use of this parameter is recommended to use [30].

3.1.9. Level. In an aquaponics system, the amount of water required is decided by the component size, i.e., fish tank. The health, growth of fish, and stress in fish are caused due to stocking density. The stocking number of fish is 20 kilograms of fish per thousand liters of water [15]. Removal of fish waste, evapotranspiration in plants, evaporation, and splashing of fish while feeding are the main causes of the water loss in all the aquaponics systems. The amount of water that is consumed daily in a hydroponic system is 0.1 to 0.3% which depends on the fish tank, hydroponic ratio, the flow of water, temperature of water specifies of fishes and plants used, and the hydroponic type of system that is used [31].

By using a slight glass or floating device, the level of water in the tanks is measured manually. Ultrasonic sensors, laser, and radar-based sensors are the most advanced sensors for measuring the level of fluid. K8AK-LS1 water level controller is used which has a maximum temperature tolerance of 50°C [17]. A water level sensor that gives an analog output when connected to an Arduino controller is used [32]. To know the level of water in the tank, an array of sensors is used [22]. A circuit built with a BC546 NPN transistor is used to construct a water overflow level sensor [33]. An

ultrasonic sensor is used to control the levels of water in the tank [23, 34].

3.1.10. Total Dissolved Solids. In water, the dissolved salts are present naturally. The number of dissolved materials, organic matter, and inorganic salts in the water represents total dissolved salt levels [35]. The desired amount of TDS for the fish is 1000 milligrams/liter but values below 2500 milligrams/liter are acceptable [13]. For many species of fish, TDS (>1000 mg/L) can be toxic. For the measurement of TDS, TDS meters are used as sensing units to measure the value of TDS in portable water. TDS can be measured using the sensor used for the measurement of electroconductivity.

3.1.11. Flow. To calculate the proficiency of filtration (solids) and biofiltration (nitrification) and to decide the availability of nutrients for plants, the flow of water in an aquaponics unit is needed. In the unit, constant flow is to be maintained to avoid deficiency of nutrients in the plants and also stress in the fishes. The measurement of flow between the grow bed and the filters is most required. Depending on the system that is adopted, the flow rate varies. Water flowing must be in such a way that more amounts of nutrients and oxygen are obtained by the plants in systems based on NFT. The flow of water must be smaller than 1-2 L/min in an NFT system [15]. To clean the water, a siphon is used in the media-based technique. To clean the water each hour, the water flow rate is to be set.

The flow of water is because of gravity in systems based on DWC. To guarantee the sufficient amount of nutrients received, the flow of water through the channels should be 1 to 4 hours. Depending on the size of the channel used and the capacity of water, the optimal flow rate of water is determined. To know the water flow between the fish tank and grow bed, a water sensor is used [4], and in between the grow bed and fish tank, the flow meter is kept [36].

3.1.12. Salinity. The quantity of salt concentration present in the water is salinity [30]. The growth and density of the fish are affected by salinity [20]. Like TDS, salinity is obtained by electroconductivity. Depending on the fish species, the required value of salinity changes.

3.1.13. Alkalinity. In an aquaponics system, the measurement of the concentration of the bases, mainly carbonate as well as bicarbonate, is alkalinity. The measure of the negative ions is the alkalinity, and the measure of positive ions is the hardness. The ability of water to withstand changes in the pH or the ability to neutralize acids is also referred to as alkalinity. There is a very high value of pH even if low levels of the acids are present [20]. The ammonia becomes toxic if the alkalinity level is high. 50 to 150 milligrams/liter of CaCO3 is the required range [13].

3.1.14. Water Hardness. The amount of the positively charged magnesium salts and calcium in the solution is measured because they are necessary for the fish metabolic reaction and also for the formation of scale and bone. Stress in fish is caused due to low levels of water hardness, and high levels are harmful because it increases the pH of water, which results in a reduced rate of absorption and nitrification in plants. The range for the hardness of water can be from 50 to 150 milligrams/liter, but for many of the species, the value > 10 milligrams/liter is acceptable [13]. TDS or electroconductivity can be used to determine water hardness [37].

3.2. Environment-Based Parameters. For obtaining stability and for better development of the fish as well as plants, it is required that the parameters related to the environment are to be monitored and controlled [7].

3.2.1. CO_2. In photosynthesis, carbon dioxide is a necessary component. The CO_2 in the air is used by the plants in indoor systems which are in large numbers. So, CO_2 is used artificially, and it is required to control the amount used. The optimum range level for many crops grown indoors is in the range of 340-1300 ppm [38]. The different amounts of CO_2 are required because it depends on the crop type, the available light, the temperature of the air, and RH. For the proper growth of fish, the carbonic acid levels should be less than 5 mg/L [20, 39]; otherwise, it is dangerous for fish. A sensor named MG811 is used to measure the amount of carbon dioxide in the air [30].

3.2.2. Air Temperature. Plant health is affected by the temperature of the air. In the aquaponics unit, the required temperature to grow the vegetable plants is 18-30°C. At temperatures greater than this, they start flowering and then to seeds [15]. For the proper transpiration of the plants, the temperature of the air is needed. When selecting temperature sensors, the range of temperature, the sensing element, the contactless or contact, and the method of calibration are to be checked. A thermistor is used to measure the temperature of air and humidity together in an aquaponics unit. A DHT11 thermistor [23] and a DHT22 thermistor are used which is having more accuracy and a range of values greater than DHT11 [38].

3.2.3. Relative Humidity. The amount of moisture in the air is relative humidity [40]. Depending on the stages of growth and the crop type used, the optimum level of relative humidity varies. Commonly, 50-80% is considered but it depends on the indoor temperature of the system. The air temperature sensor also provides relative humidity. In an aquaponics system, the DHT11 sensor is used to measure the relative humidity values [41].

3.2.4. Light Intensity. In indoor provisions, the sunlight is not available or available in less amount, which is essential for plants. In an aquaponics system to make the sunlight available to the plants, artificial lighting is used. Light is measured in intensity. Only some part of the light spectrum is used by the plants known as photosynthetically active radiation (PAR). It is the solar radiation spectral range where the photosynthetic organisms can process [42]. For a day, the crops require light for 14 to 18 hours. A light-dependent resistor (LDR) can be used for measuring the lighting system's radiation intensity. To measure the ambient light intensity, LDR is used [22, 23].

3.2.5. Media Moisture. The content of water in soil present in the media base is the media moisture. If a media-based type system is used, then it is necessary to measure the moisture of the medium. A soil moisture sensor is good to be used for this type which gives the accurate amount of water needed for the plants. The capacity of water that the soil holds is recommended to be checked. It was found that depending on the type of soil, the optimum ranges vary from 30 to 60 cbars [43]. An FC-28 can be used as a moisture sensor to measure soil moisture [38]. From the studies, the aquaponics system parameters that are required and their optimized ranges are summarized in Table 1.

Table 1: Aquaponics parameters and their optimal range.

Parameter	Optimal range
Temperature of water	17°C-30°C
Relative humidity of air	60%-80%
Dissolved oxygen level	>4 mg/L
Temperature of air	18°C-30°C
Level of water	0.02 kg/L
Salinity of water	0-2 ppt
Hardness of water	50-150 mg/L CaCO3
Flow of water	1-2 liters/min
Total ammonia-nitrogen	<2 mg/L
Nitrites	<1 mg/L
Nitrates	50 ppm to100 ppm
Alkalinity of water	50 to 150 mg/L CaCO3
Electroconductivity	100 to 2000 μS/cm
Level of carbon dioxide	340 ppm to 1300 ppm
Intensity of light	600 PPFD-900 PPFD
pH of water	6.5-7.0
Total dissolved solids	<1000 mg/L

4. Real-Time Monitoring Systems

Internet of Things, otherwise called the IoT, is an idea that plans to grow the advantages of persistently associated web networks. The integration of a controller, sensors, and the Internet into physical objects such as food gadgets and equipment allows for global information sharing. This additionally utilizes the idea of IoT because the data from the estimation of the sensor can be obtained through cell phone applications and sites from any place with the Internet association. With the presentation of computerization, keen techniques, and availability in the cultivating business, another entryway was opened for the upgrading of these aquaponics frameworks. The normal advantages of keen mechanization are a critical decrease of difficult work and a more vigorous control of the interaction by expanding the availability and availability of the boundaries and utilizing PC abilities to settle on information-driven choices [44].

4.1. Interfaces for Remote Monitoring. Checking interfaces are ordinarily a climate (intelligent or not) that shows a portion of the intrigued boundaries with regard to the cycle to the client or partner. This perception cycle is critical to ultimate choice making. IoT innovation empowers these observing interfaces to show esteems through remote organizations, even continuously.

A web application that exhibited a dashboard associated with a microcontroller to screen chosen hydroponics boundaries is used [5]. In the very year, a Raspberry Pi is used to do all the framework estimation units; at that point, the sensors' information is shipped off an electronic stage where it is put away and shown [45]. After a year, an iOS application that permitted to screen the framework climate persistently by getting information straightforwardly from the frameworks' microcontrollers is used [46]. The course of these joint efforts is going towards continuous dependability and portability (online as well as an application for cell phones).

4.2. Applications That Are Controlled Remotely. Controller applications are characterized by their capacity to flag framework actuators to communicate or modify some boundaries. With controller applications, administrators can on or off the water siphon or light when essential, change estimations of basic clocks to adjust the plants' development cycle, etc. From the inspected papers, a GSM and Arduino-based observing and controlling framework is used which sends ready message to administrators when estimations are outside explicit reaches. Graphical UIs are intended to show the data and information that could be separated from the framework [30]. The coordinated effort was utilizing Blynk, a multilanguage stage that empowers controllers of various microcontrollers like Arduino and Raspberry Pi [47]. A microcontroller along with a GSM receptor in a hydroponics framework is used. Accordingly, administrators can send messages to the receiver so continuous authority over the supply of water or temperature is attained [48]. An Arduino associated with a web worker through an Ethernet Shield, a UI was made to permit ongoing checking and control of the water-related sensor estimations, for example, switching on or off the fumes, siphons, and fog creators [38]. An IoT-based hydroponics framework that permits distant checking and control of the framework boundaries was made. The creators utilized a Modbus TCP standard convention to pull estimation information from the detecting hubs of an administrative PC [10]. A framework with a microcontroller associated with a Ubuntu IoT Cloud. The framework could be gotten to screen and control the boundaries consequently dependent on the detected inputs [49]. The creators in this segment added the controlling boundary into the situation. As of now, the perception of the boundaries in the framework is not sufficient and is important to control such boundaries for a superior framework.

Architecture has been implemented by different studies as shown in Figure 2. The aquaponics sensor mote consists of different sensors to monitor the environmental parameters and water which are required for the healthy development of the plants as well as fish. The data that is sensed from the different sensor motes are sent through wireless communication to the gateway. The gateway receives the data and provides the information from which sensor node the data has been received and displays it on the display unit.

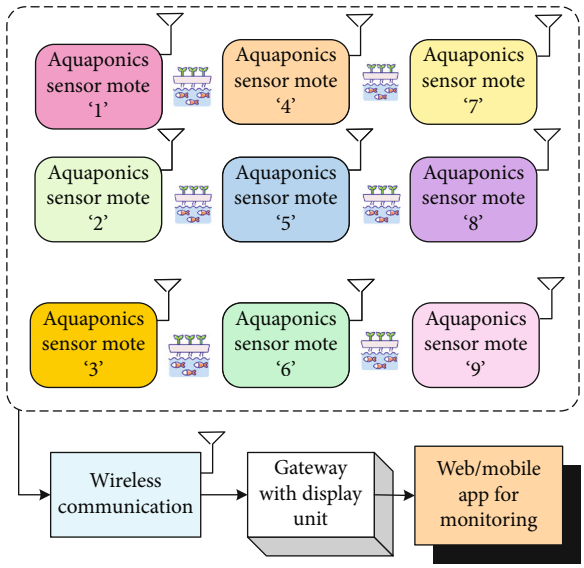


Figure 2: Remote monitoring of aquaponics system [50].

The data is then logged on the web or the mobile application Internet, and the user can monitor it from anywhere through the web/mobile app.

Table 2 illustrates the latest studies that is focused on IoT-based aquaponics platforms. From the table, it concludes that the majority of the studies implemented Wi-Fi as communication medium to transmit data to the cloud server for real-time monitoring and controlling. [51] implemented the edge computing technique in aquaponics with the ML for the automation in the aquaponics system; however, it is implemented in the small scale only. [52] implemented a technique for the optimization of the nutrients; however, they are no any information related to the data transmission from the Raspberry Pi to the cloud server. From the overall studies, it is identified that the customization hardware is necessary to carry out for meeting the requirements of aquaponics system.

In [54], the automatic triggering of a water pumping event has an accuracy of 0.9795 because of the ultrasonic sensor and soil moisture sensor, and in this study, the threshold for the intersection of union (IoU) is set to 0.5 to achieve higher accuracy, with an average precision (mAP) of 75.0 and an F1 score of 0.9556 [58]. The system appears to be functional based on the test results; nonetheless, several deviations are discovered, including an RTC test showing a delay time of 00.02.10 of RTC compared to the national standard time and an error of 2.4 percent identified on a calibrated TDS sensor testing [52]. When the lettuce's size and production were compared to those grown in uncontrolled aquaponics systems, the yield showed a considerable increase in size, with some of them reaching 40 to 45 inches in diameter, and also, the cost of managing nutritional parameters is reduced by more than 75%

4.3. Wireless Technologies. The remote innovations are seldom introduced and are generally connected to the two past areas. By the by, it was discovered that a few supporters were centered on creating some remote advances in aquaponics that improve availability. A design to screen and control a hydroponics framework with sensor data and Arduino is created. Information is effectively put away on WRT hubs and sent to OpenWrt workers utilizing the Wi-Fi module [41]. A hydroponics framework utilizing the 6LoWPAN convention and a remote sensor organization (WSN) was planned [59]. If pH and temperature values of the aquaponics exceed the threshold range [4], then GSM sends warnings to authorities and updates it on ThingSpeak. An online observing framework utilizing ThingSpeak IoT stage with Arduino Uno and ESP8266-01 that is Wi-Fi handset was built [23]. A Raspberry Pi alongside a Wi-Fi dongle to give a web network to the framework is used. The framework utilizes cloud-based stages for storing and controlling the assorted boundaries of the hydroponics framework [33]. The utilization of remote advances in the sensors or transmission of information makes way for enhancements in e-checking and control of boundaries. Table 3 illustrates the technical specifications of wireless communication protocol that can be implemented in IoT-based systems for aquaponics farming.

5. Edge-Assisted Architecture

Currently, the integration of a huge number of sensors and devices in the physical environment is generating a huge amount of data in the IoT. In traditional cloud computing, all data must be transmitted to centralized servers, and the findings must be transmitted downstream to the sensors and devices after computation [60]. This process imposes a significant load on the network, such as bandwidth, data transmission costs, and resources. Edge and fog computing overcome these challenges, as the data computation or storage is deployed at the edge of the network. Furthermore, the distributed architecture may control network traffic and prevent traffic peaks in IoT networks, lowering transmission latency between edge/cloudlet servers and end-users and reducing reaction times for real-time IoT applications when compared to standard cloud services [61]. A multilayered edge architecture is proposed to analyze the data between the cloud and the fog computing layers with low latency for IoT devices in real time [62]. An "offline-first" architecture for the low-cost and automated household aquaponics units is proposed. This moves the storage of data, machine learning, and computation away from the cloud platforms into the platforms that are preserving privacy [63].

Architecture is being implemented by different studies on edge-based computing as shown in Figure 3. The architecture consists of different sensor motes located at different locations. The sensor nodes consist of different sensors and actuators that are required for the sensing the different environmental and water-based that are required for the healthy growth of the plants and the fish. The data sensed by these sensors is sent to the edge computing node wirelessly. The data received is then analyzed and processed by the edge computing node, and also, predictive analytics is performed through computing, coprocessor, and AI model. From the

Table 2: Previous IoT-based platform for aquaponics.

Research	Objective	Advantage	Disadvantage
[53]	Automated aquaponics system to sense of pH, level, and temperature	Cloud server implemented to visualize the sensor data	Intel Edison microcontroller integrated is expensive
[54]	Automatic control of the aquaponics system using an ML algorithm	Edge computing is utilized to identify the parameter for the growth of plant and fishes	The proposed model is implemented in small scale, where the performance of system is skeptical
[55]	To control and monitor water quality and environmental parameters	Solar-based power supply for powering the nodes	Implementation of Wi-Fi in the sensor node increases the power consumption and also requires additional infrastructure for working on Internet
[56]	Remote monitoring systems using TDS sensor	Calibration of TDS sensors is carried out	Cloud server is missing in the IoT-based system
[57]	Optimizing nutrient supply using ML	Raspberry Pi is interfaced with Vernier sensors for the measurement of nutrients	No information available about data transmission and data storage

Table 3: Technical specifications of wireless communication IoT protocols.

Attributes	Zigbee	6LoWPAN	LoRa	Sigfox	NB-IoT
Frequency	868/915 MHz and 2.4 GHz	868/915 MHz and 2.4 GHz	915 MHz, 868 MHz, and 433 MHz	868/915 MHz	Licensed LTE bands
Modulation	Binary phase shift keying and quadrature phase shift keying	NA	Chirp spread Spectrum	Binary phase shift keying	Quadrature phase shift keying
Topology	Peer-to-peer, mesh, star, and tree	Mesh, star	Star of stars	Star	NA
Network	Personal area network	Personal area network	Low power wide area network	Low power wide area network	Low power wide area network
Standard	802.15.4	802.15.4	802.15.4 g	802.15.4 g	NA
Range of data transmission	10-50 meters	10-50 meters	5 km-20 km	10 km-40 km	1 km-10 km
Bitrate	20-250 kb/s	250 kb/s	50 kb/s	200 bp/s	200 kb/s

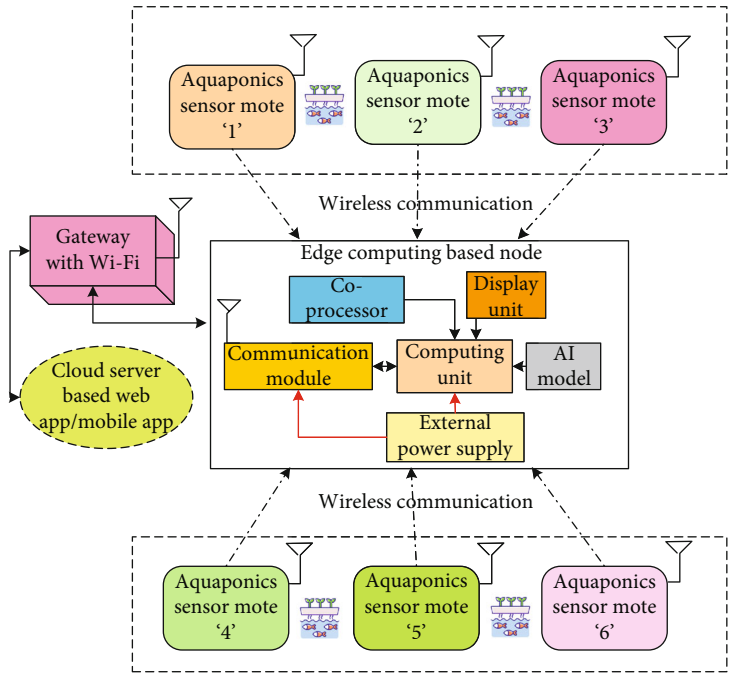


Figure 3: Edge-based computing node for real-time prediction for aquaponics.

edge computing node, the outcome/data is transmitted to the gateway. The gateway then analyzes the sensor node from which the data has been obtained, and using Wi-Fi, the data is sent to the cloud server.

6. Machine Learning Techniques Used in Aquaponics

Farmers can get more from the land by using resources sustainably with the help of artificial intelligence. Using artificial intelligence, farmers can know the conditions of temperature, weather, energy usage, water, and the condition of soil collected from their farm. Farmers are now able to use the sensor data that is captured to predict the yield and make them better equipped for natural disasters and climatic conditions using intelligent data processing techniques like machine learning. Machine learning is a branch of artificial intelligence that allows machines to learn from their mistakes. It uses computational approaches to learn directly from datasets rather than relying on a model of fixed equations.

A cloud-based monitoring system in aquaponics is developed which measures the temperature of the water, depth of water, and the value of dissolved oxygen. To monitor the fish activity, three infrared distance sensors were connected to the aquarium glass. Through the fish activity sensing, the fish metabolic rate was calculated using the regression analysis [64]. A real-time water quality monitoring system is developed based on assessing time series motion trajectories of live fish and using a neural network algorithm to estimate the frequency of pattern changes in these trajectories [65]. The author developed an ML-based IoT system for optimizing nutrient supply in the aquaponics system. The nutrient values were measured with Vernier sensors, and an actuator system was created to feed the nutrient into the environment in a closed loop. In this feature selection techniques like XG Boost classifier and recursive feature elimination with extra, tree classifier was used for ranking the features [66]. An aquaponics monitoring and control system is designed with fuzzy logic to evaluate the input and provide the proper outputs automatically. A genetic algorithm is used for the optimization of the parameters of the PDF and FPDF controllers. Better results were obtained in humidity and temperature control of the greenhouse when compared with the traditional PDF controller [67].

A method is proposed on Q-learning to get the control the factors that rely on the environment in the greenhouse and then combined with a CBR to get the optimal control of the temperature of the greenhouse [68]. A branch and bound search algorithm in a discrete model of the predictive control of greenhouse is proposed which reduced consumption of energy without affecting control accuracy [69]. A model is proposed based on a neural network based on the time series of a nonlinear autoregressive with a model based on external input. The control effect of humidity and temperature showed that the stability of the controller is more [70]. The Kalman filter algorithm was combined with the traditional PID control algorithm to control the temperature of the greenhouse which improved the control effect, the shorter response time and the higher system stability, and a better convergence [71]. Table 4 illustrates the ML model implementation in aquaponics for the water quality monitoring in the aquaponics system. Support vector machine (SVM), random forest (RF), k-nearest neighbor (k-NN), artificial neural network (ANN), Hammerstein-Wiener (HW), convolutional neural network (CNN), radial basis function (RBF), and recurrent neural network (RNN) are the few models that are addressed in the previous studies for water treatment and monitoring.

7. Recommendations

7.1. Sensors and Actuators. In an aquaponics system, the water-related and environmental parameters are to be monitored and controlled. In an aquaponics system, the sensors that are used to be much more accurate with less error because the development of plants as well as fish are affected if values are not accurate. The actuators should also be operated based on the sensor value obtained.

7.2. Communication Technologies. Wireless communication protocols play a very important role in monitoring the aquaponics units from a remote location. GSM/GPRS with personal area network technologies like Bluetooth and Zigbee is also used for transmission of the sensory data. The transmission range is limited to 100 m for these technologies. WPAN has the limitation of short-range, and GSM/GPRS has the limitation of high-power consumption. LoRa (long range) wireless communication overcomes these limitations in the technologies that have been used previously.

7.3. Edge and Fog-Based Vision Node. Edge and fog computing provides an opportunity for data processing in less time with enhanced latency. In aquaponics, the continuous monitoring of plants and fishes in terms of growth and health is highly demanded to enhance the better yield. To identify the growth and health of plants and fishes effectively, edge and fog-based vision nodes need to be incorporated. Edge and fog-based vision nodes enable to detect and predict the growth and diseases of fishes and plants in real-time.

7.4. ML Models for Prediction. Machine learning models have gained wide attention in the prediction of events based on real-time sensor data obtained from the sensors. In aquaponics, real-time prediction is highly required for maintaining the healthy growth of plants and fishes in order of enhancing productivity. The incorporation of the ML model in the vision node and edge-based sensor node enhances the system to predict depending on real-time image data and sensor data.

7.5. LoRa-Based Sensor Node and Gateway-Based Architecture. An architecture is proposed as shown in Figure 4. The proposed system consists of an aquaponics system to which different sensors are attached to sense the environmental parameters and also the water-based parameters such as humidity, temperature, light, pH, electrical conductivity, and water level. The sensors are altogether

Table 4: ML model implementation in the aquaponics system [72].

Model	Purpose	Application
SVM	Regression classification, supervised ML, and pattern analysis	Membrane-process parameter modeling, biological oxygen demand, dissolved oxygen modeling of rivers, aquaponics growth rate modeling
RF	Regression, classification, supervised ML	Adsorption process percent removal modeling, simple and hybrid dissolved oxygen modeling
k-NN	Classification, supervised ML	Classification of aquaponics growth phase
ANN	Regression, classification, supervised ML	Chlorine dosage/set-point, membrane-process parameter modeling and dissolved-oxygen concentration modeling
HW	Regression, ML model	Dissolved-oxygen concentration
CNN	Regression, classification, supervised ML, segmentation	DBP formation modeling
RBF	Regression, classification, ML function	Membrane-process parameter modeling, the adsorption process removal efficiency, and DBP formation modeling
RNN	Regression, classification, supervised ML	Suitable for time-series datasets and modeling, membrane-process parameter modeling, dissolve oxygen concentration modeling

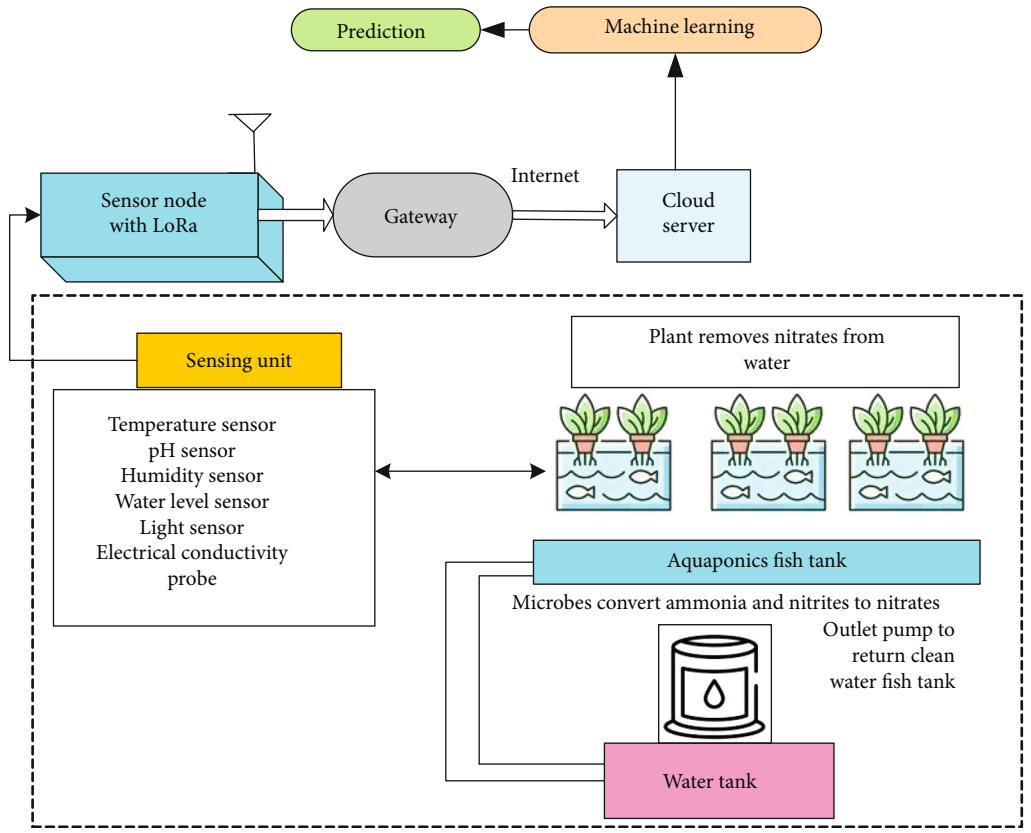


Figure 4: Proposed architecture for real-time prediction in aquaponics system.

considered a sensor node. The sensor node senses the required parameters from the different sensors. The sensed data from the different sensor nodes is collected, and the data is then sent with the help of a LoRa to the gateway. The gateway identifies the nodes from which the packets of data have been received and with the help of Wi-Fi connectivity is sent to the cloud server. The prediction is done on the data that is obtained from sensors using machine learning algorithms.

8. Conclusion and Future Scope

Food and agriculture are significant considerations that can meet the predicted food demand by the Food and Agriculture Organization (FAO) by 2050. Furthermore, the United Nations suggests that sensible water utilization through enhanced irrigation and storage technology, in conjunction with the creation of new drought-resistant crop types, can assist to sustain dryland output. Aquaponics is one of the

sustainable farming approaches that use a closed-loop and soil-less method, so wireless technologies must be integrated for real-time monitoring, controlling, and managing from any remote location. With the motivation of the above aspects, this study conducts a review of the aquaponics system, and from the review, it has identified different critical parameters that are required for the effective growth of plants and fishes. In addition to this, the study discusses the significance of wireless monitoring with the integration of sensors and communication technologies. Edge and fog computing-based architectures for the implementation of ML-based wireless systems in aquaponics for real-time prediction are also discussed. Finally, based on the review, the discussion on the limitations is presented and also recommended a few suggestions for future enhancement in aquaponics monitoring such as edge and fog-based vision nodes, ML models for prediction, LoRa-based sensor nodes, and gateway-based architecture.

Data Availability

The data presented in this study are available on request from the corresponding author.

Conflicts of Interest

The authors declare that there is no conflict of interest regarding the publication of this article.

Acknowledgments

The research was supported by the Universidad Europea del Atlántico, Santandar, Spain. The authors would like to thank and extend their kind support to the university.

References

[1] FAO - News article: 2050: a third more mouths to feedMay 2022, https://www.fao.org/news/story/en/item/35571/icode/.

[2] Food and agriculture projections to 2050 | Global Perspectives Studies | Food and Agriculture Organization of the United NationsMay 2022, https://www.fao.org/global-perspectives-studies/food-agriculture-projections-to-2050/en/.

[3] "Food security and nutrition and sustainable agriculture .:. Sustainable development knowledge platform," May 2022, https://sustainabledevelopment.un.org/topics/foodagriculture.

[4] Food security and nutrition and sustainable agriculture | Department of Economic and Social AffairsMay 2022, https://sdgs.un.org/topics/food-security-and-nutrition-and-sustainable-agriculture.

[5] B. König, J. Janker, T. Reinhardt, M. Villarroel, and R. Junge, "Analysis of aquaponics as an emerging technological innovation system," *Journal of Cleaner Production*, vol. 180, pp. 232–243, 2018.

[6] A. R. Yanes, P. Martinez, and R. Ahmad, "Towards automated aquaponics: a review on monitoring, IoT, and smart systems," *Journal of Cleaner Production*, vol. 263, p. 121571, 2020.

[7] A. J. van der Goot, P. J. M. Pelgrom, J. A. M. Berghout et al., "Concepts for further sustainable production of foods," *Journal of Food Engineering*, vol. 168, pp. 42–51, 2016.

[8] W. Kloas, R. Groß, D. Baganz et al., "A new concept for aquaponic systems to improve sustainability, increase productivity, and reduce environmental impacts," *Aquaculture Environment Interactions*, vol. 7, no. 2, pp. 179–192, 2015.

[9] S. A. Z. Murad, A. Harun, S. N. Mohyar, R. Sapawi, and S. Y. Ten, "Design of aquaponics water monitoring system using Arduino microcontroller," in *AIP Conference Proceedings*, vol. 1885no. 1, p. 020248, Ao Nang, Thailand, 2017.

[10] M. Manju, V. Karthik, S. Hariharan, and B. Sreekar, "Real time monitoring of the environmental parameters of an aquaponic system based on Internet of Things," in *2017 Third International Conference on Science Technology Engineering & Management (ICONSTEM)*, pp. 943–948, Chennai, India, 2017.

[11] Y. Wei, W. Li, D. An, D. Li, Y. Jiao, and Q. Wei, "Equipment and intelligent control system in aquaponics: a review," *IEEE Access*, vol. 7, pp. 169306–169326, 2019.

[12] F. Blidariu and A. Grozea, "Increasing the economical efficiency and sustainability of indoor fish farming by means of aquaponics-review," *Animal science and biotechnologies*, vol. 44, no. 2, pp. 1–8, 2011.

[13] M. A. Nichols and N. A. Savidov, "Aquaponics: a nutrient and water efficient production system," *II International Symposium on Soilless Culture and Hydroponics*, vol. 947, pp. 129–132, 2011.

[14] M. Odema, I. Adly, A. Wahba, and H. Ragai, "Smart aquaponics system for industrial Internet of Things," in *International Conference on Advanced Intelligent Systems and Informatics*, vol. 639, pp. 844–854, Cairo, Egypt, 2017.

[15] D. D. Kuhn, D. D. Drahos, L. Marsh, and G. J. Flick Jr., "Evaluation of nitrifying bacteria product to improve nitrification efficacy in recirculating aquaculture systems," *Aquacultural Engineering*, vol. 43, no. 2, pp. 78–82, 2010.

[16] pH meter | Definition, Principle, & Facts | BritannicaMar 2022, https://www.britannica.com/technology/pH-meter.

[17] N. M. Stone and H. K. Thomforde, *Understanding Your Fish Pond Water Analysis Report*, Cooperative Extension Program, University of Arkansas at Pine Bluff, US, 2004.

[18] T. Wada, *Theory and Technology to Control the Nutrient Solution of Hydroponics*, Plant Factory Using Artificial Light, Elsevier, 2019.

[19] C. Somerville, M. Cohen, E. Pantanella, A. Stankus, and A. Lovatelli, "Small-scale aquaponic food production: integrated fish and plant farming," *FAO Fisheries and Aquaculture Technical Paper*, vol. 589, 2014.

[20] M. A. Zamora-Izquierdo, J. Santa, J. A. Martínez, V. Martínez, and A. F. Skarmeta, "Smart farming IoT platform based on edge and cloud computing," *Biosystems Engineering*, vol. 177, pp. 4–17, 2019.

[21] J. P. Mandap, D. Sze, G. N. Reyes, S. M. Dumlao, R. Reyes, and W. Y. D. Chung, "Aquaponics pH level, temperature, and dissolved oxygen monitoring and control system using raspberry pi as network backbone," in *TENCON 2018-2018 IEEE Region 10 Conference*, pp. 1381–1386, Jeju, Korea (South), 2018.

[22] R. Sallenave, *Understanding Water Quality Parameters to Better Manage your Pond*, NM State University, Cooperative Extension Service, 2012.

[23] A. Bhatnagar and G. Singh, "Culture fisheries in village ponds: a multi-location study in Haryana, India," *Agriculture and Biology Journal of North America*, vol. 1, no. 5, pp. 961–968, 2010.

[24] A. Bhatnagar and P. Devi, "Water quality guidelines for the management of pond fish culture," *International Journal of Environmental Sciences*, vol. 3, no. 6, pp. 1980–2009, 2013.

[25] "Measuring dissolved oxygen - environmental measurement systems," Mar 2022, https://www.fondriest.com/environmental-measurements/measurements/measuring-water-quality/dissolved-oxygen-sensors-and-methods/.

[26] M. N. Mamatha and S. N. Namratha, "Design & implementation of indoor farming using automated aquaponics system," in *IEEE International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM)*, pp. 396–401, Chennai, India, 2017.

[27] B. Sreelekshmi and K. N. Madhusoodanan, *Automated Aquaponics System in Emerging Trends in Engineering, Science and Technology for Society*, Energy and Environment, CRC Press, 2018.

[28] R. V. Tyson, D. D. Treadwell, and E. H. Simonne, "Opportunities and challenges to sustainability in aquaponic systems," *HortTechnology*, vol. 21, no. 1, pp. 6–13, 2011.

[29] "Ammonia and ammonium ion measurement methods for water analysis," Mar 2022, https://www.ysi.com/parameters/ammonia.

[30] A. C. Anthonisen, R. C. Loehr, T. B. S. Prakasam, and E. G. Srinath, "Inhibition of nitrification by ammonia and nitrous acid," *Journal Water Pollution Control Federation*, vol. 48, pp. 835–852, 1976.

[31] J. M. Ebeling, M. B. Timmons, and J. J. Bisogni, "Engineering analysis of the stoichiometry of photoautotrophic, autotrophic, and heterotrophic removal of ammonia-nitrogen in aquaculture systems," *Aquaculture*, vol. 257, no. 1–4, pp. 346–358, 2006.

[32] S. Wongkiew, Z. Hu, K. Chandran, J. W. Lee, and S. K. Khanal, "Nitrogen transformations in aquaponic systems: a review," *Aquacultural Engineering*, vol. 76, pp. 9–19, 2017.

[33] D. C. Love, J. P. Fry, L. Genello et al., "An international survey of aquaponics practitioners," *PloS one*, vol. 9, no. 7, article e102662, 2014.

[34] A. M. Nagayo, C. Mendoza, E. Vega, R. K. Al Izki, and R. S. Jamisola, "An automated solar-powered aquaponics system towards agricultural sustainability in the Sultanate of Oman," in *IEEE International Conference on Smart Grid and Smart Cities (ICSGSC)*, pp. 42–49, Singapore, 2017.

[35] C. Maucieri, C. Nicoletto, R. Junge, Z. Schmautz, P. Sambo, and M. Borin, "Hydroponic systems and water management in aquaponics: a review," *Italian Journal of Agronomy*, vol. 13, no. 1, pp. 1–11, 2018.

[36] M. Mehra, S. Saxena, S. Sankaranarayanan, R. J. Tom, and M. Veeramanikandan, "IoT based hydroponics system using deep neural networks," *Computers and Electronics in Agriculture*, vol. 155, pp. 473–486, 2018.

[37] N. K. Jacob, "IoT powered portable aquaponics system," in *Proceedings of the Second International Conference on Internet of things, Data and Cloud Computing*, pp. 1–5, Cambridge, United Kingdom, 2017.

[38] T. Y. Kyaw and A. K. Ng, "Smart aquaponics system for urban farming," *Energy Procedia*, vol. 143, pp. 342–347, 2017.

[39] P. K. Weber-Scannell and L. K. Duffy, "Effects of total dissolved solids on aquatic organism: a review of literature and recommendation for salmonid species," *American Journal of Environmental Sciences*, vol. 3, 2007.

[40] "Global water, water instrumentation for environmental monitoring," Mar 2022, https://www.ysi.com/products/global-water.

[41] OMAFRA Crops Home PageMar 2022, http://www.omafra.gov.on.ca/english/crops/.

[42] B. Santhosh and N. P. Singh, "Guidelines for water quality management for fish culture in Tripura," *ICAR Research Complex for NEH Region, Tripura Center, Publication*, vol. 29, no. 10, 2007.

[43] W. Vernandhes, N. S. Salahuddin, A. Kowanda, and S. P. Sari, "Smart aquaponic with monitoring and control system based on IoT," in *2017 second international conference on informatics and computing (ICIC)*, pp. 1–6, Jayapura, Indonesia, 2017.

[44] J. C. Bakker, *Analysis of humidity effects on growth and production of glasshouse fruit vegetables ÇGOS~I*, 1991.

[45] D. Wang, J. Zhao, L. Huang, and D. Xu, "Design of a smart monitoring and control system for aquaponics based on OpenWrt," in *Proceedings of the 5th International Conference on Information Engineering for Mechanics and Materials*, vol. 21, pp. 937–942, Huhhot, Inner Mongolia, 2015.

[46] C. Barnes, T. Tibbitts, J. Sager et al., "Accuracy of quantum sensors measuring yield photon flux and photosynthetic photon flux," *HortScience*, vol. 28, no. 12, pp. 1197–1200, 1993.

[47] H. Werner, *Measuring Soil Moisture for Irrigation Water Management*, Cooperative Extension Service, South Dakota State University, US Department, 1992.

[48] P. Martinez, R. Ahmad, and M. Al-Hussein, "A vision-based system for pre-inspection of steel frame manufacturing," *Automation in Construction*, vol. 97, pp. 151–163, 2019.

[49] A. Dutta, P. Dahal, R. Prajapati, P. Tamang, and E. S. Kumar, "IoT based aquaponics monitoring system," in *1st KEC Conference Proceedings*, vol. 1, pp. 75–80, Lalitpur, Nepal, 2018.

[50] R. M. A. Haseeb-Ur-Rehman, M. Liaqat, A. H. M. Aman et al., "Sensor cloud frameworks: state-of-the-art, taxonomy, and research issues," *IEEE Sensors Journal*, vol. 21, no. 20, pp. 22347–22370, 2021.

[51] C. S. Arvind, R. Jyothi, K. Kaushal, G. Girish, R. Saurav, and G. Chetankumar, "Edge computing based smart aquaponics monitoring system using deep learning in IoT environment," *2020 IEEE Symp.Ser. Comput. Intell. SSCI*, vol. 2020, pp. 1485–1491, 2020.

[52] S. B. Dhal, K. Jungbluth, R. Lin et al., "A machine-learning based IoT system for optimizing nutrient supply in commercial aquaponic operations," vol. 22, pp. 1–14, 2022.

[53] P. M. Ferreira and A. E. Ruano, "Discrete model-based greenhouse environmental control using the branch & bound algorithm," *IFAC Proceedings*, vol. 41, no. 2, pp. 2937–2943, 2008.

[54] A. Manonmani, T. Thyagarajan, M. Elango, and S. Sutha, "Modelling and control of greenhouse system using neural networks," *Transactions of the Institute of Measurement and Control*, vol. 40, no. 3, pp. 918–929, 2018.

[55] Z. Gao, L. He, and X. Yue, "Design of PID controller for greenhouse temperature based on Kalman," in *Proceedings of the 3rd International Conference on Intelligent Information Processing*, pp. 1–4, Guilin, China, 2018.

[56] F. L. Valiente, R. G. Garcia, E. J. A. Domingo et al., "Internet of things (IOT)-based mobile application for monitoring of

automated aquaponics system," in *IEEE 10th Int. Conf. Humanoid, Nanotechnology, Inf. Technol. Commun. Control. Environ. Manag. HNICEM*, pp. 1–6, Baguio City, Philippines, 2018.

[57] T. Khaoula, R. A. Abdelouahid, I. Ezzahoui, and A. Marzak, "Architecture design of monitoring and controlling of IoT-based aquaponics system powered by solar energy," *Procedia Computer Science*, vol. 191, pp. 493–498, 2021.

[58] R. R. D. Isabella Wibowo, M. Ramdhani, R. A. Priramadhi, and B. S. Aprillia, "IoT based automatic monitoring system for water nutrition on aquaponics system," in *Journal of Physics: Conference Series*, vol. 1367, East Java, Indonesia, 2019.

[59] M. M. Elsokah and M. Sakah, "Next generation of smart aquaponics with Internet of Things solutions," in *19th International Conference on Sciences and Techniques of Automatic Control and Computer Engineering (STA)*, pp. 106–111, Sousse, Tunisia, 2019.

[60] W. Yu, F. Liang, X. He et al., "A survey on the edge computing for the Internet of Things," *IEEE Access*, vol. 6, pp. 6900–6919, 2018.

[61] J. Pitakphongmetha, N. Boonnam, S. Wongkoon, T. Horanont, D. Somkiadcharoen, and J. Prapakornpilai, "Internet of Things for planting in smart farm hydroponics style," in *International Computer Science and Engineering Conference (ICSEC)*, Chiang Mai, Thailand, 2016.

[62] K. S. Aishwarya, M. Harish, S. Prathibhashree, and K. Panimozhi, "Survey on automated aquponics based gardening approaches," in *2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT)*, pp. 1377–1381, Coimbatore, India, 2018.

[63] M. Ulum, A. F. Ibadillah, R. Alfita, K. Aji, and R. Rizkyandi, "Smart aquaponic system based Internet of Things," in *Journal of Physics: Conference Series*, vol. 1211no. 1, p. 012047, East Java, Indonesia, 2019.

[64] N. H. Kumar, S. Baskaran, S. Hariraj, and V. Krishnan, "An autonomous aquaponics system using 6LoWPAN based WSN," in *IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)*, pp. 125–132, Vienna, Austria, 2016.

[65] M. A. Romli, S. Daud, R. A. A. Raof, Z. A. Ahmad, and N. Mahrom, "Aquaponic growbed water level control using fog architecture," in *Journal of Physics: Conference Series*, vol. 1018no. 1, p. 012014, Kuching, Sarawak, Malaysia, 2018.

[66] M. Muneeb, K.-M. Ko, and Y.-H. Park, "A fog computing architecture with multi-layer for computing-intensive IoT applications," *Applied Sciences*, vol. 11, no. 24, p. 11585, 2021.

[67] P. Mpofu, S. H. Kembo, S. Jacques, N. Chitiyo, and C. Solar, "Utilizing a privacy-preserving IoT edge and fog architecture in automated household aquaponics," in *2nd African International Conference on Industrial Engineering and Operations Management, IEOM*, pp. 2281–2288, Harare, Zimbabwe, 2020.

[68] C. Lee and Y.-J. Wang, "Development of a cloud-based IoT monitoring system for fish metabolism and activity in aquaponics," *Aquacultural Engineering*, vol. 90, p. 102067, 2020.

[69] H. Ma, T.-F. Tsai, and C.-C. Liu, "Real-time monitoring of water quality using temporal trajectory of live fish," *Expert Systems with Applications*, vol. 37, no. 7, pp. 5158–5171, 2010.

[70] S. B. Dhal, M. Bagavathiannan, U. Braga-Neto, and S. Kalafatis, "Nutrient optimization for plant growth in Aquaponic irrigation using machine learning for small training datasets," *Artificial Intelligence in Agriculture*, vol. 6, pp. 68–76, 2022.

[71] M. A. Koutb, N. M. El-Rabaie, H. A. Awad, and I. A. Abd El-Hamid, "Environmental control for plants using intelligent control systems," *IFAC Proceedings*, vol. 37, no. 2, pp. 101–106, 2004.

[72] M. Lowe and R. Qin, "A review on machine learning , artificial intelligence , and smart technology in water treatment and monitoring," *Water*, vol. 14, pp. 1–28, 2022.

Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 2415726, 13 pages
https://doi.org/10.1155/2022/2415726

Research Article

Dermoscopic Image Classification Using Deep Belief Learning Network Architecture

Lubna Farhi,[1] **Saadia Mansoor Kazmi**,[1] **Hassan Imam**,[1] **Mejdal Alqahtani**,[2] **and Farhan Ur Rehman**[3]

[1]*Department of Electronic Engineering, Sir Syed University of Engineering and Technology, Karachi, Pakistan*
[2]*Industrial Engineering Department, College of Engineering, King Saud University, P.O. Box 800, Riyadh 11421, Saudi Arabia*
[3]*Department of Mechanical Engineering, University of Toronto, Toronto, Canada*

Correspondence should be addressed to Lubna Farhi; lubnafarhi@yahoo.com

Received 9 February 2022; Revised 11 April 2022; Accepted 18 April 2022; Published 25 May 2022

Academic Editor: Abdul Basit

In this paper, deep belief learning network architecture (DBL) is proposed for medical image classification in a bid to improve the diagnostics of dermal melanoma as an alternative to traditional dermoscopy. Preprocessing was carried out by using a linear Gaussian filter by eliminating high-frequency artifacts and distortion. The K-means segmentation technique was used to extract the region of interest. The DBL network was then applied to the segmented image for classification. The DBL architecture disperses the weights and hyperparameters to all positions in an image, making it possible to scale to various image sizes. The effects of overfitting were mitigated for small datasets and were achieved by optimizing the proposed network. The algorithm works effectively by fine-tuning constraints. The results showed an increase in the accuracy between the proposed model and AlexNet and LeeNet for segmented images from 8% to 47%, respectively. Similarly, an increase for nonsegmented images was observed between 2% and 48%. An average reduction of 47.8% and 41.5% in error for both segmented and nonsegmented images was recorded for dermal images. The execution time also decreased in comparison with the other architectures averaged by 8-13%, since the weights were distributed only on the clustered regions in the segmented image, as compared to the whole image thus allowing the network to classify it faster with improved accuracy.

1. Introduction

Dermal melanoma is one of the types of melanoma that is usually curable when detected and treated early. Once melanoma has spread deeper into the skin or other parts of the body, it becomes difficult to treat and can be deadly. Many people are dying in the world of skin cancer because dermal lesions are not diagnosed at an early stage. In 2020, there were between 2 and 3 million cases of skin cancer according to the World Health Organization (WHO) [1]. Early detection and accurate screening diagnostics all contribute to the prevention of skin cancer. Skin lesions appear differently from the normal appearance of skin due to various reasons, and the diagnosis can be exhaustive if done manually [2]. There is a need for a fast, accurate, and automated diagnostic process to resolve this issue. Dermal lesion segmentation and classification are an active research area where accuracy must be improved using a robust algorithm. Therefore, a lot must be done to improve the accuracy performance of automated dermal diagnosis.

Most CAD-based systems for both segmentation and classification methods use handpicked features to differentiate between normal skin and skin lesions [3]. These strategies executing on an established machine learning technique based on feature vectors are extraction and then applied to a classifier without rejecting the nature of those extracted features. However, such features are not able to identify melanoma due to differences in morphology, causing underperforming diagnosis from CAD systems [4]. Classification of melanoma is done by using a well-defined segmented area called the region of interest (ROI) to optimize the performance of these systems. It improves the classification capability, as the "region of interest" provides a better representation of melanoma attributes. The exact

classification of the melanoma skin lesions can be determined if the feature extraction steps specify only the affected area, as done by a skin specialist (dermatologist). When doing feature extraction, the addition of nonaffected skin lesion with affected skin lesion produces weak features, as the ROI is not targeted. Hence, classification results may be inaccurate. This is why segmentation is considered the first step before classification, to improve the performance of CAD systems. Another approach for designing task-adapted feature representations is to learn an architecture of increasingly complex features directly from its in-domain data [5].

Deep learning is an upgraded form of artificial neural networks since it comprises more layers that allow higher levels of abstraction and improved data predictions. Among the deep learning technologies, convolution neural networks (CNNs) have specifically proven themselves to be useful tools that are capable of handling a wide variety of computer vision tasks [6]. The success of the deep belief convolution network lies in its ability to autonomously learn midlevel and high-level abstractions from the analyzed image. This makes it a very effective tool that can be used for recognizing tumors and localization in natural images. A common CNN structure comprises multiple layers of convolution filters that are mixed with a multitude of data reduction or pooling layers. This allows the CNN to typically provide one or more probabilities or class labels as its output. In addition, the convolution filters are developed using a training dataset that educates the filters by allowing them to preprocess the image automatically without the need of tediously hand-crafting features that are application-specific [7].

Many researchers have focused on the segmentation and have not included the classification. Therefore, they have not covered the classification part which in itself is the next step [8]. Most of the researchers used standard networks for feature extraction and classification, i.e., AlexNet and U-Net [9]. Some do not have access to the published datasets, and some have worked for general imaging tasks. Most of these networks cannot give good results for dermoscopic images since dermal images are often of low quality and resolution as most are taken with mobile cameras and such. Since the adjacent and bordering pixels of an image have a similar intensity which brings about needleless load on the algorithm while the low quality of the image decreases the capability of the network in small-sized patches to learn global features [10].

Some researchers have focused on segmentation using window bounding boxes but are not achieving a precise boundary on the region of interest. Currently, there is a lot of focus on learning a maximum number of features in the area of digital imaging in a bid to improve the accuracy of detection by a convolutional neural network (CNN) architecture [11, 12]. However, most of them agree that convolutional neural network (CNN) architecture is capable to extract notable features of images quite efficiently. To start with, the most noteworthy challenge faced by CNNs is the lack of labeled training data. CNNs need data of substantial amounts that are clearly labeled for training, and many studies have been conducted on limited datasets thereby not achieving desired results [13]. It is very difficult to arrange this data due to the expense of interpretation from derma specialists and huge variants of the same skin disease [14]. Deep belief network's CNN needs numerous tunings in the network architecture as a result of overfitting and convergence issues. This tuning is done to the parameters of the network so that a comparable learning speed between all layers is achieved. Table 1 summarizes the previous works' methodologies and shortcomings.

This study is an attempt to propose a dermascopic image classification using deep belief learning convolution neural network architecture. We intend to identify and classify dermal lesions using K-means clustering segmentation that not only satisfies the highest accuracy but also reduces the execution time for all types of medical images in comparison with other architectures that have been made. Our contributions to this research are as follows:

(1) The proposed architecture is a convolution neural network for medical images using a deep belief network for small datasets. This architecture is easy to train low-resolution images

(2) It will remove overfitting and convergence problems for small datasets

(3) The algorithm is more scalable by using probabilistic pooling and weight sharing

(4) The speed and accuracy of inference needed to create a percept have also been improved. Since neurons only communicate in their stochastic binary state, the communication has also been made simple

(5) This presented a comparison of the results between the proposed network architecture and prior models for segmented and nonsegmented images showing that the former provides better features and improved accuracy in dermal image classification

This paper is organized as follows. Section 1 gives an introduction and discusses previous related work. Section 2 highlights the major mathematical methods. Section 3 shows the simulation setup. Section 4 has results and discussion in which the performance of the proposed algorithm is evaluated and the results are shown. Lastly, Section 5 presents the conclusion.

2. Methodology

2.1. Preprocessing. The first step in deep learning is to make the available dataset clean and present it in a useable manner to improve the intensities of an image with complete information and better resolution. This is done through preprocessing techniques. It is necessary to have a good quality image before segmentation is done to obtain accurate and precise results. In the presented approach, the input image is passed through a low-pass Gaussian filter to remove high-frequency artifacts thus improving the image quality through noise elimination, contrast enhancement, intensity equalization, and outlier removal. Additionally, the Gaussian distribution in 1D and 2D cases is shown in

Table 1: Summary of the related previous works.

S. no.	Author	Title	Methodology description	Shortcomings
1	Nida et al. 2019 [15]	"Melanoma lesion detection and segmentation using deep region based convolutional neural network and fuzzy C-means clustering"	A deep region-based convolutional neural network (RCNN) precisely detects the multiple affected regions in the form of bounding boxes that simplify localization through fuzzy *C* -mean (FCM) clustering"	The study is focused only on segmentation based on window bounding boxes, not on precise boundaries around the region of interest. Secondly, this did not work on classification
2	Al-Masni et al. 2020 [16]	"Multiple skin lesions diagnostics via integrated deep convolutional networks for segmentation and classification"	The authors propose an integrated diagnostic framework that combines a skin lesion boundary segmentation stage and a multiple skin lesion classification stages	The labeled skin lesion images utilized for both the training and testing were still limited in size
3	Adegun et al. 2021 [17]	"A probabilistic-based deep learning model for skin lesion segmentation"	"The authors employ an efficient mean-field approximate probabilistic inference approach with a fully connected conditional random field that utilizes a Gaussian kernel"	Here they have analyzed and segmented skin lesion images, but no classifying has been done
4	Seeja and Suresh 2019 [18]	"Deep learning based skin lesion segmentation and classification of melanoma using support vector machine (SVM)"	"The authors propose a convolutional neural network (CNN) based U-Net algorithm used for segmentation process. After feature extraction, it was fed to various classifiers"	Here the classifying is done using only one unit, and the depth is only up to 4 convolution steps
5	Liu et al. 2021 [19]	"Skin lesion segmentation using deep learning with auxiliary task"	"The authors have proposed CNN architecture using auxiliary information along with edge prediction simultaneously with the segmentation task"	The proposed method fails when the foreground region contains a dark area surrounded by an area with light color, whose appearance is more similar to the healthy skin region

Table 2: Proposed DBL network architecture.

Layer	Layer type	No. vol	Kernel size	Stride
1	Convolution 1 +ReSF	96	9 × 9	4
2	Probabilistic pooling		3 × 3	1
3	Convolution 2 +ReSF	512	7 × 7	1
4	Probabilistic pooling		3 × 3	1
5	Convolution 3 +ReSF	384	5 × 5	1
6	Convolution 4 +ReSF	384	3 × 3	1
7	Convolution 5 +ReSF	256	3 × 3	1
8	Probabilistic pooling		3 × 3	1
9	3× fully connected	4096 hidden units		

$$G(x) = \frac{1}{\sqrt{2\pi}\sigma} e^{-x^2/2\sigma^2}, \tag{1}$$

$$G(x, y) = \frac{1}{2\pi\sigma^2} e^{-\left(x^2+y^2\right)/2\sigma^2}. \tag{2}$$

The standard deviation of the distribution is σ. Isotropic Gaussian of 2D cases is circularly symmetric [20].

2.2. Segmentation. The K-means clustering method is broadly used to separate data into two or more clusters. It uses a process known as clustering to gather all the data points that have similar feature vectors in one cluster while grouping all the other data points that have dissimilar feature vectors in different clusters. K-means has a vital role in determining the difference between signal intensities of pixels in different clusters, providing a change estimation of intensities after evaluating parenchymal regions and finding connections between the morphovariations and the variations of strict parameters [21].

The K-means procedure is as follows:

Input data points x_1, x_2, x_3, x_n, and the number of clusters needed is the value of K:

(i) Pick K points as the initial centroids from the dataset, either randomly or the first K

(ii) Find the Euclidean distance of each point in the dataset with the identified K points (cluster centroids)

(iii) Assign each data point to the closest centroid using the distance found in the previous step

(iv) Find the new centroid by taking the average of the points in each cluster group

(v) Repeat (ii) to (iv) for a fixed number of iterations or till the centroids do not change

The Euclidean distance between two points p and q where $p = (p1, p2)$ and $q = (q1, q2)$,

$$d(p, q) = \sqrt{(q_1 - p_1)^2 + (q_2 - p_2)^2}. \tag{3}$$

Assign each point to the nearest cluster: if each cluster centroid is denoted by c_i, then each data point x is assigned to a cluster where distance is the Euclidean distance and S_i is the set of all points assigned to the i^{th} cluster.

$$J = \arg\ \min_{c_i \in C} \text{dist}(c_i, d)^2. \tag{4}$$

To find the new centroid from the clustered group of points where S_i is the set of all points assigned to the ith cluster,

$$c_i = \frac{1}{|S_i|} \sum_{x_i \in S_i} d_i. \tag{5}$$

Derma images are distinguished on the basis of signal intensity received from different tissues in the image. These signal intensities play a vital role in identifying and sorting the pixels into different clusters and giving a change estimation of intensities after studying dermal tissues and finding connections between the dermoscopic lesion structural variations and the variations of strict parameters [22].

2.3. Proposed Deep Belief Learning Network. Deep learning is a branch of artificial neural networks, most often used in image processing and object recognition. They are also known as space or shift-invariant artificial neural networks due to the shared-weight architecture of the convolution filters or kernels that slide along input features and give us feature maps by providing interpreted equivariant responses. The advantage of convolutional network architecture is that it converts the output of one filter applied to the subsequent layer thereby extracting valuable features of the image. The result of applying the filters to an input image is captured by the feature maps; i.e., at each layer, the feature map is the output of that layer. In neural networks, a feature map comprises a layer of hidden neurons where each coordinate represents an individual neuron. The approach used by algorithms of deep learning is to use a network of parameters that are organized by layers. Except for the input and output layers, the rest of the layers are known as hidden layers. The kernel's size determines the receptive field of that neuron and also indicates the weights of the connections between the layers of neurons as well as the neurons in the previous layer. We find that every kernel has tuned to a different orientation, spatial scale, and frequency in accordance with the training data statistics learned kernels which are comparable to edge detectors [23].

Gradient descent is used to train deep networks in a bid to reduce a predefined cost function of the output layer and is shown as the negative log-likelihood function. Among a plentitude of deep network models, the type known as deep

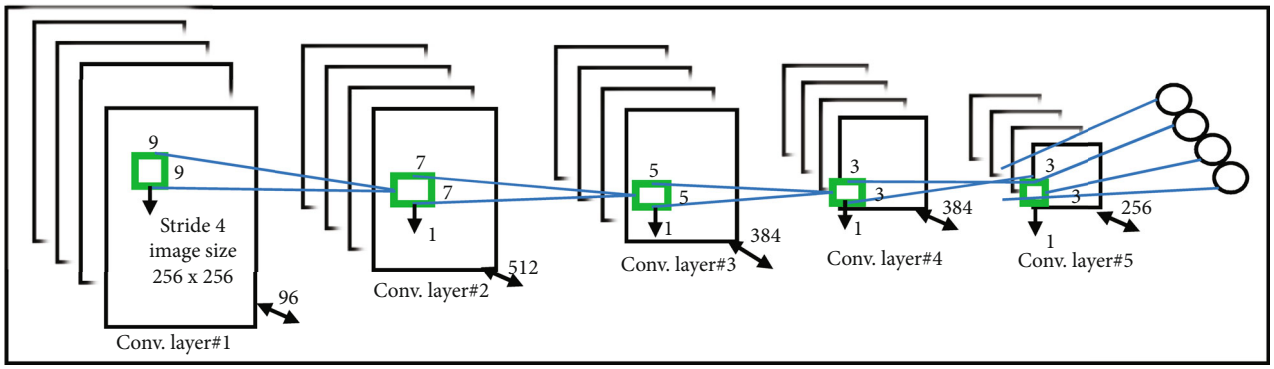


Figure 1: Proposed DBL network architecture.

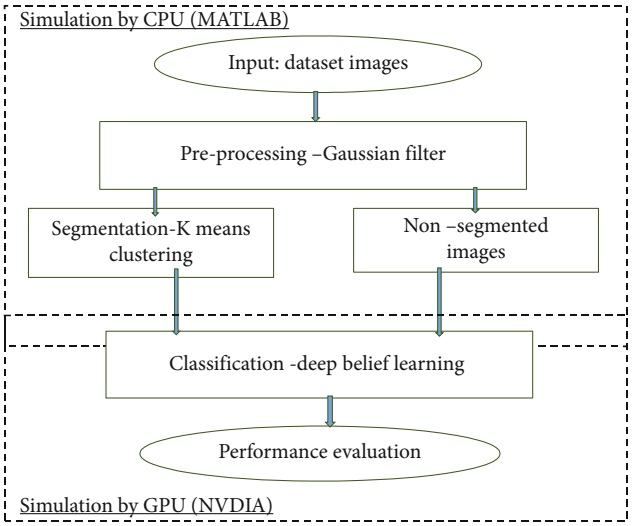


Figure 2: Simulation diagram of methodology.

belief network (DBN) architecture is the one in which each layer is initialized as a restricted Boltzmann machine (RBM) hence minimizing the RBM input energy function [24]. Since both kinds, i.e., DBNs and RBMs, do not work with the 2D structure of images to extract a given feature, the weights that are required need to be learned one by one for each pixel. This restriction results in exhaustive scaling of these network models to full camera images because of increased computational complexity. To overcome this limitation, the deep belief learning (DBL network) was employed for derma images. In this network, convolution is used to distribute the hyperparameters among all locations in an image thus allowing inferences to be done efficiently. Hence, it is due to the intrinsic nature of this network that entire images can be scaled by this model. The DBL network utilizes convolution in a deep belief restricted Boltzmann machine (DBRBM), akin to restricted Boltzmann machine (RBM) in most ways, but the weights in the DBL networks' visible and hidden layers are distributed between all pixels of an image [25].

The proposed multilayer perceptron (MLP) architecture of DBLCNN as described in Table 2 as shown in Figure 1 is quite different from the high-performance CNN models. Instead of applying correspondingly large receptive fields in the first convolution layer, e.g., 11×11 with stride 4 or s with stride 2, the input image size is $256 \times 256 \times 3$ with 96 kernels of size $9 \times 9 \times 3$ with a stride of 4 pixels which are convolved with the input at every four pixels. Our configuration is different from previous architectures in such a way that first, we have incorporated five nonlinear rectification layers instead of one, which makes the decision function more discriminative. Secondly, it controls the number of parameters by using comparatively small filter sizes and stride sizes; i.e., the 1st convolution layer has 9×9, the second convolution layer has 7×7, the third convolution layer has 5×5, and the last two convolution layers have the same size 3×3 with k channels. The first convolution layer stack is parametrized by $9^2k^2 = 81k^2$ weights while the second convolution layers require $7^2k^2 = 49k^2$ parameters; similarly, third layer parameters are $5^2k^2 = 25k^2$, and the last two convolution layers have $3^2k^2 = 9k^2$ parameters.

Small-size convolution filters have been previously used, but the nets of the proposed model are significantly deeper than theirs, and they did not evaluate images either.

The proposed architecture is similar in that it is based on very deep DBL network net with small convolution filters and the weight matrix connecting with probabilistic max-pooling. The network topology is more straightforward than other models, and this allows the net to be expanded into a deeper network in a simpler way.

Let the probabilistic statistics for restricted Boltzmann machine with binary hidden units and visible units be m and v, respectively. The probability is determined by the combined configuration of the visible and hidden units. Every possible combined configuration of the visible and hidden units has an energy as given in the equation below:

$$P(v, m) = \frac{1}{z} \exp\left(-E(v, m)\right), \tag{6}$$

where z is the partition function.

Hence, the energy function of the DBL network is

$$E(v, m) = -\sum_{i=1}^{k} \sum_{j=1}^{n_m} \sum_{r,s=1}^{n_w} m_{ij}^{k} w_{rs}^{k} v_{i+r-1,j+s-1} - \sum_{k=1}^{k} b_k \sum_{i,j=1}^{n_h} m_{ij}^{k} - d \sum_{ij=1}^{n_v} vij, \tag{7}$$

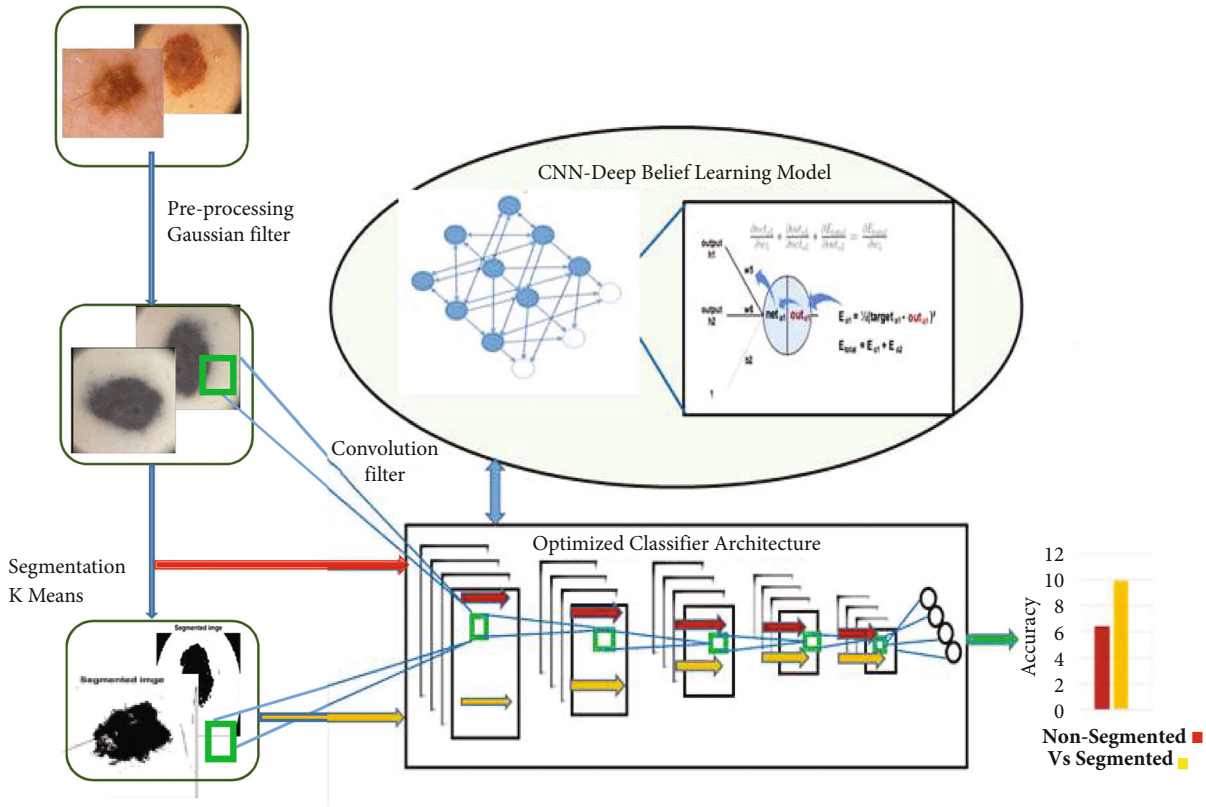


Figure 3: Proposed deep belief learning network framework.

(a) (b) (c)

Figure 4: PH^2 dataset images: (a) low contrast irregular; (b) hair and hair bubbles; (c) fuzzy borders of skin lesion.

where the hidden and visible units are m and v, respectively, and d_{jj} and b_k are the visible and hidden unit biases, respectively.

From the energy function, Gibbs sampling uses the following conditional distributions over visible and hidden layers.

$$P\left(m_{ij}^{k}=\frac{1}{v}\right)=f\sum_{k}\left(\left(w_k * v\right)_{ij}+b_k, \tag{8}$$

$$P\left(v_{ij}^{k}=\frac{1}{m}\right)=f\sum_{k}\left(\left(w_k * v\right)_{ij}+d_{ij}, \tag{9}$$

where f is the rectified unit function.

2.3.1. Rectified Unit (Activation Function). Rectified units are an important function of the design of a convolutional neural network. The activation function for output layers depends on the type of classification problem. In the proposed work, the logistic sigmoid activation function (Gibbs sampling) is the basis for the learning algorithm. The output function of a neuron for its input of x is $f(x)$.

$$f(x)=\frac{1}{\left(1+e^{-x}\right)}. \tag{10}$$

The sigmoid function maps $[-\infty,+\infty] \longrightarrow [0, 1]$. Saturation is prevented if the required targets are L2-normalized because at $f(\pm 1)=\pm 1$, linearity is at its maximum. These saturating nonlinearities are much slower than the nonsaturating nonlinearities, in the course of training time with gradient decent [26].

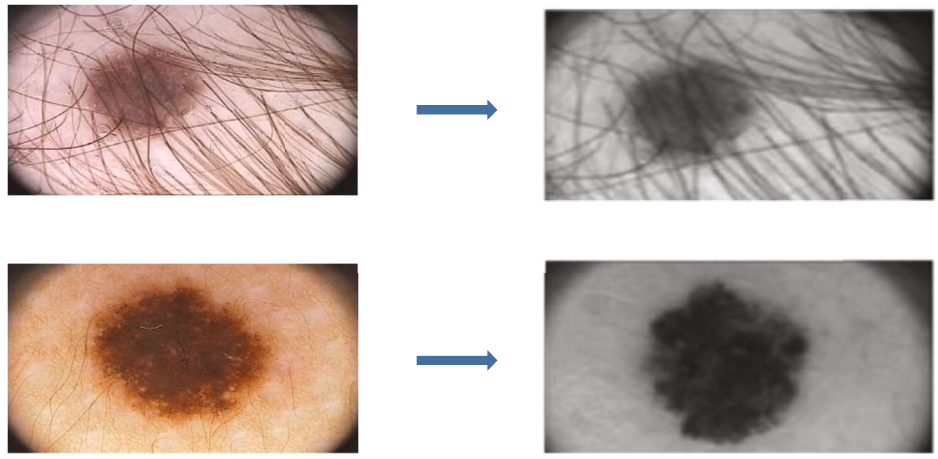


Figure 5: Preprocessing using the Gaussian filter.

2.3.2. Learning Rate and Epoch. The learning rate controls how quickly the model is adapted to the problem. Smaller learning rates require more training epochs given the smaller changes made to the weights in each update, whereas larger learning rates result in rapid changes and require fewer training epochs.

The learning rate is controlled by

$$\rho = \frac{\mu_0}{(1 + \delta t)}, \tag{11}$$

where "initial rate" is μ_0, "decrease constant" is δ, and t is the "epoch/stage"; depending on these parameters, the learning rate ρ can be increased or decreased. The learning rate for each parameter determines the error of the classifier network [27].

2.3.3. Batch Size. The batch size is the number of training samples considered when the optimization solver is updated once. Before choosing a certain batch size, several factors are kept in consideration, i.e., the computational cost and the uncertainty of update from a small batch to a large batch.

A smaller batch size produces more noise as compared to a larger batch size. However, in the presence of a large number of minima in the error function, the model may get stuck in the first minima it encounters. Hence, an ideal batch size needs to be chosen that will optimize the model by introducing more noise in the model estimate of the gradient. This noise can then be utilized to push the model out of some shallow valleys in the error function [28].

2.4. Performance Evaluation Parameters. When in the training phase, there is a vital role of accuracy measurement for architecture selection; to maximize prediction accuracy on training samples, the parameters need to be selected. In the end, in the result of the learning step, accuracy is measured to assess the architecture's predictive ability on new data. There is a risk to overfit training data as learning algorithms are trained on finite samples: the model might memorize the training samples instead of learning a general rule, i.e., the data generating model. Hence, an index of the model generalization ability having high accuracy on unseen data is a measure of the robustness of classifiers. Factors affecting accuracy of models are overfitting and underfitting. Overfitting happens when the model learns noise instead of showing the true relationship. When the training error is much lower than the generalization or testing error, the model predicted is said to be overfitted, and underfitting happens when a model is unable to capture the underlying pattern of the data. These models usually have high bias and low variance [29].

2.4.1. Accuracy. In this study of a diagnostic test to discriminate between subjects affected by a disease dermal melanoma, i.e., atypical and benign, i.e., common disease,

(i) the number of correctly classified melanoma is the true positives or TP

(ii) the number of correctly classified benign is the true negatives or TN

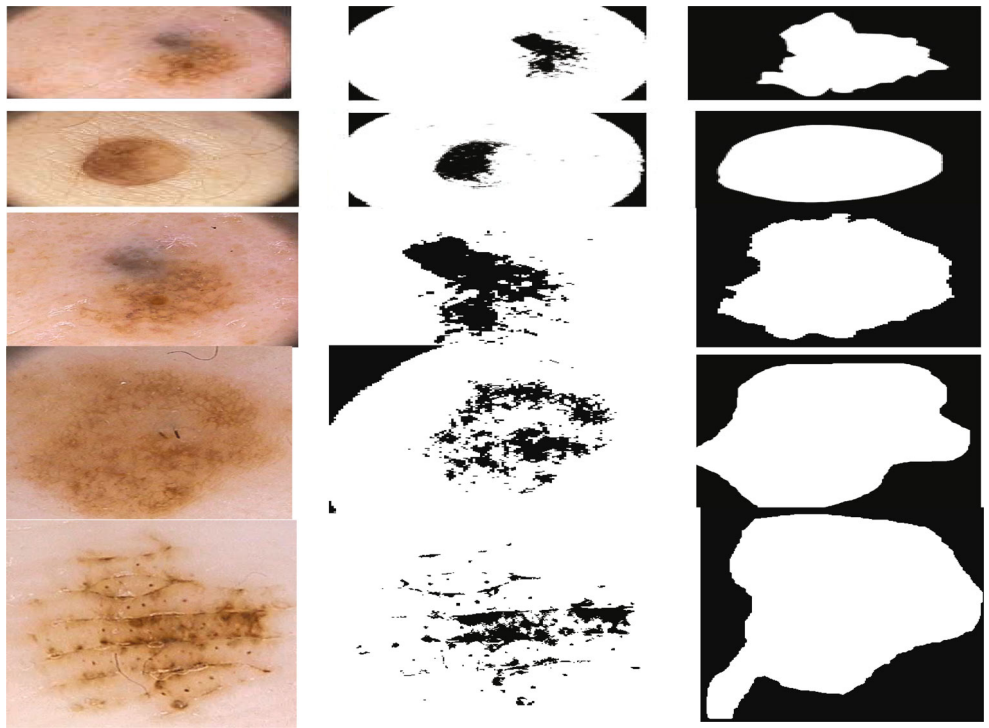
(iii) the number of controls classified as melanoma is the false positives or FP

(iv) the number of patients classified as benign is the false negatives or FN

Hence, accuracy is determined by the below equation [30]:

$$\text{Accuracy} = \frac{(\text{TP} + \text{TN})}{(\text{TP} + \text{TN} + \text{FP} + \text{FN})}. \tag{12}$$

2.4.2. Error/Loss. The selection of the output layer activation function is linked with the error or loss. The output layer activation function is the identity, or the linear activation function as the output is a simple function of the inputs. The output of the activation function is not restrained to a fixed range, hence suitable to address the regression problem. Let the training



(a) (b) (c)

Figure 6: (a) Original image (nonsegmented). (b) K-means segmented images. (c) Truth image.

Table 3: Comparison using Dice and Hausdorff methods with the truth image.

Derma Dataset	Dice similarity index (%)	Hausdorff distance (mm)
IMD076	63.8	0.56
IMD139	72.6	0.48
IMD155	75.3	0.58
IMD170	71.5	0.54
IMD018	73.3	0.51

dataset be $u = [u_1, u_2, u_3 \cdots u_i]$, having the corresponding output vectors as $v = [v_1, v_2, v_3, \cdots, v_j]$; then, backpropagation loss or error is formalized into an equation shown below, where the network output is $m_{w,\,b}(u)$ and w is the weight vector.

$$\mathrm{SSE}(\theta) = \frac{1}{2}\sum_{i=1}^{n} \left\| h_{w,b}(u_i) - v_i \right\|^2. \quad (13)$$

This is commonly called the "sum of squares error function." In binary classification, we have an error function or a "cross entropy error function" as shown below:

$$\mathrm{CE}(\theta) = -\sum_{i=1}^{n} \{ v_j \ln m(u_i) + (1 - v_i) \ln (1 - m(x_i)) \}. \quad (14)$$

3. Simulation Setup

The flowchart in Figure 2 outlines the simulation setup of dermal image classification using the deep belief learning classifier that has been implemented for this work. The preprocessing and segmentation have been done using MATLAB simulation whereas the classifying process has been carried using NVIDIA 'DIGITS'.

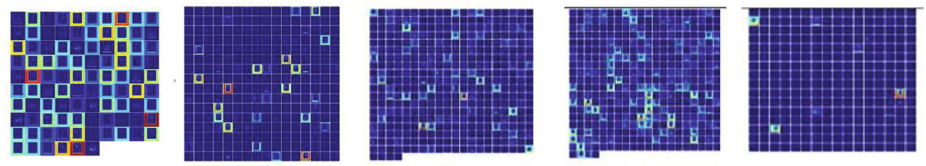
4. Results and Discussions

The proposed DBL network classifier framework is shown in Figure 3.

The PH^2 dataset includes various images of dermal lesion comprising common and atypical dermascopic images as shown in Figure 4. For the purposes of validation and the evaluation of the proposed network, a reliable ground truth image database is needed. A ground truth image database is a vital requisite, specifically in the field of dermoscopy. The compilation of the truth data is a task that must be done by a derma specialist. Each dermascopic image is to be manually segmented and annotated. For the implementation, the PH^2 dermascopic image database was used as a ground truth. The database contains a total number of 200 dermal lesions, including 100 common images and 100 atypical images [7].

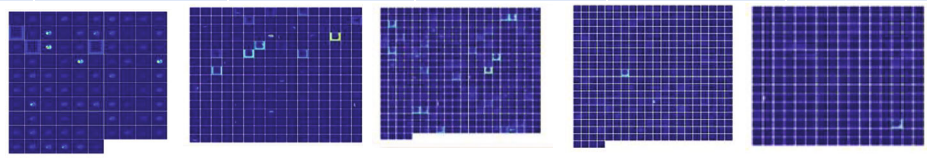
According to the classification scale of the Fitzpatrick skin type [31], all dermoscopic images are from either skin type II or III. Therefore, in the PH^2 dataset, the skin colors are represented from white to cream white. In this research, the images of the database were prudently chosen by

Non-segmented images



	Conv. 1	Conv. 2	Conv. 3	Conv. 4	Conv. 5
Parameters	11, 712	307, 456	865, 129	663, 936	442, 624
Mean	39.55	2.62	1.05	0.53	0.02
Std deviation	56.46	10.73	2.90	0.97	0.16

Segmented images



	Conv. 1	Conv. 2	Conv. 3	Conv. 4	Conv. 5
Parameters	11, 712	307, 456	865, 129	663, 936	442, 624
Mean	7.79	0.54	0.41	0.13	0.014
Std deviation	30.54	3.14	1.23	0.40	0.12

Figure 7: A pictorial interpretation of results for nonsegmented and segmented dermal lesion images.

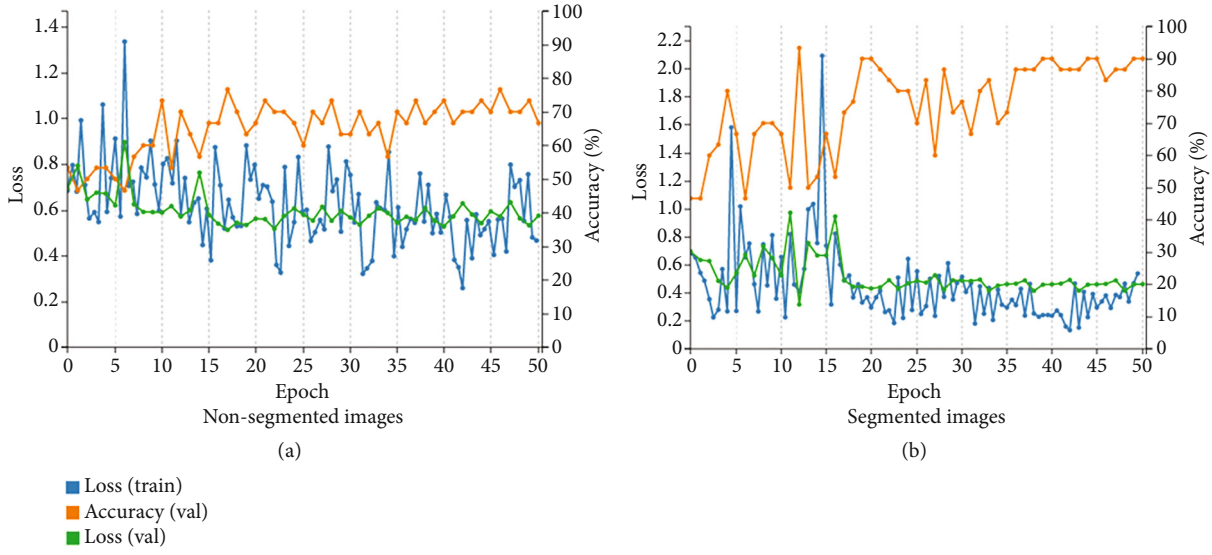


Figure 8: DBL classifier performance accuracy and loss graphs of (a) nonsegmented images and (b) segmented images.

considering their quality, resolution, and dermoscopic features. Using the somewhat standard thumb rule for deep belief learning, 70% of the images were used for training, 15% were used for validation, and the remaining 15% were used for testing. The NVIDIA deep learning GPU system was used for training and testing. The program is run on 'DIGITS'. "DIGITS simplifies common deep learning tasks such as managing data, designing and training neural networks on multi-GPU systems, monitoring performance in real time with advanced visualizations, and selecting the best performing model from the results browser for deployment. DIGITS is completely interactive so that engineers can focus on developing and teaching networks rather than programming and debugging." This method teaches and applies multilayered artificial neural networks to realize any objective or goal independent of human intervention. DBLs that are used for image classification normally use a fused combination of CNN and completely connected layers. Here, the tiled artificial neurons are applied where the fully connected layers react to visual fields of overlapping areas.

4.1. Preprocess the Images. The first step was to create and set up the dataset and preprocess the images; for this, we used a Gaussian filter which is basically a low-pass digital filter in order to remove the highest and lowest intensities from the images effectively. Having completed the preprocessing,

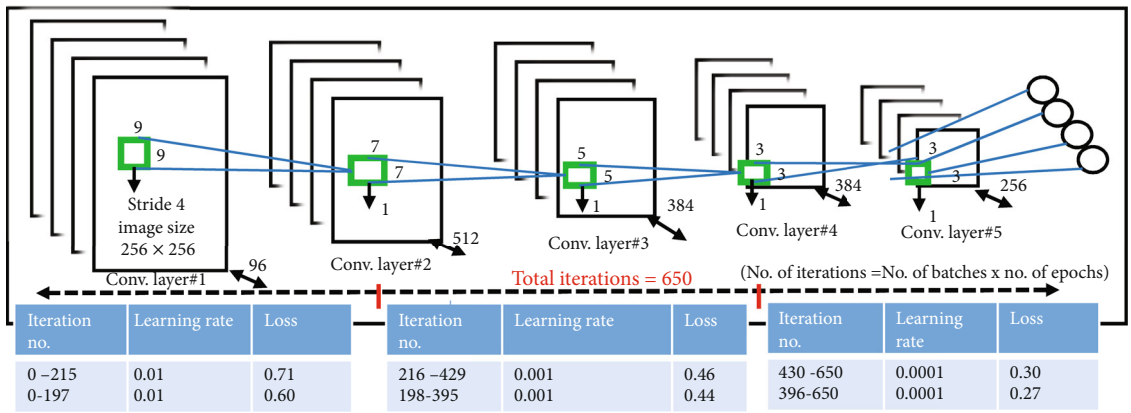


Figure 9: DBL network with iteration results.

Table 4: Performance comparison of the classifier.

Model	Accuracy (%) Maximum average	Error/loss (%) Maximum average	Execution time (sec)
Original images	76.7 73.3	76 53	370
Segmented images	93 90	31 46	340

Table 5: Comparison of cutting edge architecture models with the proposed DBL network.

	Model	Nonsegmented images Accuracy (%)	Nonsegmented images Error (%)	Segmented images Accuracy (%)	Segmented images Error (%)
Dermal dataset (200) images)	DBL model (proposed).	73.7	38.0	90.0	31.0
	DCNN model (AlexNet)	55.6	44.4	62.2	60.1
	CNN model (LeeNet)	50.1	89.0	49.2	87.0
	Probabilistic-based deep learning model	51.4	48.6	61.1	38.9
	Convolutional neural network- (CNN-) based U-Net algorithm	49.3	57.7	66.5	33.5

different routes or methods were then applied to evaluate the accuracy and effectiveness of deep belief network learning models. First, the images were passed through a Gaussian filter; then, the preprocessed derma images were used to train and test the deep belief learning classifier. Some results can be seen in Figure 5.

4.2. Segmentation. After the preprocessed images were segmented via the K-means segmentation method, the output of the K-means method was applied to the same deep belief learning classifier. Initially, the output of the segmentation steps, obtained through the K-means algorithm, has been compared with the truth images as shown in Figure 6.

The two methods, Dice similarity and Hausdorff distance, were then employed to assess and compare the accuracy of the segmented and nonsegmented images.

The Dice similarity and Hausdorff distance methods were used to show the accuracy of the segmented image.

The Dice similarity coefficient (DSC) was used as a statistical validation metric to evaluate the performance of the segmented image and the spatial overlap accuracy of automated probabilistic fractional segmentation of images. The Dice coefficient lies in the range $[0, 1]$ and has value 0 if there is no overlap between the two images and 1 if both images are identical. Hausdorff distance computes the shape similarity between the segmented image and ground truth image. The function computed the average distance from a point on the truth image to the closest point on the segmented image for forward and reverse distances, and the output distance was the minimum value from both distances; the lower the distance value, the better the match [32]. That method gives interesting results, even in the presence of noise or occlusion (when the target is partially hidden). The comparison is shown in Table 3.

4.3. Classification. In order to realize the best precision using tuning parameters, the classifier optimization is done first. The main tuning parameters for convolution are the batch size, learning rate, epochs, and kernel size. The final classification from the two routes (segmented and nonsegmented)

was then compared based on several performance-related aspects. The test results achieved after going through the above-described techniques have been applied. Then, the support vector machine classifier was trained using the stochastic gradient descent where the momentum was set to 0.9 and the weight decay value was set to 0.0005. Here, it was determined that the weight decay with respect to the network's ability to learn is important in this regard. This is because it lessens the training error that we come across in the network. A Gaussian distribution of zero mean with standard deviation of 0.01 was used to initialize the weights as well. Then, for all layers of the network, the same learning rate was used. Figure 7 shows the inference results.

We followed an experimental process in which we divided the learning rate by 10 each time; no enhancement was observed in the validation error rate as well as the current learning rate. The learning rate was started with the value of 0.01 and was reduced three times and then discontinued.

In the experimental trials, the batch size was selected to be 10 for 50 epochs. The DBL network classifier model was applied on both the nonsegmented and segmented images after optimizing all the constraints. Figure 8 shows a graph plotted to compare accuracy and loss (validation and testing loss) along for epochs for segmented and nonsegmented images.

The architecture employed for the classifier comprised five convolutional layers with kernel sizes of 9, 7, 5, 3, and 3 for each layer (for both segmented and nonsegmented images). In the DBL network, Figure 9 shows the classifier's results in the form of learning rates and loss as well as a close look at the iterations.

The general trend can be seen from the figures given in Table 4 that the average and maximum accuracy of the segmented dermal images is more than that of the nonsegmented images; similarly, the loss is lesser. Hence, the execution time for the same epochs is lesser for segmented images than for nonsegmented images thus indicating a reduced computational load.

During the training and testing time, we ran our models on the GPU in order to exploit its computational speed, reducing the execution time further. We noted that the segmented images used in the classifier model were processed 8-10 times faster than the nonsegmented classified model. Predictions for one image with the DBL model take on average 4 minutes.

As mentioned above, the accuracy, error, and execution time of the proposed DBL network were observed for the proposed classifier architecture between the segmented and nonsegmented images. Then, the performance was compared with respect to the AlexNet classifier architecture which was also carried out. Table 3 shows a comparison of implemented DBL network architecture vs. the AlexNet architecture. As can be seen from the table, the AlexNet is also a good choice for classification; however, it is hard to train low-resolution images (neurons die quickly), it has overfitting problems for small datasets, and it needs an improvement in computation.

The implemented DBL network has the following characteristics such as an improved feature space, the initial layers learning 1st-order generic features (e.g., edge detectors or color blob detectors), later layers learning higher-order features, the DBL network for joint configuration, and layers having faster convergence. Table 5 shows the performance of some commonly used deep CNN models being currently used. It is quite obvious from the results that for the derma images or 2D, the DBL network classifier surpasses most of the recent architectures for this dataset.

5. Conclusion

In this work, we have presented an optimized deep belief learning network model on dermal images for melanoma detection thereby improving classification accuracy and reducing execution time. In conclusion, the outcome of this work has indicated that the accuracy of classification of the proposed network for nonsegmented images increased within 2% to 48% when compared with AlexNet and LeeNet, and similarly for segmented images, there was an increase within 8% to 47%. We also observed that the average error for the dermal nonsegmented and segmented images was reduced within 47.8% and 41.5%. The execution time for the proposed classifier was also observed to have an average decrease within the range of 8-13% when compared with the other classifier models on dermal images. The final deduction is that as the distribution of weights in the segmented image was specifically on the clustered areas, instead of the whole image, the network had less work to do and was able to improve the accuracy as well as work faster. The presented work can improve the dermoscopic image classification complementing the doctors' capability to detect and analyze dermal images leading to a more authentic diagnosis. As a result, the diagnostic process can be less tedious, less expensive, and timely for the concerned patient.

Data Availability

We used the PH^2 dermoscopic image database.

Conflicts of Interest

We wish to confirm that there are no known conflicts of interest associated with this publication, and there has been no significant financial support for this work that could have influenced its outcome. We confirm that the manuscript has been read and approved by all named authors and that there are no other persons who satisfied the criteria for authorship but are not listed. We further confirm that the order of authors listed in the manuscript has been approved by all of us. We confirm that we have given due consideration to the protection of intellectual property associated with this work and that there are no impediments to publication, including the timing of publication, with respect to intellectual property. In so doing, we confirm that we have followed the regulations of our institutions concerning intellectual property. We further confirm that any aspect of the work covered in this manuscript has not involved either experimental animals or human patients. We understand that the corresponding author is the sole contact for the editorial

process (including editorial manager and direct communications with the office). She is responsible for communicating with the other authors about the progress, submissions of revisions, and final approval of proofs. We confirm that we have provided a current, correct email address which is accessible by the corresponding author and which has been configured to accept email.

Acknowledgments

The authors extend their appreciation to King Saud University for funding this work through Researchers Supporting Project number RSP2022R426, King Saud University, Riyadh, Saudi Arabia.

References

[1] https://seer.cancer.gov/statfacts/html/melan.html/.

[2] J. Gao, L. Wang, C. Xia et al., "Cold atmospheric plasma promotes different types of superficial skin erosion wounds healing," *International Wound Journal*, vol. 16, no. 5, pp. 1103–1111, 2019.

[3] A. Selvia, V. N. Prakash, N. Saravanan, B. Jawahar, and V. Karthick, "Skin lesion detection using feature extraction approach," *Annals of the Romanian Society for Cell Biology*, vol. 25, no. 4, pp. 3939–3951, 2021.

[4] I. Bakkouri and K. Afdel, "Computer-aided diagnosis (CAD) system based on multilayer feature fusion network for skin lesion recognition in dermoscopy images," *Multimedia Tools and Applications*, vol. 79, no. 29, pp. 20483–20518, 2020.

[5] H. Hu, A. Liu, Q. Zhou, Q. Guan, X. Li, and Q. Chen, "An adaptive learning method of anchor shape priors for biological cells detection and segmentation," *Computer Methods and Programs in Biomedicine*, vol. 208, p. 106260, 2021.

[6] A. Brunetti, D. Buongiorno, G. F. Trotta, and V. Bevilacqua, "Computer vision and deep learning techniques for pedestrian detection and tracking: a survey," *Neurocomputing*, vol. 300, pp. 17–33, 2018.

[7] W. Liu, Z. Wang, X. Liu, N. Zeng, Y. Liu, and F. E. Alsaadi, "A survey of deep neural network architectures and their applications," *Neurocomputing*, vol. 234, pp. 11–26, 2017.

[8] M. Kumar, M. Alshehri, R. AlGhamdi, P. Sharma, and V. Deep, "A DE-ANN inspired skin cancer detection approach using fuzzy C-means clustering," *Mobile Networks and Applications*, vol. 25, no. 4, pp. 1319–1329, 2020.

[9] Y. Bengio, N. Boulanger-Lewandowski, and R. Pascanu, "Advances in optimizing recurrent networks," in *2013 IEEE International Conference on Acoustics, Speech and Signal Processing*, pp. 8624–8628, Vancouver, BC, Canada, 2013.

[10] R. Baig, M. Bibi, A. Hamid, S. Kausar, and S. Khalid, "Deep learning approaches towards skin lesion segmentation and classification from dermoscopic images review," *Current Medical Imaging*, vol. 16, no. 5, pp. 513–533, 2020.

[11] L. Farhi, A. Yusuf, and R. H. Raza, "Adaptive stochastic segmentation via energy-convergence for brain tumor in MR images," *Journal of Visual Communication and Image Representation*, vol. 46, pp. 303–311, 2017.

[12] P. Tang, Q. Liang, X. Yan et al., "Efficient skin lesion segmentation using separable-Unet with stochastic weight averaging," *Computer Methods and Programs in Biomedicine*, vol. 178, pp. 289–301, 2019.

[13] A. Karpathy, J. Johnson, and L. Fei-Fei, "Visualizing and understanding recurrent networks," 2015, http://arxiv.org/abs/1506.02078.

[14] M. Goyal, A. Oakley, P. Bansal, D. Dancey, and M. H. Yap, "Skin lesion segmentation in dermoscopic images with ensemble deep learning methods," *IEEE Access*, vol. 8, pp. 4171–4181, 2020.

[15] N. Nida, A. Irtaza, A. Javed, M. H. Yousaf, and M. T. Mahmood, "Melanoma lesion detection and segmentation using deep region based convolutional neural network and fuzzy C-means clustering," *International Journal of Medical Informatics*, vol. 124, pp. 37–48, 2019.

[16] M. A. Al-Masni, D.-H. Kim, and T.-S. Kim, "Multiple skin lesions diagnostics via integrated deep convolutional networks for segmentation and classification," *Computer methods and programs in biomedicine*, vol. 190, p. 105351, 2020.

[17] A. A. Adegun, S. Viriri, and M. H. Yousaf, "A probabilistic-based deep learning model for skin lesion segmentation," *Applied Sciences*, vol. 11, no. 7, p. 3025, 2021.

[18] R. D. Seeja and A. Suresh, "Deep learning based skin lesion segmentation and classification of melanoma using support vector machine (SVM)," *Asian Pacific journal of cancer prevention: APJCP*, vol. 20, no. 5, pp. 1555–1561, 2019.

[19] L. Liu, Y. Y. Tsui, and M. Mandal, "Skin lesion segmentation using deep learning with auxiliary task," *Journal of Imaging*, vol. 7, no. 4, p. 67, 2021.

[20] L. Farhi, H. Abbasi, and R. Rehman, "Smart identity management system by face detection using multitasking convolution network," *Security and Communication Networks*, vol. 2021, 11 pages, 2021.

[21] T. N. Tete and S. Kamlu, "Detection of plant disease using threshold, k-mean cluster and ANN algorithm," in *2nd international conference for convergence in technology (I2CT)*, Mumbai, India, 2017.

[22] H. Wu, J. Pan, Z. Li, Z. Wen, and J. Qin, "Automated skin lesion segmentation via an adaptive dual attention module," *IEEE Transactions on Medical Imaging*, vol. 40, no. 1, pp. 357–370, 2021.

[23] Y. Tian, "Artificial intelligence image recognition method based on convolutional neural network algorithm," *IEEE Access*, vol. 8, pp. 125731–125744, 2020.

[24] M. R. Izadi, Y. Fang, R. Stevenson, and L. Lin, "Optimization of graph neural networks with natural gradient descent," *2020 IEEE international conference on big data (big data)*, pp. 171–179, Atlanta, GA, USA, 2020.

[25] Y. Zhang, H. Qu, C. Chen, and D. Metaxas, "Taming the noisy gradient: train deep neural networks with small batch sizes," *The Twenty-Eighth International Joint Conference on Artificial Intelligence (IJCAI)*, 2019.

[26] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," *Nature*, vol. 521, no. 7553, pp. 436–444, 2015.

[27] N. S. Zghal and N. Derbel, "Melanoma skin cancer detection based on image processing," *Current Medical Imaging*, vol. 16, no. 1, pp. 50–58, 2020.

[28] A. Ozdemir and K. Polat, "Deep learning applications for hyperspectral imaging: a systematic review," *Journal of the Institute of Electronics and Computer*, vol. 2, no. 1, pp. 39–56, 2020.

[29] Y. Hua, J. Guo, and H. Zhao, "Deep belief networks and deep learning," in *In Proceedings of 2015 International Conference on Intelligent Computing and Internet of Things*, pp. 1–4, Harbin, 2015.

[30] L. Farhi and A. Yusuf, "Comparison of brain tumor MRI classification methods using probabilistic features," in *13th IASTED International Conference on Biomedical Engineering (Bio Med)*, pp. 55–62, Innsbruck, Austria, 2017.

[31] L. Yu, H. Chen, Q. Dou, J. Qin, and P. A. Heng, "Automated melanoma recognition in dermoscopy images via very deep residual networks," *IEEE Transactions on Medical Imaging*, vol. 36, no. 4, pp. 994–1004, 2017.

[32] C. Liu, S. J. Gardner, N. Wen et al., "Automatic segmentation of the prostate on CT images using deep neural networks (DNN)," *International Journal of Radiation Oncology • Biology • Physics*, vol. 104, no. 4, pp. 924–932, 2019.

Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 4553502, 9 pages
https://doi.org/10.1155/2022/4553502

Research Article

A Hybrid Model for Intrusion Detection in IoT Applications

Mohammed I. Alghamdi

Department of Engineering and Computer Sciences, Al-Baha University, Al-Baha City 1988, Saudi Arabia

Correspondence should be addressed to Mohammed I. Alghamdi; mialmushilah@bu.edu.sa

Received 19 February 2022; Revised 11 April 2022; Accepted 25 April 2022; Published 14 May 2022

Academic Editor: Muhammad Imran

Internet of Things (IoT) networks has recently become an important component of smart cities, smart buildings, health care, and other applications. It finds it beneficial due to the inherent characteristics of low cost, compact, and low-powered IoT devices. At the same time, security remains a challenging issue in the design of IoT networks. Intrusion detection systems (IDS) can be used to identify the occurrence of intrusions in the network, i.e., abnormal activities in the network. The latest advances in machine learning (ML) and metaheuristics can be employed to design effective IDS models for IoT networks. This article develops a novel political optimizer with cascade forward neural network (PO-CFNN-)-based IDS in the IoT environment. The major intention of the PO-CFNN technique is to determine the occurrence of intrusions from the IoT environment. The PO-CFNN technique follows three major processes, namely, preprocessing, classification, and parameter optimization. Initially, the networking data is preprocessed to transform it into a useful format. Following that, the CFNN technique is employed for the identification and classification of intrusions in the IoT environment. In the final stage, the PO algorithm is applied for the optimal adjustment of the parameters involved in the CFNN model. The experimental validation of the PO-CFNN technique on a benchmark dataset stated the better outcomes of the PO-CFNN technique over recent approaches.

1. Introduction

In the digital era, the Internet of Things (IoT) is known as the most interesting advancement. The web permits associated gadgets to develop dramatically each day, and it has been suggested that more than 75 billion Internet of Things (IoT)-connected devices to be in use by 2025; according to current projections as of 2019, the installed base of IoT devices had grown by approximately thrice [1, 2]. The IoT innovation's motivation is to interconnect all objects to make all PCs smarter and make it safer to speak with people. Sensors and organizations permit everything to speak with one another straightforwardly to trade basic data [2]. Later on, it is conceivable through machine-to-machine (M2M) correspondence [3]. Various down-to-earth IoT applications can be utilized practically in many fields, like shrewd city applications (brilliant homes, savvy networks, medical services, and others), where those applications work on personal satisfaction [4]. The idea of the intrusion identification framework (IDS) aims to distinguish a danger or intrusion into the organization, and it effectively tracks the organization by recognizing likely occasions and logging data about them by halting episodes. The intrusion detection and prevention system (IDPS), which is a mix of two frameworks used to screen events happening in an organization and assess them for potential infringements or occurrences in security strategies, is the most common way of performing intrusion recognition and stopping to identify episodes [5]. Involving the IoT framework in numerous application areas like medical services, smart homes, shrewd industry, nature observing, and others gives critical advantages to the IoT framework. IoT security issues are a huge concern, which are classification, honesty, accessibility, and approval [6]. The combination of true articles with IoT, in any case, raises the scope of cybersecurity dangers every day.

Cyberspace is a fairly weak foundation, not intended to do what it does today, and on which increasing usefulness is constructed [7]. The way that the web is utilized for a wide range of basic activities at the level of people, firms, associations, and even countries has drawn in a wide range of malevolent activities. Cyberattacks can affect a wide range of structures. The issue is how to treat them. For some

different types of assault, discovery is an issue and, here and there, the primary issue. Part of the problem is that intrusion detection systems (IDS) are used to alert clients or organizations that they are under attack, or, as in the case of web applications, may not include any malware, but it depends on how a convention is handled [8].

Involving AI in intrusion discovery is not new. To be sure, it is now many years old, nearly as old as the field of intrusion detection, for example. Today, AI is not utilized strongly in intrusion identification. It is self-evident that AI could work on fundamentally improving the presentation of IDS, but what is subtler is how to operationalize this thought. There are a few explanations behind that [9]. The main one is that AI is a troublesome subject, a long way from being an adult and just security individuals appear to be keen on involving AI in intrusion identification. Individuals associated with AI appear to be substantially more intrigued by different applications, albeit in numerous ways that cybersecurity should be a characteristic space of utilization for AI [10]. The issue might lie more with cybersecurity than with the AI group. Cybersecurity extends the impression of a turbulent world without intelligence and lacking codification [11].

The authors in [12] presented several kinds of attacks in the IoT environment, and a *distributed denial-of-service* (DDoS) is a vulnerable attack. Blockchain (BC) is used to design a model for secure IoT networks and is employed for cryptocurrency transactions. A new BIoTIDS technique is derived to identify the existence of intrusions by the use of BC. It can determine the occurrence of intrusions from the IoT networks and detect DDoS attacks. Sarhan et al. [13] proposed and evaluated a standard NIDS feature set depending upon NetFlow network metadata gathering status. A set of two NetFlow enabled feature set versions are employed. Next, the authors in [14] proposed a novel feature selection for IDS by the use of information gain (IG) and gain ratio (GR) with the top 50% of features to detect DoS as well as DDoS attacks. The presented model has obtained an optimal subset of features by the use of insertion and union operations on subsets offered by the top 50% of IG and GR features. The authors in [15] presented a novel unified IDS model for the IoT environment for securing the network from various kinds of attacks, such as exploits, DoS, probes, and generics.

This article develops a novel political optimizer with cascade forward neural network (PO-CFNN-)-based IDS in the IoT environment. The major intention of the PO-CFNN technique is to define the occurrence of intrusions in the IoT environment. The PO-CFNN approach follows three major processes, namely, preprocessing, classification, and parameter optimization. Initially, the networking data is preprocessed to transform it into a useful format. Following that, the CFNN technique is employed for the identification and classification of intrusions in the IoT environment. In the final stage, the PO algorithm is applied for the optimal adjustment of the parameters involved in the CFNN technique. The experimental validation of the PO-CFNN technique on a benchmark dataset stated the better outcomes of the PO-CFNN technique over recent approaches.

2. The Proposed Model

In this study, a novel PO-CFNN approach has been developed for the identification and classification of intrusions in the IoT environment. The PO-CFNN technique follows three major processes, namely preprocessing, classification, and parameter optimization. Firstly, the networking data is preprocessed to transform it into a useful format. Then, the CFNN technique is employed for the identification and classification of intrusions in the IoT environment. In the end, the PO algorithm is used to find the best way to change the parameters in the CFNN model. CFNM-based Intrusion Detection and Classification.

During this phase, the CFNN approach was utilized for the identification and classification of intrusions in the IoT environment [16, 17]. The perceptron connection has been developed between input and output through the process of straight linking. Nonetheless, the FFNN connection intended between input and output was an ambiguous link. The linking is nonlinear in shape using an activation function from the hidden state. The system with an ambiguous link between the output and input layer was intended once the association process on perceptron and multilayer systems was collective. The system intended by this technique is called cascade forward neural network (CFNN).

$$y = \sum_{i=1}^{n} f^{i}\omega_i^i x_i + f^o\left(\sum_{j=1}^{k}\omega_j^o f_j^h\left(\sum_{i=1}^{n}\omega_{ji}^h x_i\right)\right), \tag{1}$$

whereas f^{i} indicates the activation function in the input to output layers as well as ω_i^i characterizes the weight from the input to output layers. The activation function and bias and input layer from the hidden layer denote ef^{h}:

$$y = \sum_{i=1}^{n} f^{i}\omega_i^i x_i + f^o\left(\omega^b + \sum_{j=1}^{k}\omega_j^o f^h\left(\omega_j^b + \sum_{i=1}^{n}\omega_{ji}^h x_i\right)\right). \tag{2}$$

Here, the CFNN model was executed in time sequence information. Hence, the neuron from the input layer is intervals of time sequence $X_{t-1}, X_{t-2}, \cdots, X_{t-p}$; however, the output is the existing information X_t.

Consider that going to weight vector ω of length s represents the collection of network weights and the objective function as $e = 1/2(X_t - \widehat{X})^2$.

Described Q was a positive matrix of size $s \times s$, whereas $\mathrm{Q}^{\mathrm{T}} = Q$. The stage of the method for conjugate gradient optimization is defined below:

Set $k = 0$, and choose the primary point $\Omega^{(0)}$.

Estimate the weight gradient.

$$g^{(0)} = \frac{\partial e}{\partial \omega^{(0)}} = \frac{\partial e}{\partial \omega}\bigg|_{\omega=\omega^{(o)}} = \left[\frac{\partial e}{\partial \omega_1^{(0)}} \;\; \frac{\partial e}{\partial \omega_s^{(0)}}\right]^T. \tag{3}$$

Once $g^{(0)} = 0$ afterward stop, and it gained an optimum weight $= \Omega^{(0)}$. Or else, set $d^{(0)} = g^{(0)}$.

Estimate $\alpha_k = \text{argmin}_{\alpha \geq 0} e(\omega^{(k)} + \alpha d^{(k)}) = -\, g^{(k)T} d^{(k)} / d^{(k)T} Q d^{(k)}$.

Estimate $\Omega^{(k+1)} = \Omega^{(k)} + \alpha_k d^{(k)}$.

Estimate $g^{(k+1)} = \partial e / \partial \omega^{(k+1)}$, if $g^{(k+1)} = 0$ stop and the optimal weight is $\omega^{(k+1)}$.

Estimate

$$\beta_k = \frac{g^{(k+1)T} Q d^{(k)}}{d^{(k)T} Q d^{(k)}} \tag{4}$$

Estimate $d^{(k+1)} = -g^{(k+1)} + \alpha_k d^{(k)}$.

$k = k + 1$; go to step 3.

As for the FFNN, the iteration method to weight searching on CFNN is typically termed as an epoch. Assume that the highest amount of epochs represent K. Once the iteration termination criteria could not be occurred, still the epoch$k = K$, and subsequently, the iteration method is ended. Substituting the procedure of $Qd\,(k)$ with another procedure such as the Hestenes-Stiefel model, especially, the technique $Qd^{(k)}$ is substituted with $(g^{k+1} - g^k)/\alpha_k$.

$$\beta_k = \frac{g^{(k+1)T} \left[g^{(k+1)} - g^{(k)} \right]}{d^{(k)T} \left[g^{(k+1)} - g^{(k)} \right]}. \tag{5}$$

For determining the optimum weight of the CFNN, the PO approach is employed and in that way enhances the classifier accuracy.

2.1. PO-Based Parameter Optimization. Finally, the PO algorithm is applied for optimal adjustment of the parameters contained in the CFNN model [18, 19]. PO approach is encouraged by *b*, the western political optimization algorithm which comprises 2 features. The primary statement that all the citizens try to enhance their helpfulness to win the election. PO has been comprised of 5 phases, namely, election campaign, party switching, interparty election, parliamentary affairs, party establishment, and constituency apportionment. The entire population is divided into n political parties, as follows:

$$P = \{P_1, P_2, P_3, \cdots, P_n\}. \tag{6}$$

All the parties include n party members that are given as

$$P_i = \left\{ p_i^1, p_i^2, p_i^3, \cdots, p_i^n \right\}. \tag{7}$$

All the party members induce d dimension as shown as

$$p_i^j = \left[p_{i,1}^j, p_{i,2}^j, p_{i,3}^j, \cdots, p_{i,d}^j \right]^T. \tag{8}$$

Al solutions are election candidates. Consider n electoral district as follows:

$$C = \{C_1, C_2, C_3, \cdots, C_n\}. \tag{9}$$

Assume there is a n member in all the constituencies.

$$c_j = \left\{ p_1^j, p_2^j, p_3^j, \cdots, p_n^j \right\}. \tag{10}$$

The party leader is described by the member as optimum fitness.

$$q = \text{argmin}_{1 \leq j \leq n} f\left(p_1^j \right), \forall i \varepsilon \{1, \cdots, n\}, \tag{11}$$

$$p_i^* = p_i^q. \tag{12}$$

All the party leaders are shown as

$$P^* = \{p_1^*, p_2^*, p_3^*, \cdots, p_n^*\}. \tag{13}$$

The winner of the constituency is named a member of parliament.

$$C = \{c_1^*, c_2^*, c_3^*, \cdots, c_n^*\}. \tag{14}$$

It is possible to split the population into n constituencies, and each constituency has n political parties, where $n = \sqrt{\text{Pop.Size}}$ as seen in Figure 1.

In the election campaign stage, the below equations are utilized to update the position of the probable solution.

$$p_{i,k}^j(z+1) = \begin{cases} \text{if } p_{i,k}^j(z-1) \leq p_{i,k}^j(z) \leq m^* \text{or} p_{i,k}^j(z-1) \geq p_{i,k}^j(z) \geq m^*, \\ m^* + r\left(m^* - p_{i,k}^j(z) \right); \\ \text{if } p_{i,k}^{\text{i}}(z-1) \leq m^* \leq p_{ik}^{\text{i}}(z) \text{or} p_{i,k}^{\text{i}}(z-1) \geq m^* \geq p_{i,k}^{\text{i}}(z), \\ m^* + (2r-1)\left| m^* - p_{i,k}^j(t) \right|; \\ \text{if } m^* \leq p_{i,k}^{\text{i}}(z-1) \leq p_{i,k}^{\text{i}}(z) \text{ or } m^* \geq p_{i,k}^{\text{i}}(z-1) \geq p_{i,k}^{\text{i}}(z), \\ m^* + (2r-1)\left| m^* - p_{ik}^l(z-1) \right|. \end{cases} \tag{15}$$

$$p_{i,k}^j(z+1) = \begin{cases} \text{if } p_{i,k}^j(z-1) \leq p_{i,k}^j(z) \leq m^* \text{ or } p_{i,k}^j(z-1) \geq p_{i,k}^j(z) \geq m^*, \\ m^* + (2r-1)\left| m^* - p_{i,k}^j(z) \right|; \\ \text{if } p_{i,k}^j(z-1) \leq m^* \leq p_{i,k}^j(z) \text{ or } p_{i,k}^j(z-1) \geq m^* \geq p_{i,k}^j(z), \\ p_{i,k}^j(z-1) + r\left(p_{i,k}^j(z) - p_{i,k}^j(z-1) \right); \\ \text{if } m^* \leq p_{i,k}^i(z-1) \leq p_{i,k}^j(z) \text{ or } m^* \geq p_{i,k}^j(z-1) \geq p_{i,k}^j(z), \\ m^* + (2r-1)\left| m^* - p_{i,k}^j(z-1) \right|. \end{cases} \tag{16}$$

To balance exploitation, party switch is adopted [20]. Adaptive variable λ is applied; that is drastically minimized from 1 to 0 in the entire iteration method. All the candidates

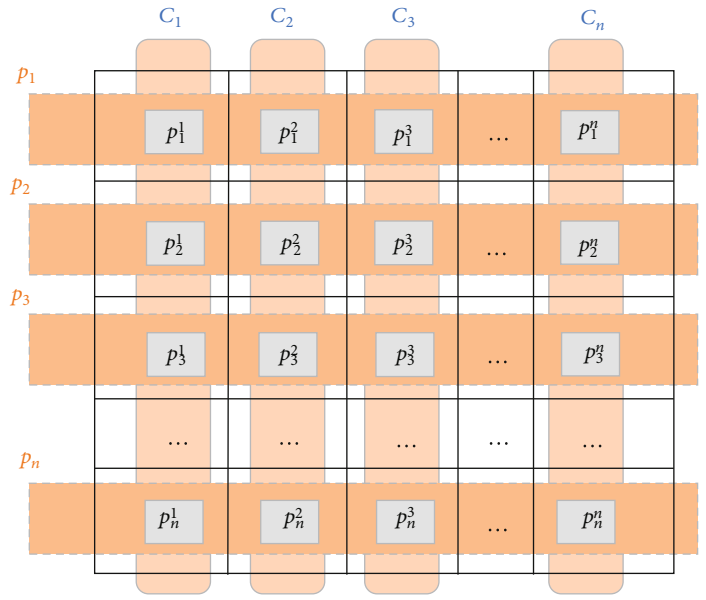


Figure 1: PO logical division of the population.

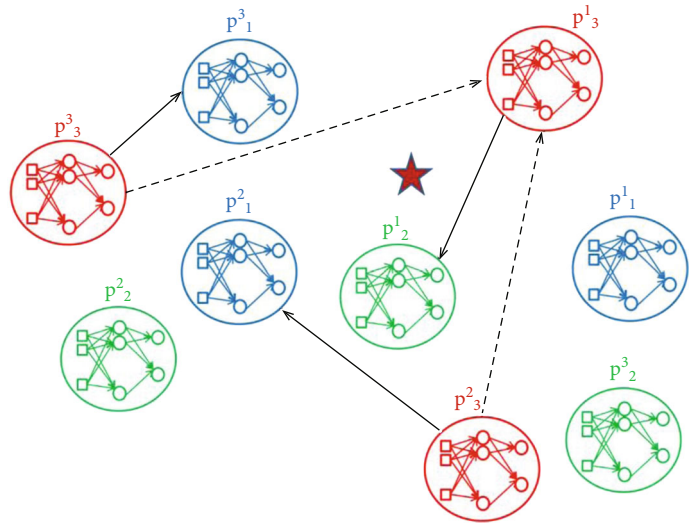


Figure 2: Depiction of the position updating of CFNNs through PO.

are chosen as per the possibility λ as well as substituted with the worst member of the arbitrarily chosen party.

$$q = \arg \max_{i \le j \le n} f\left(p_i^j\right). \tag{17}$$

During the election stage, the winner in the constituency is gained as follows:

$$q = \arg \min_{i \le j \le n} f\left(p_i^j\right), \tag{18}$$

$$c_j^* = p_q^j. \tag{19}$$

Figure 2 shows how PO updates the location of CFNNs. The position of the global optimum is shown by the star symbol. With regard to the party leader, dotted arrows show the position updating of party 3 members, and plain arrows show the position updating of party 3 members in relation to the constituency winners.

3. Performance Validation

This section investigates the intrusion detection outcomes of the PO-CFNN model on three distinct datasets with 80 : 20 for training and testing. Table 1 and Figures 3 and 4 report the comparative results of the PO-CFNN model with existing methods on the test NSL-KDD++ dataset [21]. The

Table 1: Comparative analysis of PO-CFNN technique with recent approaches to the NSL-KDD++ dataset.

Methods	Accuracy	Precision	Recall	F score
PO-CFNN	99.86	99.89	99.58	99.72
SHOLEN model [22]	99.62	99.76	99.49	99.60
ASCH model [23]	98.74	96.62	98.82	93.36
RNN model	97.70	96.25	95.55	93.36
Deep NN model	96.55	95.58	95.47	92.50
DBN model [24]	95.44	94.25	93.28	92.39

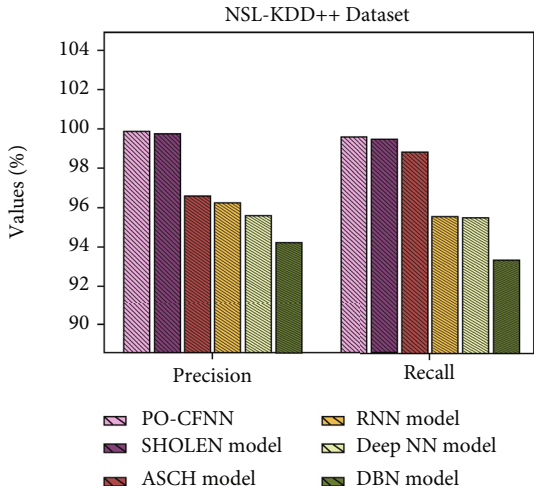


Figure 3: Prec_n and reca_l analysis of PO-CFNN technique under NSL-KDD++ dataset.

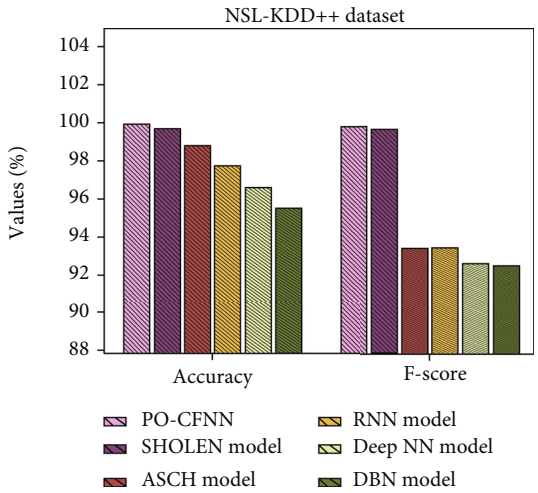


Figure 4: Acc_y and F_{score} analysis of PO-CFNN technique under NSL-KDD++ dataset.

results indicated that the DBN model has gained ineffective outcomes over the other methods with an accuracy of 95.44%. At the same time, the deep NN model has resulted in a slightly increased accuracy of 96.55%. In line with this, the ASCH and RNN models have obtained moderately improved accuracy of 98.74% and 97.70%, respectively. Though the SHOLEN model has accomplished reasonable accuracy of 99.62%, the PO-CFNN model has showcased superior results with an accuracy of 99.86%.

Figure 5 establishes the ROC analysis of the PO-CFNN technique on the NSL-KDD++ dataset. The figure exposed that the PO-CFNN technique has reached an enhanced outcome with a higher ROC of 99.9928.

Table 2 and Figures 6 and 7 report the comparative results of the PO-CFNN model with existing methods on the test UNSWNB15 dataset [25]. The results indicated that the DBN model has gained ineffective outcomes over the other methods with an accuracy of 98.92%. Simultaneously, the deep NN model has resulted in a slightly increased accuracy of 98.57%. Also, the ASCH and RNN models have obtained moderately improved accuracy of 98.88% and 98.99%, respectively. But, the SHOLEN model has accomplished reasonable accuracy of 98.99%, and the PO-CFNN model has showcased superior results with an accuracy of 99.46%.

Figure 8 depicts the ROC analysis of the PO-CFNN technique on the UNSWNB15 dataset [26]. The figure exposed that the PO-CFNN technique has reached an enhanced outcome with a higher ROC of 99.9378.

Table 3 and Figures 9 and 10 report the comparative results of the PO-CFNN technique with existing methods on the test CIDCC-2017 dataset. The results indicated that the DBN model has gained ineffective outcomes over the other methods with an accuracy of 98.83%. Likewise, the deep NN model has resulted in a slightly increased accuracy of 98.69%. The ASCH and RNN models have obtained moderately improved accuracy of 98.65% and 98.92%, respectively. Finally, the SHOLEN model has accomplished reasonable accuracy of 99.05%; the PO-CFNN model has showcased superior results with an accuracy of 99.38%.

Figure 11 portrays the ROC analysis of the PO-CFNN technique on the CIDCC-2017 dataset. The figure exposed that the PO-CFNN technique has reached an enhanced outcome with a higher ROC of 99.9900. Figure 12 provides a comparative study for all datasets as an average accuracy for all models. The figure shows the superiority of the proposed PO-CFNN model.

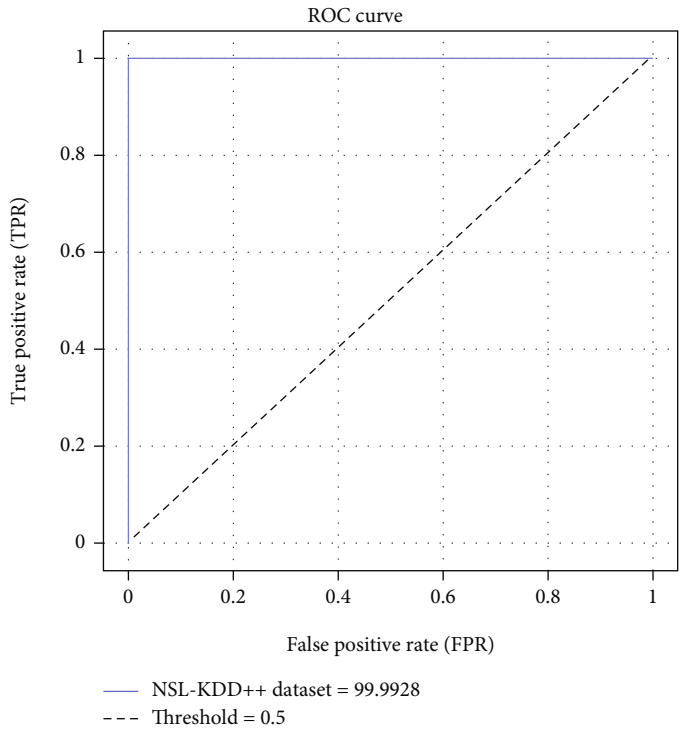


Figure 5: ROC analysis of PO-CFNN technique under NSL-KDD++ dataset.

Table 2: Comparative analysis of PO-CFNN technique with recent approaches to UNSWNB15 dataset.

Methods	Accuracy	Precision	Recall	F score
PO-CFNN	99.46	99.75	99.62	99.76
SHOLEN model	98.99	99.63	99.45	99.68
ASCH model	98.88	96.68	98.74	93.58
RNN model	98.99	96.40	97.94	94.55
Deep NN model	98.57	95.60	95.64	92.98
DBN model	98.92	94.28	93.30	93.61

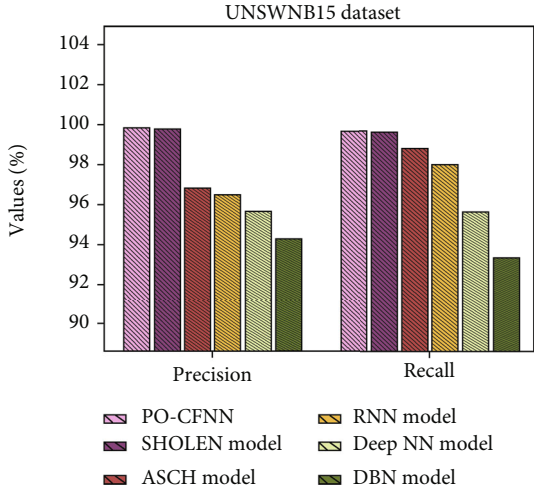


Figure 6: Prec$_n$ and reca$_l$ analysis of PO-CFNN technique under UNSWNB15 dataset.

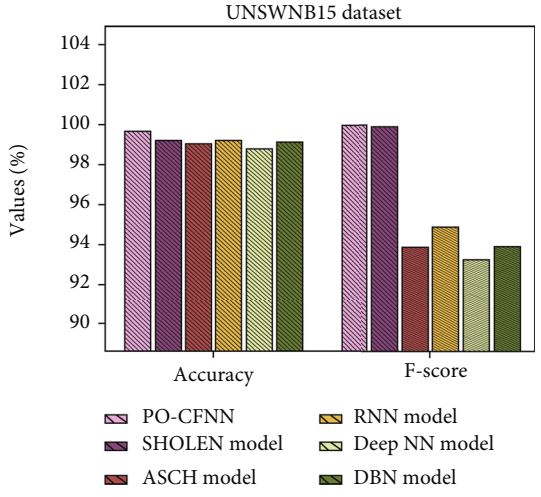


Figure 7: Acc$_y$ and F_{score} analysis of PO-CFNN technique under UNSWNB15 dataset.

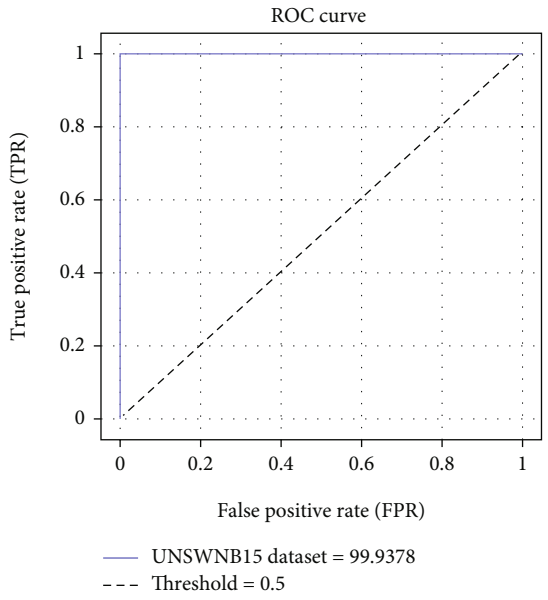


Figure 8: ROC analysis of PO-CFNN technique under UNSWNB15 dataset.

Table 3: Comparative analysis of PO-CFNN technique with recent approaches on the CIDCC-2017 dataset.

Methods	Accuracy	Precision	Recall	F score
PO-CFNN	99.38	99.69	99.66	99.69
SHOLEN model	99.05	99.61	99.52	99.54
ASCH model	98.65	95.55	98.74	93.31
RNN model	98.92	95.96	95.46	94.21
Deep NN model	98.69	93.31	92.10	90.93
DBN model	98.83	95.87	94.97	92.37

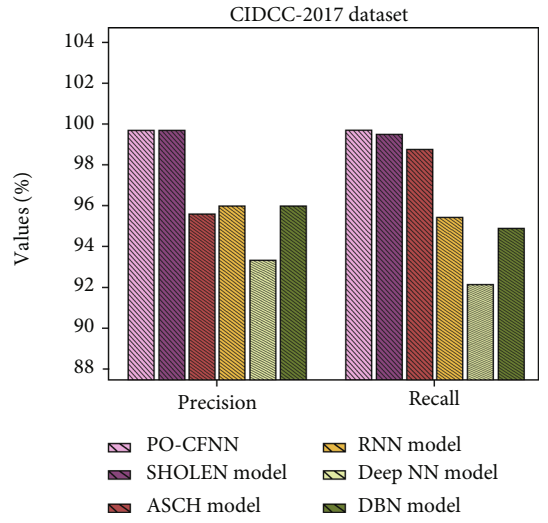


Figure 9: Prec_n and reca_l analysis of PO-CFNN technique under CIDCC-2017 dataset.

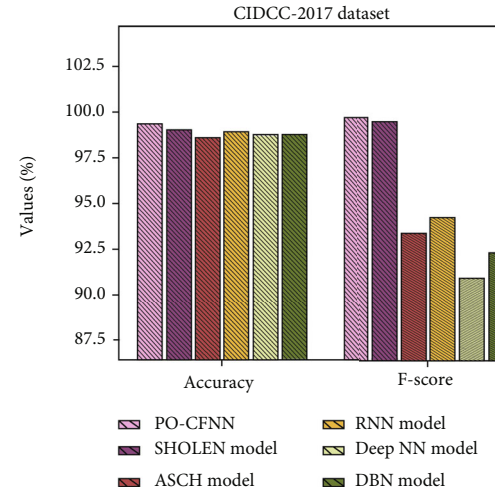


Figure 10: Acc_y and F_{score} analysis of PO-CFNN technique under the CIDCC-2017 dataset.

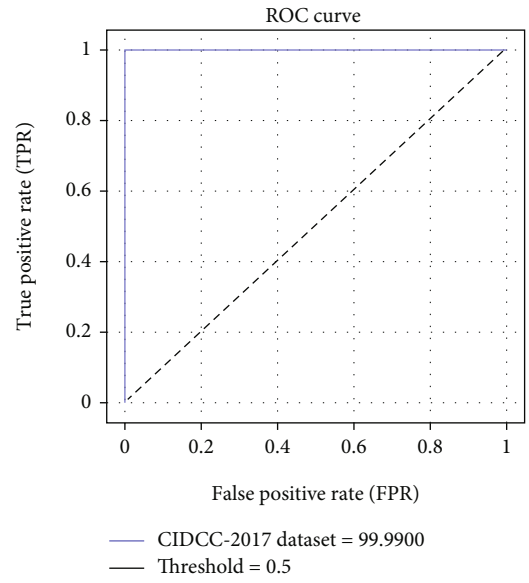


Figure 11: ROC analysis of PO-CFNN technique under the CIDCC-2017 dataset.

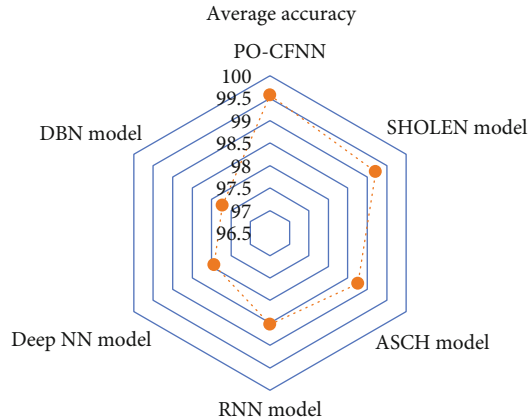


Figure 12: Average accuracy for all models with all datasets.

4. Conclusion

In this work, a novel PO-CFNN approach for identifying and classifying IoT intrusions has been created. Before classification and parameter optimization, the PO-CFNN algorithm undergoes preprocessing and preclassification. In the beginning, the network data is preprocessed to make it easier to analyze. The CFNN algorithm is used to identify and classify intrusions in the IoT environment. Final adjustments to the CFNN model's parameters are made using the PO algorithm at this point. When compared to other contemporary techniques, the PO-CFNN algorithm performed better in an experiment on a benchmark dataset. As a result, the PO-CFNN approach offers superior performance over the alternatives. In future work, feature selection techniques might be developed utilizing the metaheuristics algorithms.

Data Availability

This article develops a novel political optimizer with cascade forward neural network (PO-CFNN-)-based IDS in the IoT environment. The major intention of the PO-CFNN technique is to define the occurrence of intrusions in the IoT environment. The PO-CFNN approach follows three major processes, namely, preprocessing, classification, and parameter optimization. Initially, the networking data is preprocessed to transform them into a useful format. The CFNN technique is employed for the identification and classification of intrusions in the IoT environment. At the final stage, the PO algorithm is applied for optimal adjustment of the parameters involved in the CFNN technique. The experimental validation of the PO-CFNN technique on benchmark dataset stated the better outcomes of the PO-CFNN technique over the recent approaches.

Conflicts of Interest

The author declares that he has no conflicts of interest.

References

[1] R. Kaur, R. K. Ramachandran, R. Doss, and L. Pan, "The importance of selecting clustering parameters in VANETs: a survey," *Computer Science Review*, vol. 40, no. 2021, p. 100392, 2021.

[2] S. Smys, A. Basar, and H. Wang, "Hybrid intrusion detection system for internet of things (IoT)," *Journal of ISMAC*, vol. 2, no. 4, pp. 190–199, 2020.

[3] M. A. Rahman, A. T. Asyhari, L. S. Leong, G. B. Satrya, M. H. Tao, and M. F. Zolkipli, "Scalable machine learning-based intrusion detection system for IoT-enabled smart cities," *Sustainable Cities and Society*, vol. 61, article 102324, 2020.

[4] M. Almiani, A. Abu Ghazleh, A. Al-Rahayfeh, S. Atiewi, and A. Razaque, "Deep recurrent neural network for IoT intrusion detection system," *Simulation Modelling Practice and Theory*, vol. 101, article 102031, 2020.

[5] M. Zhong, Y. Zhou, and G. Chen, "Sequential model-based intrusion detection system for IoT servers using deep learning methods," *Sensors*, vol. 21, no. 4, p. 1113, 2021.

[6] A. R. Gad, A. A. Nashat, and T. M. Barkat, "Intrusion detection system using machine learning for vehicular ad hoc networks based on ToN-IoT dataset," *IEEE Access*, vol. 9, pp. 142206–142217, 2021.

[7] P. K. Keserwani, M. C. Govil, E. S. Pilli, and P. Govil, "A smart anomaly-based intrusion detection system for the Internet of Things (IoT) network using GWO–PSO–RF model," *Journal of Reliable Intelligent Environments*, vol. 7, no. 1, pp. 3–21, 2021.

[8] M. Ibrahim, "Intelligent differential evolution based feature selection with deep neural network for intrusion detection in wireless sensor networks," *Journal of Intelligent Systems and Internet of Things*, no. 2, pp. 78–89, 2019.

[9] J. Shareena, A. Ramdas, and H. Ap, "Intrusion detection system for IoT botnet attacks using deep learning," *SN Computer Science*, vol. 2, no. 3, pp. 1–8, 2021.

[10] P. Kumar, G. P. Gupta, and R. Tripathi, "A distributed ensemble design-based intrusion detection system using fog computing to protect the internet of things networks," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 10, pp. 9555–9572, 2021.

[11] X. Larriva-Novo, V. A. Villagrá, M. Vega-Barbas, D. Rivera, and M. Sanz Rodrigo, "An IoT-focused intrusion detection system approach based on preprocessing characterization for cybersecurity datasets," *Sensors*, vol. 21, no. 2, p. 656, 2021.

[12] A. K. Bediya and R. Kumar, "A novel intrusion detection system for internet of things network security," *Journal of Information Technology Research (JITR)*, vol. 14, no. 3, pp. 20–37, 2021.

[13] M. Sarhan, S. Layeghy, and M. Portmann, "Towards a standard feature set for network intrusion detection system datasets," *Mobile Networks and Applications*, vol. 27, no. 1, pp. 1–14, 2022.

[14] P. Nimbalkar and D. Kshirsagar, "Feature selection for intrusion detection system in internet-of-things (IoT)," *ICT Express*, vol. 7, no. 2, pp. 177–181, 2021.

[15] V. Kumar, A. K. Das, and D. Sinha, "UIDS: a unified intrusion detection system for IoT environment," *Evolutionary Intelligence*, vol. 14, no. 1, pp. 47–59, 2021.

[16] M. S. S. Abujazar, S. Fatihah, I. A. Ibrahim, A. E. Kabeel, and S. Sharil, "Productivity modelling of a developed inclined stepped solar still system based on actual performance and using a cascaded forward neural network model," *Journal of Cleaner Production*, vol. 170, pp. 147–159, 2018.

[17] B. Warsito, R. Santoso, and H. Yasin, "Cascade forward neural network for time series prediction," *In Journal of Physics: Conference Series*, vol. 1025, no. 1, p. 12097, 2018.

[18] Q. Askari, I. Younas, and M. Saeed, "Political optimizer: a novel socio-inspired meta-heuristic for global optimization," *Knowledge-Based Systems*, vol. 195, article 105709, 2020.

[19] A. Zhu, Z. Gu, C. Hu, J. Niu, C. Xu, and Z. Li, "Political optimizer with interpolation strategy for global optimization," *Plo S one*, vol. 16, no. 5, article e0251204, 2021.

[20] M. A. Taha, S. E. Assad, A. Queudet, and O. Deforges, "Design and efficient implementation of a chaos-based stream cipher," *Transactions*, vol. 7, no. 2, pp. 89–114, 2017.

[21] M. Tavallaee, E. Bagheri, W. Lu, and A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set," in *Submitted to Second IEEE Symposium on Computational Intelligence for Security and Defense Applications (CISDA)*, 2009.

[22] S. Otoum, B. Kantarci, and H. Mouftah, "A comparative study of ai-based intrusion detection techniques in critical infrastructures," *ACM Transactions on Internet Technology (TOIT)*, vol. 21, no. 4, pp. 1–22, 2021.

[23] S. Otoum, B. Kantarci, and H. Mouftah, "Adaptively supervised and intrusion-aware data aggregation for wireless sensor clusters in critical infrastructures," in *2018 IEEE international conference on communications (ICC)*, Kansas City, MO, USA, 2018.

[24] K. Jiang, W. Wang, A. Wang, and H. Wu, "Network intrusion detection combined hybrid sampling with deep hierarchical Network," *Access*, vol. 8, pp. 32464–32476, 2020.

[25] N. Moustafa, *Designing an online and reliable statistical anomaly detection framework for dealing with large high-speed network traffic*, Diss. University of New South Wales, Canberra, Australia, 2017.

[26] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward generating a new intrusion detection dataset and intrusion traffic characterization," in *4th International Conference on Information Systems Security and Privacy (ICISSP)*, Portugal, January 2018.

Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 1746373, 18 pages
https://doi.org/10.1155/2022/1746373

Research Article

OpenCBD: A Network-Encrypted Unknown Traffic Identification Scheme Based on Open-Set Recognition

Xinyi Hu,[1,2] **Chunxiang Gu**,[1,2] **Yihang Chen**,[1] **Xi Chen**,[1,2] **and Fushan Wei**[1,2]

[1]*State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou, China 450001*
[2]*Henan Key Laboratory of Network Cryptography Technology, Zhengzhou, China 450001*

Correspondence should be addressed to Chunxiang Gu; gcx5209@126.com

Received 9 February 2022; Revised 28 March 2022; Accepted 12 April 2022; Published 12 May 2022

Academic Editor: Shafiq Ahmad

The encryption of network traffic promotes the development of encrypted traffic classification and identification research. However, many existing studies are only effective for closed-set experimental data, that is to say, only for traffic of known classes, while there are often lots of unknown classes traffic in the real environment of open sets, and many studies have difficulty identifying the traffic of unknown classes and can only misclassify them as known classes. How to identify unknown traffic and classify known traffic in an open-collection environment is one of the focuses of traffic analysis research. Considering these problems, this paper proposes a novel solution, which applies the open-set recognition method to the unknown traffic identification, and constructs a model based on deep learning and ensemble learning. The method constructs a model based on a convolutional neural network and a transformer encoder and then uses a three-stage training and testing process, combined with a novel loss function, to generalize to the open space to form OpenCBD. Experiments on public datasets show that the proposed method is significantly better than other open-set identification methods. It can not only distinguish known traffic from unknown traffic but also identify specific classes of known traffic.

1. Introduction

With the wide application of encryption technology in network traffic, it becomes more and more challenging to effectively monitor and analyze network traffic, and encrypted traffic analysis technology has also become an important research topic in the field of network security [1–3]. To analyze encrypted traffic, it is first necessary to divide the traffic into different sets according to specific goals, that is, to classify and identify network traffic. Most of the existing researches are implemented in a closed environment; that is, many researches can efficiently and accurately classify and identify traffic of known classes. For example, Aceto et al. [4, 5] proposed a practical mobile traffic classification model based on deep learning which can automatically extract features. Liu et al. [6] proposed an encrypted traffic classification model FS-Net based on the recurrent neural network. Wang et al. [7] proposed App-Net, a mobile application recognition model based on RNN and CNN. Nascita et al. [8] improved a multimodal deep learning traffic classification model based on explainable artificial intelligence techniques. But some studies, while valid in closed settings, often cannot really be applied to the real world. Because the real-world environment is open, network traffic includes encrypted and nonencrypted, known and unknown, benign and malicious, standard protocols and private protocols, etc. There are many practical problems to be considered and many difficulties to overcome. If a classification method trained in a closed set is simply generalized to an open set, it is easy to misclassify samples of unknown classes into known classes [9–11]. In order to solve this problem, researchers need to develop models that can support both the classification of known class samples and the discovery of unknown class samples, so as to actively manage and prevent abnormal traffic and further create and maintain a good network environment.

In real-world identification and classification tasks, it is often difficult to obtain labels for all samples during training, but it is desirable to have the ability to identify unknown classes during testing. Therefore, open-set recognition

describes such a scenario. During testing, samples of unknown classes that have not appeared in training will appear. The classifier can not only accurately classify known samples but also identify unknown classes. In a real network environment, there are known classes of encrypted traffic and unknown classes of encrypted traffic. This is similar to the scenario of open-set recognition. Therefore, some open-set recognition methods can be used to solve the unknown traffic identification. This paper proposes an unknown traffic identification method OpenCBD based on open-set recognition. It first performs a pretraining process based on self-supervised learning on unlabeled data, so that the CBD model (CBD model was proposed in [12]; it is a self-supervised learning model containing three modules; the three modules are the CNN module—based on a convolutional neural network, BERT module—based on a transformer model encoder, dense module—based on a fully connected network) has a certain understanding of the basic characteristics of encrypted traffic. Then, the training and testing process based on ensemble learning is designed in the open set. During training, the individual model is trained based on a specific loss function on some known classes. Then, all known classes are trained through the ensemble strategy, so that the ensemble model can achieve accurate classification of known classes and identification of unknown classes in the process of open-set testing. The contributions of this paper are summarized as follows:

(i) A novel unknown traffic identification model OpenCBD is designed. It uses the idea of open-set recognition, combines deep learning and ensemble learning, learns the basic characteristics of encrypted traffic from unlabeled data, and then trains on known classes of traffic to classify and identify traffic in an open environment

(ii) A general training method suitable for open-set recognition is proposed. The method only needs to be trained on the data of the known classes and can identify the data of the unknown classes. The method adopts two-stage training: first, it randomly selects part of the known classes data to train the individual model and then integrates the individual model to train with all known classes data, so that the model can learn the special knowledge between classes

(iii) A loss function that combines the cross-entropy loss function commonly used in classification models and the II-loss function proposed for open-set recognition is proposed. The combination of the two loss functions can train the model more efficiently, making the model fit faster and more accurately, so that the classification of known classes and the identification of unknown classes can be better completed at the same time

(iv) The OpenCBD model achieves good results in unknown traffic identification and known traffic classification tasks. Furthermore, the OpenCBD model outperforms significantly compared to the baseline methods

The rest of the paper is organized as follows. Section 2 summarizes the basic knowledge and related work of open-set recognition and unknown traffic identification. Section 3 details the structure and methodology of the overall model. Section 4 introduces the specific details of the experiments and evaluates and compares the experimental results. Finally, Section 5 concludes the paper.

2. Preliminary and Related Work

This section mainly introduces the basic knowledge and researches in recent years of open-set identification and unknown traffic identification.

2.1. Open-Set Recognition. First, some definitions in open-set recognition are given.

Definition 1 (open space [13]). Given a label set $\mathcal{K}$, the known class label is a positive integer, and the unknown class label is 0. For the feature $x \in \mathbb{R}^d$, define $f \in \mathcal{H}$ to be a measurable recognition function, $f_y(x) > 0$ means that the class y can be recognized, and $f_y(x) \le 0$ means that y is not recognized, where $\mathcal{H} : \mathbb{R}^d \longrightarrow \mathbb{R}$ is the appropriate smooth space for the recognition function. For any known class of training samples $x_i \in \mathcal{K}, i = 1, \cdots, N$, the open space $\mathcal{O}$ is defined as

$$\mathcal{O} = S_O - \bigcup_{i \in N} B_r(x_i), \tag{1}$$

where $B_r(x_i)$ is a closed sphere with the training sample x_i as the center and radius r. S_O is a sphere of radius r_o, including all known positive training samples $x \in \mathcal{K}$ and open space $\mathcal{O}$.

Definition 2 (open space risk [13]). Open space risk is defined as the relative measure of positive labeled open space compared to the overall measure of positive labeled space. Then, the probabilistic open space risk $R_{\mathcal{O}}(f)$ of class y is

$$R_{\mathcal{O}}(f) = \frac{\int_{\mathcal{O}} f_y(x)\mathrm{d}x}{\int_{S_O} f_y(x)\mathrm{d}x}. \tag{2}$$

Definition 3 (openness [14]). Openness refers to the degree of openness of an open space, which consists of training classes, target classes, and test classes,

$$O = 1 - \sqrt{\frac{2 \times |C_{\mathrm{TR}}|}{|C_{\mathrm{TA}}| + |C_{\mathrm{TE}}|}}, \tag{3}$$

where $C_{\mathrm{TR}}, C_{\mathrm{TA}}, C_{\mathrm{TE}}$ represent training classes, target classes, and testing classes, respectively. Sometimes $O < 0$ may occur, so the openness after calibration is only related

to training classes and test classes,

$$O^* = 1 - \sqrt{\frac{2 \times |C_{\mathrm{TR}}|}{|C_{\mathrm{TR}}| + |C_{\mathrm{TE}}|}}. \tag{4}$$

Definition 4 (open-set risk [13]). The open-set recognition problem is to minimize both traditional empirical risk and open space risk. Given an empirical risk function R_ε, the open-set risk is defined as

$$\arg \min_{f \in \mathscr{H}} \{R_{\mathscr{O}}(f) + \lambda_r R_\varepsilon(f)\}, \tag{5}$$

where λ_r is the regularization constant.

Definition 5 (open world recognition [13]). The solution for open world recognition is represented by the quintuple $[F, \varphi, \nu, L, I]$. $F(x)$: $\mathscr{R}^d \longrightarrow \mathscr{N}$ is a multiclass open-set recognition function. The i-th class in $F(x)$ is identified by the vector function $\varphi(x)$ of the measurable recognition function $f_i(x)$, and the detector $\nu(\varphi)$: $\mathscr{R}^i$to$[0, 1]$ is determined, where $i \in \mathscr{K}_t$, $\nu(\varphi)$ determine whether the output vector of the recognition function is from an unknown class. $L(x)$: $\mathscr{R}^d \longrightarrow \mathscr{N}^+$ is the labeling process. $L(x)$ applies new unknown data U_t to time t, resulting in label data $D_t = \{(y_j, x_j)\}$, where $y_j = L(x_j) \forall x_j \in U_t$. Assuming that the label finds m new classes, the set of known classes becomes $\mathscr{K}_{t+1} = \mathscr{K}_t \cup \{i + 1, \cdots, i + m\}$. $I_t(\varphi; D_t)$: $\mathscr{H}^i \longrightarrow \mathscr{H}^{i+m}$ is the incremental learning function. $I_t(\varphi; D_t)$ extensibly learns and adds new measurable functions $f_{i+1}(x) \cdots f_{i+m}(x)$ to the measurable recognition function vector φ. Each measurable function minimizes the corresponding open space risk.

Suppose that each $f_k(x)$ outputs the probability of belonging to the k classes. And assume that $f_k(x)$ is normalized across each class. Let $\varphi = [f_1(x), \cdots, f_k(x)]$, then the multiclass open-set recognition function is

$$F(x) = \begin{cases} 0, & \text{if } \nu(\varphi(x)) = 0, \\ y^*, & \text{otherwise}, \end{cases} \tag{6}$$

where

$$y^* = \arg \max_{y \in \mathscr{K}, f_y(x) \in \varphi(x)} f_y(x). \tag{7}$$

At this point, an easy way to detect is to set an acceptable minimum threshold τ and minimize the open space risk, i.e.,

$$\nu(\varphi(x)) = f_{y^*}(x) > \tau. \tag{8}$$

Since open-set recognition was proposed, many research methods have been proposed, mainly including discriminative models and generative models. Among them, the discriminative models are mostly constructed by traditional machine learning methods and deep neural network methods, and the generative models are divided into methods based on instance generation and methods based on noninstance generation according to whether there is instance generation. There are also some studies using neural networks in these two methods. The following mainly introduces some methods based on deep neural networks, which include not only discriminative models but also generative models.

In 2016, Bendale and Boult [15] proposed OpenMax, the first open-set recognition method based on deep neural networks. OpenMax was used as a new model layer that estimated the probability that the input came from an unknown class and provided a bounded open space risk.

In 2017, Ge et al. [16] proposed a multiclass open-set recognition method Generative OpenMax (G-OpenMax). Unlike some existing studies, the unknown class was not inferred from the features of the known classes or the decision distance. It extended OpenMax by employing Generative Adversarial Networks (GANs) for new classes of image synthesis.

In 2018, Yoshihashi et al. [17] proposed an open-set recognition classification reconstruction learning method CROSR, which used latent representations for reconstruction and achieved robust unknown detection without reducing the classification accuracy of known classes.

In 2019, Oza and Patel [18] proposed an open-set recognition algorithm C2AE, which used a class-conditional autoencoder, as well as closed-set classification training and open-set recognition training. The encoder and decoder were trained in two stages, and the reconstruction error was modeled using the extreme value theory of statistical modeling to find a threshold that identified samples of known and unknown classes.

In 2020, Hassen and Chan [19] proposed a representation method based on a neural network and used this representation method to propose an open-set recognition mechanism. In this representation, instances from the same class were close to each other, while instances from different classes were further apart.

In 2020, Liu et al. [20] proposed an algorithm that uses the meta-learning technique PEELER to solve the problem of open-set recognition. It combines randomly selecting a new set of classes per episode, maximizes the loss of postentropy of these class instances, and then learns a new metric formula based on the Mahalanobis distance.

In 2021, Joseph et al. [21] proposed an open-world object detector ORE, which was based on contrastive clustering and energy-based unknown identification. Identifying and characterizing unknown instances helped reduce confusion in incremental object detection settings. In this setting, state-of-the-art performance could be achieved without additional methodologies.

In 2022, Geng and Chen [22] proposed a batch decision strategy that was aimed at extending existing open-set recognition methods for new class discovery while considering correlations between test instances. By modifying the Hierarchical Dirichlet Process (HDP), a collective decision-based open-set recognition framework CD-OSR was proposed. CD-OSR did not need to define decision thresholds and could realize open-set recognition and new class discovery at the same time.

Table 1 summarizes several open-set recognition methods mentioned in Section 2.1.

2.2. Unknown Traffic Identification. In the field of network traffic analysis, unknown traffic identification has always been an important research direction. Researchers usually use unsupervised learning or semisupervised learning to solve the tasks of identifying and detecting unknown traffic.

In 2011, Finamore et al. [23] proposed an unsupervised algorithm to identify traffic classes within aggregates. This algorithm utilized the K-means clustering algorithm and added a mechanism to automatically determine the number of traffic clusters.

In 2013, Zhang et al. [24] proposed an approach to address the problem of unknown applications in the critical case of small supervised training sets. The proposed method had a superior ability to detect unknown traffic generated by unknown applications and exploited the correlation information between real-world network traffic to improve the classification performance.

In 2013, Zhang et al. [25] proposed an iterative method to extract unknown information from a set of unlabeled traffic flows. The method combined asymmetric bagging and flow correlation to guarantee the purity of the extracted negatives and demonstrated significantly better than state-of-the-art flow classification methods under unknown applications.

In 2014, Yu et al. [26] proposed a method to classify elephant traffic using service-based statistical features for cluster analysis. Elephant traffic refers to unknown traffic generated by only a few or some types of applications.

In 2015, Shaikh and Harkut [27] proposed a framework that classifies unknown flows in the network, solving the problem of applying unknowns in critical situations with little supervised training data. Flow label propagation was proposed, which automatically and accurately labeled more unlabeled flows to enhance the ability of Nearest Clustering-based Classifiers (NCCs). Composite classification was also proposed, which combines many flow predictions to more accurately classified Bag of Flows (BoF).

In 2015, Lin et al. [28] proposed a semisupervised learning method to address the problem of an unknown protocol in critical cases where the labeled training sample set was small. With the help of flow-related information and semisupervised clustering ensemble learning, the method had a superior ability to detect unknown samples generated by unknown protocols to improve classification performance.

In 2017, Ma and Qin [29] proposed a method using deep learning techniques to identify unknown protocols in complex network environments. The method identified the protocol in the network flow according to the application layer protocol type and found out the unknown protocol. This method only used the payload information in the captured 200,000 traffic flows and achieved well unknown protocol traffic identification accuracy.

In 2018, Fu et al. [30] proposed a scheme, FlowCop, to implement traffic detection that did not belong to any predefined application in network traffic classification. It divided the test traffic into N classes and one unknown class by building multiple one-class classifiers. A feature subspace algorithm was also proposed to select salient features for each class of classifiers.

In 2019, Sabeel et al. [31] proposed two methods to predict unknown DoS and DDoS attacks based on DNN and LSTM. The method demonstrated how well deep learning-based methods perform in unknown situations and to what extent deviations from the trained model could be handled. This method can effectively identify unknown attacks.

In 2019, Zhang et al. [32] proposed a network intrusion detection method based on open-set recognition. This method fits the recognition results of known classes to Weibull distribution and then builds an Open-CNN model to estimate the probability of unknown classes from the activation scores of known classes, so as to achieve the purpose of detecting unknown attacks.

In 2020, Zhang et al. [33] proposed an autonomous learning framework to correctly classify unknown classes. The framework efficiently updated deep learning-based traffic classification models during active operation. The core of the proposed framework consisted of a deep learning-based classifier, a self-learning discriminator, and an autonomous self-labeling model. The discriminator and self-labeling process generated new datasets during active operation to support classifier updates.

In 2020, Mohamed et al. [34] proposed a method for handling unknown applications. This method enabled efficient network classification with limited supervised training sets. The proposed model applied multiple neural network algorithms to predict unknown applications. The method improved Internet performance, reduced Internet traffic, and reduced delays in transmitting data.

In 2021, Wang et al. [35] proposed an unknown protocol parsing method based on a convolutional neural network. The protocol data was preprocessed into an image, and the converted image was inputted to the convolution layer for convolution. After convolution, the data was flattened, and the flattened data was put into a fully connected neural network to analyze and predict unknown protocols.

In 2021, Li et al. [36] proposed a lightweight unknown traffic discovery model, LightSEEN, which realized traffic classification and model update in the open world under practical conditions. The overall structure of the method was based on the Siamese network, and each side used a multihead attention mechanism, a one-dimensional convolutional neural network, and a residual network to facilitate the extraction of deep flow features and the convergence speed of the network.

In 2021, Xu et al. [37] proposed the KCC (Known Central Clustering) method to deal with the open-set-based intrusion detection problem. By introducing CD-loss (Class Distance-loss), the centers of different clusters were obtained. By introducing negative samples as unknown classes for training, the threshold of known classes was obtained. Unknown intrusions were rejected by comparing with fuzzy distances.

Table 2 makes a simple classification and summary according to the specific methods used in the above-mentioned several unknown traffic identification literatures.

Table 1: Different models for open-set recognition.

Model	Reference	Open-set recognition category	Methodology	Extreme value theory	Advantages
OpenMax	[15]	Discriminative model	EVT-based calibration classification	√	First deep open-set classifier without using background samples
G-OpenMax	[16]	Generative model	Unknown generation classification	√	Combining generative adversarial networks and OpenMax
CROSR	[17]	Discriminative model	Distance	√	First neural network architecture which involved hierarchical reconstruction blocks
C2AE	[18]	Discriminative model	Reconstruction error	√	Algorithms using class conditional autoencoders
Neural-network-based representation	[19]	Discriminative model	EVT-free calibration classification	×	A loss function was proposed such that instances from the same class are close to each other, while instances from different classes are farther apart
PEELER	[20]	Discriminative model	Distance	×	Combining few-shot classification and open-set recognition
ORE	[21]	Discriminative model	Distance	×	An incremental object detector is proposed
CD-OSR	[22]	Discriminative model	EVT-free calibration classification	×	Automatically reserve space for unknown classes under test, naturally bringing new class discovery capabilities

Table 2: Summary of methods for identifying unknown traffic.

Statistical methods			Deep neural networks		
Supervised learning	Semisupervised learning	Unsupervised learning	CNN-based	Open-set recognition	Others
[25]	[28]	[23, 24, 26, 27, 30]	[29, 32, 33, 35, 37]	[32, 35, 37]	[31, 34]

We combine unknown traffic identification with open-set recognition. According to the characteristics of network encrypted traffic, we design a new open-set recognition method based on a discriminant model. Through self-supervised learning and supervised learning, it can effectively complete known traffic classification and unknown traffic identification tasks at the same time.

3. Proposed Method

To identify unknown classes that have not appeared in the training set, we propose OpenCBD, a deep learning and ensemble learning-based approach. The CBD model was proposed in [12], but it can only complete the classification task in datasets with known class traffic. In this paper, the CBD model is regarded as an individual model. First, the loss function is used to train the individual model, and then through the ensemble strategy, the individual model is fused into an ensemble model, which is extended to OpenCBD suitable for open-set data. Classify known classes and identify unknown classes in the world. The CBD model includes the CNN module, BERT module, and dense module. The detailed structure is given in Section 3.3. The overall process of OpenCBD is shown in Figure 1.

First, pretraining is performed on unlabeled data to obtain a pretrained individual model, including a CNN module with a fixed structure and parameters and a BERT module with a fixed structure and no fixed parameters. Then, perform data preprocessing on the raw data participating in the training, then input them into multiple individual models for training after obtaining the training set, then input the training set into the ensemble model for training, and then obtain the training results. Finally, data preprocessing is performed on the raw data participating in the test, and after the test set is obtained, it is inputted into the trained ensemble model, and the prediction results are the outputs.

The training process includes two stages, namely, closed-set individual training and closed-set ensemble training. The testing process is implemented in the open set. The block diagram of the three stages is shown in Figure 2.

In the following, we will introduce the data preprocessing process, pretraining process, and detailed process of the three stages.

3.1. Data Preprocessing. Data preprocessing is an essential step to achieve the goals of classification and identification. Data preprocessing mainly includes four parts: traffic split, traffic cleaning, traffic conversion, and time interval

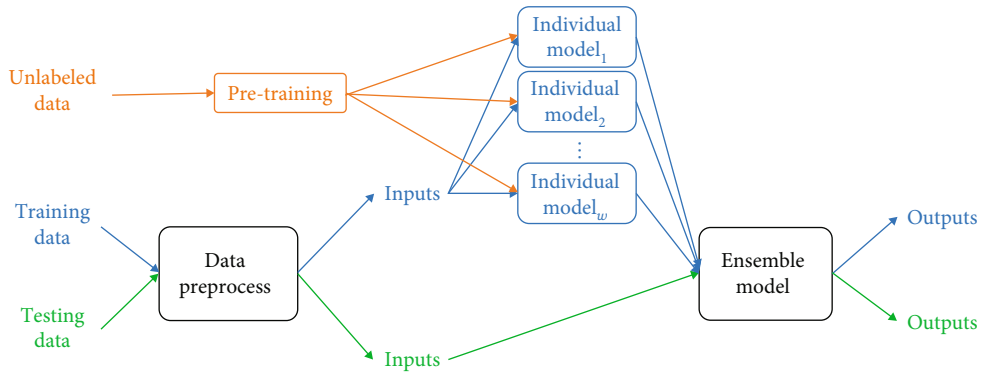


Figure 1: Overall flow chart of proposed method. The orange part represents the pretraining process, the blue part represents the training process, the green part represents the testing process, and the black part represents the process involved in both training and testing processes.

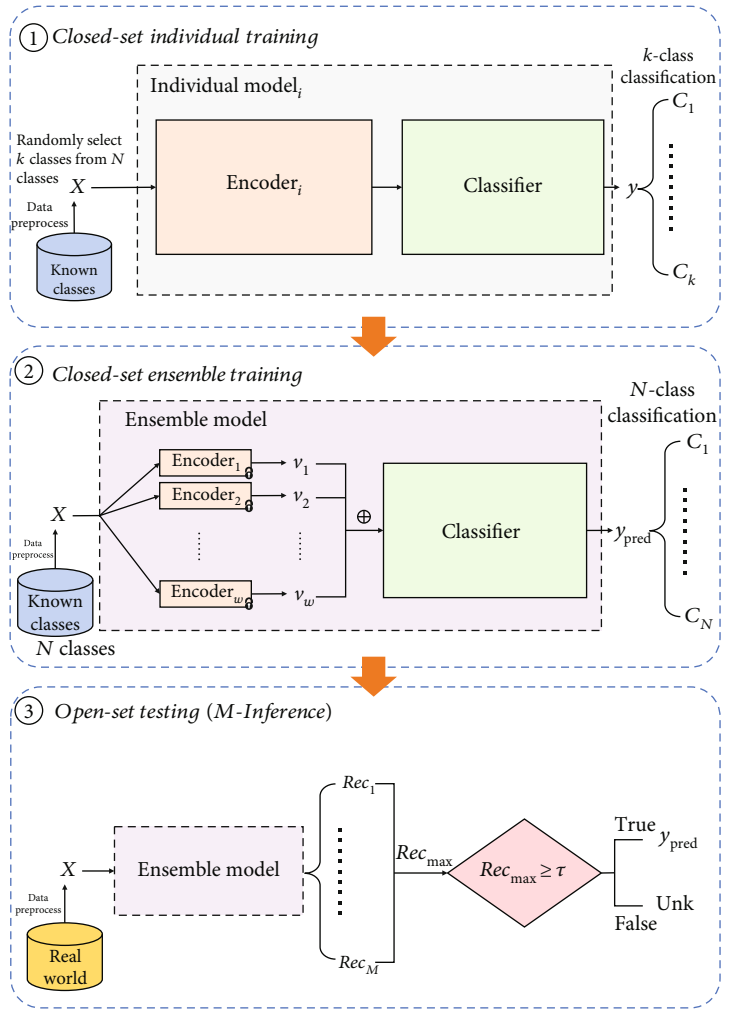


Figure 2: Block diagram of proposed method. (1) Closed-set individual training: randomly select a part of the known class data to train the individual model including the encoder and the classifier. 2) Closed-set ensemble training: using all known class data to train encoders and classifiers in w individual models, where the weights of the encoders are locked. (3) Open-set testing: the ensemble model produces M results to be identified. If the largest to-be-identified result is greater than or equal to the threshold, the test sample is classified into one of the M classes; otherwise, it is classified as unknown.

integration. Following the description in [12], we summarize the preprocessing process as Algorithm 1.

Line 2 is the traffic split. For bidirectional flow, randomly intercept 10 consecutive data packets and define these ten packets as a flow. A total of n flows are intercepted, that is, a total of $10n$ data packets.

Lines 4-9 are the traffic cleaning. Read the payload part of each packet, then unify the length, truncate the first 256 bytes of each packet, and add 0 to the insufficient, to obtain the raw sequence x,

$$x = (b_1, b_2, \cdots, b_{8\times 256}), b_i \in \mathbb{F}_2, \quad i = 1, \cdots, 2048. \tag{9}$$

Line 10 is the traffic conversion. Convert the elements in the raw sequence into decimals according to bytes to obtain a 256-dimensional vector x,

$$x = (x_1, x_2, \cdots, x_{256}), x_i \in \mathbb{F}_{2^8}, \quad i = 1, \cdots, 256. \tag{10}$$

Lines 11-16 are the time interval integration, which was first proposed in [38]. It means that according to the statistical results of the time interval of two adjacent data packets in different classes, for the interval of more than 1 s, insert a blank data packet and ignore it within 1 s. The blank data packet is represented as a 256-dimensional all-one vector $x_0 = (1, \cdots, 1, \cdots, 1)_{256}$.

The payload vector x and the time interval vector x_0 are formed into a set $\mathcal{X}$ in chronological order, and the model can be directly inputted in the next step.

3.2. Pretraining. Pretraining adopts a common pretraining method in the field of encrypted traffic analysis proposed in [12], which starts from the packet level and the flow level, and can directly deepen the model's understanding of encrypted traffic from unlabeled real-world data. This paper summarizes the method into a detailed Algorithm 2.

Lines 1-15 are the packet-based methods. For an unlabeled packet, first extract the payload part to get $x = \{x_1, x_1, \cdots, x_n\}$, and then calculate the entropy of each packet,

$$\begin{aligned} H &= -\sum_{i=1}^{n} P(x_i) \log_2 P(x_i), \quad 1 \le i \le n, \\ &\begin{cases} H(x) < H_0, & x \in \mathcal{X}_{\text{plain}}, \\ H(x) \ge H_0, & x \in \mathcal{X}_{cipher}. \end{cases} \end{aligned} \tag{11}$$

Set the threshold of entropy $H_0 = 4$. When $H \ge H_0$, the data packet label is a ciphertext data packet; when $H < H_0$, the data packet label is a plaintext data packet. Train a CBD model with labeled packets.

Lines 16-31 are the flow-based methods. First, construct positive and negative sample sets. The positive sample set S^+ contains n positive samples, and the positive sample s^+ is defined as a continuous flow F; each flow contains 10 consecutive packets,

$$\begin{aligned} S^+ &= \{s_1^+, s_2^+, \cdots, s_n^+\}, \\ s_i^+ \triangleq F^i &= \{x_1^i, x_2^i, \cdots, x_{10}^i\}, \quad 1 \le i \le n. \end{aligned} \tag{12}$$

The number of negative sample set S^- is the same as the positive sample set S^+, including n negative samples, and the negative sample s^- is defined as a discontinuous flow $\bar{F}$. It is obtained by transforming the positive samples. Each packet in the positive sample is replaced with other bags with a certain probability, and the replaced sample is called a negative sample.

$$\begin{aligned} S^- &= \{s_1^-, s_2^-, \cdots, s_n^-\}, \\ s_i^- \triangleq \bar{F}^i &= \{f(x_1^i), f(x_2^i), \cdots, f(x_{10}^i)\}, \quad 1 \le i \le n, \\ f(x_j^i) &= \begin{cases} x_j^i & (P = 0.7) \\ x_{j'}^{i'} & (P = 0.3) \end{cases}, (i', j') \ne (i, j), \quad 1 \le j \le 10. \end{aligned} \tag{13}$$

Train a CBD model with a labeled set of positive and negative samples. After completing the pretraining, enter the three-stage training and testing process.

3.3. Closed-Set Individual Training. The first stage is closed-set individual training. After the data is preprocessed, the k class data is randomly selected to train the individual model, and the k classification is completed. Each individual model is a randomly selected k class with replacement. The specific structure diagram of the individual model is shown in Figure 3.

3.3.1. Encoder. The encoder and classifier are two important parts in the individual model. The encoder is mainly used for feature extraction, the input is a matrix X, and the output is a vector $\mathbf{v}$,

$$\text{Encoder} : X \longrightarrow \mathbf{v} \in \mathcal{R}^{240}, \tag{14}$$

where X is a $n \times 256$-dimensional matrix on $\mathbb{F}_{2^8}$. The encoder mainly includes the CNN module and BERT module.

The CNN module is inputted in sequence by a row vector; that is, for the input $X = (x_1^T, \cdots, x_n^T)$ of the encoder, x_i represents the i-th input of the CNN module, $i = 1, 2, \cdots, n$. Define $f_C(\cdot)$ as the CNN module function, $f_{\text{con}_j}(\cdot)$ is the convolution function of the j-th layer in the CNN module, $f_{\text{mp}_j}(\cdot)$ is the maximum pooling function of the j-th layer in CNN module, and O_i^j is the j-th layer output for the i-th input in the CNN module, $j = 1, 2, 3, 4$; then, the output

Input: the original network traffic dataset D, the number of classes of traffic c.
Output: packet vector set $\mathscr{X}$;
For $i = 1, \cdots, c$ **do**
  Randomly select n_i consecutive 10 packets to form n_i flows;
  For $j = 1, \cdots, 10n_i$ **do**
  Read the payload part of the packet $x_{i,j}$;
  If $|x_{i,j}| < 2048$ **then**
    $x_{i,j} = [x_{i,j}, \text{zeros}(1, 2048 - |x_{i,j}|)]$;
  Else
    $x_{i,j} = x_{i,j}[1 : 2048]$;
  End if
  $x_{i,j} = \text{int}(x_{i,j}', 10)$;
  $\text{cout}_{i,j} = \text{time}(x_{i,j+1}) - \text{time}(x_{i,j})$;
  If $\text{cout}_{i,j} < 1$ second **then**
    Continue;
  Else
    Add x_0 between $x_{i,j}$ and $x_{i,j+1}$;
  End if
 End for
 Generate packet vector set $X_i = \{x_{i,1}, \cdots, x_0, \cdots, x_{i,10n_i}\}$;
End for
Return packet vector set $\mathscr{X} = X_1 \bigcup X_2 \bigcup \cdots \bigcup X_c$.

Algorithm 1: Preprocessing algorithm for traffic data.

of the CNN module is

$$\begin{aligned} f_C(\mathbf{x}_i) = O_i^4 &\in \mathscr{R}^{242}, \\ O_i^4 &= \max\left(0, f_{\text{mp}_4}\left(f_{\text{con}_4}\left(O_i^3\right)\right)\right), \\ O_i^3 &= \max\left(0, f_{\text{mp}_3}\left(f_{\text{con}_3}\left(O_i^2\right)\right)\right), \\ O_i^2 &= \max\left(0, f_{\text{mp}_2}\left(f_{\text{con}_2}\left(O_i^1\right)\right)\right), \\ O_i^1 &= \max\left(0, f_{\text{con}_1}(x_i)\right). \end{aligned} \tag{15}$$

After the CNN module is a fully connected layer, which is used to change the dimension of the vector to facilitate the input of the subsequent BERT module. Define $f_{\text{fc}}(\cdot)$ to be the fully connected function and $z_i \in \mathscr{R}^{240}$ to be the output of the fully connected layer, then

$$\boldsymbol{z}_i \triangleq f_{\text{fc}}\left(O_i^4\right) = W_1 O_i^4 + B_i = W_i f_C(\boldsymbol{x}_i) + B_i, \tag{16}$$

where W_i is the weight matrix and B_i is the bias matrix.

This is followed by a Concat layer that stitches together the outputs after n CNN modules and fully connected layers. Define $\oplus$ as the splicing symbol and Z as the output of the Concat layer, then

$$Z = \left(z_1^T, z_2^T, \cdots, z_n^T\right) = z_1 \oplus z_2 \oplus \cdots \oplus z_n = \mathop{\oplus}_{i=1}^{n} z_i, Z \in \mathbb{R}^{n \times 240}. \tag{17}$$

The BERT module consists of m transformer encoders, and Z is the input of the BERT module. Define $f_B(\cdot)$ as the BERT module function, $f_{\text{te}_t}(\cdot)$ as the t-th layer transformer encoder function in the BERT module, and v as the output of the encoder, then

$$v \triangleq f_B(Z) = f_{\text{te}_m}\left(\cdots f_{\text{te}_t}\left(\cdots f_{\text{te}_1}(Z)\right)\right), \quad t = 1, 2, \cdots, m. \tag{18}$$

3.3.2. Classifier. The classifier is mainly used to predict results, the input is a vector v, and the output is a specific class y,

$$\text{Classifier} : v \longrightarrow y \in \{1, 2, \cdots, k\}. \tag{19}$$

The classifier consists of a dense module and Softmax layer. In the dense module, define $f_D(\cdot)$ to be the function of the dense module and $F(X)$ to be the output of the dense module, then

$$F(X) \triangleq f_D(v) = \max(0, (Wv + B)), \tag{20}$$

where W represents the weight matrix and B represents the bias matrix.

Input: unlabeled dataset $D_1 = \{\mathbf{x}_{1,1},\cdots,\mathbf{x}_{1,N}\}$, D_2.
Output: pretrained model;
For $i = 1, \cdots, N$ **do**
  Extract the payload of $\mathbf{x}_{1,i}$, $\mathbf{x}_{1,i} = \{x_{1,i}^1, x_{1,i}^2,\cdots,x_{1,i}^n\}$;
  For $j = 1, \cdots, n$ **do**
    $H(\mathbf{x}_{1,i}) = 0$;
    $H(x_{1,i}^j) = -P(x_{1,i}^j) \cdot \log_2 P(x_{1,i}^j)$;
    $H(\mathbf{x}_{1,i}) = H(\mathbf{x}_{1,i}) + H(x_{1,i}^j)$;
  End for
  If $H(\mathbf{x}_{1,i}) < H_0$ **then**
    $\text{lab}(\mathbf{x}_{1,i}) = 0$ (plaintext);
  Else
    $\text{lab}(\mathbf{x}_{1,i}) = 1$ (ciphertext);
  End if
End for
$D_1{}' = \{(\mathbf{x}_{1,1}, \text{lab}(\mathbf{x}_{1,1})),\cdots,(\mathbf{x}_{1,N}, \text{lab}(\mathbf{x}_{1,N}))\}$;
Model = Model($D_1{}'$);
Randomly select m consecutive 10-packet payload parts in D_2 to form S^+, $S^+ = \{s_1^+,\cdots,s_m^+\}$;
For $a = 1, \cdots, m$ **do**
  $s_a^+ \triangleq F_a = \{x_{a,1}, x_{a,2},\cdots,x_{a,10}\}$;
  $S^- = \varnothing$;
  For $b = 1, \cdots, 10$ **do**
    If $P = 0.3$ **then**
      $f(x_{a,b}) = x_{a',b'}$, where $(a', b') \neq (a, b)$;
    Else
      $f(x_{a,b}) = x_{a,b}$;
    End if
    $s_a^- \triangleq F_a{}' = \{f(x_{a,1}), f(x_{a,2}),\cdots,f(x_{a,10})\}$;
    $S^- = S^- \bigcup s_a^-$;
  End for
End for
$D_2{}' = S^+ \bigcup S^-$;
Model = Model($D_2{}'$);
Return pretrained model.

Algorithm 2: Pretraining algorithm for network traffic model.

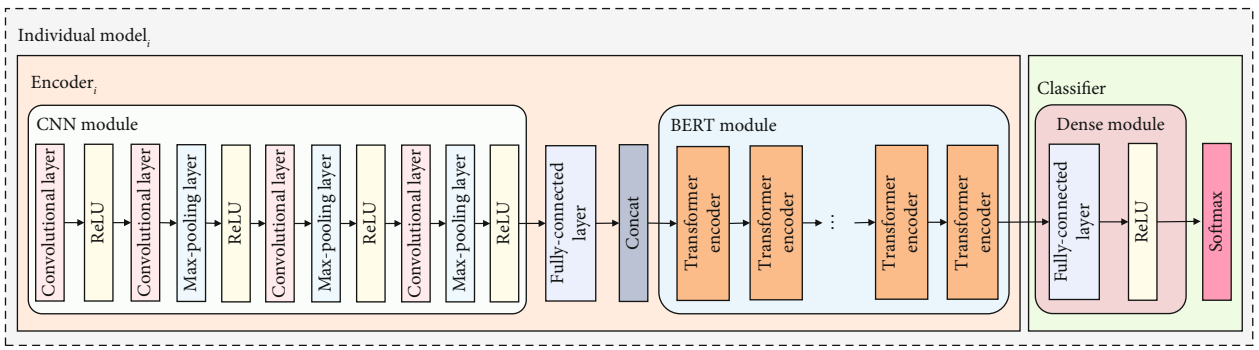


Figure 3: Structure diagram of individual model.

The last is the Softmax layer, defining $f_{\text{sm}}(\cdot)$ as the Softmax function, then

$$y = f_{\text{sm}}(f_D(v)) = \arg\max_l P(y = l|X),$$
$$P(y = l|X) = \frac{e^{F_l(X)}}{\sum_{p=1}^{k} e^{F_p(X)}}, \tag{21}$$

where $l, p \in \{1, 2, \cdots, k\}$ is the index of the class. So the output of the entire individual model is

$$y = f_{\text{sm}}(f_D(v)) = f_{\text{sm}}(f_D(f_B(Z))) = f_{\text{sm}}\left(f_D\left(f_B\left(\mathop{\oplus}_{i=1}^{n} z_i\right)\right)\right)$$
$$= f_{\text{sm}}\left(f_D\left(f_B\left(\mathop{\oplus}_{i=1}^{n} (W_i f_C(x_i) + B_i)\right)\right)\right). \tag{22}$$

3.3.3. Loss Function. Individual models are trained with a combination of cross-entropy loss and II-Loss [19].

The cross-entropy loss function is often used in classification problems, which can measure the similarity between several classes. Given a batch of samples $\{X_1, X_2, \cdots, X_A\}$, for a matrix $X_a, a = 1, 2, \cdots, A$, define its label as $\text{lab}(X_a) \in \{1, 2, \cdots, k\}$, then the cross-entropy loss of this batch of samples is

$$\text{CE-Loss} = -\frac{1}{A}\sum_{a=1}^{A}\sum_{l=1}^{k} \text{sgn}\,(X_a, l) \log P(X_a, l),$$
$$\text{sgn}\,(X_a, l) = \begin{cases} 1, & \text{lab}(X_a) = l, \\ 0, & \text{lab}(X_a) \neq l, \end{cases} \tag{23}$$

$$P(X_a, l) = P(\text{lab}(X_a) = l), \tag{24}$$

where $\text{sgn}\,(X_a, l)$ is a symbolic function, which determines whether the label of X_a is the class l. $P(X_a, l)$ is a probability function that calculates the probability that the label of X_a is the class l.

The II-Loss function can make samples of different classes farther apart and samples of the same class closer by maximizing the distance between different classes and minimizing the distance between samples and their class mean. Given a batch of samples $\{X_1, X_2, \cdots, X_A\}$, define the sample set of class l as C_l, the number of samples in C_l is $|C_l|$, the mean output of the dense module in C_l is μ_l, then

$$\{X_1, X_2, \cdots, X_A\} = C_1 \cup C_2 \cup \cdots \cup C_k,$$
$$\mu_l = \frac{1}{|C_l|}\sum_{q=1}^{|C_l|} F(X_q), \quad q = 1, 2, \cdots, |C_l|. \tag{25}$$

The II-Loss of this batch of samples is

$$\text{II-Loss} = \text{Dis(intra\_class)} - \text{Dis(inter\_class)}$$
$$= \left(\frac{1}{A}\sum_{l=1}^{k}\sum_{i=1}^{|C_l|} \|\mu_l - F(X_l)\|_2^2\right) - \left(\min_{1\le p,r\le k \& p=r} \left\|\mu_p - \mu_r\right\|_2^2\right). \tag{26}$$

The final loss function is

$$\text{Loss} = \text{CE-Loss} + \text{II-Loss} = \left(-\frac{1}{A}\sum_{a=1}^{A}\sum_{l=1}^{k} \text{sgn}\,(X_a, l) \log P(X_a, l)\right)$$
$$+ \left(\frac{1}{A}\sum_{l=1}^{k}\sum_{i=1}^{|C_l|} \|\mu_l - F(X_l)\|_2^2\right) - \left(\min_{1\le p,r\le k \& p=r} \left\|\mu_p - \mu_r\right\|_2^2\right). \tag{27}$$

3.4. Closed-Set Ensemble Training. The second stage is closed-set ensemble training. After the data is preprocessed, the ensemble model is trained with all N class known data to complete N-classification. The integrated strategy of the ensemble model adopts the learning method, which is a method of combining individual learners by training the learners. First, the encoder in the individual model is trained using a subset of the raw training dataset. Then, the ensemble model is trained with the raw training set using the output of the encoder as a feature. See Algorithm 3 for the ensemble strategy.

The training of the ensemble model takes t-fold cross-validation as an example and divides the known class dataset D and subset D' into t datasets $D_1, \cdots, D_t$ and $D'_1, \cdots, D'_t$, respectively. Let D'_j and $D'_{(-j)} = D' \setminus D'_j$ be the test set and training set corresponding to the jth individual model execution, respectively. D_j and $D_{(-j)} = D\,D_j$ are the test set and training set corresponding to the jth ensemble model execution, respectively. Given w individual learning algorithms, use the sth learning algorithm to train on $D'_{(-j)}$ to obtain an individual learner $h_s^{(-j)}$. For each sample X_i in the test set D'_j executed at the jth time, let z_{is} be the learner $h_s^{(-j)}$ on the X_i output result. Then, at the end of the entire cross-validation process, a new dataset can be generated by w individual learners $D* = \{(z_{i1}, \cdots, z_{iw}, y_i)\}_{i=1}^{R}$; the ensemble learner will use this dataset to train together with the dataset $D \setminus D'$ that does not participate in the training of individual models.

Lines 1-4 are the training of the individual model, which only uses a subset D' of the known class data D during training. Lines 5-12 are the training of the ensemble model, which uses all of the known class data D during training. The ensemble model consists of w encoders and 1 classifier. The encoder is obtained from the first stage of training, and the fixed structure and parameters remain unchanged. The classifier has the same structure as the first stage, but the specific parameters have changed. Define X as the input of the ensemble model, y_{pred} as the output, $f_D^*(\cdot)$ as the dense module function, $G(X)$ as the dense module output, and $f_{sm}^*(\cdot)$ as

Input: known classes data $D = \{(X_1, L_1), (X_2, L_2), \cdots, (X_R, L_R)\}$; individual learning algorithm $\mathscr{T}_1, \mathscr{T}_2, \cdots, \mathscr{T}_w$; ensemble learning algorithm $\mathscr{E}$.
Output: ensemble model H;
Randomly selected k classes data from D to form D', $D' \subset D$;
For $s = 1, 2, \cdots, w$ **do**
  $h_s = \mathscr{T}_t(D')$;
End for
$D^* = \varnothing$;
For $i = 1, 2, \cdots, R$ **do**
  For $s = 1, 2, \cdots, w$ **do**
    $z_{rs} = h_s(X_r)$;
  End for
  $D^* = (D \setminus D') \cup ((z_{r1}, z_{r2}, \cdots, z_{rw}), y_r)$;
End for
$h^* = \mathscr{E}(D^*)$;
$H(X) = h^*(h_1(X), h_2(X), \cdots, h_w(X))$.

Algorithm 3: Ensemble strategy.

Input: training set $\{X_1, X_2, \cdots, X_A\}$; known classes N.
Output: threshold τ;
For $i = 1, 2, \cdots, A$ **do**
  For $j = 1, 2, \cdots, N$ **do**
    $P(y = j|X_i) = e^{F_j(X_i)} / \sum_{p=1}^{k} e^{F_p(X_i)}$;
  End for
  outlier$(X_i) = \max_j P(y = j|X_i)$;
End for
sort(outlier);
Threshold set = last 1% sort(outlier);
Return τ = min (threshold set).

Algorithm 4: Threshold estimation.

Table 3: Experimental data classes.

Known/unknown	Classes
Known classes	VPN-Facebook-chat
	VPN-Facebook-audio
	VPN-Skype-chat
	VPN-Skype-file
	Facebook-chat
	Facebook-audio
	Skype-chat
	Skype-file
	VPN-Hangouts-audio
Unknown classes	Hangouts-audio
	VPN-Hangouts-chat
	Skype-audio
	VPN-sftp

Table 4: Experimental environment.

Hardware	Specific information
Graphic processing unit (GPU)	Nvidia RTX 1060TI
Memory	48 GB
Central processing unit (CPU)	Intel Core i7 6-core
Number of CPUs	Number of CPU cores: 6 Number of CPU threads: 12
Operating system (OS)	Ubuntu 18.04

the Softmax function, then

$$\text{Ensemble model}: X \longrightarrow y_{\text{pred}} \in \{1, 2, \cdots, N\},$$

$$G(X) \triangleq f_D^*\left(\sum_{s=1}^{w} v_s\right),$$

$$y_{\text{pred}} = f_{\text{sm}}^*(G(X)) = f_{\text{sm}}^*\left(f_D^*\left(\sum_{s=1}^{w} v_s\right)\right) = \arg \max_{l'} P\left(y = l'|X\right),$$

$$P\left(y = l'|X\right) = \frac{e^{G_{l'}(X)}}{\sum_{p'=1}^{N} e^{G_{p'}(X)}}, \tag{28}$$

where w is the number of encoders in the ensemble model, each encoder comes from the corresponding individual model, and the coefficients remain unchanged. $f_D^*(\cdot)$ and $f_{\text{sm}}^*(\cdot)$ have the same structure as the dense module function $f_D(\cdot)$ and Softmax function $f_{\text{sm}}(\cdot)$ in the individual model but with different coefficients. $l', p' \in \{1, 2, \cdots, N\}$ is the index of the class.

3.5. Open-Set Testing. The third stage is open-set testing. The real-world data is inputted into the trained ensemble model, and the ensemble model produces M results Rec to be identified. Compute the maximum of the M results. If the maximum value is greater than or equal to the threshold, the

Table 5: Experimental hyperparameters.

Hyperparameter name	Hyperparameter value
Epoch	80 in individual model, 60 in ensemble model
Batch	64
Plaintext packets in pretraining	256 bytes of plaintext
Ciphertext packets in pretraining	Randomly selected from ISCXVPN2016, excluding the 13 classes mentioned above, and classes and sizes are not fixed
Sample numbers of positive and negative sample sets in pretraining	5000, 5000
k in individual model	3 or 4 or 5 or 6 or 7
Dimensions of CNN module input vectors	256
Number of convolution channels in CNN module	1
Convolution kernel size in CNN module	3
Convolution stride size in CNN module	1
Pooling size in CNN module	3
Dimensions of CNN module output vectors	242
Dimensions of fully connected layer outputs in the encoder	240
n in Concat layer	15
Dimensions of BERT module input matrix	15×240
m in BERT module	8
Head numbers of multihead attention in each transformer encoder layer	12
Dimensions of BERT module output vectors	240
Dimensions of fully connected layer outputs in classifier	k in individual model, N in ensemble model
Number of encoders w in ensemble model	4 or 8 or 12
N in ensemble model	8
M in open-set testing	$N + 1 = 9$

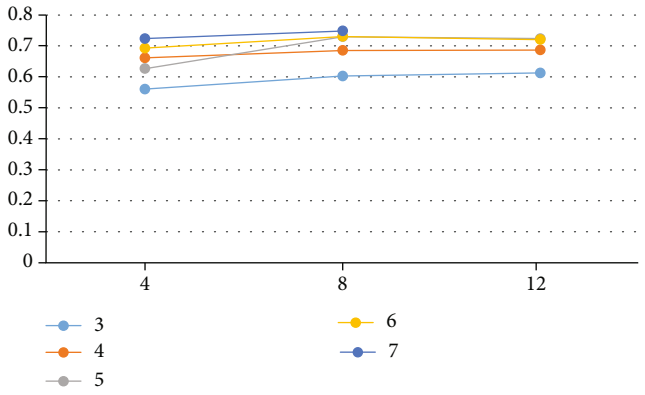


Figure 4: When the number of encoders in the ensemble model of OpenCBD is 4, 8, and 12, accuracy of the 2-class classification tasks (identifying known and unknown classes) varies as the number of known classes is randomly selected in the first training stage.

test sample is classified as one of M classes; otherwise, it is classified as unknown.

3.5.1. Threshold Estimation. The threshold for judging data classes in open-set testing is determined by outliers. Assume that 1% of the samples in the training set have noise, that is, they are abnormal outlier samples. When calculating the outlier distance for all training samples, sort them from small to large, and the largest 1% distance is the threshold. The detailed process of threshold estimation is shown in Algorithm 4.

After the threshold is determined, the to-be-identified results of the ensemble model will determine the classes of data according to whether it is greater than or equal to the threshold.

4. Experiment and Evaluation

This section mainly introduces the specific experimental content designed for the proposed model OpenCBD, including experimental environment and settings, evaluation metrics, and specific results. And then, the results are discussed to verify the validity of the OpenCBD model.

4.1. Experiment Settings. The encrypted traffic data in this paper is selected from the public dataset ISCXVPN2016 [39]. 8 classes of data are selected as known classes, 5 classes of data are selected as unknown classes, and the intersection of known and unknown data is empty. The 13 classes of data

Table 6: When the number of encoders in the ensemble model of OpenCBD is 4, 8, and 12, accuracy, precision, recall, and F1-score of the 2-class classification tasks (identifying known and unknown classes) vary as the number of known classes is randomly selected in the first training stage.

k	Accuracy			Precision			Recall			F1-score		
	w											
	4	8	12	4	8	12	4	8	12	4	8	12
3	0.5607	0.603	0.613	0.714	0.6853	0.6951	0.4775	0.6562	0.6612	0.5722	0.6704	0.6777
4	0.6615	0.6853	0.6869	0.7337	0.7459	0.7484	0.7062	0.7412	0.74	0.7197	0.7435	0.7441
5	0.6269	0.73	0.7238	0.7215	0.765	0.778	0.6412	0.81	0.7712	0.67902	0.7868	0.7746
6	0.693	0.7307	0.7207	0.775	0.7952	0.7841	0.7062	0.7575	0.7537	0.739	0.7759	0.7686
7	0.7238	0.7484	—	0.7766	0.7832	—	0.7737	0.8175	—	0.7752	0.7999	—

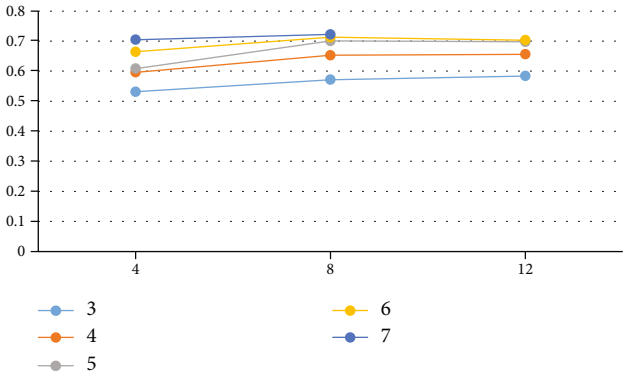


Figure 5: When the number of encoders in the ensemble model of OpenCBD is 4, 8, and 12, accuracy of the 9-class classification tasks (identifying 8 known classes and 1 unknown class) varies as the number of known classes is randomly selected in the first training stage.

include both Virtual Private Network (VPN) traffic that has been encapsulated by the VPN protocol and non-VPN traffic that has not been encapsulated by the VPN. 1000 samples are randomly selected for each class, and each sample contains 10 consecutive data packets. The specific data classes are shown in Table 3.

During the experiment, 1000 samples of each class were randomly divided into the training set and test set, with training set samples : test set samples = 9 : 1; that is, 100 samples of each class were randomly selected as the test set, and the remaining 900 samples were the training set. The training set contains training data and validation data, with training data : validation data = 9 : 1.

The experimental environment is a personal desktop, and the specific equipment information is shown in Table 4.

All codes in the experiment are run in the environment of Python 3.6.5, and the specific hyperparameter settings are shown in Table 5.

The rest of the unmentioned hyperparameters are set according to the default values of the corresponding models in Python.

4.2. Evaluation Metrics. When evaluating model performance, the class of interest is usually the positive class and the other classes are the negative classes. Evaluation metrics are usually formulated from the following four basic situations:

(1) *True positive (TP)*: predict the positive class as a positive class

(2) *False positive (FP)*: predict the negative class as a positive class

(3) *True negative (TN)*: predicts the negative class as a negative class

(4) *False negative (FN)*: predicts the positive class as a negative class

From the above four basic situations, four basic evaluation metrics can be obtained:

(1) The probability of classifying positive samples into positive classes is called TPR, also known as recall or sensitivity:

$$\mathrm{TPR} = \mathrm{Recall} = \frac{\mathrm{TP}}{\mathrm{TP} + \mathrm{FN}}. \tag{29}$$

(2) The probability of classifying a negative class sample into negative classes is called TNR, also known as specificity:

$$\mathrm{TNR} = \frac{\mathrm{TN}}{\mathrm{FP} + \mathrm{TN}}. \tag{30}$$

(3) The probability of misclassifying negative samples into positive classes is called FPR, also known as false recognition rate:

$$\mathrm{FPR} = \frac{\mathrm{FP}}{\mathrm{FP} + \mathrm{TN}} = 1 - \mathrm{TNR}. \tag{31}$$

Table 7: When the number of encoders in the ensemble model of OpenCBD is 4, 8, and 12, accuracy, precision, recall, and F1-score of the 9-class classification tasks (identifying 8 known classes and 1 unknown class) vary as the number of known classes is randomly selected in the first training stage.

k	Accuracy			Precision			Recall			F1-score		
	w											
	4	8	12	4	8	12	4	8	12	4	8	12
3	0.5315	0.5715	0.5838	0.6462	0.6717	0.6893	0.4593	0.5953	0.6051	0.5019	0.6144	0.6258
4	0.5961	0.653	0.656	0.6241	0.7137	0.723	0.5988	0.6784	0.6813	0.5994	0.6863	0.6929
5	0.6084	0.7007	0.6976	0.6991	0.7425	0.7355	0.6104	0.7446	0.7197	0.6343	0.7385	0.7227
6	0.6646	0.713	0.703	0.7419	0.7704	0.772	0.6613	0.7242	0.7186	0.6845	0.7395	0.7339
7	0.7046	0.7223	—	0.7639	0.7616	—	0.7315	0.7597	—	0.7404	0.7533	—

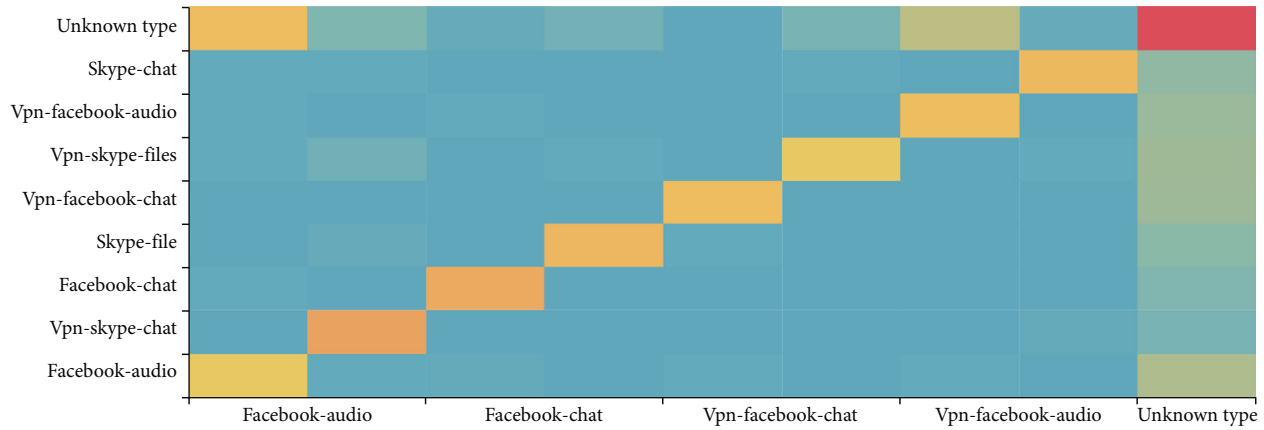


Figure 6: Confusion matrix diagram for OpenCBD doing the 9-class classification tasks. The x-axis represents the predicted classes of the output, and the y-axis represents the true classes. Warmer colors indicate larger values, and cooler colors indicate smaller values.

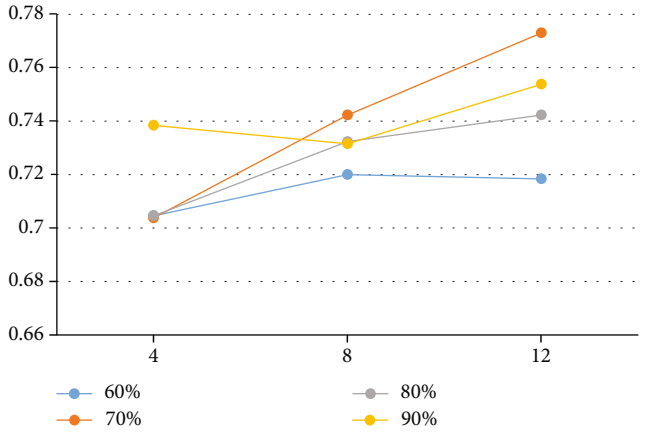


Figure 7: When the number of encoders in the ensemble model of OpenCBD is 4, 8, and 12, accuracy of the 2-class classification tasks (identifying known and unknown classes) varies with increasing percentage of known classes randomly selected.

(4) The probability of misclassifying positive samples into negative classes is called FNR, also known as the rejection rate:

$$\mathrm{FNR} = \frac{\mathrm{FN}}{\mathrm{FN} + \mathrm{TP}} = 1 - \mathrm{TPR}. \tag{32}$$

In addition, there are several other commonly used metrics:

(1) Precision refers to the proportion of true positive samples among all predicted positive samples:

$$\mathrm{Precision} = \frac{\mathrm{TP}}{\mathrm{TP} + \mathrm{FP}}. \tag{33}$$

(2) F1-score considers precision and recall comprehensively and refers to the harmonic average of precision and recall:

$$\begin{aligned} \frac{2}{\text{F1-score}} &= \frac{1}{\mathrm{Precision}} + \frac{1}{\mathrm{Recall}}, \\ \text{F1-score} &= 2 \times \mathrm{Precision} \times \frac{\mathrm{Recall}}{\mathrm{Preciaion} + \mathrm{Recall}}. \end{aligned} \tag{34}$$

(3) Accuracy refers to the proportion of all predicted correct samples to the total samples:

Table 8: When the number of encoders in the ensemble model of OpenCBD is 4, 8, and 12, accuracy, precision, recall, and F1-score of the 2-class classification tasks (identifying known and unknown classes) vary with increasing percentage of known classes randomly selected.

k	Accuracy			Precision			Recall			F1-score		
	w											
	4	8	12	4	8	12	4	8	12	4	8	12
60%	0.7046	0.72	0.7184	0.753	0.7678	0.7726	0.7737	0.7812	0.7687	0.7632	0.7744	0.7706
70%	0.7038	0.7423	0.773	0.767	0.8015	0.8371	0.745	0.7725	0.7837	0.7558	0.7867	0.8095
80%	0.7046	0.7323	0.7423	0.7619	0.786	0.8047	0.7563	0.7762	0.7675	0.759	0.7811	0.7856
90%	0.7384	0.7315	0.7538	0.7875	0.7909	0.8269	0.7875	0.7662	0.7587	0.7875	0.7784	0.7913

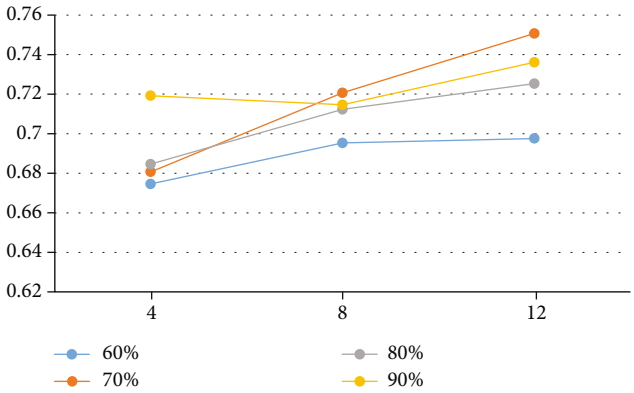


Figure 8: When the number of encoders in the ensemble model of OpenCBD is 4, 8, and 12, accuracy of the 9-class classification tasks (identifying 8 known classes and 1 unknown class) varies with increasing percentage of known classes randomly selected.

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}} = \frac{n_{\text{correct}}}{n}, \tag{35}$$

where n_{correct} represents the number of correctly predicted samples and n represents the total number of samples.

(4) In the multiclassification problem, the F1-score, precision, and recall are all calculated by macro; that is, the index of each class is calculated first, and then, the unweighted average is taken to obtain the final index:

$$\begin{aligned} \text{macro-F1-score} &= \frac{1}{C}\sum_{i=1}^{C} \text{F1-score}_i, \\ \text{Macro-precision} &= \frac{1}{C}\sum_{i=1}^{C} \text{precision}_i, \\ \text{Macro-recall} &= \frac{1}{C}\sum_{i=1}^{C} \text{recall}_i, \end{aligned} \tag{36}$$

where C represents the number of classes.

The evaluation metrics of this experiment select accuracy, precision, recall, and F1-score of binary classification and multiclassification.

4.3. Results and Discussions. According to the detailed experimental setting in Section 4.1 and the four evaluation metrics in Section 4.2, we present the specific experimental results in this section. The first is the experimental results of OpenCBD when doing 2-class classification tasks.

As can be seen from Figure 4 and Table 6, OpenCBD performs best when 7 known classes are randomly selected in the first stage of training. Because there are 8 known classes, each individual model randomly selects 7 classes for training, which enables the individual model to better understand the differences between different known classes and makes the model perform better. On the whole, the increase in the number of encoders helps to improve the performance of the model, but too many encoders will also lead to excessive time overhead of the model, and the performance improvement is no longer obvious. In Figure 4 and Table 6, when 7 known classes are randomly selected and the number of encoders is 12, there is no result. The reason is that 7 classes are randomly selected from the 8 known classes, and there are a total of $C_8^7 = 8$ possibilities. If 12 encoders are integrated, there must be repetitions.

While OpenCBD can distinguish known from unknown, it can also distinguish known classes.

It can be seen from Figure 5 and Table 7 that OpenCBD performs the best when 7 known classes are randomly selected in the first stage of training. Accuracy of 9 classes is over 72%, precision is over 76%, and recall and F1-score are over 75%.

As can be seen from Figure 6, the probability of Facebook-audio being wrongly classified into an unknown class is higher than the other 7 classes. Since there are 5 classes of data that are regarded as an unknown class, the number of unknown classes predicted as the unknown class is the largest and the color is the warmest (red).

In addition, we design different random selection methods in the first stage of training. A portion of each of the 8 classes of data is randomly selected, and the results are as follows.

As can be seen from Figure 7 and Table 8, the results of this training method are not much different from the original results, but the overall results of this method are slightly higher, all above 70%, and the highest accuracy can achieve more than 77%, and precision even exceeds 83%. Since all 8 known classes have data to participate in the training of the individual model in this method, the ensemble model learns more deeply for each known class.

Table 9: When the number of encoders in the ensemble model of OpenCBD is 4, 8, and 12, accuracy, precision, recall, and F1-score of the 9-class classification tasks (identifying 8 known classes and 1 unknown class) vary with increasing percentage of known classes randomly selected.

k	Accuracy			Precision			Recall			F1-score		
	w											
	4	8	12	4	8	12	4	8	12	4	8	12
60%	0.6746	0.6953	0.6976	0.7342	0.7544	0.7532	0.7104	0.728	0.7242	0.714	0.7363	0.7334
70%	0.6807	0.7207	0.7507	0.7523	0.7835	0.8031	0.6997	0.7326	0.7484	0.7159	0.7502	0.7685
80%	0.6846	0.7123	0.7253	0.7469	0.7779	0.7836	0.7124	0.7346	0.7357	0.7226	0.746	0.7533
90%	0.7192	0.7146	0.7361	0.771	0.7798	0.7939	0.7455	0.7317	0.7317	0.7519	0.7472	0.7526

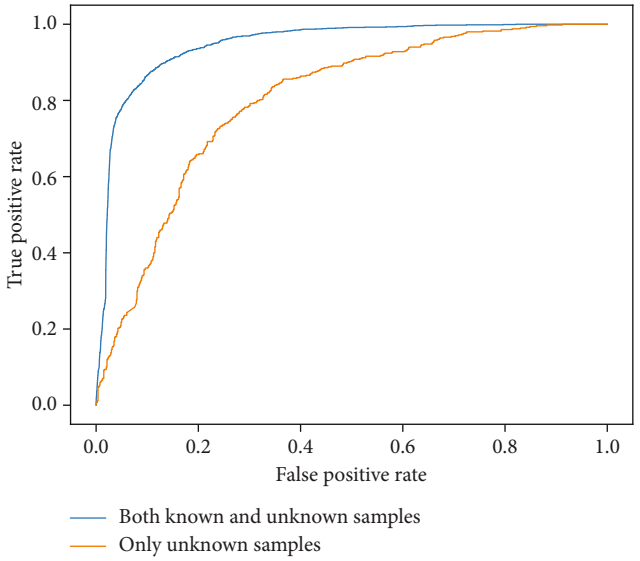


Figure 9: Area under ROC of OpenCBD when only identifying unknown class samples and both known and unknown class samples.

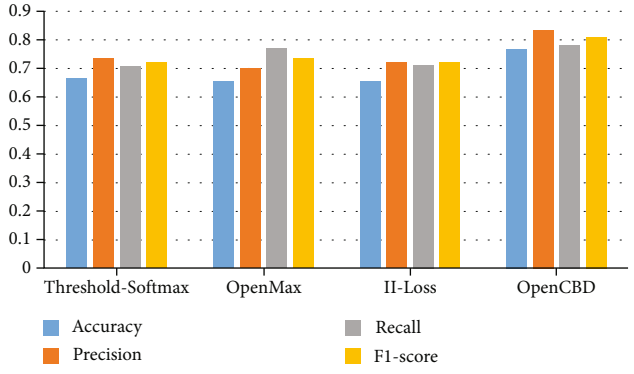


Figure 10: Performance comparison of four models on 2-class classification tasks.

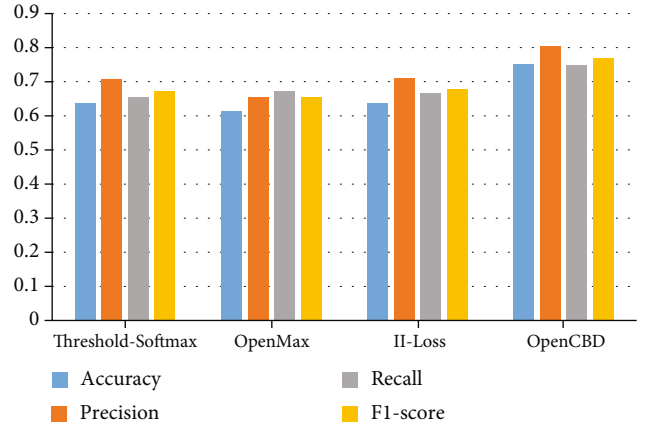


Figure 11: Performance comparison of four models on 9-class classification tasks.

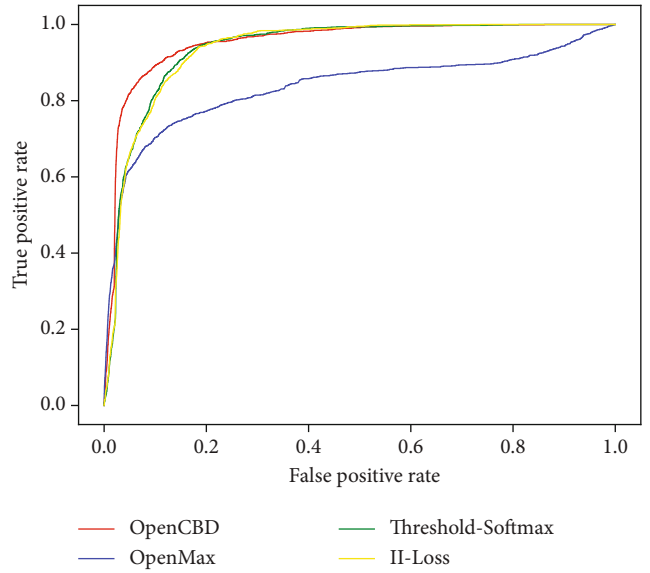


Figure 12: Area under ROC of four models.

As can be seen from Figure 8 and Table 9, when OpenCBD is doing 9-class classification tasks, the values of the 4 evaluation metrics increase with the increase of the number of encoders, and the results are better when the percentage of known classes is 70%. The highest accuracy can reach 73.61%, the highest precision is over 80%, the highest recall is nearly 75%, and the highest F1-score is 65.85%.

When the individual training selects 70% of the training set and the number of encoders is 12, the metrics of the two classes and nine classes are the highest. Therefore, we choose this ensemble method and compare the area under the ROC

curve (receiver operating characteristic curve) of identifying only unknown classes and identifying both known and unknown classes at the same time. The results are shown in Figure 9.

When verifying the performance of the OpenCBD model, we also selected several classic open-set recognition models for comparative experiments. We choose 3 models, namely, the threshold-based Softmax model [15], OpenMax model [15], and II-Loss-based model [19].

It can be seen from Figure 10 that the values of the four metrics in the 2-class classification of the OpenCBD model are basically around 80%, and the other three are around 70%. Our OpenCBD outperforms the other 3 by around 10% in the 2-class classification tasks. It can be seen from Figure 11 that in the 9-class classification, the metrics of the OpenCBD model are between 75% and 80%, and the other three are basically not more than 70%. Our OpenCBD outperforms the other 3 models by around 5%-10% in 9-class classification tasks. Figure 12 compares the area under ROC of the four models more clearly; the larger the area, the better the effect; and OpenCBD is significantly better than the other three.

5. Conclusion

In this paper, we proposed a novel model that can simultaneously identify unknown traffic and classify known traffic. The model could be trained on the known traffic of the closed set and tested on the network traffic of the open set. The model first combined the convolutional neural network and the transformer encoder to construct a deep learning-based model. Then, use the general pretraining method in the field of encrypted traffic analysis to pretrain from unlabeled traffic data, so that the model could learn the basic characteristics of encrypted traffic. Then, according to the characteristics of the open set, a three-stage training and testing process was designed. During training, choose the cross-entropy loss function suitable for classification and the II-Loss function suitable for clustering. At the same time, using the idea of ensemble learning, a traffic identification model OpenCBD based on open-set recognition was constructed. For real-world traffic data, if it belonged to a known class, the class to which it belonged can be identified, and if it belonged to an unknown class, it can be identified to belong to an unknown class. Experiments were carried out in public datasets, 8 classes of data were selected as known classes and 5 classes of data were selected as unknown classes, and a class-balanced dataset was constructed in the experiment to eliminate possible human influence to the greatest extent.

In the future work, we can consider the clustering of unknown classes of encrypted traffic and further separate unknown traffic according to its characteristics, which is convenient for further discovery and research of new classes of traffic.

Data Availability

This paper uses the ISCX public traffic dataset which is available in [39].

Conflicts of Interest

The authors declare that there is no conflict of interest regarding the publication of this paper.

Acknowledgments

This work was supported in part by the National Natural Science Foundation of China under Grant 61772548.

References

[1] M. Abbasi, A. Shahraki, and A. Taherkordi, "Deep learning for network traffic monitoring and analysis (NTMA): a survey," *Computer Communications*, vol. 170, pp. 19–41, 2021.

[2] B. Li, J. Springer, G. Bebis, and M. Hadi Gunes, "A survey of network flow applications," *Journal of Network and Computer Applications*, vol. 36, no. 2, pp. 567–581, 2013.

[3] W. Wang, M. Zhu, and J. Wang, Eds.X. Zeng and Z. Yang, "End-to-end encrypted traffic classification with one-dimensional convolution neural networks," in *2017 IEEE international conference on intelligence and security informatics (ISI)*, pp. 43–48, Beijing, China, 2017.

[4] G. Aceto, D. Ciuonzo, A. Montieri, and A. Pescapé, "Mobile encrypted traffic classification using deep learning: experimental evaluation, lessons learned, and challenges," *IEEE Transactions on Network and Service Management*, vol. 16, no. 2, pp. 445–458, 2019.

[5] G. Aceto, D. Ciuonzo, A. Montieri, and A. Pescapé, "MIMETIC: mobile encrypted traffic classification using multimodal deep learning," *Computer Networks*, vol. 165, p. 106944, 2019.

[6] C. Liu, L. He, G. Xiong, Z. Cao, and Z. Li, "FS-Net: a flow sequence network for encrypted traffic classification," in *IEEE INFOCOM 2019 - IEEE Conference on Computer Communications*, pp. 1171–1179, Paris, France, 2019.

[7] X. Wang, S. Chen, and S. Jinshu, "Automatic mobile app identification from encrypted traffic with hybrid neural networks," *IEEE Access*, vol. 8, pp. 182065–182077, 2020.

[8] A. Nascita, A. Montieri, G. Aceto, D. Ciuonzo, V. Persico, and A. Pescape, "XAI meets mobile traffic classification: understanding and improving multimodal deep learning architectures," *IEEE Transactions on Network and Service Management*, vol. 18, no. 4, pp. 4225–4246, 2021.

[9] R. Yoshihashi, W. Shao, R. Kawakami, S. You, M. Iida, and T. Naemura, "Classification-reconstruction learning for open-set recognition," in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, pp. 4016–4025, Long Beach, CA, USA, 2019.

[10] W. J. Scheirer, A. de Rezende Rocha, A. Sapkota, and T. E. Boult, "Toward open set recognition," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 35, no. 7, pp. 1757–1772, 2013.

[11] S. Cruz, C. Coleman, E. M. Rudd, and T. E. Boult, "Open set intrusion recognition for fine-grained attack categorization," in *2017 IEEE International Symposium on Technologies for Homeland Security (HST)*, pp. 1–6, Waltham, MA, USA, 2017.

[12] X. Hu, G. Chunxiang, Y. Chen, and F. Wei, "CBD: a deep-learning-based scheme for encrypted traffic classification with a general pre-training method," *Sensors (Basel, Switzerland)*, vol. 21, no. 24, p. 8231, 2021.

[13] A. Bendale and T. E. Boult, "Towards open world recognition," in *2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, pp. 1893–1902, Boston, MA, USA, 2015.

[14] C. Geng, S.-J. Huang, and S. Chen, "Recent advances in open set recognition: a survey," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 43, no. 10, pp. 3614–3631, 2021.

[15] A. Bendale and T. E. Boult, "Towards open set deep networks," in *2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, pp. 1563–1572, Las Vegas, NV, USA, 2016.

[16] Z. Y. Ge, S. Demyanov, Z. Chen, and R. Garnavi, "Generative OpenMax for multi-class open set classification," in *British Machine Vision Conference*, London, UK, 2017.

[17] R. Yoshihashi, W. Shao, R. Kawakami, S. You, M. Iida, and T. Naemura, "Classification-reconstruction learning for open-set recognition," in *2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, pp. 4011–4020, Long Beach, CA, USA, 2019.

[18] P. Oza and V. M. Patel, "C2AE: class conditioned auto-encoder for open-set recognition," in *2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, pp. 2302–2311, Long Beach, CA, USA, 2019.

[19] M. Hassen and P. K. Chan, "Learning a neural-network-based representation for open set recognition," in *Proceedings of the 2020 SIAM International Conference on Data Mining*, pp. 154–162, Cincinnati, Ohio, USA, 2020.

[20] B. Liu, H. Kang, H. Li, G. Hua, and N. Vasconcelos, "Few-shot open-set recognition using meta-learning," in *2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, pp. 8795–8804, Seattle, WA, USA, 2020.

[21] K. J. Joseph, S. H. Khan, F. S. Khan, and V. N. Balasubramanian, "Towards open world object detection," in *2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, pp. 5826–5836, 2021.

[22] C. Geng and S. Chen, "Collective decision for open set recognition," *IEEE Transactions on Knowledge and Data Engineering*, vol. 34, no. 1, pp. 192–204, 2022.

[23] A. Finamore, M. Mellia, and M. Meo, "Mining unclassified traffic using automatic clustering techniques," *Traffic Monitoring and Analysis (TMA)*, vol. 6613, pp. 150–163, 2011.

[24] C. Jun Zhang, Y. X. Chen, W. Zhou, and A. V. Vasilakos, "An effective network traffic classification method with unknown flow detection," *IEEE Transactions on Network and Service Management*, vol. 10, no. 2, pp. 133–147, 2013.

[25] J. Zhang, C. Chen, Y. Xiang, and W. Zhou, "Robust network traffic identification with unknown applications," in *Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security (ASIA CCS'13)*, Hangzhou, China, 2013.

[26] H. Yu, Y. Zhao, G. Xiong, L. Guo, Z. Li, and Y. Wang, "Poster: mining elephant applications in unknown traffic by service clustering," in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security (CCS '14)*, pp. 1532–1534, Scottsdale, Arizona, USA, 2014.

[27] Z. A. Shaikh and D. G. Harkut, "A novel framework for network traffic classification using unknown flow detection," in *2015 Fifth International Conference on Communication Systems and Network Technologies*, pp. 116–121, Gwalior, India, 2015.

[28] R. Lin, O. Li, Q. Li, and Y. Q. Liu, "Unknown network protocol classification method based on semi-supervised learning," in *2015 IEEE International Conference on Computer and Communications (ICCC)*, pp. 300–308, Chengdu, China, 2015.

[29] R. Ma and S. Qin, "Identification of unknown protocol traffic based on deep learning," in *2017 3rd IEEE International Conference on Computer and Communications (ICCC)*, pp. 1195–1198, Chengdu, China, 2017.

[30] F. Ningjia, X. Yuwei, J. Zhang, R. Wang, and J. Xu, "FlowCop: detecting "stranger" in network traffic classification," in *2018 27th International Conference on Computer Communication and Networks (ICCCN)*, pp. 1–9, Hangzhou, China, 2018.

[31] U. Sabeel, S. S. Heydari, H. Mohanka, Y. Bendhaou, K. Elgazzar, and K. El-Khatib, "Evaluation of deep learning in detecting unknown network attacks," in *2019 International Conference on Smart Applications, Communications and Networking (SmartNets)*, pp. 1–6, Sharm El Sheikh, Egypt, 2019.

[32] Y. Zhang, J. Niu, D. Guo, Y. Teng, and X. Bao, "Unknown network attack detection based on open set recognition," *Procedia Computer Science*, vol. 174, pp. 387–392, 2020.

[33] J. Zhang, F. Li, F. Ye, and H. Wu, "Autonomous unknown-application filtering and labeling for DL-based traffic classifier update," in *IEEE INFOCOM 2020 - IEEE Conference on Computer Communications*, pp. 397–405, Toronto, ON, Canada, 2020.

[34] A. A. Mohamed, A. H. Osman, and A. Motwakel, "Classification of unknown internet traffic applications using multiple neural network algorithm," in *2020 2nd International Conference on Computer and Information Sciences (ICCIS)*, pp. 1–6, Sakaka, Saudi Arabia, 2020.

[35] Y. Wang, B. Bai, X. Hei, L. Zhu, and W. Ji, "An unknown protocol syntax analysis method based on convolutional neural network," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 5, 2021.

[36] J. Li, C. Gu, F. Wei et al., "LightSEEN: real-time unknown traffic discovery via lightweight Siamese networks," *Networks*, vol. 2021, pp. 1–12, 2021.

[37] X. Shuyuan, L. Li, H. Yang, and J. Tang, "KCC method: unknown intrusion detection based on open set recognition," in *2021 IEEE 33rd International Conference on Tools with Artificial Intelligence (ICTAI)*, pp. 1343–1347, Washington, DC, USA, 2021.

[38] X. Hu, G. Chunxiang, and F. Wei, "CLD-Net: a network combining CNN and LSTM for internet encrypted traffic classification," *Security and Communication Networks*, vol. 2021, 15 pages, 2021.

[39] G. Draper-Gil, A. H. Lashkari, M. S. I. Mamun, and A. A. Ghorbani, "Characterization of encrypted and VPN traffic using time-related features," in *Proceedings of the 2nd international conference on information systems security and privacy (ICISSP)*, Rome, Italy, 2016.

Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 2335313, 14 pages
https://doi.org/10.1155/2022/2335313

Research Article

Towards Enhancing the Capability of IoT Applications by Utilizing Cloud Computing Concept

Habib Ullah Khan,[1] **Farhad Ali**,[1] **Yasser Alshehri**,[2] **and Shah Nazir**[3]

[1]*Department of Accounting and Information Systems, College of Business and Economics, Qatar University, Doha, Qatar*
[2]*Yanbu Industrial College, Royal Commission at Yanbu, Saudi Arabia*
[3]*Department of Computer Science, University of Swabi, Pakistan*

Correspondence should be addressed to Habib Ullah Khan; habib.khan@qu.edu.qa

Received 11 February 2022; Accepted 18 April 2022; Published 11 May 2022

Academic Editor: Md. Shamsul Huda

 The publication of this article was funded by Qatar National Library.

The emergence of smart and innovative applications in diverse domains has inspired our lives by presenting many state-of-the art applications ranging from offline to smart online systems, smart communication system to tracking systems, and many others. The availability of smart internet enabled systems has made the world as a global village where people can collaborate, communicate, and share information in secure and timely manner. Innovation in information technology focuses on investigating characteristics that make it easier for the people to accept and distribute innovative IT-based processes or products. To provide elastic services and resource the Internet service provider developed cloud computing to support maximal number of users. Cloud computing is a subscription paradigm in which users do not buy various resources permanently, but they purchase it with block chain-driven payment schemes (credit cards). A flexible, on-demand, and dynamically scalable computer infrastructure is offered by cloud providers to its clients on charging some amount of subscription. This research article provides an introduction of cloud computing and the integration of IoT concept, its impacts on crowd and organizations, provision of various services, and analyzing and selecting the appropriate features using probability distribution function for enhancing cloud-based IoT capabilities. In ambiguous and complex situations, decision makers use quantitative techniques combined with traditional approaches to select the appropriate one among a group of features. Probability distribution function is used to evaluate the appropriate features that will enhance the capabilities of cloud-based IoT application.

1. Introduction

Information technology has innovated our lives by presenting many state-of-the art applications ranging from healthcare to navigation systems, eHealth to m-Health systems, and many others [1]. These applications not only facilitated us by presenting routine services at doorstep but also reduced our efforts on performing different tasks. Technological fusion facilitates significant changes and encourages new IT products, processes, and services to be developed [2]. The emergence of internet of things- (IoT-) based devices has chosen new paths for the organizations to perform their normal operations with different perspectives and with more outcomes. Informational technology advancements enabled the organizations to respond technological developments in current operations by developing new capabilities that precede new opportunities. In the perspective of transformative trends in the development of information technology, cloud computing provides an environment where shared processors, laptops, computers, sensors, and various form of communication technologies are integrated to provide easy access to virtual resources [3].

The word "cloud" has originated from the telecommunication industry when providers began to use VPN networks to exchange data [4]. Clouds are some virtual computer resources, generally include server clusters, storage server, broadband resources calculations server, etc. [5]. Information technology made transferring data and computation

possible from desktops and personal computer systems to massive virtual data centers. It involves provisioning of hardware and software application supplied as Internet services in virtual data centers [6]. According to NIST *"Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability"* [7].

Virtualized resources are dynamically delivered to consumers via the Internet as services by means of devices such as laptops, computers, cell phones, and PDAs that are connected to cloud for accessing, developing, and storing program [8]. The IT efficiency and the computation power is efficiently used by scaling of hardware and software among users and business agility where IT works as a tool for deployment, processing, business analytics, and interaction by means of cell phone works in timely manner to achieve the requirements of users [9]. Resources are physically distributed and shared but are logically presented in single and complete forms. When necessary, users access the resources and pay for the quantity, but they do not manage them. To achieve the computation power, the tasks in cloud computing are distributed on the resource pool "Cloud" that consists of a huge group of computers, the storage memory, and applications in accordance to task requirements [5, 9]. Cloud computing has multiple implementation paradigms, each of which gives different offsets to organizations that migrate their processes to a cloud environment.

Resources are supplied in a firewall and retained in private clouds by the user entity. User entity manages the cloud resources with their own physical infrastructure and software's. In general, these services and resources are not shared publicly [10]. The major advantage here is that maintenance, upgradation, and security are more easily handled, and that deployment and operation are also effectively controlled [11]. When a large number of organizations build polices, share their needs, and cloud infrastructure together, then this is termed as community cloud model [10, 11]. Community cloud computing is a promising and evolving computing model for a particular community with similar issues, such as security, licensing, and governance. It uses networked alternative resources to provide the capabilities for communities to obtain cloud services. Effective collaboration between community clouds provides a strong computational capability for complicated jobs involving tasks that requires sharing of data [12].

In public clouds, provision of resources is made available to users as a service, mainly via internet, on a subscription charge (money). Users can utilize them on request without buying hardware permanently from organizations. Providers in public cloud control and manage their overall infrastructure and share resources to their users' accordingly with their demands [10]. Public cloud provides consumers with access to the cloud via various websites. Users of the cloud are only charged according to their usage and service's duration. This contributes to the reduction of the IT operating costs for individuals and organizations. Security of public cloud is less as compared with other cloud models therefore their software and applications are susceptible to various threats and therefore internal standard must be aligned with providers and users, security architectures must be updated, software maintained, and upgradation is necessary after some time. A specific strategy might be implemented to ensure security by validating the vendor and the customer from both sides. Commitment of both parties within their confines must also be well established [11]. The integration of public, private, and communal clouds forms hybrid clouds [10]. Companies of all capacities are utilizing it for cost optimizations [13]. The hybrid cloud model is the ideal solution to both the private and public world, combining public cloud model economies and efficiency with private cloud model for enhancing the security and control [14].

For utilizing all the services of cloud computing there is a need for integrating IoT with cloud technologies. Researchers are working to unite these technologies for making life easier and safer. IoT is a dynamic technology that combines various things through a communication medium for enhancing various processes of organizations. IoT is becoming a key technology for organization where massive amount of data is gathered, processed, and stored. The integration of IoT with cloud technologies will assists user in gaining virtual resources like storage system, delivery of resources, and distribution of resources. An energy-aware system is required in integrating IoT, and cloud systems as heterogeneous technologies are linked together and they produce massive amount of data that may require huge storage space and processing time. Novel IoT applications are nowadays a necessity to be developed to utilize all cloud computing services [15].

The papers will contribute to achieve the following Aims:

(i) To analyse the impact of cloud computing on organizations and society

(ii) To examine various services of cloud computing

(iii) To investigate multifeatures of cloud for motivating organization in migrating towards cloud

(iv) To evaluate cloud features using probability distribution function for enhancing the capabilities of IoT applications

2. Literature Review

Nowadays, the hybrid technologies developed for the user of global society utilize advanced computing power, low-cost embedded sensors, and analytics power to carry out their main operations. The level of connectivity between these heterogeneous devices promotes the so-called industrial revolution, which promises increased speed and efficiency. The data is transferred with the help of embedded sensor from production area to connected cloud. The data from manufacturing site is collected by means of various IoT devices, and they are analysed properly to improve the processes, to provide more services, and to enhance the efficiency of the organizations [16]. IoT provides the solution to various

problems, but their solutions are domain specific in nature as various data models and communication protocols are required to remove complexities in their processes. Researchers and scientists are working closely to implement alternative methods for application development and to provide a common interface for interaction of these hybrid devices. Moreover, such efforts culminated in many software application development tools with semiservice management processes. IoT services are frequently delivered in physically confined business units with tightly coupled software, hardware, and middleware application semantics to meet domain specific development specifications [17].

Cloud computing has been used by large organization to assist them by managing and storing IoT data received from heterogeneous devices such as cameras, computers, and sensors. There is a necessity for implementing IoT frameworks that will supply services (resource provisioning) with short response clock time and low latency in order to operate latency sensitive real-time systems such as disaster and risk management systems in smart homes. The IoT process and devices are mostly not good in achieving self-adaptability and self-configuration to work properly in environmental changes, and the performance is not decreased throughout their operation and activity [18]. Managing economic and environmental performance was a critical challenge for many enterprises. Furthermore, it is increasingly challenging for expanding globalized firms to retain acceptable provider relations in order to balance economic and environmental performance goals. Modern information technology, such as cloud computing, based on transaction cost economics, can allow companies to maintain their performance by thoroughly economizing, evaluating, and monitoring their supply chain overall wealth such as money and other assets [19]. The searching time of a data owner for accessing data from server (cloud) is high. Thus, people are using and paying additional cloud services. Another problem in the cloud environment is high overhead system. To overcome all these difficulties, "Fast" a new approach for access control was presented. A table that temporary holds information depending on the data type and status of the data owner is maintained by the cloud service provider for increasing the process of accessing and data retrieval. The cloud service provider can locate the actual owner of data quickly via the table where the information is stored. Accessing time of data is significantly decreased with the table [20].

The scheduling of tasks in cloud computing setup is playing a vital role as it enhances cloud performance. From the flourishing digital information age to the growing need for quality of service in the business setups, the task scheduling algorithms and resource scheduling challenges have motivated researchers of information technology. A revolutionary technique called the Deep Q-Lerning (DQTS) task schedule that combines the Q-Learning and deep-neural network advantages was proposed. This novel solution is designed to solve the challenge of the management of a direct acyclic graph task in cloud computing settings. The key notion of this approach is the popular Deep Q-Learning strategy in task planning, which is mainly inspired by DQL. Based on improvements in WorkflowSim, tests are carried out that take into consideration the difference in the performance and load balance in task planning. The result demonstrates that DQTS offers advantages in terms of learning ability, restraint, and scalability compared to numerous conventional algorithms preceded in WorkflowSim [21].

A new elite-based differential evolution hybrid antlion optimization algorithm was presented for the solution of multiobjective task issue planning for cloud computing environments. The MALO suggested, the multiobjective aspect of the problem, stems from the necessity to minimize making-up while at the same time maximizing the use of resources [22]. In order to increase their capacity for exploitation and avoid becoming stuck in local optimums, the antilion optimization method was strengthened by elite-based differential evolution in local research techniques. On both synthetic and actual data sets, the CloudSim Tool Kit was used to undertake two experimental series. The results show that MALO exceeded other well-known algorithms for maximization. MALO was convergent for big search spaces quicker than other algorithms, which would suit major planning difficulties. Finally, the data were examined using t-tests that demonstrated that the results were significantly surpassed by MALO [22]. Decision framework is presented to aid managers in choosing appropriate cloud solution that meets customers' needs and assessing the many economic assertions of a cloud's effectiveness. This decision framework and investigation aid managers in allocating investments and evaluating cloud options that now interact with in data centers that cached, accessed, and processed data previously, as well as cloud service capabilities from another enterprise [23].

In a multisourcing context, a mathematical decision model is designed to assist with cloud service decision. The goal was to find out which cloud computing services from various suppliers are the most suited. Cost and risks are essential to be taken into consideration for decision-making process. The three security goals of availability, integrity, and confidentiality are used to model risks. The model's operational implications are found in the model's long-term decision support and holistic decision-making strategy. Three actual scenarios are studies, and a thorough analysis was carried out using software as a tool to test and verify the proposed model [24].

Cloud service providers now provide a diverse range of services for transferring virtual applications, software, and other services, such as storage and memory, in the cloud setup. However, the availability of a diverse range of these services has made hosting of applications and services a challenging one as they require authenticable and trustable platforms to enhance efficiency of organizations and minimize cost. A utility-based decision support approach for evaluating and ranking design time prospective application deployments spanning diverse cloud services was presented. The utility model is examined utilizing MediaWiki (Wikipedia) tool, and it reveals increased efficiency for choosing cloud services when compared to alternative decision-making methodologies [25].

Decision makers rely on statistics to validate their judgments, and the prevailing prepositions is that the data are

reliable and that the decision systems will deliver the appropriate solution. It is preferable to have a situation in which the DSS gives deterministic guidance in support of a choice opportunity while evaluating the probabilistic model. Furthermore, when the data resource is unavailable, the choice should be based on a selection from potential data alternatives [26].

3. Impact of Cloud Computing on Organizations and Society

By reforming the current IT strategy for organizational growth and competing against its current counterparts, organizations modified their business model which saves their cost and operational time. Employers are moving for the rapid and dynamic working culture of the company through scalable, dynamic, and flexible IT infrastructure. Cloud computing provides important benefits for scalable, dynamic, and low-cost IT solution and high availability of services, pay-per-use, and ease of use that are beneficial for effectiveness of businesses. Because of high resources availability, larger business has high cloud adoption, whereas small and medium-sized enterprises, on the other hand, have a relatively low cloud adoption [27]. The rise of cloud computing and its money saving potential find it essential for organizations [10]. For operating complex computational tasks, cloud computing has become the leading-edge solution. It is now employed for carrying out tasks in every business process. Many organizations utilize cloud computing capabilities to provide multicontinent coverage capabilities for the provision of services such as computation, storage, hosting of application, and service level agreements [28]. Services are delivered by huge low-cost computer units connected via IP networks [29].

The adoption of one or another technology should begin by assessing the organization financial processes. IT is an integrated component of a company, or ought to be. In order to sustain or promote business processes, we require technology. The organization should investigate its operations and assess the challenges and rewards delivered to its business before it leaps into the cloud. As midsized and small organizations have fewer sophisticated operations, they should be the first sector of corporations to utilize cloud computing services [9]. Organizations adopts cloud computing when they are interested in building capacity or adding additional capabilities without spending much money, training new employees, or purchasing new software. With this technology enhancement, you can purchase any subscription or pay-per-use service virtually without having it permanently which expands IT's existing capabilities in real time over the Internet [30]. Users of cloud computing are empowered to access various cloud infrastructures on subscription basis [31].

With cloud computing, the big capital expenses in hardware are no longer required to install or manage your business for developers who have unique ideas about the new Internet services. You do not need to worry about oversubsidizing a service whose popularity does not fulfill your expectations, therefore wasting expensive resources or supplying one that becomes very popular with prospective consumers and sales [32]. The cloud systems have enabled individuals to access their information from anywhere. It has vanished the concept of physical presence of individuals near to storage system. Cloud providers can provide you the resources required to run your business or home applications virtually. This is particularly advantageous for companies that do not have the same hardware and storage capacity as a larger organization. Small businesses can save their data on the cloud to remove purchasing and storing memory equipment costs. As only the quantity of storage needed is purchased, a business can buy additional space or lower its subscription accordingly with its requirements [33].

3.1. Services Provided by Cloud Providers. The consumers utilize IT infrastructure, cloud computing, or Internet-enabled platforms to execute various applications. With the intervention of cloud, the internet-enabled platforms are integrated and made transparent to provide various services such as software, hardware, data, platforms, and network. Different type of services is provided by cloud computing including hardware as a service (Haas), software as a service (SaaS), platform as a service (PaaS), data as a service (DaaS), infrastructure as a service (IaaS), and network as a service (NaaS).

3.2. Analyzing Multifeatures for Motivating Organization in Migrating towards Cloud. Software industries, such as Microsoft, Google, and Amazon, support cloud service development. Several companies, including companies that are not technologically orientated, wish to explore the effectiveness and advantages of cloud computing. However, various research works are devoid of analyzing the necessary multifeatures for enhancing cloud-based systems. There are many aspects of cloud computing that make it hard for identifying the significant features for enhancing the capability of cloud computing. These features were analysed from various literature studies for pinpointing the reasons of organizational migration towards cloud. The details of these features are described in the subsections.

3.2.1. User Centric. When you relate to cloud, you can share and download messages, documents pictures, and applications as what is stored on the cloud becomes yours on subscription basis. Collaboration and communication with others are also provided in cloud setup. You can also utilize a device working in cloud environment on various payment schemes [34].

3.2.2. Task Centric. Task centric capability is provided by cloud to users as it focuses on what you need to achieve and how the cloud will provide you the required services [34].

3.2.3. Powerfulness. With the help of a single desktop pc, connecting hundreds or thousands of computers in the cloud generate a rich computer power. Because data is kept in the cloud, users may get additional information from various repositories immediately. As with a desktop computer, you are not restricted just to a single data source [34].

3.2.4. Intelligent. Enormous of data is stored on cloud. The cloud can use algorithm and artificial intelligence to analyze and predict things' situation in advance. They can also perform efficient decision on data [34].

3.2.5. Broad Network Access. These computer resources (hardware, software, and processor) are offered to the users of cloud on Internet, and they are used by different client apps located on a consumer site with heterogeneous devices (such mobile phones, computers, and personal digital assistant) [35].

3.2.6. Resource Pooling. Computing resources from a cloud service vendor will be 'supplied' to serve many users via the multitenancy model or the resources virtualization model that are dynamically assigned and reassigned according to consumer requirements using varied physical and virtual resources. Two key elements specialization and economies of scale have encouraged the development of such a pool-based computing paradigm. A pool-based approach results in the actual computing resources being 'invisible' to consumers who generally lack control or information about their locations, orientation, and originalities (e.g., the database, CPUs, etc.). For instance, customers are unaware about the data and its presence in the cloud [35].

3.2.7. Measured Service. Several users (i.e., multiple tenants) pool and share the computer resources, and the cloud architecture can employ adequate mechanisms and methods to measure and evaluate the use of those resources by means of measurement capability of each individual user [35].

3.2.8. Consistency. Consistency concerns how updates are distributed between duplicate copies. It is a matter of whether data elements are the same on various places. Moreover, how do individuals view things whether they see the same value or if they see different values [36]? Cloud service providers can pick a consistent level in accordance with the apps' access patterns. The most optimization efforts are therefore concentrated on providing appropriate compensation between consistency and performance [37].

3.2.9. Failure Handling. Failure handling [36] is the ability of a cloud system to react to hardware or software failures. It means that the system can operate even when faults or malfunctions occur.

3.2.10. Fault Tolerance. Fault tolerance is dynamic which results in unanticipated computing system behaviour's [34]. Cloud systems have high ratio of fault tolerance or self-healing ability [35–38]. Studies like [39] explained how to achieve fault-tolerance. Error management method is mainly important for distributed systems that are prone to failure. In case of any failure, the system must reexecute for ensuring efficiency and effectiveness. Cloud-based system must have a mechanism for identifying and tracking defects and correcting the defects without system crash.

3.2.11. Reliability. Reliability [38–40] is a key challenge in cloud computing as it is a key matric for accessing performance of a system. Reliability indicates the capacity of a cloud system or device to operate appropriately for a given time period under stated conditions.

3.2.12. Flexibility. Flexibility means that a system has the capacity to react promptly and cost effectively to potential internal or external changes that influence value supply. The rapid change in organizational setup poses various challenges for organization. Flexibility is a key factor for maintaining the overall structure of organization towards a change [41].

3.2.13. Virtualization. Virtualization utilizes software to establish a computer-based abstraction layer, which allows physical parts of a computer to be separated into several virtual machines—usually called virtual ones—into processors, storage, VMs, etc. [42]. Cloud computing helps to improve data storage and access via the Internet and the cloud. This is accomplished by virtualization. Virtualization produces a genuine hardware abstraction layer known as cloned hardware over a real hardware [43]. Due to virtualization property, cloud computing is gaining much importance [44]. Virtualization is crucial to improve efficiency and effectiveness of cloud computing [45]. Virtualization is utilized by organizations for testing and development, dynamic load balancing, and server consolidation [46].

3.2.14. Robustness. The robustness of cloud system can be increased with the increasing in fault tolerance capability of cloud. Robustness increases the availability and reliability of a system [47]. Cloud system has the ability to normally operate under unpredictable condition [48, 49].

3.2.15. Scalability. Cloud computing is a scalable and simple approach for client users to gain entree to a wide range of virtualized resources which can be automatically deployed to satisfy various requirements [50]. Scalability is the characteristics of cloud system to manage and control a vast number of resources. Scalability of hardware's [51], software's, and memory must be provided to increase the efficiency and effectiveness of various cloud processes. To deal with the competitive and unpredictable nature of shared cloud infrastructure, humans have built scaling, which is the most sophisticated, efficient, and intelligent artifact. To accommodate demand spikes and reduce downtime, apps and infrastructure must be scalable. A service can be scaled if the increasing traffic can be managed by increasing server capacity [52, 53].

3.2.16. Autonomy. Autonomy in the cloud system is a major concern. Failed services are restarted through a recovery procedure, which allows the system to return automatically to its right execution without user intervention [54, 55]. Cloud computing is an autonomous system that distributes resources automatically and enable users to connect with the cloud to carry out various operations such as designing, deploying, and operating various application and processes without the participation of cloud provider's [56]. In order to deal with efficient management of resources, autonomy of cloud providers must be achieved [57].

3.2.17. Recovery. Recovery guarantees that services work properly. The cloud system is automatically recovered if functional error occurs [55]. Mandrake is a solution for autonomous recovery without human interference from simple cloud failures [58]. Automated, efficient control, introspection, and retrieval mechanisms should be used as much as feasible in cloud systems. Automated recovery, particularly, is necessary to maintain dependability and availability in the long run since human interference is not rapid and not each circumstance can be predicted. Automated recovery can be effective for monitoring and detailed identification of accurate causes in order to prevent future failure from occurring [59].

3.2.18. Accountability. In a cloud system, accountability must be assured because resources are shared among many cloud organizations [60]. Accountability is probably a fundamental notion both in the cloud and in new methods that contribute to increasing cloud computing trust. These strategies should be used appropriately [61].

3.2.19. Assurance of Services. Assurance of services are key factors to be considered in cloud for provision of various infrastructure services [62].

3.2.20. Performance. Cloud computing provides high performance by providing high computation, storage, and infrastructure [63] services. When compared to in-house computing infrastructures, cloud computing improves performance and lowers operational expenses [64]. The performance of cloud computing can be increased by utilizing various tools such as Map Reduce, MPI, Hadoop, CAP3, Dryad, and CGL [65].

3.2.21. Efficacy. Efficacy is an ability to complete the work at the required or satisfactory level. The efficacy of work can be boosted by using cloud resources [66]. Cloud resource may be scheduled by utilizing algorithm to improve efficacy [67].

3.2.22. Upgradation. The emergence cloud technology requires the upgradation of corresponding technology to manage large users and data [68, 69]. Cloud computing helps in the online upgradation of various software's and hardware's to meet the requirements of its users [70]. Online upgradation of the software may start when a user log in to cloud system [66]. The virtual upgradation of cloud infrastructure will save money and time of users and cloud organizations in carrying out various tasks.

3.2.23. Collaboration. Collaboration is a mutual process in which two or more entities participate to accomplish a specific goal. Cloud computing focuses on team collaboration for carrying out various tasks [71]. These tasks may be related to designing, development, and implementation of various tasks and methods. Collaboration among cloud providers and users is the key influences for organization to migrate towards cloud computing [72].

3.2.24. Throughput. Cloud computing provides high throughput to various processing tasks [73]. The increased throughput is due to the multiparticipating tenants that have enormous storage space, multiprocessing speed that allocates resources to various participating entities virtually and in a dynamic manner [74–76] that speed up the execution time and increases the throughput of a system.

3.2.25. Accessibility. The ability to access and utilize an entity or a system is termed as accessibility. The concept focuses on enabling access to people, to utilize various resources provided by provider's organizations. Cloud computing provides accessibility [77, 78] to data [62] and distribution of resources via computer networks [79].

3.2.26. Serviceability. Serviceability means providing various services to user such as installing application, configuring devices, and monitoring various systems and products for technical support personnel, identify hardware and software failures, debugging or identification of faults for root causes assessments, analysis, evaluations, and provision of hardware or software and their maintenance to resolve problems and restore the product into service [80]. In self-serviceability, users are provided with the resources like storage, memory, processor, according to their needs on a subscription basis. These resources are allocated to users by providers virtually in a dynamic manner [48, 81].

3.2.27. Real-Time. Cloud computing is a scalable and real-time service provision model. The computing resources supplied by cloud providers to various entities are real-time and can be rescheduled on demand [82], enabling real-time provisions of services, products, and software solutions over the communication link (Internet) [83, 84].

3.2.28. Connectivity. Cloud computing's emergence and booming is having an unprecedented impact both on the conventional enterprise connectivity market and on IT architecture and on the computing setup of enterprises [85]. The connectivity of IoT devices and cloud technologies will enhance processing power of various processes, and their integration may create novel methods for sharing resources in cloud computing ecosystem [86]. Cloud computing provides a virtualized connectivity for people and organizations [87] [88].

3.2.29. Concurrency. For improving efficiency, concurrent cloud processes are carried out [89]. With concurrent processes, the data may be accessed or retrieved for various databases in less time [90], and as multiple threads of a process are created [91], it will enhance the efficiency of overall processing of a system.

3.2.30. Rapid Elasticity. To meet the interests of end users, computer resources are not permanently allocated, but they are immediately allocated on demand, i.e., there is no direct commitment between users, and no signed contract with providing organization. Resources may properly be scaled to be used and they must be released as soon as their need is accomplished. In addition, the resource provision appears to be infinite as consumption can increase with the passage of time to satisfy the highest requirements of users at any specific time [35].

Table 1: Evaluating feature relevancy.

Features	[34]	[35]	[36]	[111]	[38]	[41]	[42]	[47]	[51]	[56]	[55]	[60]	[62]	[63]	[66]	[69]	[72]	[73]	[78]	[80]	[82]	[86]	[89]	[95]
User centric	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✗	✓
Task centric	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✓	✗	✓	✓	✗	✓	✗
Powerfulness	✓	✗	✗	✗	✓	✓	✗	✗	✗	✓	✗	✓	✗	✗	✓	✗	✓	✗	✗	✓	✗	✗	✗	✓
Intelligent	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Broad network	✗	✓	✓	✗	✓	✗	✓	✗	✗	✓	✗	✗	✓	✗	✗	✓	✗	✓	✓	✓	✗	✗	✗	✗
Resources	✓	✓	✓	✗	✓	✓	✓	✗	✗	✓	✓	✗	✓	✓	✓	✗	✗	✓	✓	✓	✓	✓	✓	✓
Measurement	✗	✓	✗	✗	✓	✓	✗	✗	✓	✓	✗	✓	✓	✗	✗	✗	✗	✗	✗	✓	✓	✓	✗	✗
Consistency	✗	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗
Failure control	✗	✗	✓	✗	✓	✗	✗	✗	✗	✗	✓	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗
Fault tolerance	✗	✗	✓	✓	✓	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗
Reliability	✓	✓	✓	✗	✓	✓	✗	✓	✗	✗	✓	✓	✓	✓	✓	✗	✓	✗	✓	✓	✗	✗	✗	✗
Flexibility	✓	✓	✓	✓	✗	✓	✗	✗	✓	✗	✗	✓	✓	✓	✗	✗	✓	✓	✓	✓	✗	✓	✗	✗
Virtualization	✓	✓	✗	✗	✓	✗	✓	✗	✓	✓	✓	✗	✓	✓	✓	✓	✗	✗	✗	✓	✗	✓	✗	✗
Robustness	✗	✗	✓	✗	✓	✗	✗	✓	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗	✓	✗	✗
Scalability	✗	✓	✓	✓	✗	✓	✓	✗	✓	✓	✓	✗	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✗
Autonomy	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Recovery	✗	✗	✓	✗	✓	✗	✗	✗	✗	✗	✓	✗	✗	✓	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗
Accountability	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗
Assurance	✗	✗	✗	✗	✓	✓	✓	✓	✓	✓	✗	✓	✓	✗	✓	✗	✗	✗	✗	✓	✓	✗	✗	✗
Performance	✓	✓	✓	✗	✓	✓	✓	✗	✓	✗	✗	✓	✗	✓	✓	✗	✗	✓	✓	✓	✗	✓	✗	✗
Efficacy	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗
Upgradation	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✗	✓	✗	✗	✗	✗
Collaboration	✓	✓	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✓	✗	✓	✓	✗	✗	✗	✗
Throughput	✗	✗	✓	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✓	✗	✗	✗	✗	✗	✗
Accessibility	✗	✓	✗	✗	✓	✓	✓	✗	✗	✗	✗	✗	✗	✓	✓	✗	✓	✗	✓	✓	✗	✗	✗	✗
Serviceability	✗	✓	✗	✗	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	✓	✓	✓	✓	✓	✗	✗
Real-time	✓	✓	✗	✓	✓	✗	✗	✓	✗	✗	✗	✗	✓	✗	✓	✗	✗	✓	✓	✗	✗	✓	✗	✗
Connectivity	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗	✓	✓	✗	✗	✗	✓	✓	✓	✓	✗
Concurrency	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✓	✗
Elasticity	✗	✓	✓	✓	✓	✓	✗	✓	✓	✓	✗	✗	✓	✓	✓	✗	✓	✗	✓	✗	✓	✓	✗	✗
Resource management	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✗	✓	✓	✓	✓	✗	✓	✓	✓
Cost reduction	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✗	✓

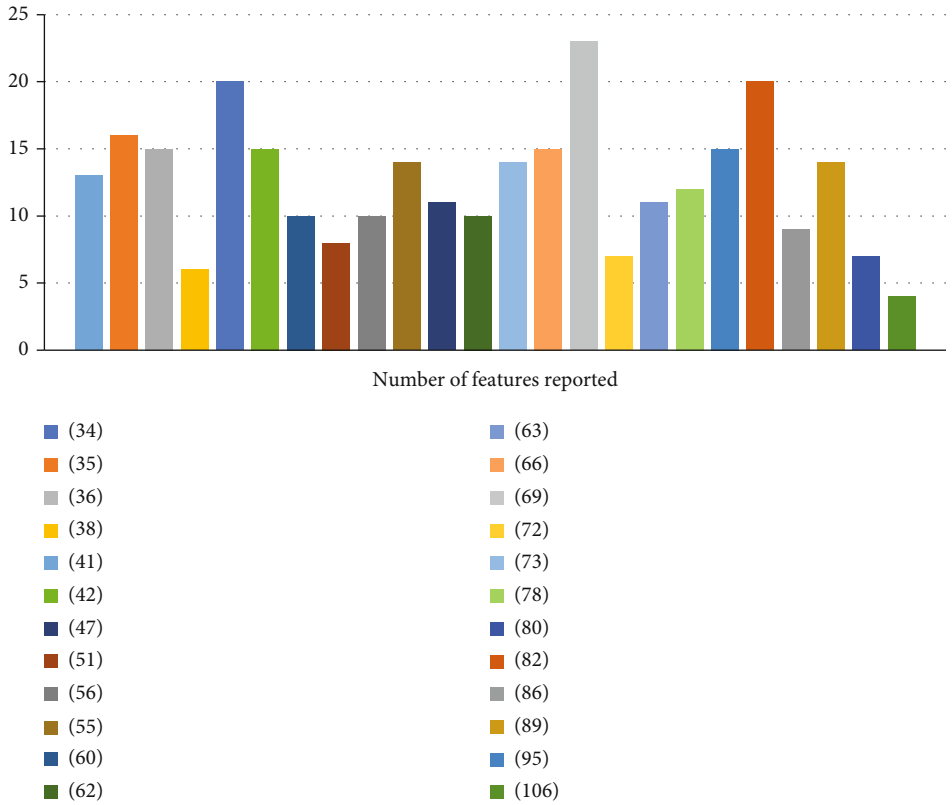


Figure 1: Evaluation of features based on selected article.

3.2.31. Resource Management. Cloud computing offers various services to users from a resources pool. These resources include various cloud infrastructure, software, and applications [92]. Users can be released from burden of data storage and maintenance by utilizing virtual resources [93]. Cloud computing facilitates the decentralization of the data in many configurable resources [94]. Multitudes of resources are available on cloud that can be utilized accordingly with the requirement [95]. Resources are pooled and dynamically assigned to users according to their demands [96–98]. Maximization of profit is achieved by the optimum resource usage [99], and it can also increase the performance of organization [100].

3.2.32. Cost Reduction. Cost reduction is as a major cloud feature [101]. The cost of tasks is minimized as users have not to buy things permanently but for time being whenever required.

4. Experimental Setup and Results

To tackle global competitiveness challenges, companies are continuously struggling to select relevant features. The decisions become more complex as the decision-makers in the cloud environment setup have to analyse a broad variety of appropriate features based on competing criteria. Various multidecision making approaches are now available in order to support these selection procedures. Probability-based distribution function was utilized for selecting features based on their occurrence in relevant research articles. Multiattribute is optimized based on specific constraints [102]. Probability distribution is a function that represents the possibility occurrence of a specific value in an experiment [103].

4.1. Feature Selection. Selection of appropriate features is commonly employed in machine learning to tackle complex problems. Inserting several attributes into the feature model increases the calculation and raises the dilemma of severe dimensionality. By selecting the most relevant feature, a massive and complex data set is minimized [104]. While dealing with a gigantic amount of data, it is more difficult for decision maker to make an optimum decision. The capability of decision making can be improved by using decision support system [105] and features selection techniques. The precision of existing feature set is not affected [106]. When handling a manipulated set of features, specification of procedures that select appropriate features is necessary. FS is compulsory is extensively demanded when dealing with contemporary situations like inadequate or chaotic features. Selection of features is regressively used in diverse areas such as image processing [107], identification patterns [108], text classification [109, 110], and data mining [104]. Features are mostly selected to reduce simulation time, boost prediction, performance and extract enriched information that are hidden in available set of data. Resultantly, the accurate feature may promise for achieving high identification and recognition results.

Based on the data replicated in Table 1, the statistical analysis is performed to extract the most suitable feature that can be used for the performance evaluation of cloud computing.

Table 2: Statistical analysis of features using different mathematical evaluation techniques.

Features	Frequency	Probability $P(x)$	Features occurred in a paper (x)	Mean $= x * P(x)$	$(x-m)^2 * p(x)$
User centric	13	0.040625	13	0.528125	0.070316559
Task centric	7	0.021875	16	0.35	0.407413544
Powerfulness	9	0.028125	15	0.421875	0.309188507
Intelligent	1	0.003125	6	0.01875	0.100975372
Broad network access	10	0.03125	20	0.625	2.160925598
Resource pooling	18	0.05625	15	0.84375	0.618377014
Measured service	10	0.03125	10	0.3125	0.088659973
Consistency	3	0.009375	8	0.075	0.127262054
Failure handling	5	0.015625	10	0.15625	0.044329987
Fault tolerance	6	0.01875	14	0.2625	0.100539734
Reliability	14	0.04375	11	0.48125	0.02049115
Flexibility	14	0.04375	10	0.4375	0.124123962
Virtualization	13	0.040625	14	0.56875	0.21783609
Robustness	6	0.01875	15	0.28125	0.206125671
Scalability	2	0.00625	7	0.04375	0.137146057
Autonomy	6	0.01875	11	0.20625	0.008781921
Automated recovery	3	0.009375	12	0.1125	0.000933929
Accountability	11	0.034375	15	0.515625	0.377897064
Assurance of services	14	0.04375	20	0.875	3.025295837
Performance	1	0.003125	9	0.028125	0.022518341
Efficacy	3	0.009375	14	0.13125	0.050269867
Upgradation	9	0.028125	7	0.196875	0.617157257
Collaboration	4	0.0125	4	0.05	0.738120239
Throughput	9	0.028125	12	0.3375	0.002801788
Accessibility	16	0.05	15	0.75	0.549668457
Serviceability	10	0.03125	20	0.625	2.160925598
Real-time	8	0.025	9	0.225	0.180146729
Connectivity	4	0.0125	14	0.175	0.067026489
Concurrency	15	0.046875	7	0.328125	1.028595428
Rapid elasticity	20	0.0625	4	0.25	3.690601196
Resource management	19	0.059375	2	0.11875	5.568610199
Cost reduction	19	0.059375	1	0.059375	6.77800473

These features are analysed from various research articles, and a statistical method is applied to check their probability in these articles.

The various features are analysed during the studies from relevant research articles. These articles are evaluated using probability and distribution functions based on their occurrence in certain selected article occurrences, the higher bar value in a chart represents the most suitable articles based on analysed features. Figure 1 represents the evaluation of features in different studies.

4.2. To Evaluate Cloud Features Using Probability Distribution Function for Enhancing the Capabilities of IoT Applications. Probability distribution function is followed for assigning weighting criteria to every individual feature based on the occurrence and its applicability and importance in certain research articles. Following are the selected weighting criteria. The prime objective of this probability distribution function in this research work is to tag the most frequently used feature in the domain of cloud development. In our case elasticity, cost reduction, resource management, resource pooling, accessibility, reliability, and flexibility are the most frequently used performance metrics (features) for the validation and applicability testing purposes. After evaluating the relevant research articles, the statistical approach comprised of means, probability, and standard deviation is used, as depicted in equations (1), (3), and (5).

To calculate the chance of occurrence for a certain event is termed as probability. It can be represented by $P(X)$ where "X" represents the event, while "P" represents the chance of occurrence. It can be mathematically represented by

$$P(X) = \frac{Number\ \text{of}\ favourable\ outcome}{Total\ Number\ \text{of}\ favourable\ outcomes}, \quad (1)$$

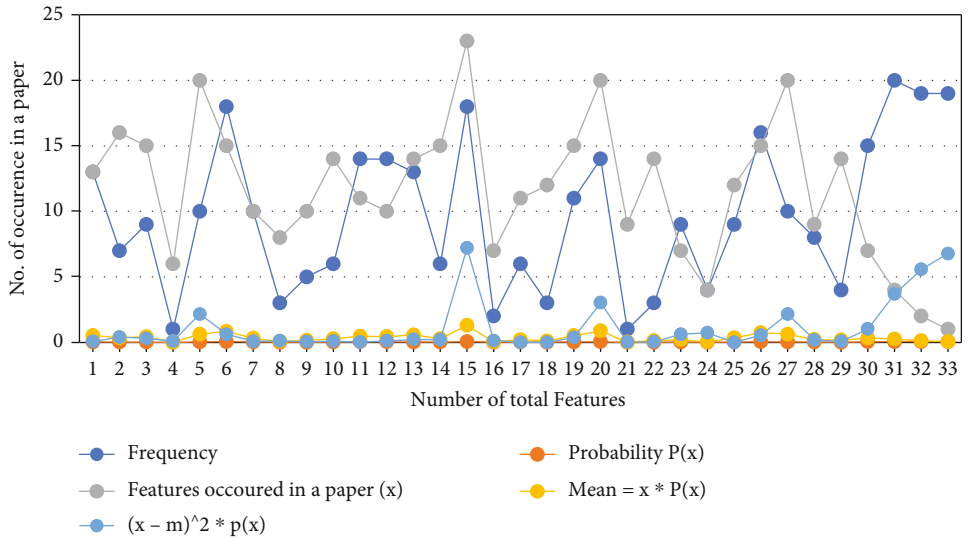


Figure 2: Performance evaluation of different cloud computing-based features using statistical analysis.

or

$$P(X) = \frac{n(X)}{n(S)}, \tag{2}$$

where $n(X)$ represents the number of favourable outcomes, and $n(S)$ represents the total number of events.

The mean can be defined as the average or central calculated value of a well-defined set of numbers and can be used for calculating the central propensity of data. Central propensity is the measure which distinguishes the complete set of data or distribution over a single value. It represents the precise description of entire data. Mean can be represented by

$$Means = \frac{Sum\ of\ All\ data\ Points}{Number\ of\ data\ Points}, \tag{3}$$

or

$$\mu = x \times P(x), \tag{4}$$

where μ represents the means for the number of occurrence, and x represents number of samples.

The degree of deviation of the data points with respect to its average points (mean) is known as the standard deviation. It can be represented as

$$\sigma = (x - \mu)^2 \times P(x), \tag{5}$$

where σ represents the standard deviation.

Based on this statistical analysis, the features are evaluated based on their occurrence in most relevant studies. The higher the probability of the feature, the higher is their significant to cloud providers. The underlined result is depicted in Table 2.

Figure 2 represents the probability of the features based on the number of occurrences in the most relevant research articles. The high probability depicts the list of the most relevant and suitable feature that can be selected for the evaluation in the proposed research domain.

5. Conclusions and Future Suggestions

Cloud computing is predicted to revolution IT services. Cloud computing converges the IT efficiency where computation power is efficiently used by scaling of hardware and software among users and business agility where IT works as a tool for deployment, processing, business analytics, and interaction by means of cell phone works in timely manner to achieve the requirements of users. With providing incredible opportunities for enhancing business processes, organizations wish to invest in cloud-related technologies [112]. Identifying and implementing a technical and complicated approaches such as cloud computing is not simple, and it requires analyzing its key aspects. With the abrupt technological changes, decision making is becoming crucial due to large contradicting features available in domain of cloud computing. In this research study, probability distribution function is utilized for assigning weighting criteria to feature based on their occurrence and applicability. The prime objective of the probability distribution function is to elicit the most frequently used feature in the domain of cloud development. Features are mostly selected to reduce simulation time, boost prediction, performance and extract enriched information that are hidden in available set of data. Resultantly, the accurate feature may promise for achieving high identification and recognition results. Organizations, such as Pinterest, Vivino, Kroger, game loft, eBay, PayPal, and Google, are using the services of cloud providers to provide their customer ease and comfort in their life activities.

Data Availability

Data is available and included in the paper.

Conflicts of Interest

The authors declare that there is no conflict of interest regarding the publication of this paper.

Acknowledgments

This work was supported by the Qatar foundation, Doha, Qatar, under Grant IRCC-2021-010.

References

[1] A. Kumar, P. Kumar, S. C. J. Palvia, and S. Verma, "Online education worldwide: current status and emerging trends," *Journal of Information Technology Case and Application Research*, vol. 19, no. 1, pp. 3–9, 2017.

[2] B. Bowonder, T. Miyqake, and T. M. Singh, "Emerging trends in information technology: implications for developing countries," *International Journal of Information Management*, vol. 13, no. 3, pp. 183–204, 1993.

[3] F. Ruzic, "Digital organizations enhancement with information and operational technologies convergence," in *Encyclopedia of Organizational Knowledge, Administration, and Technology*, pp. 966–981, IGI Global, 2021.

[4] L. M. Kaufman, "Data security in the world of cloud computing," *IEEE Security & Privacy Magazine*, vol. 7, no. 4, pp. 61–64, 2009.

[5] S. Zhang, H. Yan, and X. Chen, "Research on key technologies of cloud computing," *Physics Procedia*, vol. 33, pp. 1791–1797, 2012.

[6] A. Ghazizadeh, "Cloud computing benefits and architecture in e-learning," in *2012 IEEE seventh international conference on wireless, mobile and ubiquitous technology in education*, pp. 199–201, Takamatsu, Japan, 2012.

[7] P. Mell and T. Grance, "The NIST definition of cloud computing. National Institute of Standards and Technology," *Information Technology Laboratory, Version*, vol. 15, 2009.

[8] B. Furht, *Cloud computing fundamentals*, Springer, 2010.

[9] M.-G. Avram, "Advantages and challenges of adopting cloud computing from an enterprise perspective," *Procedia Technology*, vol. 12, pp. 529–534, 2014.

[10] G. Lewis, *Basics about Cloud Computing*, Software engineering institute carniege mellon university, Pittsburgh, 2010.

[11] Y. Jadeja and K. Modi, "Cloud computing-concepts, architecture and challenges," in *2012 International Conference on Computing, Electronics and Electrical Technologies (ICCEET)*, pp. 877–880, Nagercoil, India, 2012.

[12] F. Hao, G. Min, J. Chen et al., "An optimized computational model for multi-community-cloud social collaboration," *IEEE Transactions on Services Computing*, vol. 7, no. 3, pp. 346–358, 2014.

[13] J. Weinman, "Hybrid cloud economics," *IEEE Cloud Computing*, vol. 3, no. 1, pp. 18–22, 2016.

[14] D. S. Linthicum, "Emerging hybrid cloud patterns," *IEEE Cloud Computing*, vol. 3, no. 1, pp. 88–91, 2016.

[15] T. Baker, M. Asim, H. Tawfik, B. Aldawsari, and R. Buyya, "An energy-aware service composition algorithm for multiple cloud-based IoT applications," *Journal of Network and Computer Applications*, vol. 89, pp. 96–108, 2017.

[16] P. Ferrari, A. Flammini, S. Rinaldi, E. Sisinni, D. Maffei, and M. Malara, "Impact of quality of service on cloud based industrial IoT applications with OPC UA," *Electronics*, vol. 7, no. 7, p. 109, 2018.

[17] F. Li, M. Vögler, M. Claeßens, and S. Dustdar, "Towards automated IoT application deployment by a cloud-based approach," in *2013 IEEE 6th international conference on service-oriented computing and applications*, pp. 61–68, Koloa, HI, USA, 2013.

[18] S. Pandiyan, T. S. Lawrence, V. Sathiyamoorthi, M. Ramasamy, Q. Xia, and Y. Guo, "A performance-aware dynamic scheduling algorithm for cloud-based IoT applications," *Computer Communications*, vol. 160, pp. 512–520, 2020.

[19] D. G. Schniederjans and D. N. Hales, "Cloud computing and its impact on economic and environmental performance: a transaction cost economics perspective," *Decision Support Systems*, vol. 86, pp. 73–82, 2016.

[20] S. Namasudra, R. Chakraborty, S. Kadry, G. Manogaran, and B. S. Rawal, "FAST: Fast accessing scheme for data transmission in cloud computing," *Peer-to-Peer Networking and Applications*, vol. 14, no. 4, pp. 2430–2442, 2021.

[21] Z. Tong, H. Chen, X. Deng, K. Li, and K. Li, "A scheduling scheme in the cloud computing environment using deep Q -learning," *Information Sciences*, vol. 512, pp. 1170–1191, 2020.

[22] L. Abualigah and A. Diabat, "A novel hybrid antlion optimization algorithm for multi-objective task scheduling problems in cloud computing environments," *Cluster Computing*, vol. 24, no. 1, pp. 205–223, 2021.

[23] S. Kaisler, W. H. Money, and S. J. Cohen, "A decision framework for cloud computing," in *2012 45th Hawaii International Conference on System Sciences*, pp. 1553–1562, Maui, HI, USA, 2012.

[24] B. Martens and F. Teuteberg, "Decision-making in cloud computing environments: a cost and risk based approach," *Information Systems Frontiers*, vol. 14, no. 4, pp. 871–893, 2012.

[25] S. G. Sáez, V. Andrikopoulos, M. Bitsaki, F. Leymann, and A. Van Hoorn, "Utility-based decision making for migrating cloud-based applications," *ACM Transactions on Internet Technology (TOIT)*, vol. 18, no. 2, pp. 1–22, 2018.

[26] S. Russell, V. Yoon, and G. Forgionne, "Cloud-based decision support systems and availability context: the probability of successful decision outcomes," *Information Systems and e-Business Management*, vol. 8, no. 3, pp. 189–205, 2010.

[27] M. Shuaib, A. Samad, S. Alam, and S. T. Siddiqui, "Why adopting cloud is still a challenge?—a review on issues and challenges for cloud migration in organizations," in *Advances in Intelligent Systems and Computing*, pp. 387–399, Springer, Singapore, 2019.

[28] R. Buyya, J. Broberg, and A. M. Goscinski, *Cloud Computing: Principles and Paradigms*, vol. 87, John Wiley & Sons, 2010.

[29] L. Qian, Z. Luo, Y. Du, and L. Guo, "Cloud computing: an overview," in *Lecture Notes in Computer Science*, pp. 626–631, Springer, Berlin, Heidelberg, 2009.

[30] E. Knorr and G. Gruman, "What cloud computing really means," *InfoWorld*, vol. 7, pp. 1–17, 2008.

[31] S. K. Garg, S. Versteeg, and R. Buyya, "A framework for ranking of cloud computing services," *Future Generation Computer Systems*, vol. 29, no. 4, pp. 1012–1023, 2013.

[32] M. Armbrust, A. Fox, R. Griffith et al., "A view of cloud computing," *Communications of the ACM*, vol. 53, no. 4, pp. 50–58, 2010.

[33] A. Huth and J. Cebula, *The Basics of Cloud Computing*, United States Computer, 2011.

[34] S. P. Mirashe and N. V. Kalyankar, "Cloud computing," 2010, https://arxiv.org/abs/1003.4074.

[35] T. Dillon, C. Wu, and E. Chang, "Cloud computing: issues and challenges," in *2010 24th IEEE international conference on advanced information networking and applications*, pp. 27–33, Perth, WA, Australia, 2010.

[36] S. Bykov, A. Geller, G. Kliot, J. R. Larus, R. Pandya, and J. Thelin, "Orleans: cloud computing for everyone," in *Proceedings of the 2nd ACM Symposium on Cloud Computing*, pp. 1–14, New York, 2011.

[37] H.-E. Chihoub, S. Ibrahim, G. Antoniu, and M. S. Perez, "Consistency in the cloud: When money does matter," in *2013 13th IEEE/ACM International Symposium on Cluster, Cloud, and Grid Computing*, pp. 352–359, Delft, Netherlands, 2013.

[38] E. Bauer and R. Adams, *Reliability and availability of cloud computing*, John Wiley & Sons, 2012.

[39] W. Duan, M. Hu, Q. Zhou et al., "Reliability in cloud computing system: a review," *Journal of Computer Research and Development*, vol. 57, no. 1, p. 102, 2020.

[40] M. Manglik, N. Rawat, and M. Ram, "Reliability and availability analysis of a cloud computing transition system under multiple failures," *International Journal of Quality & Reliability Management*, vol. 37, no. 6/7, pp. 823–835, 2020.

[41] S. S. Bharadwaj and P. Lal, "Exploring the impact of cloud computing adoption on organizational flexibility: a client perspective," in *2012 International Conference on Cloud Computing Technologies, Applications and Management (ICCCTAM)*, pp. 121–131, Dubai, United Arab Emirates, 2012.

[42] International Business Machines, *Virtualization*, IBM Cloud Education, 2021, http://www.ibm.com/cloud/learn/virtualization-a-complete-guide.

[43] G. Goel, P. Tanwar, V. Bansal, and S. Sharma, "The challenges and issues with virtualization in cloud computing," in *2021 5th International Conference on Trends in Electronics and Informatics (ICOEI)*, pp. 1334–1338, Tirunelveli, India, 2021.

[44] V. Sivaraj, A. Kangaiammal, and A. S. Kashyap, "Enhancing fault tolerance using load allocation technique during virtualization in cloud computing," in *2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS)*, pp. 1798–1801, Coimbatore, India, 2021.

[45] J. K. Meena and R. K. Banyal, "Efficient virtualization in cloud computing," in *2021 5th International Conference on Computing Methodologies and Communication (ICCMC)*, pp. 227–232, Erode, India, 2021.

[46] A. Rashid and A. Chaturvedi, "Virtualization and its role in cloud computing environment," *International Journal of Computer Sciences and Engineering*, vol. 7, no. 4, pp. 1131–1136, 2019.

[47] F. Chauvel, H. Song, N. Ferry, and F. Fleurey, "Evaluating robustness of cloud-based systems," *Journal of Cloud Computing*, vol. 4, no. 1, pp. 1–17, 2015.

[48] C. Pahl, P. Jamshidi, and O. Zimmermann, "Architectural principles for cloud software," *ACM Transactions on Internet Technology (TOIT)*, vol. 18, no. 2, pp. 1–23, 2018.

[49] S. Talwani and I. Chana, "Fault tolerance techniques for scientific applications in cloud," in *2017 2nd International Conference on Telecommunication and Networks (TEL-NET)*, pp. 1–5, Noida, India, 2017.

[50] M. M. Falatah and O. A. Batarfi, "Cloud scalability considerations," *International Journal of Computer Science and Engineering Survey*, vol. 5, no. 4, pp. 37–47, 2014.

[51] O. Knodel, P. R. Genssler, and R. G. Spallek, "Virtualizing reconfigurable hardware to provide scalability in cloud architectures," in *International Conference on Advances in Circuits, Electronics and Micro-electronics (CENICS)*, Dresden, Germany, 2017.

[52] J. Y. Lee and S. D. Kim, "Software approaches to assuring high scalability in cloud computing," in *2010 IEEE 7th International Conference on E-Business Engineering*, pp. 300–306, Shanghai, China, 2010.

[53] S. Lehrig, H. Eikerling, and S. Becker, "Scalability, elasticity, and efficiency in cloud computing: a systematic literature review of definitions and metrics," in *Proceedings of the 11th International ACM SIGSOFT Conference on Quality of Software Architectures*, pp. 83–92, New York, 2015.

[54] J. Toutouh, A. Muñoz, and S. Nesmachnow, "Evolution oriented monitoring oriented to security properties for cloud applications," in *Proceedings of the 13th International Conference on Availability, Reliability and Security*, New York, 2018.

[55] T. B. Sousa, H. S. Ferreira, F. F. Correia, and A. Aguiar, "Engineering software for the cloud: automated recovery and scheduler," in *Proceedings of the 23rd European Conference on Pattern Languages of Programs*, pp. 1–8, New York, 2018.

[56] P. Asrani, "Mobile cloud computing," *International Journal of Engineering and Advanced Technology*, vol. 2, pp. 606–609, 2013.

[57] E. Feller and C. Morin, "Autonomous and energy-aware management of large-scale cloud infrastructures," in *2012 IEEE 26th International Parallel and Distributed Processing Symposium Workshops & PhD Forum*, pp. 2542–2545, Shanghai, China, 2012.

[58] K. Carson, J. Thomason, R. Wolski, C. Krintz, and M. Mock, "Mandrake: implementing durability for edge clouds," in *2019 IEEE International Conference on Edge Computing (EDGE)*, pp. 95–101, Milan, Italy, 2019.

[59] S. Konno and X. Défago, "Approximate QoS rule derivation based on root cause analysis for cloud computing," in *2019 IEEE 24th Pacific Rim International Symposium on Dependable Computing (PRDC)*, pp. 33–3309, Kyoto, Japan, 2019.

[60] O. Iliashenko, E. Lukianchenko, and N. Lohyeeta, "A selection approach to the criteria for evaluating cloud platforms for conducting IT projects," in *Proceedings of the International Scientific Conference-Digital Transformation on Manufacturing, Infrastructure and Service*, New York, 2020.

[61] S. Pearson, "Toward accountability in the cloud," *IEEE Internet Computing*, vol. 15, no. 4, pp. 64–69, 2011.

[62] N. M. A. Al-Jaser, "A survey on cloud computing security–challenges and trust issues," *International Journal of Computer Science and Information Security (IJCSIS)*, vol. 18, no. 5, 2020.

[63] J. Wu, L. Ping, X. Ge, Y. Wang, and J. Fu, "Cloud storage as the infrastructure of cloud computing," in *2010 International Conference on Intelligent Computing and Cognitive Informatics*, pp. 380–383, Kuala Lumpur, Malaysia, 2010.

[64] J. Ribes González, *Cryptographic Techniques for Securing Data in the Cloud*, Universitat Rovira i Virgili, 2018.

[65] O. Alzakholi, H. Shukur, R. Zebari, S. Abas, and M. Sadeeq, "Comparison among cloud technologies and cloud performance," *Journal of Applied Science and Technology Trends*, vol. 1, no. 2, pp. 40–47, 2020.

[66] G. N. Iyer, "Cloud Testing," in *Encyclopedia of Cloud Computing*, pp. 327–337, Wiley, 2016.

[67] H. Singh, A. Bhasin, and P. Kaveri, "SECURE: efficient resource scheduling by swarm in cloud computing," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 22, no. 2, pp. 127–137, 2019.

[68] M. S. Goel, R. Kiran, and D. Garg, "Impact of cloud computing on ERP implementations in higher education," *Institutions*, vol. 2, no. 6, 2011.

[69] N. S. More and R. B. Ingle, "Research issues for energy-efficient cloud computing," in *Intelligent Computing and Information and Communication*, pp. 265–272, Springer, 2018.

[70] M. Shanbhog, "Cloud computing adoption: influencing factors on online firms," in *Innovative Data Communication Technologies and Application*, pp. 799–808, Springer, 2021.

[71] M. Younas, D. N. A. Jawawi, M. A. Shah et al., "Elicitation of nonfunctional requirements in agile development using cloud computing environment," *IEEE Access*, vol. 8, pp. 209153–209162, 2020.

[72] P. Gupta, A. Seetharaman, and J. R. Raj, "The usage and adoption of cloud computing by small and medium businesses," *International Journal of Information Management*, vol. 33, no. 5, pp. 861–874, 2013.

[73] N.-H. Sun, Y.-G. Bao, and D.-R. Fan, "The rise of high-throughput computing," *Frontiers of Information Technology & Electronic Engineering*, vol. 19, no. 10, pp. 1245–1250, 2018.

[74] X. Chen, H. Wang, Y. Ma, X. Zheng, and L. Guo, "Self-adaptive resource allocation for cloud-based software services based on iterative QoS prediction model," *Future Generation Computer Systems*, vol. 105, pp. 287–296, 2020.

[75] D. Bruneo, F. Longo, A. Puliafito, M. Scarpa, and S. Distefano, "Software rejuvenation in the cloud," in *Proceedings of the 5th International ICST Conference on Simulation Tools and Techniques*, pp. 8–16, New York, 2012.

[76] A. K. Mandal, S. Changder, and A. Sarkar, "Selection of services for data-centric cloud applications: a QoS based approach," in *2013 2nd international conference on advanced computing, Networking and Security*, pp. 102–107, Mangalore, India, 2013.

[77] H. Singh, S. Tyagi, and P. Kumar, "High availability and accessibility of services in cloud environment," in *2018 4th International Conference on Computing Sciences (ICCS)*, pp. 67–71, Jalandhar, India, 2018.

[78] M. Lecznar and S. Patig, "Cloud computing providers: characteristics and recommendations," in *Lecture Notes in Business Information Processing*, pp. 32–45, Springer, Berlin, Heidelberg, 2011.

[79] P. Géczy, N. Izumi, and K. Hasida, "Cloudsourcing: managing cloud adoption," *Global Journal of Business Research*, vol. 6, no. 2, pp. 57–70, 2012.

[80] Wikipedia, *Serviceability*https://en.wikipedia.org/wiki/Serviceability_(computer).

[81] C. Ye, A. Islam, J. Wei, D. Chen, M. Huang, and W. Du, "Towards a scalable and efficient open cloud marketplace," in *Proceedings of the 7th Asia-Pacific Symposium on Internetware*, pp. 102–111, New York, 2015.

[82] J. Wu, Y. Wu, Z. Wu, M. Yang, and Y. Wang, "Vulcloud: scalable and hybrid vulnerability detection in cloud computing," in *2013 IEEE Seventh International Conference on Software Security and Reliability Companion*, pp. 225-226, Gaithersburg, MD, USA, 2013.

[83] J. Cai and Q. Hu, "Analysis for cloud testing of web application," in *The 2014 2nd International Conference on Systems and Informatics (ICSAI 2014)*, pp. 293–297, Shanghai, China, 2014.

[84] S. Patidar, D. Rane, and P. Jain, "A survey paper on cloud computing," in *2012 second international conference on advanced computing & communication technologies*, pp. 394–398, Rohtak, India, 2012.

[85] Y. Ni, C. L. Xing, and K. Zhang, "Connectivity as a service: outsourcing Enterprise connectivity over cloud computing environment," in *2011 International Conference on Computer and Management (CAMAN)*, pp. 1–7, Wuhan, China, 2011.

[86] M. Malathi, "Cloud computing concepts," in *2011 3rd International Conference on Electronics Computer Technology*, pp. 236–239, Kanyakumari, India, 2011.

[87] F. Baroncelli, B. Martini, and P. Castoldi, "Network virtualization for cloud computing," *Annals of Telecommunications-Annales Des Télécommunications*, vol. 65, no. 11-12, pp. 713–721, 2010.

[88] S. Ewenike, E. Benkhelifa, and C. Chibelushi, "Classifying collaborative approaches for cloud based collaborative software development," in *2017 International Conference on the Frontiers and Advances in Data Science (FADS)*, pp. 47–52, Xi'an, China, 2017.

[89] J. Grundy, G. Kaefer, J. Keung, and A. Liu, "Guest editors' introduction: software engineering for the cloud," *IEEE Software*, vol. 29, no. 2, pp. 26–29, 2012.

[90] S. Yan, L. He, J. Seo, and M. Lin, "Concurrent healthcare data processing and storage framework using deep-learning in distributed cloud computing environment," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 4, pp. 2794–2801, 2020.

[91] M. P. K. Shelke, M. S. Sontakke, and A. Gawande, "Intrusion detection system for cloud computing," *International Journal of Scientific & Technology Research*, vol. 1, no. 4, pp. 67–71, 2012.

[92] B. P. Rao, P. Saluia, N. Sharma, A. Mittal, and S. V. Sharma, "Cloud computing for internet of things & sensing based applications," in *2012 Sixth International Conference on Sensing Technology (ICST)*, pp. 374–380, Kolkata, India, 2012.

[93] P. A. Boampong and L. A. Wahsheh, "Different facets of security in the cloud," in *Proceedings of the 15th Communications and Networking Simulation Symposium*, pp. 1–7, New York, 2012.

[94] A. Alsirhani, P. Bodorik, and S. Sampalli, "Improving database security in cloud computing by fragmentation of data," in *2017 International Conference on Computer and Applications (ICCA)*, pp. 43–49, Doha, Qatar, 2017.

[95] A. Ashraf, B. Byholm, and I. Porres, "A multi-objective ACS algorithm to optimize cost, performance, and reliability in the cloud," in *2015 IEEE/ACM 8th International Conference on Utility and Cloud Computing (UCC)*, pp. 341–347, Limassol, Cyprus, 2015.

[96] A. V. Almeida, M. M. Borges, and L. Roque, "The European open science cloud: a new challenge for Europe," in

Proceedings of the 5th International Conference on Technological Ecosystems for Enhancing Multiculturality, pp. 1–4, New York, 2017.

[97] P. Chawla, I. Chana, and A. Rana, "Framework for cloud-based software test data generation service," *Software: Practice and Experience*, vol. 49, pp. 1307–1328, 2019.

[98] L. Peiyu and L. Dong, "The new risk assessment model for information system in cloud computing environment," *Procedia Engineering*, vol. 15, pp. 3200–3204, 2011.

[99] V. Khoshdel, S. A. Motamedi, S. Sharifian, and M. Farhadi, "A new approach for optimum resource utilization in cloud computing environments," in *2011 1st International eConference on Computer and Knowledge Engineering (ICCKE)*, pp. 314–321, Mashhad, Iran, 2011.

[100] T. Mehmood, S. Latif, and S. Malik, "Prediction of cloud computing resource utilization," in *2018 15th International Conference on Smart Cities: Improving Quality of Life Using ICT & IoT (HONET-ICT)*, pp. 38–42, Islamabad, Pakistan, 2018.

[101] X. Li, Y. Li, T. Liu, J. Qiu, and F. Wang, "The method and tool of cost analysis for cloud computing," in *2009 IEEE International Conference on Cloud Computing*, pp. 93–100, Bangalore, India, 2009.

[102] G. Kecek and F. Demirağ, "A comparative analysis of TOPSIS and MOORA in laptop selection," *Research on Humanities and Social Sciences*, vol. 6, p. 2225, 2016.

[103] wikipedia, *Probability distribution*https://en.wikipedia.org/wiki/Probability_distribution.

[104] S. Kashef and H. Nezamabadi-pour, "A new feature selection algorithm based on binary ant colony optimization," in *The 5th Conference on Information and Knowledge Technology*, pp. 50–54, Shiraz, Iran, 2013.

[105] Y. Huang, S. Nazir, J. Wu, F. Hussain Khoso, F. Ali, and H. U. Khan, "An efficient decision support system for the selection of appropriate crowd in crowdsourcing," *Complexity*, vol. 2021, Article ID 5518878, 11 pages, 2021.

[106] H. Liu and L. Yu, "Toward integrating feature selection algorithms for classification and clustering," *IEEE Transactions on Knowledge and Data Engineering*, vol. 17, no. 4, pp. 491–502, 2005.

[107] S. Khan, S. Nazir, A. Hussain, A. Ali, and A. Ullah, "An efficient JPEG image compression based on Haar wavelet transform, discrete cosine transform, and run length encoding techniques for advanced manufacturing processes," *Measurement and Control*, vol. 52, no. 9-10, pp. 1532–1544, 2019.

[108] H. Chen, S. Khan, B. Kou, S. Nazir, W. Liu, and A. Hussain, "A smart machine learning model for the detection of brain hemorrhage diagnosis based internet of things in smart cities," *Complexity*, vol. 2020, Article ID 3047869, 10 pages, 2020.

[109] S. Khan, H. Ali, Z. Ullah, N. Minallah, S. Maqsood, and A. Hafeez, "KNN and ANN-based recognition of handwritten Pashto letters using zoning features," 2019, http://arxiv.org/abs/1904.03391.

[110] S. Khan, A. Hafeez, H. Ali, S. Nazir, and A. Hussain, "Pioneer dataset and recognition of handwritten Pashto characters using convolution neural networks," *Measurement and Control*, vol. 53, no. 9-10, pp. 2041–2054, 2020.

[111] V. Gupta, B. P. Kaur, and S. Jangra, "An efficient method for fault tolerance in cloud environment using encryption and classification," *Soft Computing*, vol. 23, no. 24, pp. 13591–13602, 2019.

[112] J. Peng, X. Zhang, Z. Lei, B. Zhang, W. Zhang, and Q. Li, "Comparison of several cloud computing platforms," in *2009 Second international symposium on information science and engineering*, pp. 23–27, Shanghai, China, 2009.

Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 3896840, 14 pages
https://doi.org/10.1155/2022/3896840

Research Article

Interest-Based Content Clustering for Enhancing Searching and Recommendations on Smart TV

Malang Jan,[1] Shah Khusro,[1] Iftikhar Alam,[2] Inayat Khan,[3] and Badam Niazi[4]

[1]*Department of Computer Science, University of Peshawar, 25000, Pakistan*
[2]*Department of Computer Science, City University of Science and Information Technology, Peshawar 25000, Pakistan*
[3]*Department of Computer Science, University of Buner, Buner, 19290, Pakistan*
[4]*Department of Computer Science, University of Nangarhar, 2600, Afghanistan*

Correspondence should be addressed to Badam Niazi; niazi5.48@gmail.com

Received 12 February 2022; Accepted 12 April 2022; Published 5 May 2022

Academic Editor: Muhammad Imran

Smart TV has become a pervasive device due to its support for numerous entertainment options. These capabilities of smart TV make it attractive for viewers and researcher. Besides, a plethora of multimedia content continues to grow, which makes searching and browsing the desired content a difficult, time-consuming, and contributes to cognitive overload problem. In the case of smart TV, making clusters of the related content based on user's interest is among the best solutions. In this connection, this study proposed a dynamic approach for clustering the TV-related online multimedia content and presenting them in a manageable format on smart TV to mitigate the issue of searching and relevant recommendations. We collected and clustered the content from diverse data sources based on the viewer's interest. This further recommends novel content to the viewers without social metadata, such as rates, tags, which is normally insignificant in for smart TV viewership due to its shared nature. We used bisecting *K*-means, Lingo, and Suffix Tree Clustering (STC) algorithms. A comparative analysis of these algorithms and suitability in the context of smart TV is also presented. Results show that the proposed approach enhances search results and recommends relevant content based on user's interests.

1. Introduction

In this digital era, the popularity of smart TV is increasing day by day. Smart TV is a device that have traditional flavour of television along with an operating system and support internet connectivity for streaming services. This smart TV have changed the entertainment paradigm in many folds [1]. The statistics show that almost 94.2 million people are using smart TV in the United States (https://www.statista.com/statistics/718737/number-of-smart-tv-users-in-the-us/) only. Smart TV is a platform based on the full support of Web2.0 features where a user can read and write the online content [2]. It supports and provides content from diverse data sources like online stored video, video on demand (VoD) services, video clips, social networking sites, and support for online streaming channel [3]. Besides these multiple content facilities, smart TV also offers new features like Set-Top Boxes (STBs), connection facilities with smart handheld devices like smartphones and tablets [4].

The abundance of multimedia content on smart TV is one of the main causes of attraction for the users. The rapidly growing content on social networking sites, such as YouTube, Dailymotion, and Instagram, creates and generates users' big data sources. These data sources are becoming richer day by day and growing overwhelmingly. However, the users feel difficulty in searching for their desired content, such as searching for channels or programs [5–8]. One such popular social video-sharing website is YouTube, where users upload five hundred hours of videos per minute on YouTube [9]. The growing rate of such content creates trouble for the users to search the desired videos among these rich multimedia data. Searching for the required channels on a smart TV is a major issue as it is based on a linear search (bottom-up) using a traditional remote control [10,

11]. Due to unique features of smart TV and remote control, searching content is a major issue compared to handheld devices like smartphones and tablets. The reason behind least interest in the smart TV compared to other handheld devices is that the handheld devices provide one-touch and are easy to use for accessing the vast collection of online content. At the same time, smart TV is a lean-back device working well with the traditional remote control and other digital devices attached to the smart TV. These features lead a user to tedious task of searching and hurts user feelings [12, 13]. Thus, the searching process on this platform leads to the content overload problem.

Different techniques and methods are presented in the literature to provide and recommend videos based on the different features to the users [11]. The study [14] presented the video based on vector approach and deep learning method of image-based features (objects) extracted from video keyframes. Some works targeted the audio and visual features to classify videos [15, 16]. Besides audio and visual features, the study in [17] presented an approach based on multiple features. Both visual and textual features are selected to cluster the videos. The clustering technique plays a significant role in classifying videos in this domain and is one of the possible solutions for making searching and recommendation more viable and significant [18]. Figure 1 depicts the general approach of content clustering.

The recommendation approach uses user's profile and item's profile data and recommends a relevant data item that is supposed to be relevant to a user or group of users. It has different approaches, such as implicit feedback, explicit feedback, and hybrid approaches [19]. The implicit feedback are navigation and type of sites watching, whereas explicit feedback are likes, dislikes, ratings, and keywords. In hybrid approaches, we combine all these approaches [20].

In this paper, we presented a personalized content-based (CB) recommendation approach based on user previous watching history and presented the results in clusters. Unlike the collaborative filtering (CF) approach, which sometimes provides undesired content based on the neighbour profile (using the rating or number of views information), the presented method in this work offers desired and related content based on the user's interests. The method is providing/suggesting multiple contents to the user from the diverse data sources (YouTube, Dailymotion, etc.) based on their interests (favourite watched programs) by grouping related/similar content into clusters. Clustering or cluster analysis is one of the most commonly used unsupervised machine learning methods, which determines similarities between data points and combines similar data into one group (cluster) without any labelled data [21, 22]. In Figure 1, the data point may be text documents, web pages, or video content. The objectives and contributions of the paper are:

(i) To present the user with related sets of content from diverse sources to overcome the issues of cognitive overload

(ii) The paper presents a novel method of content extraction from diverse data sources (YouTube, Dailymotion, etc.) based on watching activity/interest

(iii) The paper further provides meaningful clusters for searching the desired and related content to a user on smart TV

(iv) A subjective study has been conducted for evaluating the user's satisfaction, ease of searching, and browsing for both preclustered and postclustered approaches

(v) Lastly, the paper provides a comparison of clustering algorithms in the domain TV-related content clustering like movies, dramas, and songs and suggests suitable clustering algorithms for these contents

The remainder of the paper is divided into the following sections. Section 2 provides a literature review for this work. Section 3 describes the proposed a solution and discusses its methodology. Sections 4 and 5 describe results and evaluation, and Section 6 concludes the work with future research direction.

2. Related Work

This section provides compact yet comprehensive detail on relevant literature in the context of smart TV domain. This section further provides how different content like stored video, online streaming channels, and programs are clustered and how they are recommended based on clusters and user's preferences. Limitations of the existing work are also discussed in details. A plethora of literature is available on machine learning and clustering techniques [23], which this portion also discusses.

2.1. Clustering Techniques Based on Users Preferences. In context of TV watching, a user preference refers to the interests of the certain programs watched by a user [20, 24] or the user preference to the other content based on their interests watched previously by a user [25]. By examining the preferences of the users, different approaches and techniques are presented [26, 27], which recommends similar content to the users, and reduce the content overload problem. Similar to the user preferences, [28] presents a study on the user's experience and their factors in the domain of smart TV and discussed different studies and their factors, such as ease of use, accessibility, personalization, content diversity, and browsing content. It determined the comprehensive set of factors that affect the user's satisfaction and usage differently. The study [29] clustered the users based on their preferences to provide top-N recommendations for a user in each cluster. The approach offers recommendations based on the other users' preferences within the same clusters. This recommendation technique has limitations, as unwanted content is recommended to the target user based on the neighbour items/users in the same cluster. Similarly, Wu et al. [30] proposed an approach to reduce channel selection paths and provide fast and smooth channel selection based on the user's previous history. The proposed approach presented an efficient navigation approach, which minimizes the channel searching, and selection seeks distance for a

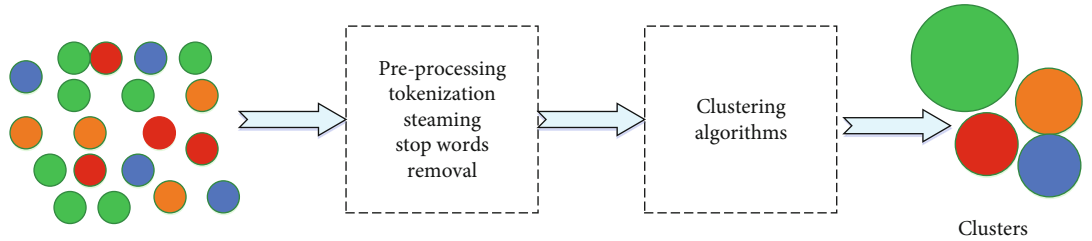


Figure 1: General content clustering approach.

user, using the remote-control device based on the next and previous button consequence. For example, a user often switches from news to funny channel, this preference shows the user interests, and it must be closely positioned. The hierarchical clustering schemes were used to construct a sequence of channels and provide close pairs of channels based on users' frequently switching channels.

2.2. Clustering Techniques Based on Visual Features. The videos on the web contain different features (i.e., visual and textual), and based on these features, different techniques and approaches are presented to reduce the information overload problem. Liu et al. [27] proposed an approach for clustering videos return from web search results by using visual features to reduce searching space. The proposed approach clusters similar videos into a cluster to eliminate the duplicate videos returned from the user query results on the web to provide the smooth searching of the relevant video among many videos. Visual content (frames) are matched using the signature-based similarity method to find the similarity between videos. The video frame histogram is calculated in the study [31]. Based on frame histogram, the similarity between videos were calculated, and the affinity propagation (AP) clustering algorithm [32] was used to group similar videos into the cluster. Yang et al. targeted the static video summarization problem for clustering and proposed a novel clustering-based method for static video summarization [32]. They proposed a novel clustering algorithm called Video Representation Based on High-Density Peak Search (VRHDPS). The proposed method includes four steps: (i) presampling, (ii) video frame representation, (iii) clustering, and (iv) static video summarization results. Similarly, [33] also presented a clustering method based on the deep learning technique by extracting the image-based features from the frames. The approaches mentioned above are based on visual features extracted from the videos. The main drawback of the visual features is that it is an expensive process because extracting visual features from lengthy videos is an expensive task.

2.3. Clustering Techniques Based on Textual and Visual Features. The studies [34, 35] presented web video clustering based on multiple features to overcome the limitation of video clustering based on visual features. This proposed system includes the following components: (i) video acquisition and preprocessing, (ii) preprocessing of text information, and (iii) video clustering and results in visualization. In the first step, metadata about videos from YouTube is collected using the TubeKit open-source YouTube crawler. The information was stored in a local database indexed with a video ID. Second, the authors used their previous work for video processing. With the help of principal component analysis (PCA), the sequence of video frames is transformed into bounded coordinate system (BCS) to form a new coordinate system [25]. BCS uses the bounded principal component (BPC) to remove the noise in frames histogram. In text preprocessing, the text was compared according to their common words in the metadata. The similarity between sentences was calculated according to common words in their sentences. Only tags, titles, and description similarities are calculated. At last, all feature set (visual content, title, tags, and description) was clustered using the clustering algorithm, and the result was visualized for the user. Using the clustering methods AP (affinity propagation) and normalized cut (NC), the experiment results show the best results on higher textual feature weighting than the visual feature.

Another work [36] targeted the multiple model videos to categorize them. The videos on the web are various features and type like home video uploaded by users (low quality), social information of the videos, and professional videos (TV drama, movies, etc.) with low and high quality; size of the videos, nonprofessional videos, and textual information about videos like tags and description title are targeted. The proposed approach consists of three steps, i.e., feature extraction, classification, and fusion. Their visual features, semantic features, surrounding text, and audio features were extracted to represent videos for categorization. Semantic features were extracted from videos using two approaches [37], video annotation (concept) and visual words. Based on the classifiers' results for different features for each category, the results are fused to achieve a final category about videos. The study [25] proposed the playlist-based video clustering method (PV-clustering) by claiming that the proposed method is inexpensive as compared to the existing approaches, which were having some problems, like low-quality text information in the metadata, difficulty in extracting visual content, and noise in the information of users viewing behaviour. The proposed method consists of three steps: playlist information acquisition, video similarity calculation based on the selected features, and video clustering. First, the authors collected the information from YouTube-like Playlist id (Pid), Video id (Vid), video title, and description. This information was expressed in a binary playlist-video incident matrix. Cosine similarity measure was used to compute the similarity between the binary playlist-video incident matrix of the video, and a clustering

algorithm is applied to these features. The limitation of the presented work is that several videos on the web platform or YouTube do not contain playlist information.

2.4. Recommendations Based on Clustering on TV Platform. Cluster analysis also plays an important role in the recommendation [19, 38]. Once the clusters are created from content or users, the recommendation is carried on these clusters to provide relevant content according to their interests [39–41]. Recommending desired and relevant content to the users reduces the content overload problem. Three approaches are mostly used in the recommendation, i.e., collaborative filtering (CF), content-based filtering (CBF), and hybrid [42]. In the CF approach, the content is recommended to a user based on similar users' preferences. Based on their preferences, the users' similarity is analyzed, and content is recommended to the target user. Different techniques and methods in the domain of TV are presented in the literature to provide CF-based recommendations to the users, i.e., based on similar users' interests [43], based on items rating clustering [36], and recommending movies based on rating information [25]. Content-based (CB) recommendation provides the content to the users based on the item's features and user profile. In this approach, the user's history is examined to determine the user's interest in items. Similar items are recommended to the users based on their feature's similarity (their description, type, genre, etc.). The hybrid recommendation approach combines the characteristics of both CF and CBF approaches to provide more effective and accurate items/content to the users. A detailed review of the recommender systems in the domain of television (TV) is presented in [44, 45].

The study [46] presented an exploratory study about grouping users based on their watching patterns (behaviour) using the clustering technique. The authors presented the user modelling approach to overcome the cold start problem and recommend using the K-means clustering algorithm with Euclidean distance metric for experimental results. The study [47] extended this work and presented Catch-TV Recommendations. The proposed approaches for recommending content similar to the previously watched content and new content where the users are not familiar with them. The recommendation approaches presented by the authors are subscribed series recommendations, new series recommendations, and combining recommendation. The channel recommendation technique for the live streaming platform Twitch is presented in [48]. The proposed approach consists of three steps to recommend relevant channels to a user. In the first step, the users' preference is identified using their time on each channel, game, and language. In the second step, the users are clustered according to similar preferences. The obtained preferences are channel, game, and language. The well-known K-means clustering algorithm was used to cluster the user's preferences. In the last step, after clustering results, based on the users' preferences within the same cluster for each channel, game, and language, the top-n relevant channels were recommended. Similarly, [49] presented a personalized channel real-time recommendation system (PCRS) framework in the IPTV system via deep learning using the users' watching and channel switching sequence history. The work targeted the channel switching history and does not consider the other information like metadata, user profile, and social connection.

The popularity of the channels is considered in the recommender system to provide appropriate recommendations for the users. Artificial neural network (ANN) provides appropriate recommendations for popular and unpopular channels. The popular/hot channels are recommended to the users with the help of ANN trained data from the previous popular channels watching logs called hot artificial neural network (HANN). The unpopular/cold channels are recommended to the users with the help of ANN trained data from the previous unpopular channels watching logs called CANN (cold artificial neural network). The framework produces better results than the author's previous recommendation based on the history of user switching channels [50]. Further, the movie recommendation using Apache-Spark is presented in [14], and multichannel feature vectors by efficient collaborative filtering recommendations are also proposed [15].

The methods and approaches that cluster the users based on the other user preferences may sometimes provide an undesirable recommendation. This recommendation technique has limitations where undesirable content is recommended to the target user based on the neighbour items/users in the same cluster. In this situation, the personalized content-based (CB) recommendation technique provides more relevant and desired content to the users than the collaborative filtering recommendation method. Our proposed approach is based on a content-based recommendation technique based on the user interest, as described in the next section in detail.

2.5. Hard and Soft Clustering. Various clustering algorithms are available in the literature, but selecting suitable clustering algorithms depends on the dataset and domain where applicable [51]. This section only discusses two types of clustering algorithms and the suitability of the clustering algorithms in TV-related content. In the result section that the soft cluster algorithm provides precise results compared to the hard-clustering algorithm, K-means [52], one of the most widely used clustering algorithms, fails to provide precise and accurate results compared to the soft clustering algorithm. Comparisons and discussions are provided in the results section in detail.

The partition-based method is called the flat clustering method. In this method, a set of flat clusters is created. It is a popular and most widely used clustering technique. Unlike hierarchical clustering techniques that generate a dendrogram, partition-based clustering algorithms aim to partition the data into groups of similar data points. The cluster assignments may be hard or soft [53, 54]. In the hard clustering method, the data objects are divided into several unique homogenous datasets called a partition. Each partition represents a cluster. Each data object must belong to only one cluster in the hard-based method. A well-known

example of this type of method is the K-means clustering algorithm. Flat clustering (hard) can be defined as follows:

Given (i) a set of documents $D = (d_1, d_2, \cdots, d_n)$, (ii) desired number of clusters, K, and (iii) an objective function that evaluates the quality of clustering, the clustering task is to compute an assignment γ: $D \longrightarrow \{1, 2, \cdots, K\}$ that minimizes (or in certain cases maximizes) the objective function [53].

Hard clustering (classical approach) assigns data point or object to just one cluster. On the other hand, the soft clustering approach assigns data points or object to more than one cluster [55]. The soft flat clustering method is based on the membership value where a document may be assigned to more than one cluster. Soft flat clustering is also called fuzzy clustering because it is based on the membership values belonging to a particular cluster [56]. The membership values are in the interval of (0, 1). The value zero represents the low similarity in the cluster, while one indicates the high similarity of the data points in the cluster. The membership value of the data points or documents within the cluster specifies the closeness of the data points to a cluster [57].

3. Proposed Methodology

This section presents the proposed methodology, as depicted in Figure 2—based on the user interest captured from their favourite watched program. To find the favourite user program, we need to analyse the list of programs watched by a user. Thereupon, we need to choose those channels or programs mostly watched by a user based on the time spent on each program. The longer time spent on the program means that users like that content. The fewer watched program based on the time proportion confirms that the user is not interested in the consumed channels or programs. The steps of the proposed methodology are briefly described below:

(i) In the first step, the user's browsing and watching activities on a smart TV are captured and analyzed to find their interests. The user's interests are captured from the channel they are watching more often by capturing the content type and the dwell time on each watched content type

(ii) The metadata related to the user's watched content is extracted in the second step. This metadata, which contains program name, description, and type, will then be searched for and matched with the metadata of content present on other data sources (i.e., YouTube and Twitter). The matched content is then collected

(iii) The metadata from matched content (from diverse data sources) is extracted in the third step. Based on this extracted metadata, the content is clustered, which will then be recommended to the user

The proposed methodology is shown in Figure 2. We used metadata of the videos to provide the content to a user. Using only the metadata about the content is that textual features yield better results than those provided by the visual [58, 59]. Apart from providing better results, metadata is less expensive than the visual features because extracting visual features from lengthy videos is an expensive task.

As shown in Figure 3, in the first step, the user's watching activities on smart TV are captured and analyzed to find their preference. User preference refers to the interest in certain programs watched by a user on the television [60] or the user preference to the other content based on their interest watched previously by a user [61]. This interest capturing is done using their watching routine by looking at the channel being watched, the program type on that channel during this specific time, and duration time on each watched program.

For example, if a user watches a horror movie daily, the recommended items should include horror movies or dramas. Table 1 is an example of a user who watched a TV program, assuming that the user has watched four different programs. By analyzing this information, the metadata is captured about the watched programs, which are then used for future recommendations in clusters to the user.

The metadata related to the user's watched content is extracted in the second step. For example, suppose a user has watched a specific content (e.g., horror movie). In that case, according to this extracted metadata, all metadata about this movie will be collected, including its name, type, and description, to look for more content from diverse data sources. The similarity between these features is examined with the help of similarity measures. Different similarity measures are presented in the literature to find the similarity between items based on their features. To find the similarity between these extracted features from user interests and collected features from diverse data sources, the cosine similarity technique is used, one of the most widely used similarity measures [52, 62]. It computes the similarity between two documents. Given the two documents d_i and d_j, then their cosine similarity is

$$\mathrm{Sim}\left(d_i, d_j\right) = \cos\left(\theta\right) = \frac{\left(d_i \bullet d_j\right)}{\left(\left\|d_i\right\| * \left\|d_j\right\|\right)}. \tag{1}$$

The $(\bullet)$ represents in Equation (1) the product of two vectors, where $\|d\|$ represents the document's length. The matched content is then extracted and are clustered. Finally, the collected content from the previous step is clustered using the clustering algorithms. To this end, to provide and create quality clustering results from the collected content, Carrot2 open sources Java API (http://project.carrot2.org/download.html) is used. Carrot2 consists of different clustering algorithms, including bisecting K-means, STC (Suffix Tree Clustering) [63], and Lingo [14] to provide the clustering results from the content. STC algorithm in the Carrot2 framework is explained in [64]. The K-means clustering algorithm is also implemented in Carrot2, one of the most widely used in this field [65]. K-means clustering algorithm is also the best choice when clustering similar users' program preferences in the domain of television watching behaviour [49]. In this work, the bisecting K-means (a

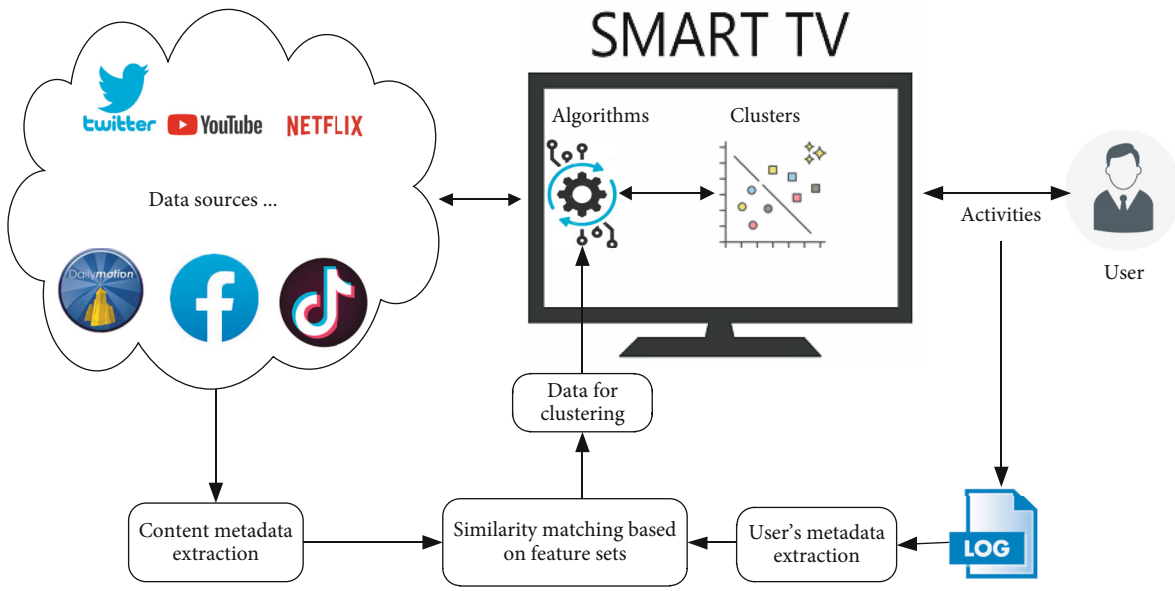


Figure 2: Schematic diagram of the proposed methodology.

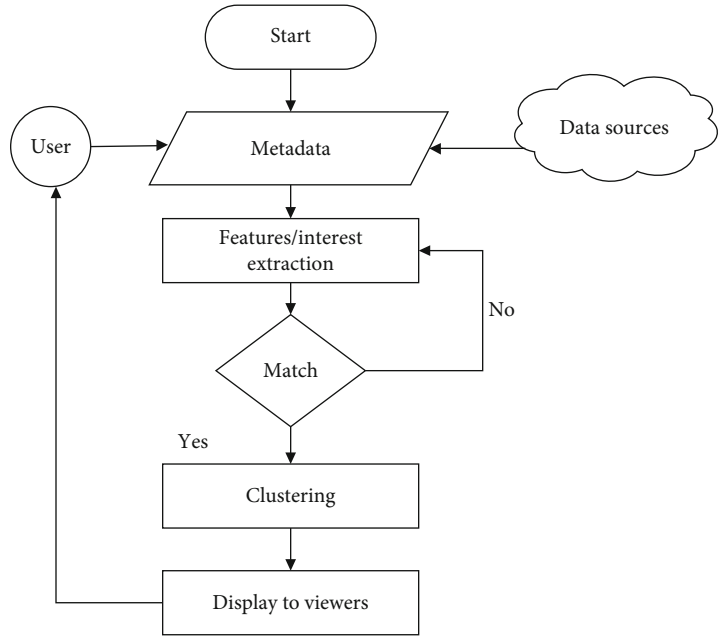


Figure 3: Flowchart of the overall process.

variant of K-means) is used, and STC and Lingo clustering algorithms are considered for comparison purposes. The reason behind choosing the bisecting K-means is that the bisecting K-means produce quality clustering results compared to the regular K-means clustering algorithm [50]. The following Algorithm 1 shows the overall process of the system.

The basic steps of the bisecting K-means clustering algorithm start with a single cluster (all documents) and work in the following manner [33]; in the splitting step as shown in Algorithm 1, we pick a cluster to split, then bisecting step occurs that uses K-means algorithm to split the cluster into two subclusters. The process is repeated until the highest overall similarity (to minimize the sum of overall clusters) is achieved.

4. Results and Analysis

This section will explain the results and the datasets used in experimental results. The subsection elaborated the overall data collection process, metadata extraction, clustering approach, and results.

Table 1: Example of a user watching activity (*h* means hours and *m* means minutes).

Program	P1	P2	P3	P4
Name	BBC	CNN	Mr. Bean	Speed-Records
Type	News	News	Funny	Songs
Time	10 h	5 h	1 h	30 m

```
{
Start
Step i:          Splitting step cluster (C)
                   Select (C) to split (SP);
Step ii:        Bisecting step;
                   K-means algorithm to (SP)
                   Divide (C) into two sub-clusters.
Step iii: Repeat step (ii) and choose the (SP)
Step iv: Repeat until best (C) results.
End
}
```

Algorithm 1:

4.1. Data Collection. We created a dataset by recording the user's watched program history in this work. The purpose of this initial step is to infer some information about user interests. The interests are collected from their log files on smart TV. We have targeted a relatively smaller group of users (i.e., family members in the home). Our dataset consists of 8-week log records of the watched programs. We extracted important metadata from this dataset to search similar content on the diverse data sources. Based on the user watched history, we have collected the metadata of five hundred channels for experimentation, which we believe are enough to fulfil our experimentation needs. For an online collection of data sources, the carrot2 API is used to have a large dataset for further experiments.

4.2. Metadata Extraction Approach. A user's interests are captured from their watched history by analyzing their watch-log. Apache Tikka API (https://tika.apache.org) is used to extract the metadata from a user who watched the program. Apache Lucene (http://lucene.apache.org) has been used to index this information for offline clustering. Take an example where a user has watched a news program recorded in his log file.

4.3. Extracting Metadata from Downloaded Content. The extracted metadata from the user interests was used to search and collect the content from the diverse data sources. The search was performed using the metadata of the user interests. The metadata from the obtained results have been extracted using the Apache Tikka API and indexed using the Apache Lucene. This indexed metadata was used in the experimentation. The metadata was extracted from the log record using Apache Tikka. A screenshot of the process is shown in Figure 4.

4.4. Content Clustering. The features extracted from the user interests (metadata) are used to search and match with collected metadata from diverse data sources. The collected content based on the cosine similarity matching scores is clustered using the clustering algorithms. Carrot2 provided algorithms are used for this task to provide the clustering results based on the collected information. Take an example where a user has watched a news program recorded in his log file. Figure 5 shows the results based on a user-watched program using the bisecting *K*-means clustering algorithm (news in this result).

STC algorithm collected the most news channel in one big cluster, as shown in Figure 6 labelling results. Further, STC provided some balance and small clusters like the latest news cluster. The results presented in Figure 7 presents some novel content (i.e., Johnny English cluster of funny clips) to recommend the related content without considering the ratings and number of views information. Thus, the approach provides related content to the users based on the users watched programs (in our case Mr. Bean funny clips) and presents the results in the form of the cluster to reduce the search space and provide novel related content (i.e. Johnny English Strike Again new movie) to the users effectively without considering the ratings or number of views information. The reason behind ignoring the rating or number of views information is that sometimes users are interested in the content based on their type (i.e., horrors), and recommending other types of content like action or romantic may dishearten the user feel—this our main work to recommend related content to the users based on their previous watched history.

4.5. User's Satisfaction. The clustering approach yields better user satisfaction and ease in the searching process. A subjective study was conducted to evaluate the approaches used in this paper on real-time and actual watching scenarios. We took a random sample of 31 mature audiences. The browsing/navigation, searching, and user's satisfaction was measured in both preclustered and postclustered approaches. A questionnaire of 5 rating scale was used for all three parameters, i.e., ease of searching, browsing, and user's satisfaction. The ease in content browsing in a smart TV has been evaluated and found that browsing for content in the preclustered approach was difficult, as shown in the statistical test (Table 2).

As shown in the following Table 3, the *P* value is less than the alpha value 0.05, and hence, we can say that the difference between preclustered and postclustered approaches is significant. The user's satisfaction in the below subsection shows that the difference is due to good results generated by the clustered approaches.

4.6. Ease of Searching and Browsing. The user's satisfaction has been evaluated using statistical tests. The *P* value is less than the alpha (0.05), and hence, we can conclude that the difference is significant. The better average (3.74) for the postclustering approach than the preclustering approach (2.38) shows that users feel more satisfied. Similarly, searching for relevant content in the postclustered approach

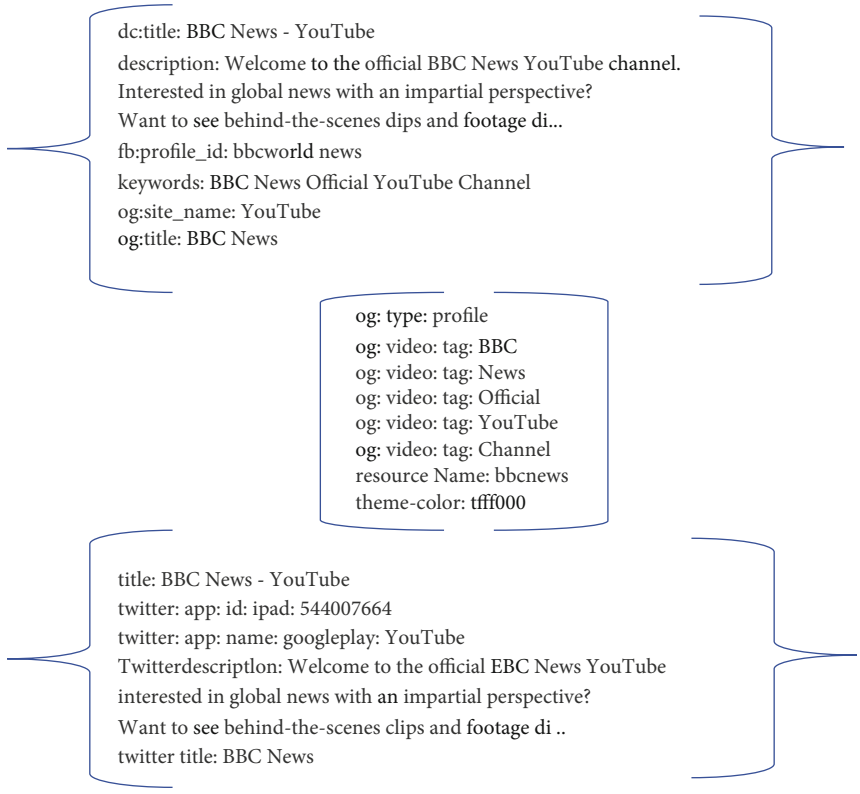


Figure 4: Metadata extracted from the BBC news channel.

Channel, ABC, Business (4 docs)
[0] Watch CNN International Live TV from USA - Online TV channel
http://www.freeintertv.com/view/id-200
[I8] Watch France 24 Live
https://www.france24.com/en/live
[42] Channels Television - Breaking Nigerian News, Today's News...
https://www.channel.stv.com
[33] ABC News Live Stream Video ABC News
https://aLicnews.go.com/Live/video/special-live-l-1447S486
Live, BBC, UK (4 docs)
[15] BBC News Channel Live UK – YouTube
https://www.youtube.com/watch ?v=HXeGpCFGu-k
[31] News Breakfast
https://en.wikipedia.org/wiki/News_Breakfast
[45] India Today Live TV: Free Live TV, Live News Streaming and live
https://www.indiatoday.in/intemational-livetv
[57] Watch BBC News UK Live Stream-BBC News Online
http://www.Iivenewsm.ag.com/bbc-news-uk-live-stream/

Figure 5: Clustering results using the bisecting K-means.

LINGO Algorithm Cluster Labeling:
Updated to the Latest News (4 docs, score: 24.99)
World News (4 docs, score: 14.09)
ARY News is a Pakistani News Channel (3 docs, score: 14.74)
Watch Dunya (3 docs, score: 29.97)
ARY Digital (2 docs, score: 28.94)
Television Network (2 docs, score: 8.82)g
Pakistan, News, TV (31 docs, score: 53.32)
STC Algorithm Labeling:
Latest News, Breaking News, Live TV (6 docs, score: 12.59)
BOL News, 92 News HD (5 docs, score: 9.94)
Channel (18 docs, score: 9)
Urdu News (7 docs, score: 7.91)
Watch (15 docs, score: 7.5)
K-Means Algorithm Cluster Labeling:
ARY, YouTube, Geo (4 docs)
Dunya, Aaj, Largest (4 docs)
News, Updates, Breaking (4 docs)
HD, PTV, Soaps (3 docs)
News, Streaming, Video (3 docs)

Figure 6: Some cluster labeling results.

produced better results. As shown below (Table 3), an ANOVA test depicts that the searching becomes easy compared to the preclustered approach.

5. Comparison and Evaluation

We compared three clustering algorithms on selected features. Table 4 summarizes the results of the three clustering algorithms. The results show that STC and Lingo provide better clustering results than bisecting K-means. STC provides different sized clusters containing quality results, while Lingo creates more precise clustering labels and assigns content to these clusters. Figure 7 provides cluster labelling results from Lingo, STC, and bisecting K-means algorithms. Unlike other clustering algorithms, the Lingo algorithm assigns a more precise label to clusters than the other clustering methods because Lingo first creates clusters labels

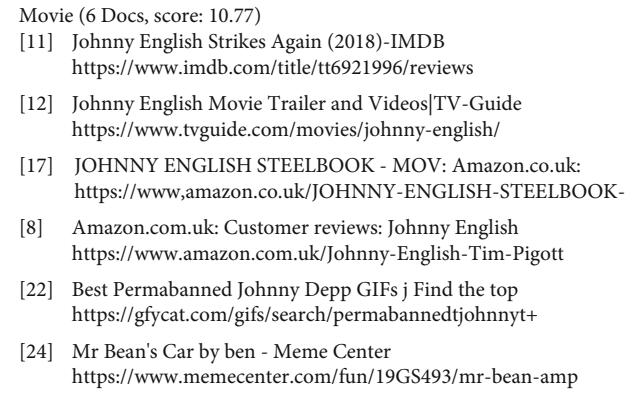


Figure 7: Novel content clusters based on the user interest.

Table 2: ANOVA: single factor.

(a) Summary

Groups	Count	Sum	Average	Variance
Preclustered	31	48	1.548387	0.389247
Postclustered	31	129	4.16129	0.606452

(b) ANOVA

Source of variation	SS	Df	MS	F	P value	F crit
Between groups	105.8226	1	105.8226	212.5594	2.20695E-21	4.001191
Within groups	29.87097	60	0.497849			
Total	135.6935	61				

Table 3: ANOVA: single factor.

(a) Summary

Groups	Count	Sum	Average	Variance
Preclustered	31	53	1.709677	0.546237
Postclustered	31	115	3.709677	0.546237

(b) ANOVA

Source of variation	SS	Df	MS	F	P value	F crit
Between groups	62	1	62	113.5039	1.84E-15	4.001191
Within groups	32.77419	60	0.546237			
Total	94.77419	61				

using the vector space model and then assigns content to these clusters [66]. The result present in Figure 7 shows that bisecting K-means and STC algorithms created some inappropriate labels for the cluster, i.e., soaps word in label assigned by bisecting K-means.

In contrast, STC assigns news, live, channel words in the label due to big clustering results (big cluster compare to others). The bisecting K-means algorithm provides good results, but its nonoverlapping behaviour limits it, i.e., it gives hard clusters where one item cannot be in two clusters at a time, and this very feature of the bisecting K-means algorithm limits its applicability in our scenario. Further, labels of clusters are created from single words, and all content (items) in the cluster may not be similar to the label.

Bisecting the K-means algorithm is one the most widely used algorithms; however, selecting an appropriate clustering algorithm depends on the dataset and domain where it is better applicable. In our case, both STC and Lingo are

Table 4: Comparison of clustering algorithms.

Algorithms	Cluster type	No of clusters	Cluster size	Clusters labels
Bisecting K-means	Hard	10	Small	Less meaningful
Lingo	Soft	17	Small	More meaningful
STC	Soft	15	Big, balance	Meaningful

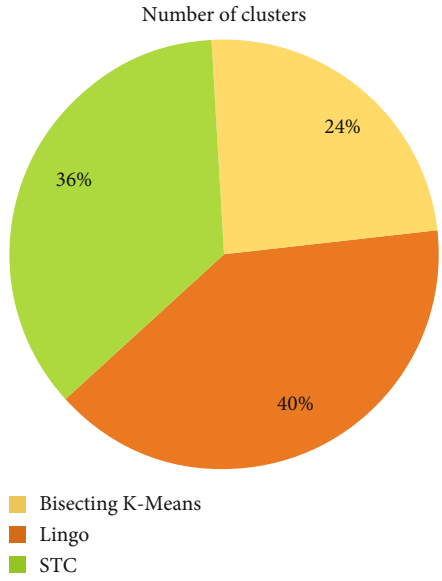


Figure 8: Number of clusters produced by different algorithms.

the best choice for clustering TV programs because it provides overlapped clustering results compared to the bisecting K-means algorithm, which provides hard clusters. The hard-clustering results are inappropriate when a user selects any cluster and does not find the desired program. For example, if a movie type is an action and adventure, then this movie must be placed in both action and adventure clusters. Whenever a user selects any cluster (either action or adventure), then the user can watch the movie in both clusters. If a movie (top rated) is placed in the action cluster only (in the case of hard clustering) and a user is interested in the adventure cluster, then they will miss this movie. Due to this situation, we need to present overlapped clustering results to the users on smart TV.

We evaluated the results of clustering algorithms using five evaluation measures, i.e., contamination [65], precision, recall, F-measures, and normalized mutual information (NMI). Figure 8 shows the result of the news topic. As we can see in the results, the Lingo algorithm provides the best result compared to the STC algorithm. Bisecting the K-means algorithm provides some better results on contamination and precision measures. However, bisecting K-means fail to deliver better results on F-measures. If we examine the comparison in Table 4, we can see that bisecting K-means provides hard clustering results, and both Lingo and STC algorithms provide soft clustering results. Due to this reason, bisecting K-means provide some better results from Lingo and STC algorithms. Overall, the Lingo algorithm provides quality results, meaningful labels for each cluster, and overlapped clustering results. In this situation, the Lingo clustering algorithm is suitable for clustering content to a user in TV-related content.

Figure 9 provides the overall results and comparison (five categories) of the Lingo, STC, and bisecting K-means algorithms. The five categories were news, funny videos, movies, songs, and dramas, as shown in Figure 9. The objective was to select suitable features and clustering algorithms to recommend/suggest the content to the user in clusters without considering ratings or the number of views information.

We have targeted the textual features because they provide better results than the visible results, which are computationally expensive [49, 50]. The limitation of the presented method is that it provides inappropriate results where the textual features are ambiguous. This situation is common in the YouTube video platform, where the user provides ambiguous information to the videos. Similarly, language problems are also associated with this scenario where the user provides textual information other than English. The presented work is suitable for channels or programs providing rich metadata (textual information), and based on this metadata; similar content is presented to the users. We compared three clustering algorithms. Hundreds of clustering algorithms are presented in the literature, and the selection of clustering algorithms depends on the set of features and domains where applicable [66]. We only targeted the hard

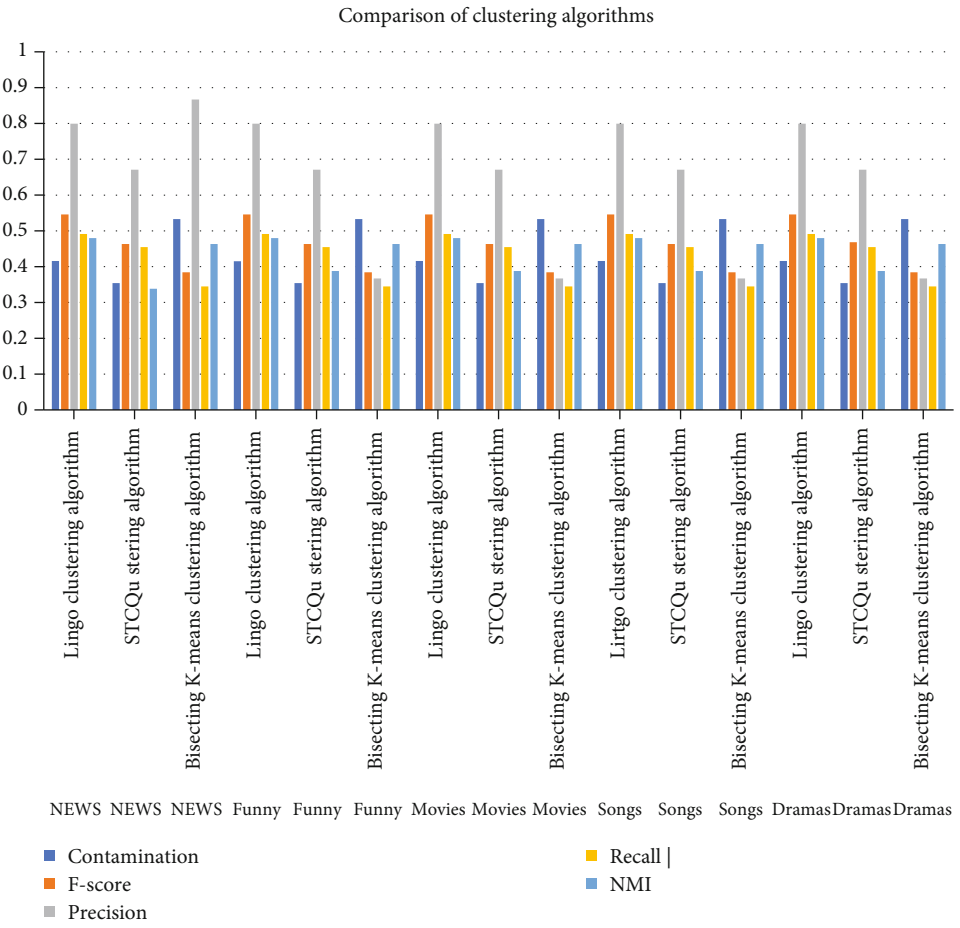


Figure 9: Comparison of clustering algorithms on news, funny videos, movies, songs, and dramas.

and soft clustering algorithms and considered these selected algorithms' labelling results. The reason behind the selection of this algorithm is to suggest a suitable clustering algorithm (hard or soft) in the domain of TV-related content and also suggest a suitable algorithm that creates meaningful cluster labels for user.

6. Conclusion and Future Work

Smart TV is changing the way users watch programs. The support of web 2.0 features and the huge amount of content available is the attracting force of the smart TV. The availability of content is always handy, but it sometimes happens that searching in this large collection of content becomes hard and annoying. The same is the case with smart TV users, where it is becoming increasingly difficult to find the desired content in time and with ease. Several solutions have been proposed to solve this content overload problem. In this research work, we have applied the clustering technique to address the problem of content overload on a smart TV. The motivation behind this research work is that a user tends to have some likes and dislikes while watching TV. These likes and dislikes can be monitored to know the behaviour and taste of the smart TV user. We captured the watching activities of the users, and based on these activities, we have collected similar content from multiple diverse data sources and have presented them to the user in the form of clusters. But to make sure that similar relevant content is retrieved from outside diverse data sources, we extracted features from the user-watched content. Based on those features, we searched for more relevant and similar content. When the user watches a certain program, all the similar and relevant content is clustered and presented. This way, the user only looks for the desired cluster and does not need to search randomly for the desired content. Three algorithms (bisecting K-means, STC, and Lingo) are compared to our collected dataset for comparison purposes. The proposed solution reduces the search time and reduces the content overload problem.

In the future, we are looking to introduce the time factor while clustering the retrieved relevant content on a smart TV. Moreover, the comparative analysis of these algorithms for rich multimedia data can further elaborate the discussion. There are certain specific times when users tend to watch certain specific programs, e.g., news late at night or a bit of music in the morning. Therefore, including the time factor, we believe that the proposed content clusters will improve further. We are planning to look at other factors in the future, e.g., the user's age and language, etc. We believe that the results will improve considerably by further increasing the features on which the clusters are created.

Data Availability

The data that support the findings of this study are available upon request from the first author.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] M. Khan, S. Khusro, I. Alam, S. Ali, and I. Khan, "Perspectives on the design, challenges, and evaluation of smart TV user interfaces," *Scientific Programming*, vol. 2022, 14 pages, 2022.

[2] J. He, "Construction of internet TV industry ecosystem based on data mining technology," *Wireless Communications and Mobile Computing*, vol. 2022, 9 pages, 2022.

[3] I. Alam, S. Khusro, and M. Khan, "Factors affecting the performance of recommender systems in a Smart TV environment," *Technologies*, vol. 7, no. 2, p. 41, 2019.

[4] I. Khan and S. Khusro, "Towards the design of context-aware adaptive user interfaces to minimize drivers' distractions," *Mobile Information Systems*, vol. 2020, 23 pages, 2020.

[5] Y. Elkhatib, R. Killick, M. Mu, and N. Race, "Just browsing? Understanding user journeys in online TV," in *Proceedings of the 22nd ACM International Conference on Multimedia*, pp. 965–968, Orlando, Florida, USA, 2014.

[6] M. Khan, S. Khusro, and I. Alam, "Smart TV-based lifelogging systems: current trends, challenges, and the road ahead," in *Information and Knowledge in Internet of Things*, Springer, 2022.

[7] I. Khan, S. Khusro, N. Ullah, and S. Ali, "AutoLog: toward the design of a vehicular lifelogging framework for capturing, storing, and visualizing LifeBits," *IEEE Access*, vol. 8, pp. 136546–136559, 2020.

[8] I. Khan, S. S. Rizvi, S. Khusro, S. Ali, and T.-S. Chung, "Analyzing drivers' distractions due to smartphone usage: evidence from AutoLog dataset," *Mobile Information Systems*, vol. 2021, 14 pages, 2021.

[9] T. Lian, Z. Chen, Y. Lin, and J. Ma, "Understanding the pulse of the online video viewing behavior on smart TVs," in *Chinese National Conference on Social Media Processing*, pp. 331–342, Beijing, China, 2017.

[10] K. Watanabe, Y. Miyake, N. Nakamichi, T. Yamada, and T. Ozeki, "Remote touch pointing for smart TV interaction," in *IEEE 3rd Global Conference on Consumer Electronics (GCCE)*, pp. 232–235, Tokyo, Japan, 2014.

[11] I. Alam and S. Khusro, "Tailoring recommendations to groups of viewers on smart TV: a real-time profile generation approach," *IEEE Access*, vol. 8, pp. 50814–50827, 2020.

[12] X. Wu, C.-W. Ngo, Y.-M. Zhu, and Q. Peng, "Boosting web video categorization with contextual information from social web," *World Wide Web*, vol. 15, no. 2, pp. 197–212, 2012.

[13] I. Khan and S. Khusro, "ConTEXT: context-aware adaptive SMS client for drivers to reduce risky driving behaviors," *Soft Computing*, pp. 1–18, 2022.

[14] H. Zhang, J. Chai, Y. Wang, M. An, B. Li, and Q. Shen, "Application of clustering algorithm on TV programmes preference grouping of subscribers," in *IEEE International Conference on Computer and Communications (ICCC)*, pp. 40–44, Chengdu, China, 2015.

[15] N. Chang, M. Irvan, and T. Terano, "A TV program recommender framework," *Procedia Computer Science*, vol. 22, pp. 561–570, 2013.

[16] S. Pyo, E. Kim, and M. Kim, "Automatic and personalized recommendation of TV program contents using sequential pattern mining for smart TV user interaction," *Multimedia Systems*, vol. 19, no. 6, pp. 527–542, 2013.

[17] M.-W. Kim, E.-J. Kim, W.-M. Song, S.-Y. Song, and A. R. Khil, "Efficient recommendation for smart TV contents," in *International Conference on Big Data Analytics*, pp. 158–167, New Delhi, India, 2012.

[18] D. Huang, C.-D. Wang, J.-H. Lai, and C.-K. Kwoh, "Toward multidiversified ensemble clustering of high-dimensional data: from subspaces to metrics and beyond," *IEEE Transactions on Cybernetics*, pp. 1–14, 2021.

[19] H. Ko, S. Lee, Y. Park, and A. Choi, "A survey of recommendation systems: recommendation models, techniques, and application fields," *Electronics*, vol. 11, no. 1, p. 141, 2022.

[20] I. Alam, S. Khusro, and M. Khan, "Personalized content recommendations on smart TV: challenges, opportunities, and future research directions," *Entertainment Computing*, vol. 38, article 100418, 2021.

[21] S. Chander and P. Vijaya, *Unsupervised learning methods for data clustering*, Elsevier, 2021.

[22] J. B. Rebecca, V. Ramalingam, V. Sugumaran, and D. Rajkumar, "Predictive analysis of online television videos using machine learning algorithms," in *Fundamentals and Methods of Machine and Deep Learning: Algorithms, Tools and Applications*, John Wiley & Sons, Inc., 2022.

[23] P. Singh, *Fundamentals and Methods of Machine and Deep Learning: Algorithms, Tools, and Applications*, John Wiley & Sons, 2022.

[24] J. Jang and Y. Y. Mun, "Determining and validating smart TV UX factors: a multiple-study approach," *International Journal of Human-Computer Studies*, vol. 130, pp. 58–72, 2019.

[25] C.-Y. Lin and H.-S. Chen, "Personalized channel recommendation on live streaming platforms," *Multimedia Tools and Applications*, vol. 78, no. 2, pp. 1999–2015, 2019.

[26] H. Kim, J. Crowcroft, and F. M. Ramos, "Efficient channel selection using hierarchical clustering," in *IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, pp. 1–9, San Francisco, CA, 2012.

[27] S. Liu, M. Zhu, and Q. Zheng, "Mining similarities for clustering web video clips," in *International Conference on Computer Science and Software Engineering*, pp. 759–762, Hubei, China, 2008.

[28] X. Wu, A. G. Hauptmann, and C.-W. Ngo, "Practical elimination of near-duplicates from web video search," in *Proceedings of the 15th ACM International Conference on Multimedia*, pp. 218–227, Augsburg, Germany, 2007.

[29] B. J. Frey and D. Dueck, "Clustering by passing messages between data points," *Science*, vol. 315, no. 5814, pp. 972–976, 2007.

[30] J. Wu, S.-H. Zhong, J. Jiang, and Y. Yang, "A novel clustering method for static video summarization," *Multimedia Tools and Applications*, vol. 76, no. 7, pp. 9625–9641, 2017.

[31] Z. Huang, H. T. Shen, J. Shao, X. Zhou, and B. Cui, "Bounded coordinate system indexing for real-time video clip search," *ACM Transactions on Information Systems (TOIS)*, vol. 27, no. 3, pp. 1–33, 2009.

[32] L. Yang, J. Liu, X. Yang, and X.-S. Hua, "Multi-modality Web video categorization," in *Proceedings of the International Workshop on Workshop on Multimedia Information Retrieval*, pp. 265–274, Bavaria, Germany, 2007.

[33] Z. A. A. Ibrahim, M. Saab, and I. Sbeity, "VideoToVecs: a new video representation based on deep learning techniques for video classification and clustering," *SN Applied Sciences*, vol. 1, no. 6, pp. 1–7, 2019.

[34] M. Kamie, T. Hashimoto, and H. Kitagawa, "Effective Web video clustering using playlist information," in *Proceedings of the 27th Annual ACM Symposium on Applied Computing*, pp. 949–956, Trento, Italy, 2012.

[35] D. Liu, X. Qu, Y. Wang et al., "Unsupervised temporal video grounding with deep semantic clustering," 2022, https://arxiv.org/abs/2201.05307.

[36] M. Xu, S. Berkovsky, S. Ardon, S. Triukose, A. Mahanti, and I. Koprinska, "Catch-up TV recommendations: show old favourites and find new ones," in *Proceedings of the 7th ACM Conference on Recommender Systems*, pp. 285–294, Hong Kong, China, 2013.

[37] E. Ntoutsi, K. Stefanidis, K. Nørvåg, and H.-P. Kriegel, "Fast group recommendations by applying user clustering," in *International Conference on Conceptual Modeling*, pp. 126–140, Florence, Italy, 2012.

[38] H. H. C. Nguyen, B. T. Khiet, and T. T. Nguyen, "An effective method for clustering-based web service recommendation," *International Journal of Electrical & Computer Engineering*, vol. 12, no. 2, pp. 1571–8708, 2022.

[39] S. Gong, "An efficient collaborative recommendation algorithm based on item clustering," *Advances in Wireless Networks and Information Systems*, vol. 72, pp. 381–387, 2010.

[40] M. Ahmed, M. T. Imtiaz, and R. Khan, "Movie recommendation system using clustering and pattern recognition network," in *IEEE 8th Annual Computing and Communication Workshop and cConference (CCWC)*, pp. 143–147, Las Vegas, 2018.

[41] D. Véras, T. Prota, A. Bispo, R. Prudêncio, and C. Ferraz, "A literature review of recommender systems in the television domain," *Expert Systems with Applications*, vol. 42, no. 22, pp. 9046–9076, 2015.

[42] M. Riyahi and M. K. Sohrabi, "Providing effective recommendations in discussion groups using a new hybrid recommender system based on implicit ratings and semantic similarity," *Electronic Commerce Research and Applications*, vol. 40, article 100938, 2020.

[43] M. Xu, S. Berkovsky, I. Koprinska, S. Ardon, and K. Yacef, "Time dependency in TV viewer clustering," in *UMAP Workshops*, Montreal, Canada, 2012.

[44] C. Yang, S. Ren, Y. Liu, H. Cao, Q. Yuan, and G. Han, "Personalized channel recommendation deep learning from a switch sequence," *IEEE Access*, vol. 6, pp. 50824–50838, 2018.

[45] S. Aggarwal, D. Goswami, M. Hooda, A. Chakravarty, and A. Kar, "Recommendation systems for interactive multimedia entertainment," in *Data Visualization and Knowledge Engineering*, Springer, 2020.

[46] C. Yu, H. Ding, H. Cao, Y. Liu, and C. Yang, "Follow me: personalized IPTV channel switching guide," in *Proceedings of the 8th ACM on Multimedia Systems Conference*, pp. 147–157, Taipei, Taiwan, 2017.

[47] A. Maheshwari, A. Kumari, A. Kumari, N. Kumar, and B. M. Nandini, "Movie recommendation system using Apache Spark," in *3rd National Conference on Image Processing, Computing, Communication, Networking and Data Analytics*, p. 280, New Delhi, India, 2018.

[48] H.-R. Zhang, F. Min, Z.-H. Zhang, and S. Wang, "Efficient collaborative filtering recommendations with multi-channel feature vectors," *International Journal of Machine Learning and Cybernetics*, vol. 10, no. 5, pp. 1165–1172, 2019.

[49] A. Hindle, J. Shao, D. Lin, J. Lu, and R. Zhang, "Clustering web video search results based on integration of multiple features," *World Wide Web*, vol. 14, no. 1, pp. 53–73, 2011.

[50] V. Mekthanavanh, T. Li, J. Hu, and Y. Yang, "Web video clustering based on emotion category," in *Proceedings of the 2018 International Conference on Big Data Engineering and Technology*, pp. 87–91, Chengdu, China, 2018.

[51] F. U. Siddiqui and A. Yahya, "Quantitative analysis methods of clustering techniques," in *Clustering Techniques for Image Segmentation*, Springer, 2022.

[52] A. K. Jain, "Data clustering: 50 years beyond K-means," *Pattern Recognition Letters*, vol. 31, no. 8, pp. 651–666, 2010.

[53] C. D. Manning, P. Raghavan, and H. Schütze, *Introduction to Information Retrieval*, vol. 1, Cambridge University Press, Cambridge, 2012.

[54] A. Kumar, A. Nayyar, S. Upasani, and A. Arora, "Empirical study of soft clustering technique for determining click through rate in online advertising," in *Data Management, Analytics and Innovation*, Springer, 2020.

[55] M. B. Ferraro and P. Giordani, "Soft clustering," *Wiley Interdisciplinary Reviews: Computational Statistics*, vol. 12, no. 1, article e1480, 2020.

[56] M. Li, L. Wen, and F. Chen, "A novel collaborative filtering recommendation approach based on soft co-clustering," *Physica A: Statistical Mechanics and its Applications*, vol. 561, article 125140, 2021.

[57] V. K. Singh, T. J. Siddiqui, and M. K. Singh, "Evaluating hard and soft flat-clustering algorithms for text documents," in *Proceedings of the Third International Conference on Intelligent Human Computer Interaction (IHCI 2011)*, pp. 63–76, Prague, Czech Republic, 2013.

[58] A. Huang, "Similarity measures for text document clustering," in *Proceedings of the Sixth New Zealand Computer Science Research Student Conference (NZCSRSC2008)*, pp. 49–56, Christchurch, New Zealand, 2008.

[59] R. Xu and D. Wunsch, "Survey of clustering algorithms," *IEEE Transactions on Neural Networks*, vol. 16, no. 3, pp. 645–678, 2005.

[60] O. E. Zamir and O. Etzioni, *Clustering Web Documents: A Phrase-Based Method for Grouping Search Engine Results*, University of Washington, 1999.

[61] S. Osiński, J. Stefanowski, and D. Weiss, "Lingo: search results clustering algorithm based on singular value decomposition," in *Intelligent Information Processing and Web Mining*, Springer, 2004.

[62] J. Stefanowski and D. Weiss, "Carrot 2 and language properties in web search results clustering," in *International Atlantic Web Intelligence Conference*, pp. 240–249, Madrid, Spain, 2003.

[63] X. He, M.-Y. Kan, P. Xie, and X. Chen, "Comment-based multi-view clustering of web 2.0 items," in *Proceedings of the 23rd International Conference on World Wide Web*, pp. 771–782, Seoul, Korea, 2014.

[64] M. Steinbach, G. Karypis, and V. Kumar, "A comparison of document clustering techniques," in *KDD workshop on text mining*, pp. 525-526, Boston, USA, 2000.

[65] S. Osinski and D. Weiss, "A concept-driven algorithm for clustering search results," *IEEE Intelligent Systems*, vol. 20, no. 3, pp. 48–54, 2005.

[66] S. Solorio-Fernández, J. A. Carrasco-Ochoa, and J. F. Martínez-Trinidad, "A review of unsupervised feature selection methods," *Artificial Intelligence Review*, vol. 53, 2, pp. 907–948, 2020.

Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 4275243, 12 pages
https://doi.org/10.1155/2022/4275243

Research Article

A Cost Effective Identity-Based Authentication Scheme for Internet of Things-Enabled Agriculture

Bilal Hassan,[1] Abeer Abdulaziz AlSanad,[2] Insaf Ullah,[3] Noor Ul Amin,[1] Muhammad Asghar Khan,[3] M. Irfan Uddin,[4] and Jimmy Ming-Tai Wu[5]

[1]*Department of Information Technology, Hazara University, Mansehra, KP, Pakistan*
[2]*Information Systems Department, College of Computer and Information Sciences, Imam Mohammad Ibn Saud Islamic University, Riyadh 11432, Saudi Arabia*
[3]*Hamdard Institute of Engineering & Technology, Hamdard University, Islamabad 44000, Pakistan*
[4]*Institute of Computing, Kohat University of Science and Technology, Kohat 26000, Pakistan*
[5]*College of Computer Science and Technology, Shandong University of Science and Technology, Shandong, China*

Correspondence should be addressed to Jimmy Ming-Tai Wu; wmt@wmt35.idv.tw

Received 27 December 2021; Accepted 30 March 2022; Published 25 April 2022

Academic Editor: Daniel G. Reina

The Internet of Things (IoT) has revolutionized practically every industry, including agriculture, due to its fast expansion and integration into other industries. The application of IoT in agriculture motivates farmers to use their resources wisely and allows for better field monitoring and decision-making, resulting in increased agricultural productivity. Because IoT-enabled agriculture systems need the use of various types of sensors that collect data (such as soil moisture and humidity) and then transmit it over the network. IoT-based agriculture systems, on the other hand, are always vulnerable to security threats. Authentication is one of the assured options for addressing the security concern, since it only enables an authorized party to access the data. Existing authentication schemes typically use the Rivest-Shamir-Adleman (RSA) algorithm and elliptic curve cryptography (ECC), which has a greater computational and communication cost. Furthermore, the security of the majority of existing authentication schemes is not verified using any security tool. As a result, we propose an identity-based authentication scheme for IoT-enabled agriculture in this article. To ensure that our scheme is cost-effective, we employ hyperelliptic curve cryptography (HECC). Our scheme surpasses existing authentication schemes in terms of computational cost and communication overhead while providing better security, according to a thorough investigation of performance and security.

1. Introduction

The history of the Internet of things is very old, but the term "Internet of Things (IoT)" was first used by Kevin Ashton in 1999. The word things refers to a physical object that can be a car, mobile, sensors, or any other appliance, etc., and the word internet refers to the fact that things are connected through the internet [1]. Nowadays, in the field of technology, IoT-based applications such as connected cars, smart healthcare, and environmental monitoring are making a revolution never seen before in the history of mankind. One of those domains in which IoT is making huge progress in agriculture. According to recent research, in 2050, the world population will be touching 9.8 billion which is atleast 25 percent increase from today's number [2]. As a result, food consumption will increase, resulting in a 59 to 98 percent increase in demand for food supply by 2050 [3]. To cope with the needs of a greater food supply and to improve the agricultural yield with less amount of labor and resources, IoT-based agriculture applications can perform a very significant role.

Like other IoT-based systems, the core task of an IoT-based agriculture system is data. IoT-based agriculture systems must have the ability to collect data with precision, store it for further analysis, and act on it based on the gained insight [4]. The IoT-based agriculture system, which is shown in Figure 1, mainly consists of sensors and other smart objects that gather and monitor data such as

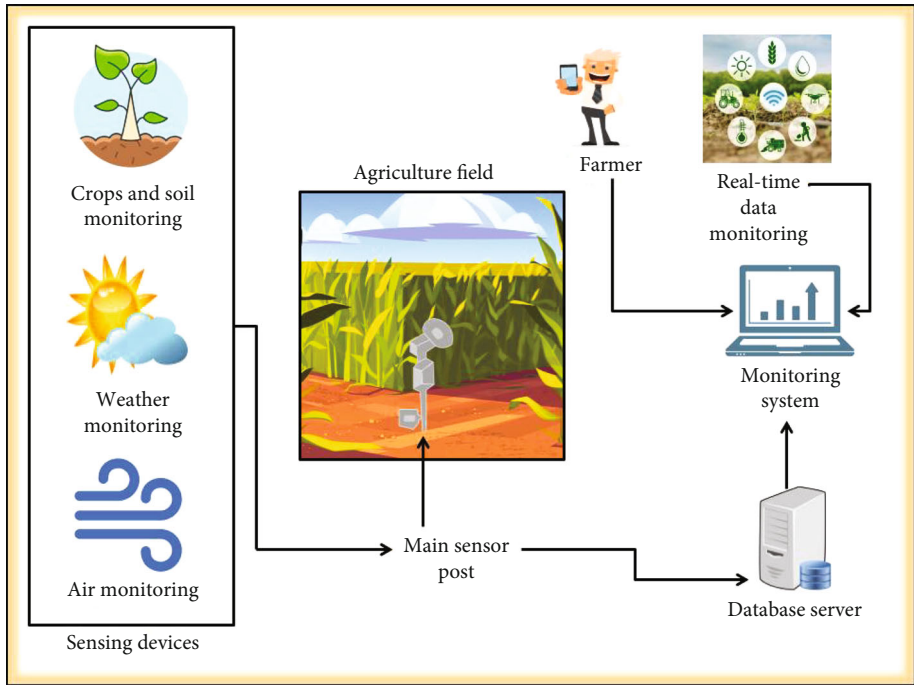


Figure 1: Basic architecture of Internet of Things-based agriculture [2].

humidity, soil moisture, and temperature. These sensors are connected to the main sensor post, called a gateway, through a specific network topology such as Zigbee and RFID. The information is stored on the database server. In the IoT, data processing is supported by decision support systems that monitor and analyze a huge amount of data. Such analysis helps in efficient decision-making for solving the problem. Bad weather forecasts and incorrect irrigation usually result in economic loss for farmers, so the use of a decision support system results in ineffective use of resources [5, 6]. The farmers can visualize the information gathered and can act on the situation accordingly. Not only can it assist the farmer in harvesting efficiently but it can also help save time and cost.

Use of IoT in agriculture leads to precision agriculture, which has many benefits, such as high productivity and reduced environmental effects due to less use of fertilizers and pesticides [6]. In recent times, advances in sensors have had a good impact on agriculture. These sensors measure soil moisture, temperature, humidity, water content, etc. Data collected from these sensors is analyzed, and then decisions are taken on that basis. The collected data from sensors in IoT-based agriculture is usually transferred over the network, which presents a greater security risk. Ensuring a secure and reliable transfer of information is one of the main goals of WSN in agriculture. Lack of secure data transfer will eventually lead to authentication, integrity, and confidentiality being compromised. Due to the fact that agriculture-based IoT applications cover a large land area and due to limitation of WSN, a specific mechanism should be used to ensure data security and privacy [5]. One approach is to use an authentication scheme that ensures that only an authentic/authorized person can access the data that results in integrity, authentication, and nonrepudiation.

The authentication schemes are normally based on public-key cryptosystem algorithms. One of the main applicable types of PKI is identity-based cryptography (IBC), which solves most of the problems possessed by public-key cryptography [7]. The IBC makes use of user identity to create user public key while private keys are generated by a private-key generator (PKG). So, authentication schemes which are based on IBC will be the most favourable need for IoT -based agriculture applications. These schemes are actually based on Rivest-Shamir-Adleman (RSA)/Discrete Logarithm problem. But due to resource conservative nature of sensor nodes, it is considered expensive. RSA algorithm [8] which is based on public-key cryptography requires large storage space due to the 1024 bit key size. Also, due to huge computation, it is not suitable for limited resourced sensors. But with improvements in elliptic curve cryptography (ECC), provides new ways to apply public-key cryptography with better performance [9]. Identity-based signature which rely on ECC only uses 160-bit key size, and its performance in terms of computation cost and communication overhead is better. But it is still not suitable for tiny resource constraint sensors. A better approach is another generalized form of elliptic curve called hyperelliptic curve (HEC) which only requires 80-bit key size while providing the same level of security as provided by RSA, bilinear pairing, and ECC. Based on this discussion, we can say HEC is a better choice for resource constraint sensors.

Based on the abovementioned limitations, we designed a scheme called identity-based authentication well suited for IoT-enabled agriculture. Some of the major features which

denote the contributions of our research work in this paper are mentioned below:

(i) Firstly, we introduce the basic structure for identity-based authentication and afterward construct the scheme suitable for IoT-based agriculture

(ii) An informal security analysis has been performed which demonstrates that the proposed scheme is robust to various security attacks regarding authentication, forward secrecy, and replay attack, respectively

(iii) We also performed formal security testing by simulating the code using Scyther simulation tool, and the results indicate that the proposed scheme is robust

(iv) We also carry out a detailed performance comparison of the proposed scheme with existing schemes in terms of communication overhead and computational cost, which indicates that the proposed scheme is more cost-efficient

2. Preliminaries

2.1. Hyperelliptic Curve. Hyperelliptic curve (HEC) comes under the category of algebraic curves which was proposed by Neal Koeblitz. It is a generalized form of elliptic curve cryptography (ECC) and provides an alternative solution for elliptic curve cryptography [10]. For ECC, the genus is equal to 1, but for, HEC genus is ≥1.

Let f_g be a finite field, and g is the genus of HEC over that field having order g ≥ 2. Hyperelliptic curve of $g \geq 2$ is shown in

$$HEC : x^2 + h(y)x = f(y), \tag{1}$$

where

(i) $h(y)$ is the polynomial, and the degree is $h(y) \leq g$,

(ii) $f(y)$ is the monic polynomial where degree of $f(y) \leq 2g + 1$.

Note: The points on HEC are different as compared to ECC because these points do not form a group. They form an Abelian group which is called the Jacobian Group J_{HEC} [11]. The order of J_{HEC} is mentioned in

$$(y_{t-1})^{2g} \leq J_{HEC}\left(f_g\right) \leq (y_{t+1})^{2g}. \tag{2}$$

2.2. Divisor. Suppose p is a set of points over hyperelliptic curve (HEC), and divisor d is the finite sum of point's p over HEC [12]. This is mentioned in

$$d = \sum_{p \in HEC} \left(m_p p\right). \tag{3}$$

Note: Under addition, the divisors form a group as shown in

$$\sum_{p \in HEC} \left(m_p p\right) + \sum_{p \in HEC} \left(n_p p\right) = \sum_{p \in HEC} \left(m_p + n_p\right) p. \tag{4}$$

2.3. Hyperelliptic Curve Discrete Logarithm Problem. Let us suppose we have a divisor d which is selected from the Jacobian group J_{HEC}.A random private number L is chosen from the finite field.

$$d1 = L.d. \tag{5}$$

The problem of finding L from Equation (5) is called as hyperelliptic curve discrete logarithm problem (HECDLP) [13].

Note: Hyperelliptic curve cryptography security depends upon solving HECDLP.

3. Related Work

In 2009, Du et al. [14] proposed a routing-driven scheme for key management in a heterogeneous sensor network. This scheme is based on the concept that a node only communicates with a small portion of nodes, and the communicating node only needs to establish communicating keys with its neighbors called c-neighbors. Elliptic curve cryptography is used in this scheme to maintain a good level of security by providing resistance against known attacks. The benefit of this scheme is that it reduces the communication overhead in key management. It also reduces storage space and energy consumption, but the major flaw is that H-sensor takes a lot of storage space. In 2011, Boujelben et al. [15] proposed a scheme for key management in heterogeneous sensor networks based on identity-based cryptography (IBC). IBC is a form of public-key cryptography in which a public key is generated from a unique known identifier likewise an email address or IP address or some other sort of identity. In a heterogeneous sensor network, using the concept of IBC a node can establish a secure key with any other nodes while only knowing the public identity of other nodes. This approach uses two types of keys (1) a pair-wise shared key between two communicating nodes and (2) a cluster key which is a shared key between all the nodes present in the cluster. The advantage of this scheme is that it provides good security by offering resilience against eavesdropping, replaying of the message, node capture attack, etc. The drawback of this scheme is that it lacks message identification. Moreover, its performance by means of energy consumption and computational cost is not efficient.

In 2014, Turkanovic et al. [16] designed a scheme for ad hoc wireless sensor network. It is built on the notions of IoT and is claimed lightweight by authors due to use of simple hash and XOR operations. Rather than just involving a gateway, this scheme allows the user to communicate directly with the sensor node for key agreement. It provides good resilience against replay attack and denial of service attack but at the same time lacks user anonymity and resistance against impersonation attack. Moreover, this scheme communication overhead and storage overhead is on the higher

side. In 2016, Mehmood et al. [17] proposed an intercluster-based multiple key distribution scheme for wireless sensor network (WSN). Their proposed scheme focuses on improving the security of the cluster head in a wireless sensor network. For that purpose, the security implementation is done in two phases. Phase 1 involves the authenticity of the cluster head, and phase 2 involves the recovery process of the cluster head when cluster head functioning comes to a halt. The advantage of this scheme is that when a cluster head consumes more energy and its battery life is about to be drained, it shifts its management responsibility to another node and withdraw itself. The drawback of this scheme is that its security is still not enough because it is not resistant to attacks like replay attack, denial of service attack, and many more. Shen et al. [18] proposed a multilayer authentication protocol and a key establishment mechanism for a wireless body area network. The proposed scheme is based on ECC and hash-based media access control (MAC). The advantage of this scheme is that it provides security properties such as authentication, integrity and confidentiality, and resilience against key escrow. The drawback of this scheme is that it is susceptible to several attacks which include replay attack and sensor node attack. Wu et al. [19] pointed out the flaws in scheme [20] and presented a new scheme for the Internet of things- (IoT-) based WSN. This scheme is based on ECC and provides mutual authentication between the user, the sensor, and the gateway. This scheme provides several IoT security properties that come under confidentiality, integrity, authentication, authorization, and freshness. The drawback of this scheme is that its communication cost is higher which make this scheme inefficient for IoT-based applications.

In 2017, Wang et al. [21] found out that [22, 23] are not resistant enough against offline dictionary attack and impersonation attack and lack user anonymity and forward secrecy. The authors of [21] proposed an enhanced scheme that tackle abovementioned shortcomings, and their scheme security is proved using Burrows-Abadi-Needham (BAN) logic and heuristic analysis. Apart from providing resistance against several attacks, their scheme also provides user anonymity and forward security. The drawback of it is that it requires high computational cost and communication overhead. In 2018, Li et al. [24] proposed an ECC-based authentication protocol with privacy preservation for the Internet of Industrial Things (IIOT). Apart from privacy protection and bidirectional authentication, the proposed scheme also provides several security properties which include resistance against replay attack, impersonation attack, etc. This scheme lacks performance efficiency by means of communication overhead. In 2019, Harbi et al. [25] proposed a key management scheme to secure information exchange in Internet of things (IoT). The author was able to point out the flaws related to security in [17] and designed a new scheme based on identity-based encryption. The benefit [25] brings is that it provides data confidentiality and resists several known attacks. The drawback of [25] is that if the attacker gains access to the master key, all the session keys will be compromised. Yuan et al. [26] proposed a novel key management scheme for heterogeneous wireless sensor networks. Their scheme is based on the pairing-free identity-based digital signature algorithm which not only ensures identity authentication but also guarantees the security of the key establishment mechanism. The benefit of this scheme is that it keeps the information about the location of the starting node private. Moreover, this scheme also provides message authentication and provide protection against node capture attacks. The drawback of this scheme is its relatively high memory consumption. The computation and communication cost is relatively high which does not suite resource constraint WSN nodes.

4. Network Model

The proposed scheme network model is shown in Figure 2, which consists of three main components such as agriculture sensors, private key generator (PKG), and data user. The symbols used in the proposed scheme are illustrated in Table 1.

4.1. Agriculture Sensors. The agriculture sensor network consists of different types of sensors that gather and monitor a variety of data related to crops. These sensors are used in multiple ways likewise with drones, on the crop leaves or stems, and sometimes placed inside the soil. The node with a temperature sensor constantly monitors the temperature, while the node with a soil moisture sensor calculates the water level within the soil. Similarly, a node with a rain sensor detects the rainfall if there is the predictability of rainfall, a node with humidity sensors measures the humidity level in the air, and a node with a carbon dioxide sensor detects the level of carbon dioxide because it helps plants in photosynthesis. Apart from that, a node with a light sensor measures light intensity, a node with wind sensors detects the speed and direction of the wind, and a node with a leaf sensor measures the water level present inside the plant. For reliable and timely communication, a communication technology is deployed in the form of 5G or Sigfox which provides the ability of fast data transfer, wide coverage area and low energy consumption [27, 28]. The agricultural sensor nodes are connected to the controller which verifies the authenticity of data user when it receiver the request.

4.2. Private Key Generator. PKG is an arbitrator which core task is to create private and public key for controller and data users. The PKG has its own public and private master keys. Data user or controller provides its unique ID, which is combined with the master private key to create private keys. Afterwards, computing respective actor's private keys, PKG generates public key for controller and data user.

4.3. Data User. The data user is responsible for the monitoring of data gathered by sensors. When a data user requires access to the data gathered by sensors, it approaches the controller. The controller firstly makes sure whether the data user is authorized. Authentication takes place between the data user and the controller for such purpose, and when the data user is found authentic, a secret key is shared between the two parties for exchange of information.

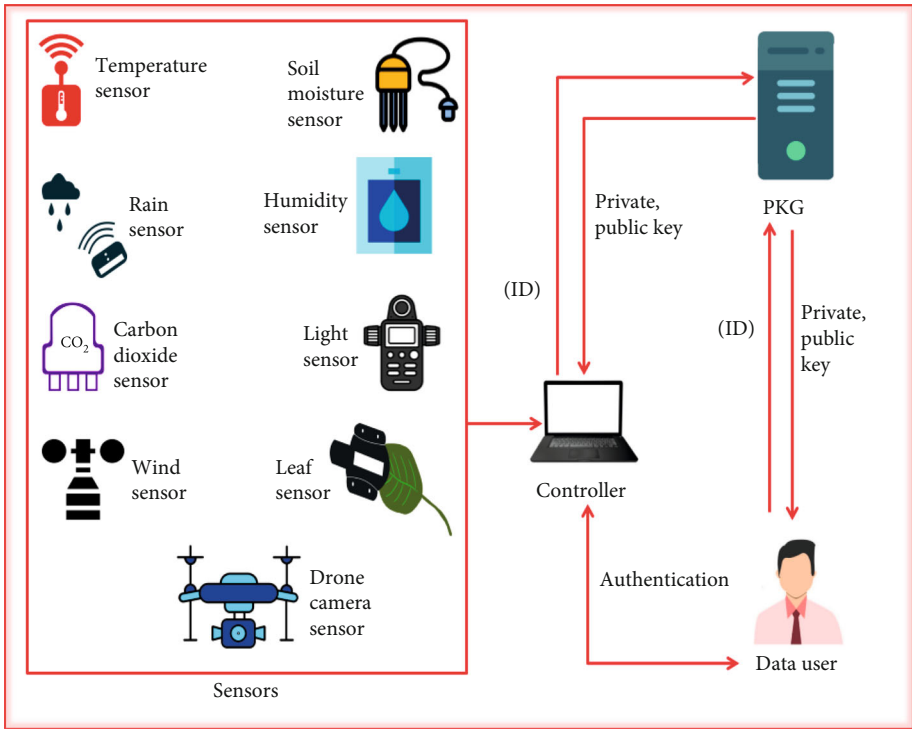


Figure 2: Flow of the proposed scheme.

Table 1: Notations used in the proposed algorithm.

S.no	Notation	Explanation
1	PKG	Private key generator
2	$\hbar_u, \hbar_v$	Hash function
3	$\mathscr{D}$	Divisor of hyperelliptic curve
4	$\varkappa$	Private key of PKG
5	$\mathfrak{S}$	Public key of PKG
6	γ_{di}	Private key of the device
7	φ_{di}	Public key of the device
8	ℓ	Randomly selected private number
9	$\Phi, \mathscr{K}$	Secret keys
10	η	Signature

5. Proposed Identity-Based Authentication Scheme

In this section, we propose the identity-based authentication scheme that contains the following three parts:

(1) Setup: PKG selects a hyperelliptic curve with genus 2 that utilizes 80 bits key size. Further, it selects finite field F^q from the hyperelliptic curve with the range of $q \geq 2^{80}$ and two one way hash functions $(\hbar_u, \hbar_v)$. Then, it compute $\mathfrak{S} = \varkappa.\mathscr{D}$, where $\mathscr{D}$ indicates the divisor of hyperelliptic curve and $\varkappa$ and $\mathfrak{S}$ represent the private and public key of PKG

(2) Registration phase: when a device from agriculture sensor networks requests for public and private key with identity (id_{di}), then PKG can register it by computing $\gamma_{di} = \varkappa.\hbar_u(id_{di})$ as a private key and $\varphi_{di} = \gamma_{di}.\mathscr{D}$ as a public key for id_{di}. At the end of this process, PKG sends $(\gamma_{di}, \varphi_{di})$ to the device of id_{di} using insecure network

(3) Authentication and key management phase: in this phase, we consider two devices, let say DS^1 and DS^2, which are act for the authentication and key management using the following steps:

(i) Suppose DS^1 wants to make a communication with DS^2, then it first computes $\zeta = \ell.\mathscr{D}$, where ℓ is the randomly selected private number from hyperelliptic curve finite field; further, it generates the secrete key $\mathscr{K} = \ell.\varphi_{DS^2}$ and $\Phi = \hbar_v(\mathscr{K})$. At the end, it generates the signature $\eta = \ell/\Phi + \gamma_{DS^1}$ and send $\psi = (\eta, \zeta)$ to DS^2

(ii) After reception of ψ, DS^2, compute $\mathscr{K} = \zeta.\gamma_{DS^2}$ and accept ψ if $\zeta = \eta(\varphi_{DS^1} + \Phi.\mathscr{D})$, where $\Phi = \hbar_v(\mathscr{K})$. Then, it set $\mathscr{K}$ is a secret key

5.1. Correctness. Here, DS^2 can generate secrete key $\mathscr{K} = \zeta.\gamma_{DS^2}$ using the following steps

$$\zeta.\gamma_{DS^2} = \ell.\mathscr{D}.\gamma_{DS^2} = \ell.\gamma_{DS^2}.\mathscr{D} = \ell.\varphi_{DS^2} = \mathscr{K}. \quad (6)$$

Table 2: Comparison of security performance.

Schemes	S1	S2	S3	S4	S5	S6	S7	S8
Du et al. [14]	No	Yes	No	No	No	No	No	Yes
Boujelben et al. [15]	Yes	Yes	No	Yes	No	No	Yes	Yes
Turkanovic et al. [16]	Yes	No	Yes	Yes	No	No	No	No
Mehmood et al. [17]	No	No	No	No	No	No	No	No
Shen et al. [18]	No	Yes	No	Yes	No	No	No	No
Wu et al. [19]	No	Yes	No	Yes	No	Yes	Yes	Yes
Wang et al. [21]	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Li et al. [24]	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes
Harbi et al. [25]	No	No	Yes	Yes	Yes	Yes	Yes	No
Yuan et al. [26]	Yes	Yes	No	No	No	No	Yes	Yes
Proposed scheme	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

S1: Resists replay attack, S2: Resists forward secrecy attack, S3: Resists DoS attack, S4: Resists eavesdropping attack, S5: Resists impersonation attack, S6: Provides device anonymity, S7: Provides mutual authentication, S8: Resists node capture attack.

Table 3: Computational cost comparison with respect to major operations used.

Scheme	Sender	Receiver	Total
Mehmood et al. [17]	4SM + 1P	3SM + 1P	7SM + 2P
Shen et al. [18]	5SM	5SM	10SM
Wu et al. [19]	2SM	2SM	4SM
Wang et al. [21]	2SM	4SM	6SM
Li et al. [24]	2SM	3SM	5SM
Harbi et al. [25]	4SM + 1P	4SM + 1P	8SM + 2P
Yuan et al. [26]	2SM	3SM	5SM
Proposed scheme	2HECDM	3HECDM	5HECDM

And it verifies ψ as if $\zeta = \eta(\varphi_{DS^1} + \Phi.\mathscr{D})$ using the following steps

$$\begin{aligned} &= \eta(\varphi_{DS^1} + \Phi.\mathscr{D}) = \left(\frac{\ell}{\Phi + \gamma_{DS^1}}\right)(\varphi_{DS^1} + \Phi.\mathscr{D}) \\ &= \left(\frac{\ell}{\Phi + \gamma_{DS^1}}\right)(\gamma_{DS^1}.\mathscr{D} + \Phi.\mathscr{D}) \\ &= \left(\frac{\ell}{\Phi + \gamma_{DS^1}}\right)((\gamma_{DS^1} + \Phi))\mathscr{D} = \ell.\mathscr{D} = \zeta \end{aligned} \tag{7}$$

hence proved.

6. Security Analysis

In this section, we performed an informal security analysis of our schemes with existing schemes such as Du et al. [14], Boujelben et al. [15], Turkanovic et al. [16], Mehmood et al. [17], Shen et al. [18], Wu et al. [19], Wang et al. [21], Li et al. [24], Harbi et al. [25], and Yuan et al. [26]. The comparison of security performance of our scheme with different existing schemes is shown in Table 2 which clearly indicates that our scheme outperforms existing authentication schemes by providing essential security properties such as mutual authentication, device anonymity, and forward secrecy. Moreover, it also provides resistance against known attacks such as replay attack, eavesdropping attack, and denial of service attack.

Table 4: Comparison of computational cost in milliseconds.

Scheme	Sender	Receiver	Total
Mehmood et al. [17]	18.78 ms	17.81 ms	36.59 ms
Shen et al. [18]	4.85 ms	4.85 ms	9.7 ms
Wu et al. [19]	1.94 ms	1.94 ms	3.88 ms
Wang et al. [21]	1.94 ms	3.88 ms	5.82 ms
Li et al. [24]	1.94 ms	2.91 ms	4.85 ms
Harbi et al. [25]	18.78 ms	18.78 ms	37.56 ms
Yuan et al. [26]	1.94 ms	2.91 ms	4.85 ms
Proposed scheme	0.96 ms	1.44 ms	2.4 ms

6.1. Mutual Authentication. The scheme we introduced provides mutual authentication between controller and data user on the basis of signature which is generated by controller $\eta = \ell/\Phi + \gamma_{DS^1}$ and at the receiving using $\zeta = \eta(\varphi_{DS^1} + \Phi.\mathscr{D})$ and it passes through verification process. So, in this regard, we can say that our scheme meets the mutual authentication security requirement.

6.2. Device Anonymity. Our designed scheme provides device anonymity during the authentication and key management stages; the identity of the communicating devices is not included in the transmitted message. The intruder must obtain the private key γ_{di} and solve the equation $\gamma_{di} = \varkappa.\mathscr{h}_u(id_{di})$ in order to retrieve the device's identity, which is impossible in this case. So, from the above discussion, we can say that the proposed scheme provides the device anonymity property.

6.3. Replay Attack. In such attacks, the intruder intercepts the message transmitted between the controller and data user and then the intruder launches an attack by replaying that old intercepted message. But our scheme makes it impossible for an intruder to do so by using the fresh secret key at every section, hence ensuring the freshness of key, and it makes our scheme robust against replay attacks.

6.4. Forward Secrecy. Forward secrecy guarantees that if the private key of one of the communicating parties is compromised, it will not affect the secret key established for the communication. In our scheme, if an intruder gains access to the private key γ_{di} of one of the communicating parties, he/she will not be able to generate secrete key $\mathscr{K} = \zeta.\gamma_{\mathrm{di}}$ because that intruder needs to solve the HECDLP which is almost impossible. Thus, our schemes provide forward secrecy.

6.5. Nonrepudiation. The term nonrepudiation refers that a sender cannot deny the information it sent. In our scheme, the sender includes his signature η with the transmitted message ψ and only the legal controller or data user can compute

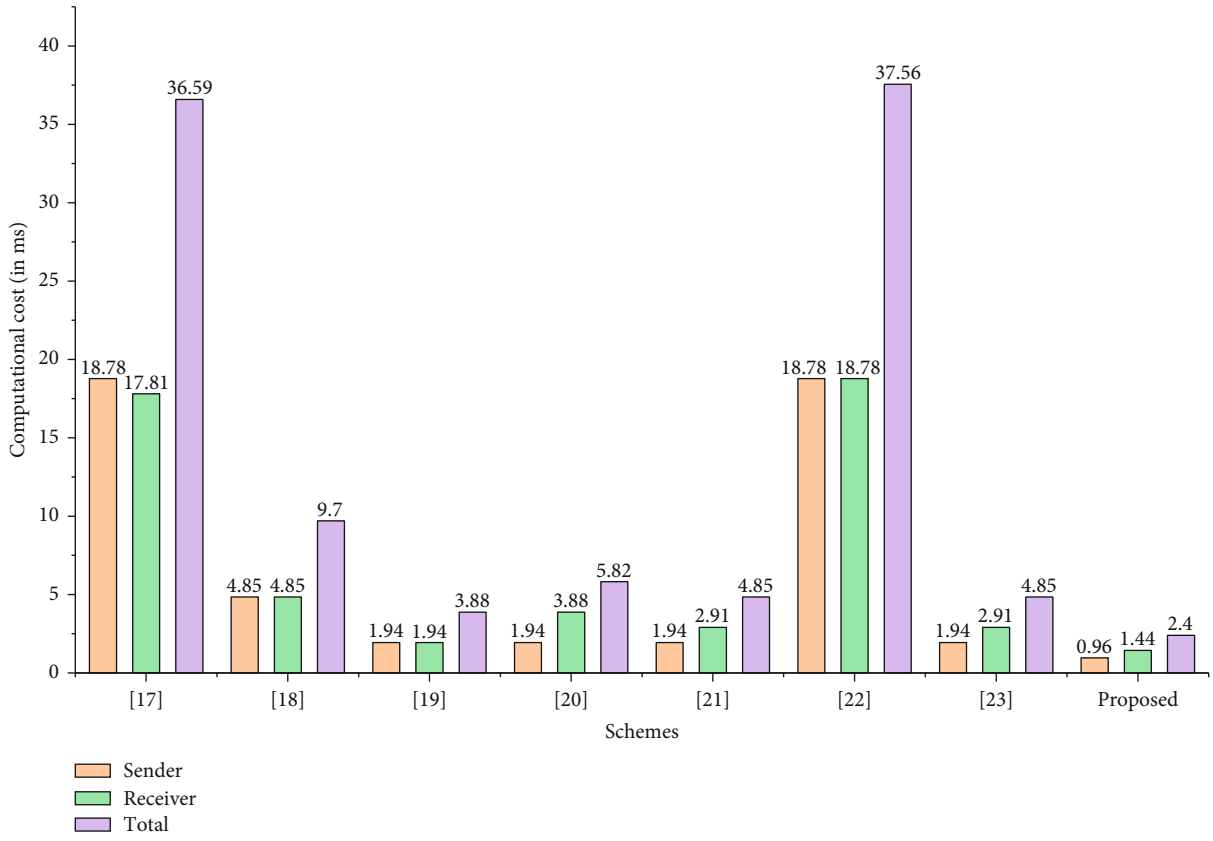


Figure 3: Computational cost comparison in milliseconds.

Table 5: Communication overhead comparison in bits.

Scheme	Total overhead	In bits
Mehmood et al. [17]	3(q)	480
Shen et al. [18]	6(q)	960
Wu et al. [19]	5(q)	800
Wang et al. [21]	4(q)	640
Li et al. [24]	4(q)	640
Harbi et al. [25]	4(q)	640
Yuan et al. [26]	3(q)	480
Proposed scheme	3(n)	240

the secrete key $\mathscr{K}$ and can pass the authentication. Hence, our mechanism provides nonrepudiation.

6.6. Denial of Service Attack. This type of attack occurs by increasing the flow of traffic to the intended server or party until it has fully crashed. Our scheme prevents such attacks by accepting the data received from the authenticated party. When controller receives message ψ from data user, it checks the signature η and accepts ψ if $\zeta = \eta(\varphi_{DS^1} + \Phi.\mathscr{D})$; otherwise, it discards that request.

6.7. Eavesdropping Attack. Whenever there is an exchange of information during transmission in the network, there is a possibility that an intruder might gain access to information secretly. This threatens information confidentiality as well as integrity. Our scheme avoids this attack because information is encrypted using secrete key $\mathscr{K}$, and it is impossible for the intruder to gain access to secret key $\mathscr{K}$ because $\mathscr{K}$ is computed using a random private number ℓ.

6.8. Sybil Attack. In such an attack, an attacker usually guesses the identity of a device from the message that is being transmitted over the network. However, in our scheme, the attacker cannot do so because the message ψ only contains η, ζ, where $\eta = \ell/\Phi + \gamma_{\text{di}}$ and does not include information regarding identity of transmitting device, thus providing stability against Sybil attack.

6.9. Impersonation Attack. In such attack, the attacker impersonates the identity of the another participant in the network. In our scheme, in order to impersonate another node, the intruder will require to forge a signature η and for doing so he/she needs ℓ which is not feasible because of HECDLP.

6.10. Node Capture Attack. This kind of attack involves capturing the sensor node to gain keys that can be further utilized for eavesdropping on the network traffic. Such an intrusion endangers the confidentiality and integrity of the network. Our scheme makes it impossible for an attacker to obtain information about an uncaptured node by using the information of the captured node since each sensor has

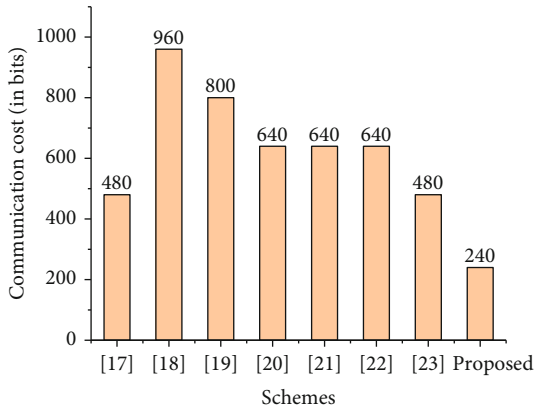


Figure 4: Communication overhead comparison (in bits).

its own unique private key γ_{di}, and a pair of devices communicating have a secret shared key $\mathcal{K}$. Thus, one node capture does not impact the communication between other sensor nodes because of need to compute ℓ which is impossible due to HECDLP.

7. Performance Comparison

In this section, we compare our scheme with existing schemes in terms of computational cost and communication overhead.

7.1. Computational Cost. In this section, we compare the computational cost of our proposed scheme with existing authentication schemes which include Mehmood et al. [17], Shen et al. [18], Wu et al. [19], Wang et al. [21], Li et al. [24], Harbi et al. [25], and Yuan et al. [26]. For that purpose, we have only considered major operations such as scalar multiplication of elliptic curve (SM), pairing operation (P), and hyperelliptic curve divisor multiplication (HECDM) because these operations are assumed to be costly. Table 3 shows the comparison with existing schemes with respect to major operations being used. Our scheme has a lower computational cost because we have not used scalar multiplication of elliptic curve and pairing operations. We have made use of hyperelliptic curve cryptography due to which our scheme saved a lot of computational cost. Moreover, Table 4 and Figure 3 also indicate the computational cost comparison in milliseconds (ms). We did so by keeping in mind the experimental results produce in [29], the observations are made by using these system specifications

(i) Intel Core i74510U CPU

(ii) 2.0 GHz with 8 GB RAM

(iii) Windows 7

(iv) Multiprecision Integer and Rational Arithmetic C Library (MIRACL)

The authors of [29] indicate that scalar multiplication (SM) of elliptic curve takes 0.97 ms, pairing operation (P) takes 14.90 ms, and hyperelliptic curve divisor multiplication (HECDM) takes 0.48 ms [30].

7.1.1. Computational Cost Reduction. To calculate the reduction in computational cost, the formula shown in Equation (8) is used [31, 32].

$$\left(\frac{\textit{Existing scheme} - \textit{Proposed scheme}}{\textit{Existing scheme}}\right) * 100. \quad (8)$$

(i) Computational cost reduction from Mehmood et al. [17] is $((36.59 - 2.4)/36.59) * 100 = 93\%$

(ii) Computational cost reduction from Shen et al. [18] is $((9.7 - 2.4)/9.7) * 100 = 75\%$

(iii) Computational cost reduction from Wu et al. [19] is $((3.88 - 2.4)/3.88) * 100 = 38\%$

(iv) Computational cost reduction from Wang et al. [21] is $((5.82 - 2.4)/5.82) * 100 = 58\%$

(v) Computational cost reduction from Li et al. [24] is $((4.85 - 2.4)/4.85) * 100 = 50\%$

(vi) Computational cost reduction from Harbi et al. [25] is $((37.56 - 2.4)/37.56) * 100 = 93\%$

(vii) Computational cost reduction from Yuan et al. [26] scheme is $((4.85 - 2.4)/4.85) * 100 = 50\%$

7.2. Communication Overhead. In this section, we compare our scheme with existing schemes such as Mehmood et al. [17], Shen et al. [18], Wu et al. [19], Wang et al. [21], Li et al. [24], Harbi et al. [25], and Yuan et al. [26] in term of extra bits that a message is carrying with it. For achieving this, we have assumed that the length of elliptic curve $|q| = 160$ bits, bilinear pairing $|G| = 1024$ bits, hyperelliptic curve $|n| = 80$ bits. Table 5 and Figure 4 clearly indicate that the communication overhead of our scheme is far less than other existing schemes. Moreover, we also calculated the communication overhead reduction our scheme achieved.

7.2.1. Communication Overhead Reduction. To calculate the reduction in communication overhead, Equation (8) is used.

(i) Communication overhead reduction from Mehmood et al. [17] is $((480 - 240)/480) * 100 = 50\%$

(ii) Communication overhead reduction from Shen et al. [18] is $((2720 - 240)/2720) * 100 = 91\%$

(iii) Communication overhead reduction from Wu et al. [19] is $((3040 - 240)/3040) * 100 = 92\%$

(iv) Communication overhead reduction from Wang et al. [21] is $((2240 - 240)/2240) * 100 = 89\%$

(v) Communication overhead reduction from Li et al. [24] is $((2080 - 240)/2080) * 100 = 88\%$

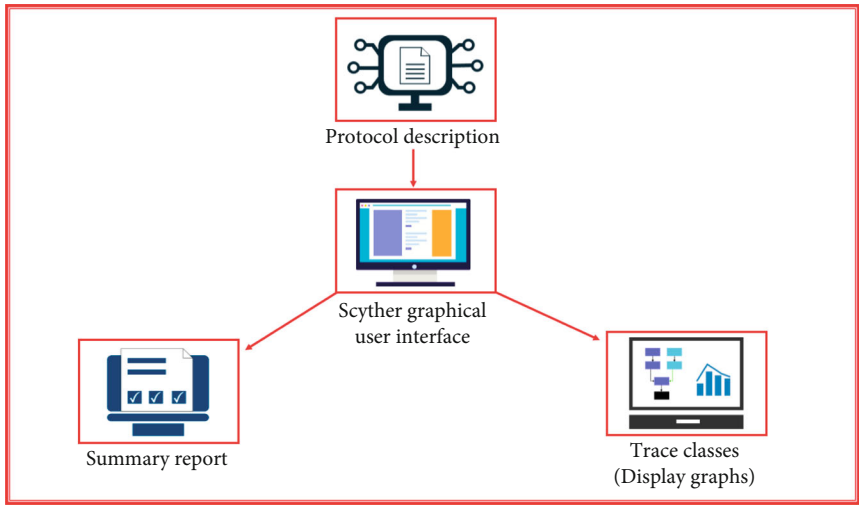


Figure 5: Scyther graphical user interface [33].

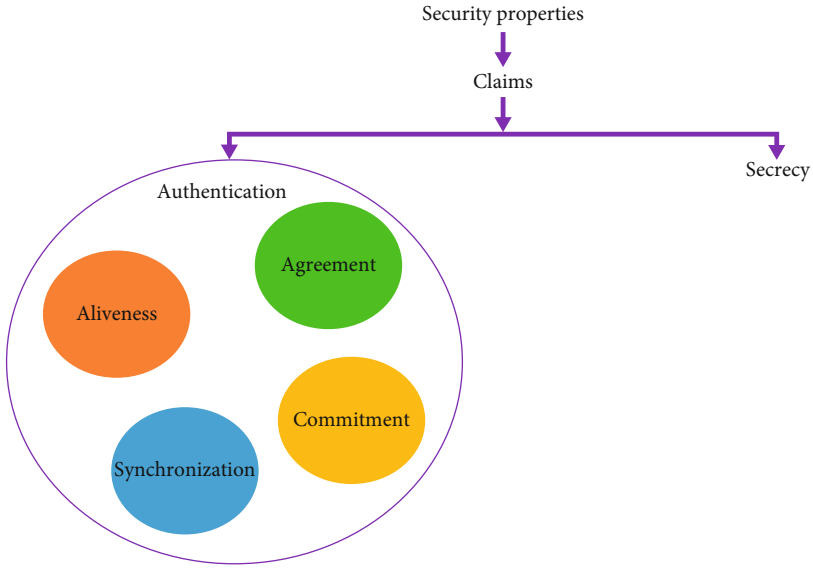


Figure 6: Scyther claims.

(vi) Communication overhead reduction from Harbi et al. [25] is $((4320 - 240)/4320) * 100 = 94\%$

(vii) Communication overhead reduction from Yuan et al. [26] is $((480 - 240)/480) * 100 = 50\%$

8. Conclusion

This paper presents a cost-effective identity-based authentication scheme for the IoT-enabled agriculture. To enhance the efficiency of this identity-based authentication scheme, we have made use of HECC, which gives our scheme the potential to be cost-effective. This scheme ensures security properties such as authentication, forward secrecy, and non-repudiation. The detailed security analysis of our proposed schemes proves that it is resistant against several security attacks such as replay attack and eavesdropping attack. We carried out a detailed performance analysis, and the results indicate that our scheme is more efficient than existing schemes in terms of communication overhead and computational cost. Moreover, we validated the security of our scheme using Scyther, which is a tool for validation of security protocols. The validation results prove that our scheme is secure and is a well-suited choice for IoT-enabled agriculture applications.

Appendix

A. Scyther Tool

To simulate and validate our protocol, we have used Scyther [33] which is a simulation tool designed to perform analysis on security protocols. The reason for choosing this tool is because of its ability to find vulnerabilities in the protocol

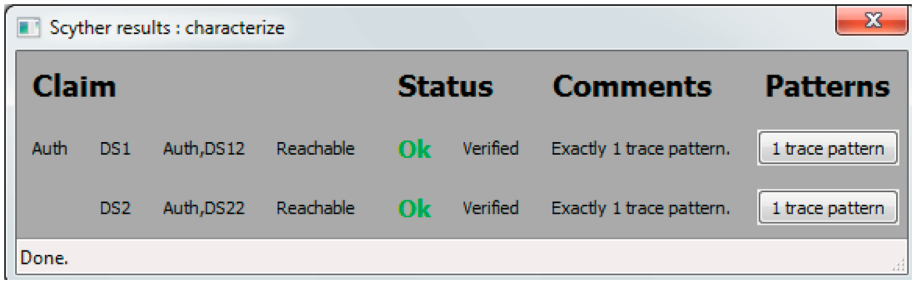


Figure 7: Simulation result of the proposed scheme.

Figure 8: Security validation of the proposed scheme.

and its greater verification speed. We have used Scyther graphical user interface in Figure 5 to simulate and validate our protocol. To analyze the protocol, there are three modes in Scyther: (1) verification of claims, (2) automatic claims, (3) and characterization. Claims are events that are used to specify security properties as shown in Figure 6. These claim events include different forms of authentication and secrecy. We have used verification of claim mode to validate whether the security properties we claimed holds. If a claim does not hold, then the status is labeled as false, and on the other hand, upon the successful claim, the status is labeled as OK. We have used the "Secret" claim to check whether the

information is kept secret from the adversary, and the claim result turned out to be "OK" which indicates a successful claim. Afterward, we have used the "Alive" claim to check whether the intended communicating partner is alive and our claim was successful. Agree claim was used to check on the agreement on the data exchanged between the communicating parties and two agreement claims we used "Weakagree" and "Niagree" both results indicate successful claim. Lastly, we have employed the "Nisynch" claim to check that the messages received by the receiver are not replayed and are not decrypted by the intruder and the result was successful. In case we quickly want to validate our protocol without writing the claims, this is where automatic claim mode work by automatically generating all the claims and making it easy for the user to access the properties of the protocol. While performing analysis on the protocol, the characterization mode allowed us to characterize roles. This provides a finite number of traces, and in case of a problem, we made a modification based on analysis. Also, we employed alternate way to reach a certain event in the case of an attack; there were few different behaviors available and we assessed all kind of possible behaviors that leads to a certain protocol event which in other terms also referred as complete characterization [33–35].

B. Simulation Results

This section includes the simulation results of the proposed scheme which is simulated using the Scyther tool. The simulation results of our protocol indicate that our proposed scheme is safe and vigorous against security attacks, as shown in Figures 7 and 8.

Data Availability

All the data is incorporated in this article.

Conflicts of Interest

The authors declare that they have no conflicts of interest regarding the present study.

References

[1] R. Hassan, F. Qamar, M. K. Hasan, A. H. M. Aman, and A. S. Ahmed, "Internet of Things and its applications: a comprehensive survey," *Symmetry*, vol. 12, no. 10, p. 1674, 2020.

[2] A. P. Antony, K. Leith, C. Jolley, J. Lu, and D. J. Sweeney, "A review of practice and implementation of the internet of things (IoT) for smallholder agriculture," *Sustainability*, vol. 12, no. 9, p. 3750, 2020.

[3] R. Q. Grafton, J. Williams, and Q. Jiang, "Food and water gaps to 2050: preliminary results from the global food and water system (GFWS) platform," *Food Security*, vol. 7, no. 2, pp. 209–220, 2015.

[4] V. S. Rubio and F. R. Mas, "From smart farming towards agriculture 5.0: a review on crop data management," *Agronomy*, vol. 10, no. 2, p. 207, 2020.

[5] P. Mall, R. Amin, A. K. Das, M. T. Leung, and K.-K. R. Choo, "PUF-based authentication and key agreement protocols for IoT, WSNs and smart grids: a comprehensive survey," *IEEE Internet of Things Journal*, 2022.

[6] M. Ayaz, M. A. Uddin, Z. Sharif, A. Mansour, and E. H. M. Aggoune, "Internet-of-Things (IoT)-Based smart agriculture: toward making the fields talk," *IEEE Access*, vol. 7, pp. 129551–129583, 2019.

[7] G. Sharma, S. Bala, and A. K. Verma, "PF-IBS: Pairing-free identity based digital signature algorithm for wireless sensor networks," *Wireless Personal Communications*, vol. 97, no. 1, pp. 1185–1196, 2017.

[8] P. Mall and R. Amin, "EuDaimon: PUF-based robust and lightweight authenticated session key establishment protocol for IoT-enabled smart society," *IEEE Systems Journal*, pp. 1–8, 2021.

[9] C.-M. Chen, S. Liu, S. Ashraf Chaudhry, Y.-C. Chen, and M. Asghar khan, "A lightweight and robust user authentication protocol with user anonymity for IoT-based healthcare," *Computer Modeling in Engineering & Sciences*, vol. 131, no. 1, pp. 307–329, 2022.

[10] V. Sureshkumar, P. Chinnaraj, P. Saravanan, R. Amin, and J. Rodrigues, "Authenticated key agreement protocol for secure communication establishment in vehicle-to-grid environment with FPGA implementation," in *IEEE Transactions on Vehicular Technology*, 2022.

[11] I. Ullah, N. U. Amin, A. Almogren, M. A. Khan, M. I. Uddin, and Q. Hua, "A lightweight and secured certificate-based proxy signcryption (CB-PS) scheme for e-prescription systems," *IEEE Access*, vol. 8, pp. 199197–199212, 2020.

[12] I. Ullah, N. U. Amin, M. Naeem et al., "A novel provable secured signcryption scheme????: a hyper-elliptic curve-based approach," *Mathematics*, vol. 7, no. 8, 2019.

[13] Z. Ullah, A. Zeb, I. Ullah et al., "Certificateless proxy re-encryption scheme (CPRES) based on hyper elliptic curve for access control in content-centric network (CCN)," *Mobile Information Systems*, vol. 2020, Article ID 4138516, 13 pages, 2020.

[14] X. Du, M. Guizani, Y. Xiao, and H. H. Chen, "Transactions papers A routing-driven elliptic curve cryptography based key management scheme for heterogeneous sensor networks," *IEEE Transactions on Wireless Communications*, vol. 8, no. 3, pp. 1223–1229, 2009.

[15] M. Boujelben, H. Youssef, R. Mzid, and M. Abid, "IKM – an identity based key management scheme for heterogeneous sensor networks," *Journal of Communications*, vol. 6, no. 2, pp. 185–197, 2011.

[16] M. Turkanovic, B. Brumen, and M. Holbl, "A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the internet of things notion," *Ad Hoc Networks*, vol. 20, pp. 96–112, 2014.

[17] A. Mehmood, M. M. Umar, and H. Song, "ICMDS: secure inter-cluster multiple-key distribution scheme for wireless sensor networks," *Ad Hoc Networks*, vol. 55, pp. 97–106, 2017.

[18] J. Shen, S. Chang, J. Shen, Q. Liu, and X. Sun, "A lightweight multi-layer authentication protocol for wireless body area networks," *Future Generation Computer Systems*, vol. 78, pp. 956–963, 2018.

[19] F. Wu, L. Xu, S. Kumari, and X. Li, "A privacy-preserving and provable user authentication scheme for wireless sensor networks based on internet of things security," *Journal of Ambient Intelligence and Humanized Computing*, vol. 8, no. 1, pp. 101–116, 2017.

[20] W.-B. Hsieh and J.-S. Leu, "A robust user authentication scheme using dynamic identity in wireless sensor networks," *Wireless Personal Communications*, vol. 77, no. 2, pp. 979–989, 2014.

[21] C. Wang, G. Xu, and J. Sun, "An enhanced three-factor user authentication scheme using elliptic curve cryptosystem for wireless sensor networks," *Sensors*, vol. 17, no. 12, p. 2946, 2017.

[22] J. Jung, J. Moon, D. Lee, and D. Won, "Efficient and security enhanced anonymous authentication with key agreement scheme in wireless sensor networks," *Sensors*, vol. 17, no. 3, p. 644, 2017.

[23] Y. Park and Y. Park, "Three-factor user authentication and key agreement using elliptic curve cryptosystem in wireless sensor networks," *Sensors*, vol. 16, no. 12, p. 2123, 2016.

[24] X. Li, J. Niu, M. Z. A. Bhuiyan, F. Wu, M. Karuppiah, and S. Kumari, "A robust ECC-based provable secure authentication protocol with privacy preserving for industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3599–3609, 2018.

[25] Y. Harbi, Z. Aliouat, A. Refoufi, S. Harous, and A. Bentaleb, "Enhanced authentication and key management scheme for securing data transmission in the internet of things," *Ad Hoc Networks*, vol. 94, article 101948, 2019.

[26] E. Yuan, L. Wang, S. Cheng, N. Ao, and Q. Guo, "A key management scheme based on pairing free identity based digital signature algorithm for heterogeneous wireless sensor networks," *Sensors*, vol. 20, no. 6, p. 1543, 2020.

[27] A. Lavric, A. I. Petrariu, and V. Popa, "Long range Sigfox communication protocol scalability analysis under large-scale, high-density conditions," *IEEE Access*, vol. 7, pp. 35816–35825, 2019.

[28] Y. Tang, S. Dananjayan, C. Hou, Q. Guo, S. Luo, and Y. He, "A survey on the 5G network and its impact on agriculture: challenges and opportunities," *Computers and Electronics in Agriculture*, vol. 180, article 105895, 2021.

[29] C.-T. Li, C.-C. Lee, C.-Y. Weng, and C.-M. Chen, "Towards secure authenticating of cache in the reader for RFID-based IoT systems," *Peer-to-Peer Networking and Applications*, vol. 11, no. 1, pp. 198–208, 2018.

[30] M. A. Khan, H. Shah, S. U. Rehman et al., "Securing internet of drones with identity-based proxy signcryption," *IEEE Access*, vol. 9, pp. 89133–89142, 2021.

[31] C.-M. Chen, B. Xiang, K.-H. Wang, K.-H. Yeh, and T.-Y. Wu, "A robust mutual authentication with a key agreement scheme for session initiation protocol," *Applied Sciences*, vol. 8, no. 10, p. 1789, 2018.

[32] I. Ullah, A. Alomari, N. U. Amin, M. A. Khan, and H. Khattak, "An energy efficient and formally secured certificate based signcryption for wireless body area networks with the internet of things," *Electronics*, vol. 8, no. 10, p. 1171, 2019.

[33] C. J. F. Cremers, *Scyther-Semantics and Verification of Security Protocols, [Ph. D. thesis]*, Eindhoven University of Technology, Netherlands, 2006.

[34] H. Yang, V. Oleshchuk, and A. Prinz, "Verifying group authentication protocols by scyther," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, vol. 7, no. 2, pp. 3–19, 2016.

[35] S. A. H. Seno, M. Nikooghadam, and R. Budiarto, "An efficient lightweight authentication and key agreement protocol for patient privacy," *Computers, Materials & Continua*, vol. 69, no. 3, pp. 3495–3512, 2021.

Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 7901587, 13 pages
https://doi.org/10.1155/2022/7901587

Research Article

Modern Energy Optimization Approach for Efficient Data Communication in IoT-Based Wireless Sensor Networks

L. Sathish Kumar,[1] Sultan Ahmad,[2] Sidheswar Routray,[3] A. V. Prabu,[4] Abdullah Alharbi,[5] Bader Alouffi,[6] and S. Rajasoundaran[1]

[1]*School of Computing Science and Engineering, VIT Bhopal University, Madhya Pradesh, India*
[2]*Department of Computer Science, College of Computer Engineering and Sciences, Prince Sattam Bin Abdulaziz University, Al-Kharj 11942, Saudi Arabia*
[3]*Department of Computer Science and Engineering, School of Engineering, Indrashil University, Rajpur, Mehsana, Gujarat, India*
[4]*Department of Electronics and Communication Engineering, Koneru Lakshmaiah Education Foundation, Guntur, India*
[5]*Department of Information Technology, College of Computers and Information Technology, Taif University, P. O. Box 11099, Taif 21944, Saudi Arabia*
[6]*Department of Computer Science, College of Computers and Information Technology, Taif University, P. O. Box 11099, Taif 21944, Saudi Arabia*

Correspondence should be addressed to Sultan Ahmad; s.alisher@psau.edu.sa

Received 13 February 2022; Revised 2 March 2022; Accepted 5 March 2022; Published 14 April 2022

Academic Editor: Shafiq Ahmad

Many researchers are drawn to mobile wireless sensor networks (WSN) and the Internet of Things (IoT) because of the significant challenges of power consumption and network connectivity. A technique that takes into consideration the characteristics such as network probability, the identified region of individual nodes, and the radius of the whole identified region is presented in this article. Free-space propagation is carried out in the region of interest. This approach assures network connection, long-term communication sustainability, and maximum energy efficiency. It was discovered that a mathematical network model can be built using the probability theory. It has been possible to examine and evaluate the changes in sensor nodes as a function of distance from the detection region using this approach. As a result, a correlation has been established between a network's communication radius and the identified region. Additionally, a novel method has been developed to reduce energy consumption and sustain connectivity through boosting the connectivity feature. Notably, IoT-based WSN architectures require more energy optimization than any other network, because they have resource-limited nodes. Also, a simulation plot of the proposed approach's mathematical network scheme is shown to show if it works. The proposed method consumes much less energy averagely 40% compared to the existing methods, which are LEACH, ZTR, and DSR when the radius is 100.

1. Introduction

Nowadays, wireless device and IoT device usage is increasing. For that reason, low power consumption and minimum cost systems are integrated with mobile applications. This integration happens with the support of low power and minimum cost sensor nodes. This system is defined as an IoT-based wireless sensor network because it self-organizes itself. It is common to practice to utilize these networks to monitor the environment, weather conditions, combat surveillance, structural health monitoring, and clinical factors. It all comes from the sensor nodes, which then send it to the IoT network's control stations.

The majority of the sensor network is powered by batteries, which are included in the package. Undersea communication, natural catastrophes, implantable nodes, and a variety of other critical circumstances are all possible. Battery life and energy consumption must be minimized while the appropriate

level of network connectivity is maintained for the network to function properly [1]. As a result, a WSN's ability to sustain its energy level is directly correlated to its ability to use less power [2, 3]. The battery life is also extended as a result of the reduced power usage, allowing the network to operate more effectively. At the same time, IoT-based networks use various types of sensor nodes and gateway nodes.

In addition to determining network topologies and power allocations, network connectivity is a critical consideration in network planning and design. Several scholars have worked to improve network connection and minimize energy usage by proposing better solutions, both theoretically and practically. Percolation is a branch of graph theory and a probability that is used to investigate various network configurations [4]. There is a lot of scientific and social research that is used as a starting point for looking at different graphs based on how quickly things move.

As a follow-up study to previous research, this paper investigates the optimal level of power for a given node and its coverage to ensure network connectivity. The most energy-intensive function for an IoT sensor node is data transmission. As a result, the transmit power of a sensor node directly affects its coverage area and the other way around. The node coverage and network connection will be harmed if the transmit power is reduced to extend battery life. As a last resort, more closely spaced nodes may be necessary. The location and distance between nodes in mobile sensor networks are stochastic, necessitating probabilistic modeling to estimate power coverage enhancement. The IoT-based MWSN's main difficulty is to sustaining connectivity while upholding energy levels, by way of the fact of interaction changes at every point in the network. Data transfer is a critical part of this project, as it must be done quickly and efficiently while also ensuring that the network's connectivity is maintained. This study presents an IoT WSN model that seeks to achieve this goal. The suggested model is tested using mathematical and simulation-based analyses.

In the first half of this article, the fundamentals of IoT, wireless sensor networks, their main difficulties, and the necessity for specific parameters to make the network perform more efficiently are discussed. Some recent wireless sensor network research is presented in Section 2. It is shown in Section 3 how to use mathematical models to model networks, which takes into account factors such as network probability and radius. Section 4 depicts the system's network architecture and a proposed energy-efficient connection method. In Section 5, simulation results are shown on graphs, and the work is concluded with a section on the validation of the mathematical model. Power consumption and network connectivity are big challenges in mobility and IoT devices. A technique that takes into consideration characteristics such as network probability, the identified region of individual nodes, and the radius of the whole identified region is presented in this article. This approach assures network connection, long-term communication sustainability, and maximum energy efficiency. Also, this method consumes much less energy averagely 40% compared to the existing methods, which are LEACH, ZTR, and DSR when the radius is 100.

2. Related Work

Research in the domain of wireless sensor networks uses a variety of methods to examine various variables and circumstances. In this part, we will take a look at some connected pieces of literature. Ad hoc networks, a common method of building modular sensor networks, have been the subject of current studies into network coverage and routing algorithms. Naghibi and Barati [5] propose a method for geographically dividing a network into smaller cells.

Single-hop and multihop cells can be found in each cell. There is a new energy-efficient geographic routing protocol (EGPRM) that utilizes two mobile sinks for data collection from sensor nodes. Conventional approaches are compared to EGPRM, as well. It is proposed that wireless sensor nodes use RL Sleep, a temperature-adaptive intelligent sleep scheduling approach. Reinforcement learning implies that the nodes examine the surroundings and respond accordingly, for example, by transmitting, listening, or sleeping, depending on the scenario. Improved network connections may also be shown in the simulation findings [6].

According to [7], an efficient distributed MAC optimization strategy can cut energy consumption by 88%, node latency by 84%, and connectivity overhead by 80%. In addition, the method is associated with those already in use. Many different types of data centers examine the performance and power management of diverse clusters. An autonomous power management system has been proposed by Bithika et al. to increase the system's efficiency as well as volume in terms of presentation and cost [8]. HF for single, multicore, and parallel architectures focuses on power-aware scheduling algorithm challenges [9].

An EOSR (Energy Optimization Secure Routing Protocol) has been created to protect WSNs against rogue nodes. When compared to previous approaches, simulation findings demonstrate that EOSR is superior [10]. The current routing protocol for WSNs is compared in this paper (static and mobile). When conducting the investigation, the survey takes into account factors such as energy efficiency strategies, network life span, and network topology. Also, certain restricted routing systems are simulated and compared [11]. Based on current traffic circumstances, this study provides an energy-efficient ADMC-MAC protocol. The first method prioritizes the cluster head with the most energy, while the second is dependent on the current traffic situation and the node's duty cycle. This enhances the system's overall performance and efficiency. It has also been shown that ADMC is more energy-efficient than the S-MAC, M-Mac, and ADMC-Mac [12].

Nodes, communication ranges, and connectedness are all studied in [13] using graph theory and statistical methods. In addition to the simulation findings, the authors of this work discussed the underlying mathematics. When assessing connectivity and coverage [14], it is important to evaluate the distribution of nodes in a region. In their findings, they concluded that a high node density is the best way to ensure that all nodes are connected. Log-normal shadowing was used to study a wireless sensor network transmission model by Agrawal and Patwari. A

long-standing issue with the network connection between nodes was ultimately resolved by the authors [15]. For wireless sensor networks, Chai et al. developed a power-efficient method [16]. The researchers have come up with a way to keep sensors safe that is 60% more effective than other methods.

In [17], Ashutosh and all of us talked about the numerous types of data transmission routing protocols that exist. They illustrate and compare several wireless sensor network routing mechanisms. The authors of this research [18] discussed how to follow a computer network's fastest and most optimal path while being risk and energy-sensitive. As an alternative to the existing SLA provisioning models, they came up with a risk energy-aware SLA provisioning model (RSEP). TORA, DSR, DSDV, OLSR, and AODV [19, 20] are also compared in a comparative review.

Haque and Baroudi devised a dynamic routing protocol for network longevity in the same way as authors are suggested an energy-efficient protected circle directing protocol for load complementary and enhancing network lifespan [21]. A method for improving WSN connection is presented by Renato et al. [22]. In addition, Kim and Kim [23] have provided an IEEE 802.15.4 clustering technique that is effective for the frequency series. Most of the works provided more energy consumption.

A lot of work has been done in the definition of coverage region, connection, power efficiency, data communication, and clustering systems, as well as security procedures and MAC-based structure with various elements as can be seen in Section 3. All of these limitations must be implemented for a long-term wireless mobile sensor network. As a result, this research proposes a novel probabilistic method for a mobile network together with a mathematical model against energy wastages. The research demonstrates how mobile sensor nodes' energy consumption may be optimized while their network connection is increased. Section 5 demonstrates simulated charts.

3. Mathematical Modeling

An IoT WSN is made up of a collection of "Nd" sensor nodes, each with a unique serial number indicated by X1, 1, 2, …, and Nd [24, 25]. Based on the graph theory, the distance between the nodes "a" and "b" is Dab. The node's communication range is designated by the letter "r." The nodes "a" and "b" form a communication channel if Dab $> r$. There are "M" different paths that can be taken in wireless sensor networks, ranging from zero to a multiple of $\mathrm{Nd}(\mathrm{Nd}-1)/2$. For the network to be considered full, M must equal $\mathrm{Nd}(\mathrm{Nd}-1)/2$.

A large number of sensor nodes are often installed in a well-defined region by a top node density in static WSNs used to monitor a large area. Poisson's distribution may be seen in the node distribution. Compared to a static WSN, a node in an IoT mobile WSN (MWSN) can connect with a lower number of other nodes at any given moment. In addition, the surrounding nodes often form and break connections. As a result, the network becomes less reliable and uses more energy. A network model and energy-saving strategies used in a static wireless sensor network may not deliver the necessary service level; thus, this article explains the network model used in a mobile WSN (MWSN). "A" is the detection region employed in this paper's network model, where $A = r2$ and the node's connectivity probability $\mathrm{Pq} = r2/A = 0.2$. This factor represents the ratio of the node's transmission area to its identified region. Figure 1 depicts the general layout of the monitored region.

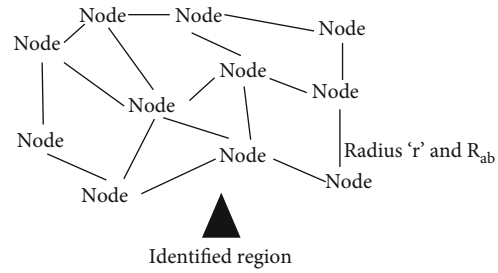


Figure 1: Architecture of IoT WSN-focused region.

3.1. Probability Theory for Connectivity. The nodes in the monitoring region are dispersed in a fashion that follows a binomial distribution, as was demonstrated in a previous study. Because the nodes in this network move about, the connectedness of the system follows a binomial distribution, as shown in this study, which is based on the probability theory (CC, Pr). In M trials, only "CC" occurrences are successful in a binomial event like [M, CC]. To link to all M networks, a node in a network will do just that: connect to as many as it can. CC is the number of connections formed, or how many nodes are active and within this node's communication range. This is the output of the binomial event. CC is one of the M total nodes with an active connection.

The greater the network connectivity, the higher the value of CC. The "Radius" represents the radius of the node coverage. When "Radius" is less, the number of nodes within the communication range is also smaller. As a general rule, the binomial probability theory may be applied to both small and large datasets. Furthermore, because the nodes in the targeted region are dispersed, the binomial distribution is assumed to be invalid because it cannot be applied to a continuously distributed population. There are more than 20 nodes, and the transmission probability is below 0.3; hence, the wireless sensor network follows a binomial distribution. The predicted value of a binomial distribution may be defined as $A[k] = MNr$ where $\mathrm{Pq} = \pi r2/A$, so $A[k] = N\pi r2/A$.

The sensor's node connectivity "CC" is based on the binomial theory, and as a result, the network connectivity probability is

$$P(x = CC) = \sum_{x=0}^{n} \binom{n}{x} \left\lfloor \left(\frac{\pi r^2}{s}\right) \left(1 - \frac{\pi r^2}{s}\right)^{n-x} \right\rfloor, \quad (1)$$

where P is the probability and CC is the connectivity component.

For a given value of "CC," the relationship between "r" and its nearby nodes may be found in Equation (1) [26].

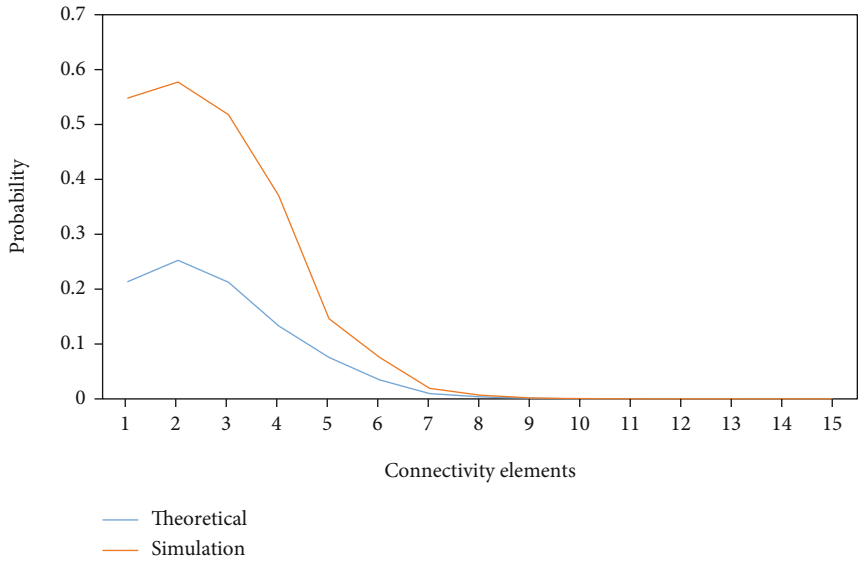


Figure 2: Radius: 20.

The portability of a wireless node or the nearby nodes affects the value of "*n*." As a result, a greater transmit power is required to achieve the specified connection factor value. So that more power can be sent, this raises the node's energy consumption. It is possible to reduce overall energy usage by increasing the nodes' transmit power in addition to increasing network connection probability. Nodes around it can run at a reduced energy level, thereby allowing them to share in some of the power. This means that, unless a pair of nodes requires simultaneous bidirectional transmission, all nodes do not have to function at the same communication power or with the same coverage region. Section 4.1 goes into further detail about the suggested algorithm for achieving this network energy optimization.

In terms of connection probabilities, we have observed that "Radius" has an influence. As a result, in order to maximize the network's connectedness, we compute the variation of "Radius" in relation to the probability of connection. The percentage of alteration of Pq in relation to Radius may be calculated by taking the partial derivative of Equation (1) with "Radius." Using partial derivatives and equating the equations to zero, it is possible to discover the optimal values. In order to arrive at an optimal value, partial derivation of Equation (1) is critical.

4. Architecture of Network

Sensors, a microcontroller, and scheme software for data computation make up the fundamental paradigm of portable sensor networks [27]. There are three types of nodes in the model of the simple MWSN depicted in Figure 2: organization nodes, sensor nodes, and receiver-node components. These nodes have a transceiver to help with data and control signal transmission. Sensor nodes gather data, which is subsequently sent to a central processing node for further processing. Actuators, motion support, positioning, and power regeneration are all controlled by this system. [27]. Nodes in MWSN are distributed around the monitoring region of space in a random manner. Data is collected by the sensor nodes and transferred to other nodes through one or more hops to the sink. The data is sent to the coordination node over a wide area network from the sink node. In the end, the data is processed and delivered to the end-user through a remote connection.

In an IoT mobile wireless sensor network, it is extremely difficult to uphold connectivity whereas the communication systems are still operational (MWSN). It is difficult to sustain a specific level of power in MWSN since the point of interaction changes constantly, and a fast-moving network demands a lot of energy. Maintaining connection while maximizing energy efficiency requires monitoring the node's coverage area and transmit power. With these two factors, we can retain connection while optimizing the energy level of the surrounding nodes.

The term "completely connected wireless network" refers to a network where all nodes may readily communicate and exchange data over a wireless setup that uses either a single-hop or a multihop configuration. For MWSN, this study provides an energy-efficient network connecting approach that achieves excellent node coverage while conserving energy to the minimum necessary level. It has also been looked into and studied to find the best energy solutions in a probability model.

4.1. Proposed Modern Optimization Algorithm. The radius of communication (Radius) and the energy stages of nearby nodes are two elements that have been shown to have a significant impact on mobile wireless sensor network connection in Section 4.1. When the network's connectedness rises to a value of "CC," the change in communication radius may be calculated using Equations (1) and (2) [26]. MWSN's redundancy rises when nodes occur outside of the set range or limit of nodes, putting exceptional stress on the communication network [22, 28]. As a result, in addition to

optimizing the energy consumption of individual nodes, the network as a whole is also given consideration. One of the most critical aspects of a mobile WSN is the amount of energy used by the sensor devices, which are powered by batteries.

The sensor will die if the battery energy falls below a certain onset, defeating the purpose of installing the network. Additionally, this work proposes a method that ensures connection while simultaneously reducing energy use. The network's communication radius may be determined using Equation if the number of nodes "*N*" and the identified region "*A*" are known (2). It follows the binomial distribution *B* (CC, Pq) where Pq = *A*/*A* and Pq is the transmission probability of the wireless sensor network. As more sensors are added to a certain region, the likelihood of network connectivity will rise to "CC." In addition, as the coverage area expands, the number of nearby nodes becomes more readily available, increasing the connection factor. As a result, the huge transmit power Ptr is supported to sustain connectivity by these surrounding nodes, which share in the energy.

The PNC method is designed for sensor nodes that often swap their points of contact in a mobile wireless sensor network. Ei is the name given to the group of nodes that surround a given node I. Due to the nature of sensor nodes being movable, they are linked in a random form [29, 30]. An area's hub is the final node to receive the data, which is subsequently passed on to the other nodes in the area [31, 32]. Each head node in a specific region transmits data to the base station, where it is further processed. When a cycle is complete, the head node switches to a new position to better utilize the available energy. This occurs when data is sent from a node to the cluster head.

The quantity of sensors *N* should be set to X1, 2, *N*. "*A*" encompasses the whole target region. An identifies the portion of the map that is being focused on outside of the overall area. A node's communications range is denoted by the letter "*r*," while its connectivity is denoted by the number CC: step 1: initialize and compute the values of all parameters. Values for "*N*" and "*A*" have been established. There is a fixed value for the numbers "*N*" and "*A*," which are 50 and 50 km^2, respectively. As a result of this phase, the energy of adjacent nodes can be used to sustain connectivity if necessary. Increasing the communication radius in step 3 expands the coverage area for nodes in the vicinity. Step 4 justifies the requirement that the network will have the maximum number of nodes linked if the coverage area of nearby nodes increases. If there are a lot of linked nodes, then there is a high possibility of a big net transmitted power that is utilized to maintain connection by minimizing energy consumption. When a node's energy level is low, the nodes around it donate to the other node, ensuring network communication.

5. Results and Discussions

5.1. Implementation Details. Table 1 lists the parameters needed for a simulation-based analysis of performance. There is a maximum of 50 nodes (*N*) in area "*A*," and the communication radius ("Radius") ranges from 10 meters to 60 meters. At a speed of 25 meters per second and a total area of 50 kilometers squared, this equals 90 kilometers per hour. Due to the difficulties in deploying nodes over a wide region due to the high cost and complexity [33, 34], a solution for a specific area was needed. In addition, this study

Table 1: Parameters of simulation for mobile communications.

S. No.	Factors	Values
1	MR (monitoring area)	50 km sq.
2	*N* (no. of nodes)	50
3	Radius (radius of communication)	10 meters to 80 meters
4	Speed (mobility)	30 m/sec

Table 2: Theoretical values of probability and connectivity components: constant radius.

CC	Theoretical: probability *X* (Prob)			
	Radius = 20	Radius = 30	Radius = 40	Radius = 50
1	0.2183	0.0213	0.000376	0.000000813
2	0.2581	0.0628	0.00245	0.00000747
3	0.2173	0.2031	0.00623	0.00005
4	0.1358	0.2612	0.0231	0.000181
5	0.0772	0.2154	0.041	0.000732
6	0.0356	0.2732	0.0621	0.002
7	0.00987	0.2315	0.0921	0.00532
8	0.00386	0.0943	0.2136	0.0205
9	0.000856	0.0643	0.2297	0.0204
10	0.000214	0.0482	0.2318	0.0412
11	0.000042	0.024	0.2205	0.0607
12	0.00000803	0.00732	0.0999	0.08
13	0.00000213	0.00371	0.0855	0.0984
14	0.000000201	0.00204	0.0644	0.2121
15	0.0000000301	0.000423	0.0426	0.209

Table 3: Simulation values of probability and connectivity components: constant radius.

CC	Simulation: probability *X* (Prob)			
	Radius = 20	Radius = 30	Radius = 40	Radius = 50
1	0.3421	0.0211	0.000576	0.000000523
2	0.3321	0.0632	0.00465	0.0000743
3	0.3123	0.2134	0.00513	0.0007
4	0.2428	0.2435	0.026	0.000954
5	0.0721	0.2854	0.048	0.00265
6	0.042	0.2743	0.0632	0.00092
7	0.00969	0.2354	0.0954	0.00375
8	0.00301	0.156	0.2143	0.02
9	0.000848	0.062	0.2432	0.0275
10	0.000248	0.0409	0.3544	0.0436
11	0.0000423	0.031	0.2543	0.0684
12	0.00000809	0.00754	0.0996	0.072
13	0.00000343	0.00386	0.0843	0.0963
14	0.000000213	0.00206	0.0643	0.2453
15	0.0000000398	0.000453	0.0454	0.275

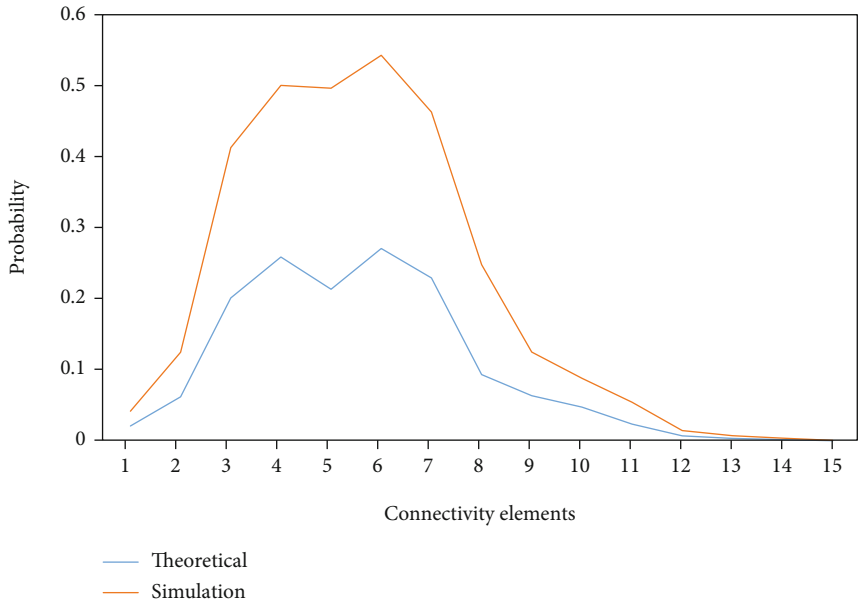


Figure 3: Radius: 30.

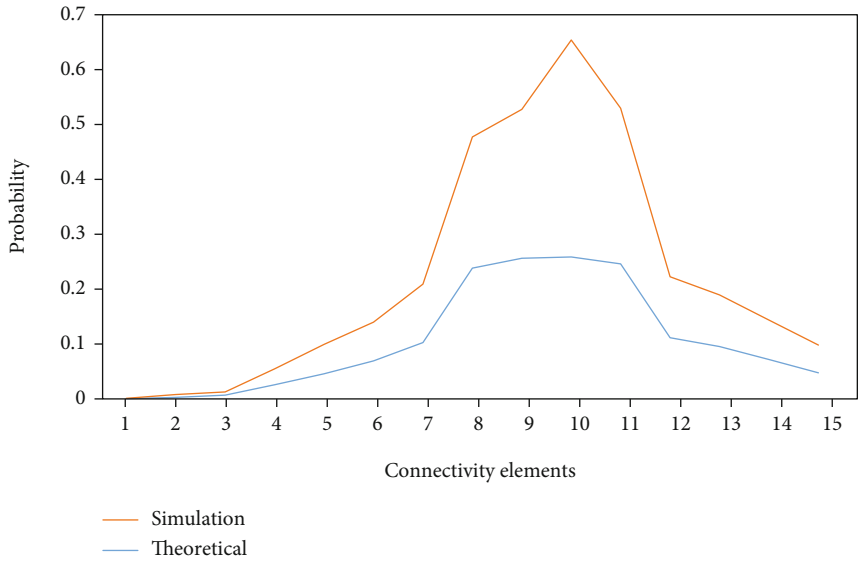


Figure 4: Radius: 40.

also includes simulation work along with the suggested technique in order to maximize energy usage while retaining connection. By distributing the energy of neighboring nodes, the procedure ensures the network's connection and reduces energy usage. In the suggested method, the influence of transmitted power is also illustrated.

Mathematical analysis was used to calculate network probability in the preceding section. The application of equations aids in the identification of the link between the communication radius and the likelihood of network connectivity [35, 36]. To demonstrate the validity of this, we built a scenario using the parameters listed above and ran it through a simulation in the MATLAB tool. The diagrams demonstrate the placement of nodes in the desired location for additional dispensation.

Figure 1 depicts the sensor nodes' elementary placement in the targeted region. 0.5 m is equal to one division in the 60 km sq. targeted region in the following graphs [37]. Two different situations are used in the simulation performance. When the communication radius is fixed in the first condition, the link between the connectivity factor and network probability may be seen [38]. When the connection factor is fixed, the fluctuation in communication radius is observed with respect to the network probability in other conditions [39, 40]. Section 5.2 includes graphs to illustrate each of the two scenarios.

5.2. Results and Comparison. Parameter numerical values are included in Tables 2 and 3, which show the findings of both theoretical and simulation studies. As seen in Figure 3, the

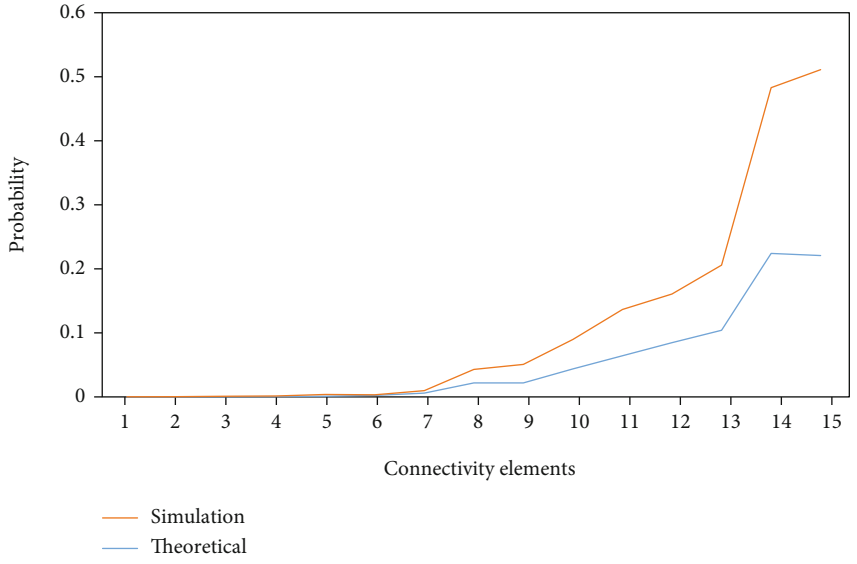


Figure 5: Radius: 50.

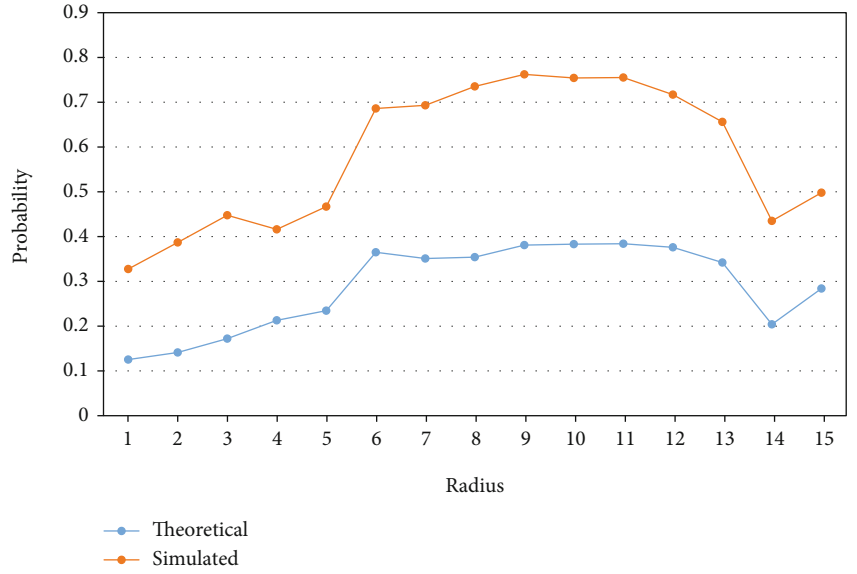


Figure 6: $r = 0.2$.

numerical values of these graphs are displayed in a graphical form. Figure 4–8 show the simulation outcomes with a constant communication radius. The connection factor of a portable wireless sensor network is shown in all four figures as a function of network probability in each case. To monitor a region, theoretical and simulation findings are compared. When the value of "Radius" 20 is constant, the communication radius is constant and the connectivity characteristic is modified based on its chance of being connected, As shown in Figure 4, when "CC" = 2, the Pq is at its highest point A. Figure 4 shows a Radius value of 30 and a maximum CC value of 6. Figure 4 shows "Radius" values of 50 and 60, with "CC" values of 20 and 36.

The calculated values of the network likelihood in relation to node coverage are shown in Tables 4–7. A constant value of network connectivity is shown in each table, as well as theoretical and simulated values for that connectivity. Due to a quota on the number of values, only the sample data that achieve a peak value are shown in the corresponding tables. This is true for the full 10-60 m range of node coverage "Radius."

Simulated results are shown below, with a fixed network connection factor and a variable network probability. In Figure 2, the network probability achieves a maximum at a communication radius of "Radius" = 18 when CC = 2.

In Figures 3 and 4, the probability reaches a maximum at "Radius" = 30 and 40 when CC = 5 and 9, respectively. A look at Figure 4 shows that the network probability is at its maximum peak when the "Radius" value is 50 and declines to 0.06 when it is 55. At this point, CC has been fixed at 15.

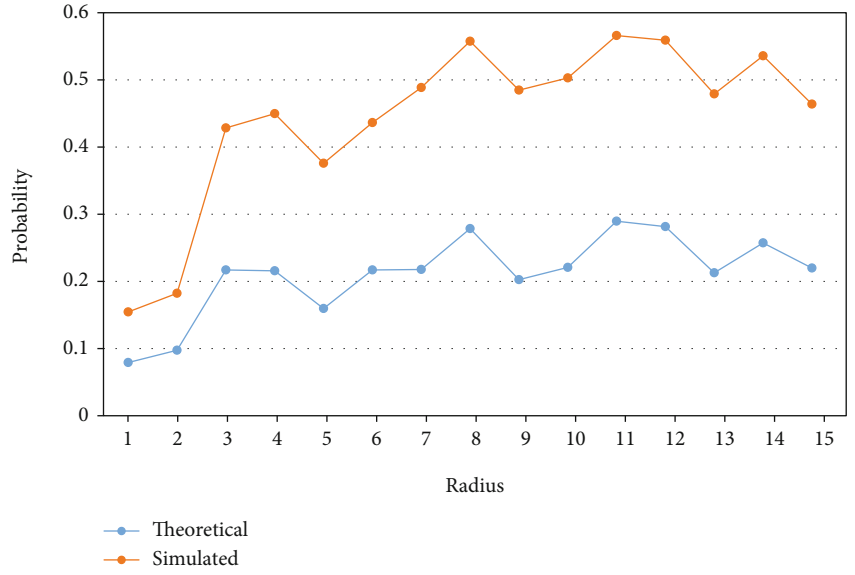


Figure 7: $r = 0.5$.

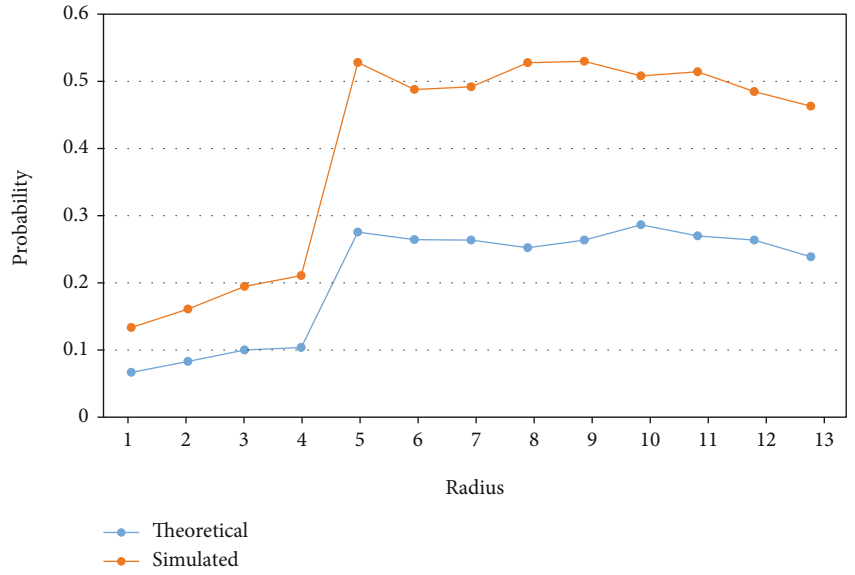


Figure 8: $r = 0.9$.

According to the preceding sections, adjacent nodes give energy when a specific node processes data and its energy level is depleted, so that the overall energy consumption is minimized. In addition, it has been shown that as the radius of coverage area increases, connection and energy levels remain stable. Calculating the sensor node's total energy is simple.

$$Tm_n = \sum_{i=1}^{N} \text{Node } i, \tag{2}$$

$$Node\, I = M_{Ai} + M_{Bi} + M_{Bij}, \tag{3}$$

$$M_{Ai} = PQ_i + Tm_j + Km_j + CC_j, \tag{4}$$

$$M_{Bi} = PQp + Tm_x + Km_x + CC_x, \tag{5}$$

$$M_{Bij} = Tm_w + Km_w + CCs_w. \tag{6}$$

In Equation (2), "Tm" is the time in milliseconds, "CC" means voltage in millivolts, "Km" means current in milliamps, "PQ" means the distance of the packet in bytes, and ESwi, ERi, and ETi are the power consumption in communication, starting, and transferring, correspondingly, in the aforementioned equations [41, 42]. When compared to other current algorithms, the simulation results show that our approach uses less energy while still improving the coverage area, as we had hoped. There are a variety of techniques and a suggested algorithm to choose from when it comes to

Table 4: Comparison when the Radius constant value is 0.2.

Radius	Probability (Prob) for CC = 0.2	
	Theoretical	Simulated
10	0.1253	0.2023
11	0.1412	0.2456
12	0.1721	0.2754
13	0.213	0.203
14	0.2345	0.2324
15	0.365	0.321
16	0.351	0.3421
17	0.354	0.3812
18	0.381	0.3812
19	0.383	0.3712
20	0.384	0.3712
21	0.376	0.341
22	0.342	0.314
23	0.204	0.231
24	0.284	0.214

Table 5: Comparison when the Radius constant value is 0.5.

Radius	Probability (Prob) for CC = .5	
	Theoretical	Simulated
20	0.0782	0.0743
21	0.0963	0.0836
22	0.2143	0.2087
23	0.213	0.231
24	0.1576	0.2134
25	0.2143	0.2165
26	0.215	0.2674
27	0.275	0.2754
28	0.2	0.2786
29	0.218	0.2785
30	0.286	0.2728
31	0.278	0.274
32	0.21	0.263
33	0.254	0.275
34	0.217	0.241

Table 6: Comparison when the Radius constant value is 0.9.

Node coverage (r)	Network probability (Prob) for CC = 0.9	
	Theoretical	Simulated
30	0.0643	0.0643
31	0.08	0.075
32	0.0964	0.0912
33	0.0999	0.1032
34	0.2654	0.2432
35	0.2546	0.2154
36	0.254	0.2198
37	0.243	0.2654
38	0.254	0.2564
39	0.276	0.2134
40	0.26	0.2354
41	0.254	0.213
42	0.23	0.216

Table 7: Comparison when the Radius constant value is 0.9.

Node coverage (r)	Network probability (Prob) for CC = 1.5	
	Theoretical	Simulated
35	0.0067	0.0054
36	0.00936	0.00843
37	0.0254	0.0213
38	0.0298	0.0245
39	0.0354	0.0325
40	0.0412	0.0477
41	0.0512	0.0562
42	0.0687	0.0586
43	0.0712	0.0781
44	0.0843	0.0833
45	0.0999	0.0934
46	0.1054	0.1054
47	0.208	0.206
48	0.21	0.205
49	0.213	0.222
50	0.276	0.208

determining how much energy is needed to cover a certain radius [43, 44].

It is shown in Figure 9 that a number of algorithms are compared in terms of their graphical representations. The simulation results show that the PNC algorithm uses less energy than the other algorithms currently in use. Because of the neighbour node energy sharing idea introduced in Section 4, the suggested solutions are more suited to energy minimization while still preserving network connection [45]. In addition, it sustains the energy stages in relation to the exposure radius of the beam [46]. To begin, this section compares and contrasts a few current studies in wireless sensor network technology. It is seen in Table 8 how they worked around their restrictions.

As can be seen from the comparison table, some researchers are more concerned with the network connection and improving longevity, while others are more concerned with network energy efficiency. Because working in a mobile context is so difficult, most researchers have focused on static wireless sensor networks. Even though it is a time-consuming operation to analyze a mobile network, we attempted to focus on the most important issues: energy efficiency and connection in a mobile context. Energy optimization algorithms for a mobile wireless sensor network are proposed in this study. In order to verify the accuracy of the model's output, simulation graphs are included with the source code.

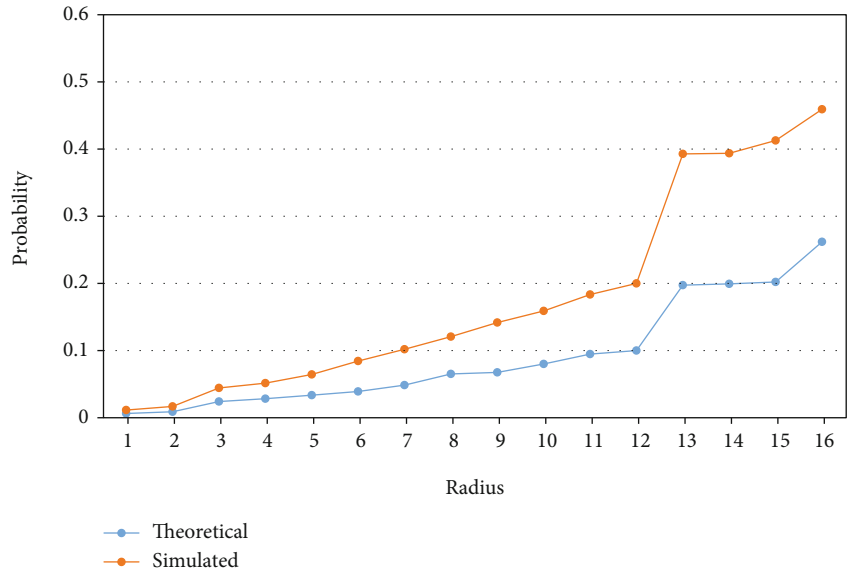


Figure 9: $r = 0.15$.

Table 8: Energy optimization comparison of proposed approaches vs. existing approaches.

No.	Radius (meters)	LEACH	ZTR	DSR	Proposed
1	10	90	100	148	87
2	20	100	140	210	89
3	30	110	160	230	115
4	40	120	170	260	120
5	50	130	180	270	125
6	60	135	180	275	130
7	70	140	183	277	135
8	80	142	185	278	140
9	90	145	187	280	141
10	100	150	190	290	142

Wireless sensor networks have long faced the difficulty of optimizing energy consumption. When there are mobile nodes in the network, maintaining connectivity becomes much more difficult. It is proposed a method to maximize energy by sharing each other's energy via surrounding nodes while controlling network connectivity, based on the notion of network complexity owing to high mobility nodes. Network routing table (NRT) helps to build flexible connectivity between the nodes. Nodes (X) and the node coverage radius (r) of the proposed technique are optimized such that a minimum number of nodes (X) remain active in order to maintain the network's complete connectivity while r is minimized to reduce energy consumption.

Nodes' battery and transmit power statuses are constantly being updated in the NRT. If X is increased, for example, more nodes are made active, and the communication range r is lowered in order to keep the energy usage low when the nodes in a region are running low on battery levels. As a control parameter, the V factor (network connectivity) has been introduced [47, 48].

A comparison of the values obtained through mathematical analysis (theoretical) and simulation is shown in Figures 4 and 5. These results support our hypothesis about the validity of the binomial distribution. Increasing the number of sensor nodes or the communication range is an easy way to increase network connection. As the radius of communication increases, so too does the possibility of a network reaching its maximum connection level. As a result, the network is expected to be more efficient. According to this study, raising the connectivity factor above a specific number diminishes the network likelihood, as the more active node pathways increase the delay in the network beyond the threshold value of link failure for that particular radius of coverage. When numerous active nodes broadcast redundant data, the network becomes congested.

In Figure 5, it can be shown that when the value of the communication radius "r" is constantly increased, the network probability decreases once a certain threshold is reached while the connection factor is fixed. As a result, network connectivity and energy conservation are not

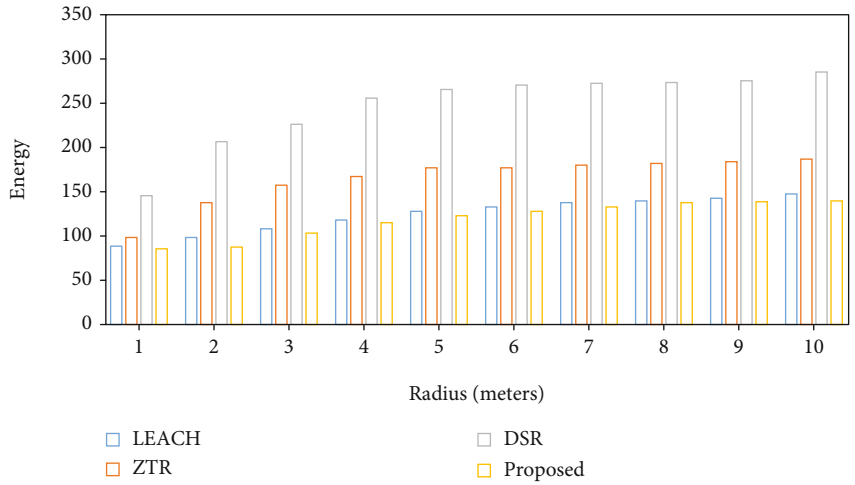


Figure 10: Plot representation of energy optimization comparison of proposed approaches vs. existing approaches.

guaranteed. A greater radius may be used to reduce energy consumption while maintaining connectivity.

Figure 10 demonstrates that the proposed method consumes much less energy averagely 40% compared to the existing methods, which are LEACH, ZTR, and DSR when the radius is 100. According to this experiment, the proposed works consume limited energy than the existing works. The observations from Figure 10 illustrate the optimal utilization of links and node beacons.

6. Conclusion

Getting the most out of an IoT-based wireless sensor network has always been a problem. Maintaining a stable network connection when nearby nodes' locations vary at random is becoming increasingly difficult because of the prevalence of mobile devices. According to the findings, IoT-based mobile sensor network connections can only be extended up to a certain point while still retaining optimal energy usage. Mathematical and simulation evidence back up these claims as well as a proposed technique for selecting coverage and connection with surrounding nodes. Updating the information in the list to allow energy sharing among nearby nodes represents the notion of updating the routing table with adjacent node status and calculating optimal transmit power. As a result, we can be sure that the network connection has a binomial distribution.

Free-space propagation is the only consideration in this paper's research. This may be taken a step further by considering the impact of adjacent node interference and multipath fading on the intensity of the received signal. In order to achieve desirable levels of the signal-to-interference noise ratio, more transmit power may be required. It can also be thought of as a battery life consideration. Artificial intelligence techniques such as the convolutional neural network (CNN) could be used in the future to figure out how much energy a vehicle needs based on how fast it moves.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflict of interest.

Acknowledgments

We deeply acknowledge Taif University for Supporting this research through Taif University Researchers Supporting Project number (TURSP-2020/231), Taif University, Taif, Saudi Arabia.

References

[1] H. Mostafaei, M. U. Chowdhury, and M. S. Obaidat, "Border surveillance with WSN systems in a distributed manner," *IEEE Systems Journal*, vol. 12, no. 4, pp. 3703–3712, 2018.

[2] Z. Liu, T. Tsuda, H. Watanabe, S. Ryuo, and N. Iwasawa, "Data driven cyber-physical system for landslide detection," *Mobile Networks and Applications*, vol. 24, no. 3, pp. 991–1002, 2019.

[3] D. Feng, C. Jiang, G. Lim, L. J. Cimini, G. Feng, and G. Y. Li, "A survey of energy-efficient wireless communications," *Communications Surveys & Tutorials*, vol. 15, no. 1, pp. 167–178, 2013.

[4] L. Wang, T. Han, Q. Li, J. Yan, X. Liu, and D. Deng, "Cell-less communications in 5G vehicular networks based on vehicle-installed access points," *IEEE Wireless Communications*, vol. 24, no. 6, pp. 64–71, 2017.

[5] M. Naghibi and H. Barati, "EGRPM: energy efficient geographic routing protocol based on mobilesink in wireless sensor networks," *Sustainable Computing: Informatics and Systems*, vol. 25, p. 100377, 2020.

[6] P. S. Banerjeea, S. N. Mandala, D. Deb, and B. Maiti, "RL-sleep: temperature adaptive sleep scheduling using Reinforcement learning for sustainable connectivity in wireless sensor

networks," *Sustainable Computing: Informatics and Systems*, vol. 26, p. 100380, 2020.

[7] A. L. Kakhandki, S. Hublikar, and Priyatamkumar, "Energy efficient selective hop selection optimization to maximize lifetime of wireless sensor network," *Alexandria Engineering Journal*, vol. 57, no. 2, pp. 711–718, 2018.

[8] B. Khargharia, S. Hariri, F. Szidarovszky, M. Houri, H. El-Rewini, S. U. Khan, I. Ahmad, and M. S. Yousif, Eds., "Autonomic power & performance management for large-scale data centers," *International Parallel and Distributed Processing Symposium*, 2007.

[9] H. F. Sheikh, H. Tan, I. Ahmad, S. Ranka, and P. Bv, "Energy- and performance-aware scheduling of tasks on parallel and distributed system," *ACM Journal on Emerging Technologies in Computing Systems*, vol. 8, no. 4, pp. 1–37, 2012.

[10] T. Yang, X. Xu, L. Peng, L. Tonghui, and L. Pan, "A secure routing of wireless sensor networks based on trust evaluation model," *Procedia Computer Science*, vol. 131, pp. 1156–1163, 2018.

[11] L. K. Ketshabetswe, A. M. Zungeru, M. Mangwala, J. M. Chuma, and B. Sigweni, "Communication protocols for wireless sensor networks: a survey and comparison," *Heliyon*, vol. 5, no. 5, p. e01591, 2019.

[12] G. Sakyaa and V. Sharma, "ADMC-MAC: energy efficient adaptive MAC protocol for missioncritical applications in WSN," *Sustainable Computing: Informatics and Systems*, vol. 23, pp. 21–28, 2019.

[13] C. Ambekar, V. Kalyankar, V. Raina, and M. Gund, "Energy efficient modeling of wireless sensor networks using random graph theory," *International Journal on Recent Trends in Engineering & Technology*, vol. 10, no. 2, pp. 10–18, 2014.

[14] H. Wang, F. Meng, H. Luo, and T. Zhou, "A location-independent node scheduling for heterogeneous wireless sensor networks," in *Third International Conference on Sensor Technologies and Applications*, Glyfada, Greece, 2009.

[15] P. Agrawal and N. Patwari, "Correlated link shadow fading in multi-hop wireless networks," *IEEE Transactions on Wireless Communications*, vol. 8, no. 8, pp. 4024–4036, 2009.

[16] B. Chai, R. Deng, P. Cheng, and J. Chen, "Energy-efficient power allocation in cognitive sensor networks: a game theoretic approach," *Proceedings of the Ad Hoc and Sensor Networking Symposium*, Anaheim, CA, USA, 2013.

[17] H. Mostafaei and M. S. Obaidat, "Learning automaton-based self-protection algorithm for wireless sensor networks," *Let Networks*, vol. 7, no. 5, pp. 353–361, 2018.

[18] A. Sharma, R. Kumar, and P. Kaur, "Study of issues and challenges of different routing protocols in wireless sensor network," in *Fifth international Conference on image information processing*, Shimla, India, 2019.

[19] A. Sharma and R. Kumar, "A framework for risk-energy aware service-level agreement provisioning (RESP) for computing the quickest path," *Journal of Computer Networks and Communications*, vol. 2019, 8 pages, 2019.

[20] A. Sharma and R. Kumar, "Performance comparison and detailed study of AODV, DSDV, DSR, TORA and OLSR routing protocols in ad hoc networks," in *Fourth International Conference on Parallel, Distributed and Grid Computing*, Waknaghat, Solan, India, 2017.

[21] M. E. Haque and U. Baroudi, "Dynamic energy efficient routing protocol in wireless sensor networks," *Wireless Networks*, vol. 26, no. 5, pp. 3715–3733, 2020.

[22] R. E. Moraes, W. W. dos Reis, H. R. Rocha, and D. J. Coura, "Power-efficient and interference-free link scheduling algorithms for connected wireless sensor networks," *Wireless Networks*, vol. 26, no. 5, pp. 3099–3118, 2020.

[23] A. Mehto, S. Tapaswi, and K. K. Pattanaik, "A review on rendezvous based data acquisition methods in wireless sensor networks with mobile sink," *Wireless Networks*, vol. 26, no. 4, pp. 2639–2663, 2020.

[24] L. Chan, K. Gomez Chavez, H. Rudolph, and A. Hourani, "Hierarchical routing protocols for wireless sensor network: a compressive survey," vol. 26, Tech. Rep. 5, Wireless Networks, 2020.

[25] J.-W. Kim and J.-W. Kim, "Energy efficient clustering algorithm for the mobility support in an IEEE 802.15.4 based wireless sensor network," *Wireless Networks, Spriger*, vol. 25, no. 6, pp. 3441–3452, 2019.

[26] M. J. Evans and J. S. Rosenthal, *Probability and Statistics*, The Science of Uncertainty, 2009.

[27] P. Le Nguyen, Y. Ji, Z. Liu, H. Vu, and K. V. Nguyen, "Distributed hole-bypassing protocol in WSNs with constant stretch and load balancing," *Computer Networks*, vol. 129, pp. 232–250, 2017.

[28] V. K. Chawra and G. P. Gupta, "Memetic algorithm based energy efficient wake-up scheduling scheme for maximizing the network lifetime, coverage and connectivity in three-dimensional wireless sensor networks," *Wireless Personal Communications*, vol. 123, pp. 1507–1522, 2022.

[29] S. Routray, P. P. Malla, S. K. Sharma, S. K. Panda, and G. Palai, "A new image denoising framework using bilateral filtering based non-subsampled shearlet transform," *Optik*, vol. 216, p. 164903, 2020.

[30] L. Dong and G. Ren, "Optimal and low complexity algorithm for energy efficient power allocation with sensing errors in cognitive radio networks," in *Sixth International Conference on Wireless Communications and Signal Processing*, pp. 600–605, 2014.

[31] S. Routray, A. K. Ray, and C. Mishra, "An efficient image denoising method based on principal component analysis with learned patch groups," *Signal, Image and Video Processing*, vol. 13, no. 7, pp. 1405–1412, 2019.

[32] E. Yilmaz, "A half-duplex two-way relay station assisted cellular uplink and downlink communications," in *European Wireless 2021; 26th European Wireless Conference*, pp. 1–7, 2021.

[33] S. Rajasoundaran, A. V. Prabu, S. Routray, P. P. Malla, G. S. Kumar, and Y. Qi, "Secure routing with multi-watchdog construction using deep particle convolutional model for IoT based 5G wireless sensor networks," *Computer*, vol. 187, pp. 71–82, 2022.

[34] S. Begam, G. S. Sabeena, T. T. Ngan, and R. Sharma, "Similarity measure of lattice ordered multi-fuzzy soft sets based on set theoretic approach and its application in decision making," *Mathematics*, vol. 8, no. 8, p. 1255, 2020.

[35] V. Thanh, S. Rohit, K. Raghvendra, and S. Le Hoang, "Crime rate detection using social media of different crime locations and twitter part-of-speech tagger with Brown clustering," *Journal of Intelligent Fuzzy Systems*, vol. 38, no. 4, pp. 4287–4299, 2020.

[36] P. T. Nguyen, D. H. Ha, M. Avand et al., "Soft computing ensemble models based on logistic regression for groundwater potential mapping," *Applied Sciences*, vol. 10, no. 7, p. 2469, 2020.

[37] S. Jha, R. Kumar, L. Hoang Son et al., "Deep learning approach for software maintainability metrics prediction," *IEEE Access*, vol. 7, pp. 61840–61855, 2019.

[38] E. A. Devi, K. C. Ramya, K. S. Kumar et al., "Energy aware metaheuristic optimization with location aided routing protocol for MANET," *CMC-Computers, Materials & Continua*, vol. 71, no. 1, pp. 1567–1580, 2022.

[39] R. Kumar and T. Amgoth, "Reinforcement learning based connectivity restoration in wireless sensor networks," *Applied Intelligence*, 2022.

[40] S. Mahfoudh, P. Minet, and I. Amdouni, "Energy efficient routing and node activity scheduling in the OCARI wireless sensor networks," *Future Internet*, vol. 2, no. 3, pp. 308–340, 2010.

[41] S. Rajasoundaran, A. V. Prabu, S. Routray et al., "Machine learning based deep job exploration and secure transactions in virtual private cloud systems," *Computers & Security*, vol. 109, article 102379, 2021.

[42] N. Tuah, M. Ismail, and K. Jumari, "Energy-efficient improvement for heterogeneous wireless sensor networks," *Information Technology Journal*, vol. 11, no. 12, pp. 1687–1695, 2012.

[43] H. Mostafaei and M. S. Obaidat, "A distributed efficient algorithm for self-protection of wireless sensor networks," in *Proceedings of the 2018 IEEE International Conference on Communications*, Kansas City, MO, USA, May 2018.

[44] R. Soundararajan, N. Palanisamy, R. Patan, G. Nagasubramanian, and M. S. Khan, "Secure and concealed watchdog selection scheme using masked distributed selection approach in wireless sensor networks," *IET Communications*, vol. 14, no. 6, pp. 948–955, 2020.

[45] C. D. V. Soto, "Wireless sensor network energy model and its use in the optimization of routing protocols," *Energies*, vol. 13, no. 3, p. 728, 2020.

[46] M. Elshrkawey, S. M. Elsherif, and M. Elsayed Wahed, "An enhancement approach for reducing the energy consumption in wireless sensor networks," *Information Sciences*, vol. 30, no. 2, pp. 259–267, 2018.

[47] S. Rajasoundaran, A. V. Prabu, G. S. Kumar, P. P. Malla, and S. Routray, "Secure opportunistic watchdog production in wireless sensor networks: a review," *Wireless Personal Communications*, vol. 120, no. 2, pp. 1895–1919, 2021.

[48] A. Gayathri, A. V. Prabu, S. Rajasoundaran et al., "Cooperative and feedback based authentic routing protocol for energy efficient IoT systems," *Concurrency and Computation: Practice and Experience*, p. e6886, 2022.

Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 8725767, 17 pages
https://doi.org/10.1155/2022/8725767

Review Article

Transforming the Capabilities of Artificial Intelligence in GCC Financial Sector: A Systematic Literature Review

Habib Ullah Khan,[1] **Muhammad Zain Malik**,[1] **Mohammad Kamel Bader Alomari**,[1] **Sulaiman Khan**,[1] **Alanoud Ali S. A. Al-Maadid**,[2] **Mostafa Kamal Hassan**,[1] **and Khaliquzzaman Khan**[3]

[1]*Department of Accounting and Information Systems, College of Business and Economics, Qatar University, Doha, Qatar*
[2]*Department of Finance and Economics, College of Business and Economics, Qatar University, Doha, Qatar*
[3]*College of Business Administration, American University in the Emirates, Dubai, UAE*

Correspondence should be addressed to Habib Ullah Khan; habib.khan@qu.edu.qa

Received 30 January 2022; Revised 4 March 2022; Accepted 21 March 2022; Published 5 April 2022

Academic Editor: Md. Shamsul Huda

 The publication of this article was funded by Qatar National Library.

Identity and access management is a business process framework that makes it easier to maintain genuine user identities and regulate access to sensitive assets. The word "access control" refers to an organization's policy for authorizing access procedures, the mechanisms that implement and enforce the policy, and the model that the policy and procedures are built on. Adopting new technology may give rise to specific cyber threats that decrease or degrade business operations. The paper has designed to discuss the artificial intelligence-based access control system as a necessary component of governing and safeguarding the financial sector's information assets in the Gulf Cooperation Council (GCC) region. Due to the dynamic and complicated nature of security rules for access control, organizations that employ web-enabled remote access in conjunction with applications access deployed over several networks face various obstacles, including increased operational complexity and monitoring concerns. Organizations spend a vast budget on securing their business. As the industry trend has shifted to intelligent internet-based companies on the same side, the cyber threat has become a challenge for the researcher to find the solution. A systematic research is conducted to fill the gaps in the existing literature by picking the most relevant research papers (126) from the four most reputable online repositories based on the four research questions specified. These research topics aim to evaluate the current situation from many perspectives and provide new avenues for future study to be studied soon to maintain high security and authenticity inside financial sectors of the GCC's countries.

1. Introduction

Human involvement and technological advancements have paved the road for prosperity in human life [1]. Individuals use the Internet as a communication tool to cooperate, communicate, and express their opinions about numerous topics and obtain information and use various technologies such as cell phones and other gadgets [2]. The Internet of Things (IoT) is a new technology that will transform the Internet age over the next several years. Digitally connected factories, facility management, production flow management, inventory management, safety, security, health care, logistics, supply chain optimization, and other industries may all benefit from IoT [3]. Information systems and smart Internet of things- (IoT-) based solutions have enriched our lives by offering several state-of-the-art applications in various fields, including healthcare, navigation, tracking, smart security, smart homes, smart buildings [4], and smart appliance management systems. Transportation, healthcare [5], the house, entertainment, and other daily activities have all been altered by IoT-based applications [6]. Al-Azawi et al. [7] compared several AI-assisted cybersecurity solutions. The digital age changed business paradigms by allowing businesses to join the market with specific financial advantages [8]. Mobile information systems will continue to function as facilitators of innovation and will support entrepreneurship in

sustainable ways throughout the world [9]. Because of the proliferation of portable devices and the availability of the Internet, mobile learning (M-learning) has exploded in popularity in recent years. The success stories of next generation mobile information systems have been supplemented by the usage of this unique technology in learning and training [10].

Due to the unpredictability of the economic climate and fierce competition, even the well-run businesses are vulnerable to failure and financial disaster. So, whether financial difficulty in publicly traded firms can be projected properly and quickly is dependent on the development of the company, the interest of various investors, and the capital market order [11]. Organizations are interested in altering their company operations and incorporating computer-assisted technologies to serve their clientele [12]. Criminal activity is rising in our society daily. A huge number of threats and acts of violence occur in the community due to this exponential growth. People require security systems and improved living conditions to provide serenity to their lives and raise their living standards. As new technology evolves, it harms the globe in the form of cyber-attacks [13]. Organizations and individuals must endure harmful damage and cyber-attacks on their information systems. Any firm must take security action based on risk assessments in every period of information system modernization. There are other risk analysis approaches to choose from, but the qualitative method is the most effective. The qualitative approach helps the company to make timely decisions about information security [14]. Farooq and Otaibi [15] gave a paper at a symposium on reducing security risks in information systems. Information system security risk management is critical to an organization's commercial performance (ISSRM). The ISSRM ensures privacy, data security, and consistency.

Artificial intelligence (AI) is defined as "the practice of making machines intelligent, with intelligence being the attribute that allows an entity to function correctly and predictably in its environment." Artificial intelligence (AI) is the capacity of a machine to work intelligently by accurately reading incoming inputs and applying these teachings to achieve defined objectives and activities via a flexible design [16]. It is a result of human intelligence. AI is the intelligent base software that focuses on various human intelligence systems compound operations such as image processing, decision-making, speech recognition, and language processing. AI is a fictional technology that has altered many aspects of our life, including transportation, health, marketing, banking, and shopping [17]. In this industrial revolution, artificial intelligence (AI) is playing a key role. It can guard against cyber-attacks, viruses, and illegal access to the information system. AI can help with a variety of cybersecurity challenges. Multiple AI approaches, such as deep learning, machine learning, and concept of knowledge, can be used to reduce the cyber threat [7].

Due to the unpredictability of the economic climate and fierce competition, even the well-run businesses are vulnerable to failure and financial disaster. So whether financial difficulty in publicly traded firms can be projected properly and quickly is dependent on the development of the company, the interest of various investors, and the capital market order. Many investigators used AI to strengthen the security of information systems and interconnected devices in order to overcome security concerns and dangers. AI approaches assist machines in solving key issues in the same way that people do. AI can detect a variety of dangerous threats and assaults that can affect an organization's system. Using machine learning and deep knowledge, AI approaches respond in real time to numerous threats on the information system. Machine learning is a form of artificial intelligence that assists in identifying the ornament contained in incoming data [17].

Meanwhile, AI is being imposed on the education industry by the rapid advancement of information technology. Educational companies introduced the individual adaptive learning system (IALP) to support student enrolment and probe. It aims to aided teaching system, personalized learning that creates the classroom environment management, individual evaluation, and institute administration system to support the student enrolment and probe [18]. Rapidly changing needs, wants, and behavior of customers are influencing world economics, financial institutions, countries, the budget deficit, and business profitability and revenue aspects, while another view of economic development and financial crises, rapidly changing needs, wants, and behaviors of customers are influencing world economics, financial institutes, countries, and the budget deficit. Thuraisingham discussed the effects of robots and artificial intelligence on corporate economics and potential future study topics [19]. The technique and analysis of business trends and projections concerning sales, income, profits, and expenditures are all part of business forecasting. The goal of business forecasting is to give relevant data based on prophecy. Many businesses must gather this data in order to achieve their objectives [20]. The following are the main contribution of this systematic analysis:

(i) For recognizing the difficulties facing or faced by financial sector of GCC region most typically

(ii) To describe many strategies offered to address these difficulties, as well as where these solutions fall short

(iii) How artificial intelligence-based solutions have been used to handle these problems and how they may be enhanced to ensure high levels of security and authenticity, and

(iv) To identify the social and economical importance of AI on our lives and other government and nongovernment organizations

(v) Based on this systematic analysis, new research directions must be proposed to ensure the safety and security of the organizations for both employees and employers

The rest of the paper is organized as follows. Section 2 represents the background study, while Section 3 outlines the systematic protocol followed for this assessment work. Section 4 details the assessment criteria followed for

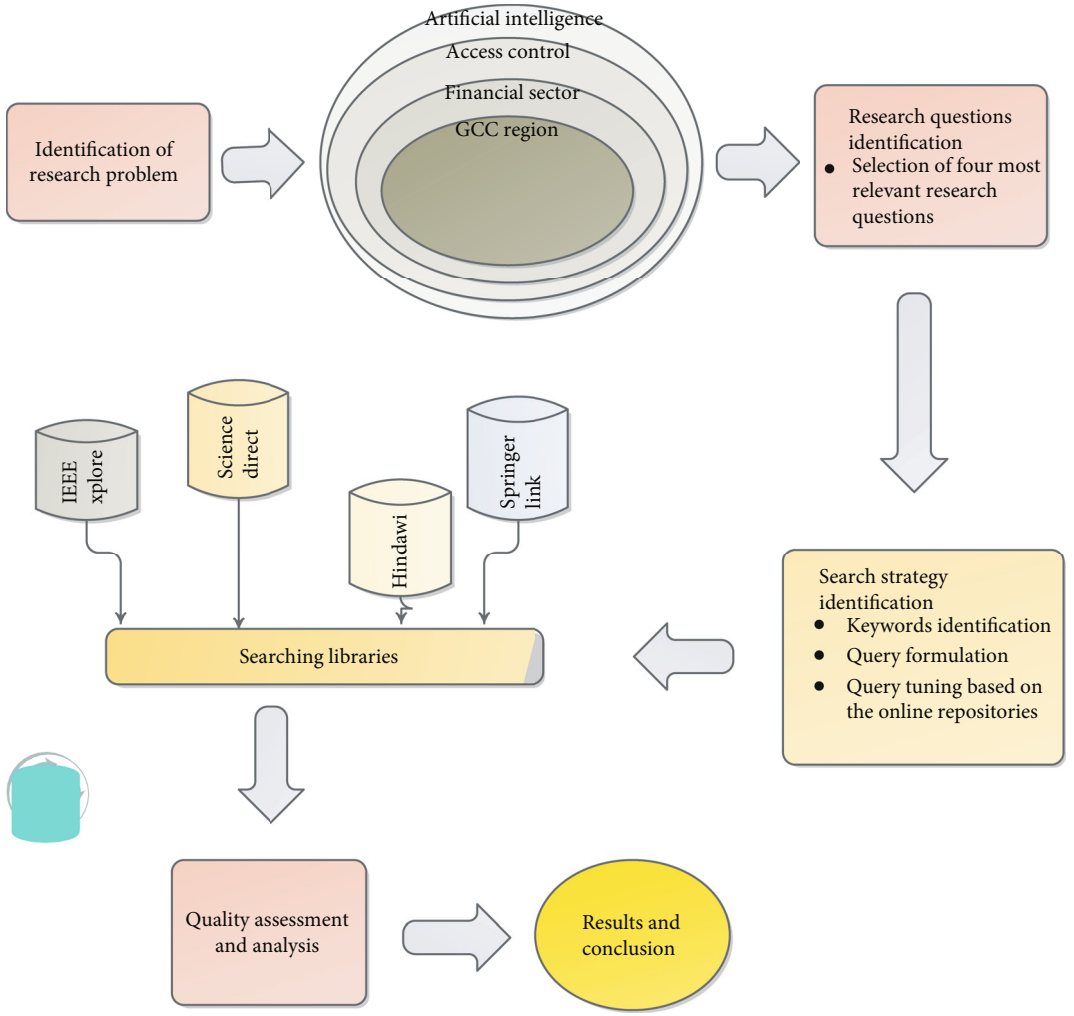


Figure 1: Proposed systemic literature review research procedure.

Table 1: Research questions.

S. no	Research questions	Description
RQ1.	What are the various types of organizational security risks faced by employees working within the GCC region?	This question primarily focuses on extracting the information regarding different types of security issues most commonly faced by the employees and the people residing in the GCC region.
RQ2.	By utilizing AI capabilities as evidence, how many proactive approaches are proposed to counter organizational security risks in the GCC region?	The primary goal of this research question is to compile a list of various AI-based strategies that have been created to reduce organizational safety and security concerns in the GCC region. In addition, this inquiry aims to provide a new research direction for improving the capabilities of existing models or developing a new upgraded model.
RQ3.	Based on the extant findings, how can we improve the capabilities of the available authentication systems in the GCC organizations?	Based on the literature, this research topic aims to increase the organization's ability to improve the existing authentic systems to assure high security and ethnicity in GCC-based organizations.
RQ4.	What are the social and economic impacts of AI on financial bodies operating in the GCC region?	AI has a significant impact all around the world. This research topic aims to demonstrate the social and economic effects of AI-based solutions in the financial sectors of the GCC region.

evaluation purposes. Section 5 briefly explains the results and discussion section. Section 6 presents the limitations of this research work followed by the conclusion in Section 7 of the paper.

2. Background Study

Artificial intellect (AI) is a new scientific technology that may simulate and expand human intelligence technology applications. AI is a study area at the crossroads of social science, natural science, and technological science. AI can process information in a way that is akin to human thinking and awareness. AI employs a procedural way to develop and extend the core of intelligence, resulting in a new sort of intelligent computer that behaves similarly to humans. The researchers investigated the influence and impact of AI on stakeholders, consumers, and businesses in the industry to improve the business [1]. Artificial intelligence (AI) has become a danger to people who labour manually as new information technology has been implemented. This danger exists for financial institutions as well. Despite this, investment in AI FinTech has not slowed due to the uncertainty that AI provides to mandatory customers, operators, and financial controllers. AI offers various social benefits to increase its credibility in financial institutions and win public acceptance [2].

Small enterprises contribute significantly to a country's economy. Almost 98 percent of businesses in the United States are small businesses with less than 100 employees. These companies employ a total of 36% of the workforce. It represents a market sector eager to improve its businesses using modern information technologies [3]. Because of blockchain technology, corporate governance has taken a new direction. A reliable and effective GITS (global information transmission system) will require a reliable value to the transmission system, the cornerstone of blockchain technology. A reliable and effective GITS (global information transmission system) will require a reliable deal to the transmission system, the cornerstone of blockchain technology. By employing cryptography, blockchain creates a mutually dispersed system that may achieve an agreement without personal intervention. By using cryptography, blockchain creates a mutually dispersed system that may execute a contract without personal intervention. Blockchain is a consensus method that acknowledges the advantages of reaching an agreement between two or more devices without the need of humans. Blockchain applications and cyber-physical systems are transforming traditional business models, technical procedures, and industrial processes. The Bitcoin network's blockchain symbolizes 1.0 technology [4].

An information system innovation is a sophisticated mechanism for administering distributed ledgers to the blockchain [5]. The key features of the traditional notebook system have aroused interest in blockchain technology due to frequent validations of operational transactions for validity, the secrecy of the encoded parties to the transaction, the inaccessibility of the control center, and the establishment of money. Cryptocurrencies are the well-known real-world solution to this new technology. It has about 2000 variations of various modifications. The ever-increasing revenue from cryptocurrencies, especially in the heavily regulated crypto industry, has taken control of exchanges and even specialized bank services as a new asset [6]. Machine vision remains a difficult issue that draws scholars to conduct research in this area. Machine vision systems (MVS) that are inspired by human vision systems have been developed (HVS) [7].

Table 2: Articles selection and final database development process.

Online databases	Papers selected based on title	Papers selected based on abstract	Papers selected based on content provided
IEEE Xplore	252	96	35
ScienceDirect	244	127	39
Hindawi	231	96	27
Springer Link	211	66	25
Total			126

Artificial intelligence (AI) is a broad area of development that can offer a variety of advantages to enterprises. Following an immense quantity of data and a large increase in computing capabilities over the last few years, businesses have increasingly resorted to AI to generate economic value [8]. Global financial services are being reshaped as a result of fast technological advancements and increased competition. AI has recently attracted a lot of attention [9]. Organizations have implemented AI applications to generate more business value in increased sales, revenue, enhanced company efficiency, and cost savings [10]. According to a recent study published in the MIT Sloan Management Review, more than 80% of businesses see AI as a planned opportunity. AI is viewed as a tool to achieve a competitive edge by over 85% of respondents [11]. Various firms invest in AI technology to deal with organizational challenges and revenue development; nevertheless, some businesses fail to see AI's worth [12].

3. Research Protocol

SLR examines and determines a subject of interest by identifying a set of most relevant research questions in the selected research domain. In the SLR process, the research questions serve as a cornerstone. SLR uses a thorough, reliable, and verifiable technique to offer a fair appraisal of a research subject [21]. Many academics in diverse domains like healthcare systems [22], networking [23], crowdsourcing [24], and many others use SLR work to explore the extant and identify the gaps in the literature and define new research direction for the researchers to explore. This SLR method summarizes the literature on artificial intelligence and machine learning approaches used in financial institutions. Following are the list of the objectives that are aimed to be achieved by this systematic research work.

Analyze the current research activity in light of the four research topics that have been defined. These questions aim to outline the existing based on AI models developed to ensure high security in organizations, different types of

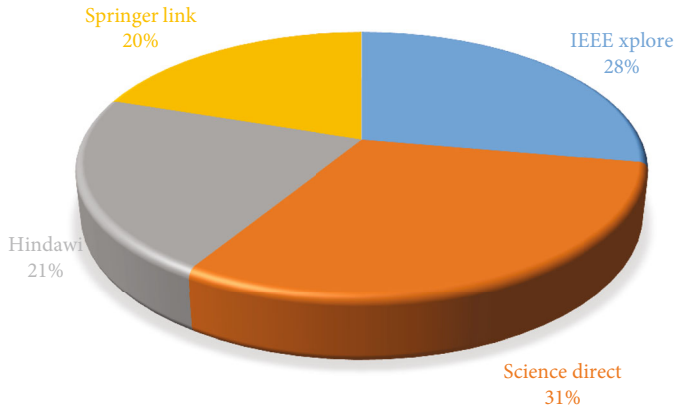


Figure 2: Online libraries for the proposed research.

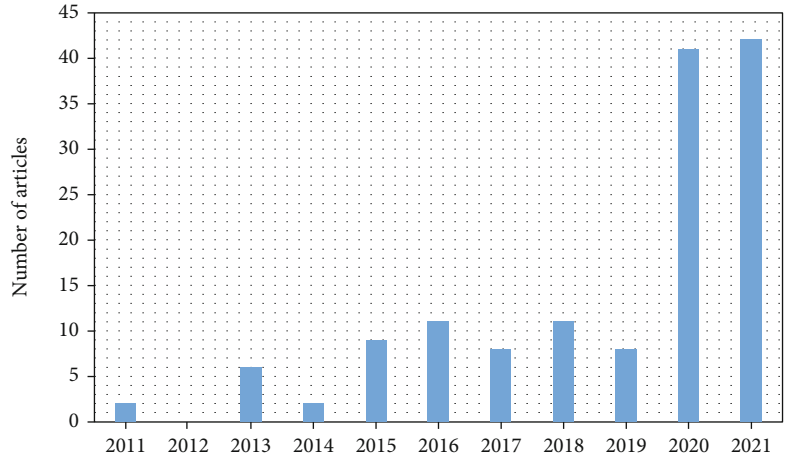


Figure 3: Year-wise detail of selected papers.

threats that employees in organizations commonly face, different architectures and tools suggested for mitigating the security risks faced during unwanted situations, and different implications of AI on diverse domains within the organization.

This SLR project attempts to identify significant flaws in existing solutions and propose new future research areas to fill up the gaps. These new study paths will eventually aid firms and staff in assuring high authenticity for their security ways, preventing data leaking, and combating intruder attacks.

The most relevant research publications were chosen from four peer-reviewed internet sources for this SLR project. The researchers will be able to discover the most relevant research publications in the AI area and analyses them using this list of the most relevant research articles.

This SLR paper is being carried out following the guidelines defined by Mishra and Yadav and Daya [26, 27]. The review protocol of this SLR has depicted in Figure 1. It consists of seven main steps: (1) selection of research q, (2) identification of research question, (3) search strategy, (4) selection appropriate studies, (5) review online libraries for most relevant papers selection, (6) quality assessment, and (7) conclusion and future direction. All these stages are described with full description in Figure 1.

3.1. Research Question. Research questions (RQ) are just like the corner stone of any SLR work. The most relevant and highly precised RQs (by considering different aspects in a certain topic of interest) ensure the validity and applicability of the SLR work. To conduct this SLR work, we formulated a set of four RQs to explore the proposed field from different aspects. The details regarding the research questions and the underlined descriptions are detailed below in Table 1.

3.2. Keyword Finalization. After formulating the research questions, the new activity is to identify the most suitable keywords that resultantly helped in accumulating relevant articles from the selected online repositories. The finalized most relevant articles retrieved are "*SECURITY, SAFETY, RISKS, THREATS, MITIGATE, MINIMIZE, EMBEDDED, DEPPLY, EVIDENCE, PROOF, CAPABILITY, ABILITY, ORGANIZATION, SECTOR, INSTITUTE, IMPACT, OR EFFECT.*" These keywords are used for the query development according to the database requirements and tuned further for best outcomes (for the retrieval of satisfactory results in terms of relevant articles).

3.3. Query Selection. To accelerate the articles accumulation process from the selected peer-reviewed libraries, the query

Table 3: List of security threats reported in the literature.

S. no	Type of security threat	Description	References
1.	Cyber security	Cyber security has become a topic of worldwide concern and relevance. More than 50 countries have already released a policy statement defining their official positions on cyberspace, cybercrime, and cyber security. Participants with a prior understanding of cyber security could differentiate between distinct cyber-attacks; however, beginner participants were not sensitive to the assault types. For security analysis in corporate networks, it is critical to capture the unpredictable parts of cyber security. However, there has been little research into whether modelling techniques accurately capture such uncertainty, as well as how to design models that are effective in reality. An attack graph depicts the logical causation relationships across numerous privileges and configuration settings in an enterprise network, illustrating probable multistage assaults. Traditional methodologies and technologies to collect, parse, normalize, search, analyze, display, and explore the massive amount of security events gathered by security information and management systems are increasingly reaching their physical limits in many businesses (SIEM). Traditional SIEM devices are meant to statically correlate security events and provide warnings for possible cyber threats in any security operations center (SOC). Every day, billions of security events are generated by a typical company network with thousands of IT systems. The risk management process aids executive decision-making, helping managers and owners to fulfill their fiduciary duty of safeguarding their companies' assets. This critical procedure should not take a long time to complete. The strategy used by an organization to ensure the confidentiality, availability, integrity, nonrepudiation, accountability, authenticity, and dependability of its IT systems is known as information security. The potential use of artificial intelligence technology to ensure data protection. The benefits of utilizing machine learning to analyze data security incidents are demonstrated. A look at some of the most popular commercial information security tools today. The objective of AI applications is to solve problems that take an expert a long time to solve in a short amount of time. The generated model is capable of performing the needed activities in the same manner as an expert advisor. Furthermore, the built software may be utilized by virtually anyone, even if an expert is not present in the business	[15–20, 28–34]
2.	Information security risk (ISR)	The security risks associated with each cloud delivery model differ and are based on a variety of factors, including the sensitivity of information assets, cloud topologies, and security measures implemented in a specific cloud environment. For a better knowledge of essential areas of emphasis in the cloud computing environment, as well as detecting threats and vulnerabilities, use this information risk management approach. Selecting a technique for conducting an information security risk analysis can be difficult for businesses. There are a variety of risk analysis approaches accessible today, some of which are qualitative and others of which are quantitative. The purpose of all of these approaches is to calculate the total risk value. Based on its unique requirements, an organization must choose the best technique. The main goal of information security is to protect an organization's important resources, such as hardware, software, and financial resources, as well as tangible and intangible assets. An organization's security objectives can be addressed by using appropriate security procedures and policies. Artificial intelligence technology excels at supervising and managing tasks in which humans fall short, hence, its use in networking has increased performance and security.	[5, 17, 21–23, 35–38]
3.	Network security	A network risk assessment evaluates the network(s) that your company and workers utilize on a daily basis. Using risk assessment tools, the evaluation helps identify the threats to your essential systems and sensitive data. Cyber-attacks are growing more complicated, and reliable intrusion detection is becoming more difficult (ID). Failure to prevent infiltration can compromise security services such as data integrity, privacy, and availability. The fast growth of computer networks (CNs) has changed how people think about network security. Intrusion detection systems (IDS) are used to detect all types of computer activity and hostile network (NW) traffic that standard firewalls cannot detect. Personal computer users, businesses, and the military have all become more concerned about network security. With the introduction of the internet, security has become a big concern, and studying the history of security helps for a better understanding of how security technologies emerged. Many security issues were possible due to the internet's structure. Firewalls and encryption methods are used by many enterprises to protect themselves from the internet. Businesses construct an "intranet" to stay connected to the internet while protecting themselves from potential risks.	[24, 26, 27, 33]
4.	Security and safety	The attribute or state of being safe, such as being devoid of danger, employment stability, freedom from dread or anxiety, freedom from the risk of being laid off. With changes made both worldwide and nationally, technological breakthroughs improve the way we live. These	[17, 39–43]

Table 3: Continued.

S. no	Type of security threat	Description	References
		technological advancements also have unintended consequences in the form of security risks. The use of artificial intelligence (AI) allows to solve complicated problems in the same way that people do. The artificial intelligence (AI) technology detects several assaults that threaten the application and system security of a company. The state of being safe the absence of the possibility of damage, danger, or loss. The ability to avoid or minimize damage, risk, or loss. A contraption or mechanism used to avoid harm or risk. Risk, safety, and security are all ideas that have attracted a lot of scholarly attention. There are a number of assumptions concerning their nature and relationship that have been made. Risk, safety, and security are often used in everyday discourse, in addition to academic contexts.	

Table 4: List techniques suggested mitigating security risks.

S. no	Techniques for mitigating security risk	Description	References
1.	Predictive models	Aviation accident investigators have found runway excursion as a significant contributing element in airline landing accidents caused by pilots maintaining an unsafe approach to landing. The goal of this study was to use machine learning to construct and evaluate prediction models for unstable approach risk misperception (UARM) in the National Airspace System	[44]
2.	ISSRM	Organizations' information system security risk management (ISSRM) is critical to their success. ISSRM ensures the availability, integrity, and privacy of information. However, especially in today's enterprises, where activities are done in a complex and interrelated setting, this latter remains a tough region to build and sustain. A well-defined strategy to produce business value is accomplished when an organization's business services and strategic planning are matched with proactive ISSRM operations. To do so, we'll look at risk management methodologies and security modelling languages to see why EAM may be beneficial. The relevance of business intelligence tools as an integrated solution for the insurance industry is growing due to the expanding data sizes in today's business sectors, as well as the requirement of risk management. The majority of the time, these tools have been employed to produce successful risk management.	[45, 46]
3.	Adaptive learning systems	Each discipline is meant to be designed as a workflow for a certain application area made of modules reflecting the necessary areas of knowledge, based on the ideas of "knowledge areas" and "application areas." Through so-called adaptive learning systems, it is possible to significantly improve education by introducing dynamic principles and customization in the curriculum. Furthermore, the management of adaptation may be accomplished using artificial intelligence technologies, which the authors have expertise with in the field of cybersecurity.	[18]
4.	Firewall technology	People's demands for network information technology are growing in tandem with the rapid advancement of science and technology. Artificial intelligence has arisen and is being used in a variety of industries to suit people's unique demands. The goal of incorporating artificial intelligence with computer network technology is to maximize the benefits of both technologies. In this way, computer networks may be utilized to make people's lives and work easier, and AI's function can be customized and humanized. It can also help to preserve information security and improve network administration at the same time. When compared to other defensive technology systems, the intelligent firewall system's combination of AI with firewall provides a greater level of intelligence and information processing impact.	[47]

is formulated *("SECURITY" OR "SAFETY" OR "RISKS" OR "THREATS") AND ("MITIGATE" OR "MINIMIZE") AND ("EMBEDDED" OR "DEPPLY") AND ("EVIDENCE" OR "PROOF" OR "CAPABILITY" OR "ABILITY") AND ("SECTOR" OR " ORGANIZATION " OR "INSTITUTE" OR "IMPACT" OR "EFFECT").* This query is fine-tuned depending on the gathered results and the libraries that have been chosen. The 126 most relevant research papers are picked based on the title, abstract, and content of the research piece. The next paragraph contains a detailed summary of the compiled research publications.

3.4. Review Online Libraries and Final Article Database Development. We selected four of the most peer-reviewed online repositories to accumulate the most relevant research articles for the proposed SLR work, including Hindawi,

Table 5: Social and economical impacts of artificial intelligence.

S. no	Types of impacts	Description	References
1.	Fraud detection	Because the mobile channel may accommodate practically any sort of payment, financial theft in the IoT ecosystem is a rapidly expanding concern. Financial fraud in mobile payments has emerged and is becoming more widespread as a result of the fast development of mobile commerce and the IoT environment. Financial fraud causes financial loss in the real world; hence, a highly precise approach of financial fraud detection in an IoT context is required. Furthermore, our technique suggested a machine-learning-based overall procedure for identifying financial fraud and compared it to artificial neural networks for detecting fraud and processing vast volumes of financial data.	[59, 60]
2.	New product innovation	Product lifecycle management (PLM) encompasses a wide range of technical, business, and management operations that occur throughout the lifespan of a product, from the conception of an intangible notion through the recycling of a finished product. AI theories, algorithms, and technologies to distinct stages of PLM (i.e., product design, production, and service) in the context of smart manufacturing.	[61]
3.	Financial prediction models	Despite the rapid development of information science and technology, as well as computer networks, in the last decade, interdisciplinary research that promotes cross-fertilization of disciplines, and the application of research methods used in many other disciplines to financial market forecasting, it remains extremely difficult to predict the current and future state of financial markets. Due to the support of current financial market theories, as well as the relationship between global financial markets and the particular of the forecasting time horizon, financial market forecasting is a difficult study issue.	[62]
4.	Internet supply chain finance	Enterprise green operation is a commercial activity that incorporates environmental preservation into the whole operation and management process of a company. It necessitates that environmental preservation be the driving principle of corporate operations and that every link of business management be founded on it. Furthermore, with the liberalization of the financial sector, banks are no longer the exclusive source of supply chain finance in the nation, owing to the enormous financing demands of SMEs. The use of the internet and big data technologies to address the problem of information symmetry in small and medium-sized firms, as well as to break the chicken-neck of small and medium-sized business finance.	[63]
5.	Interbank offered rate	The interest rate at which banks lend money to one another in the money market is known as the interbank offer rate. Shibor can correctly and timely represent the capital supply and demand connection in the money market as a market-oriented core interest rate, and its changes will immediately transmit and impact China's financial sector. Research is to forecast and investigate the volatility and trend of interbank offer rates, which are the rates at which banks lend money to one another in the money market.	[64]
6.	Financial performance evaluation	In today's competitive market, both businesses and academic institutions place a premium on financial performance evaluation studies. The quality of financial performance has a direct impact on the long-term viability of businesses. Enterprises are paying greater attention to the use of financial performance assessment analysis to promote the sound growth of the entire company as the enterprise management concept deepens. The study-related variables effecting company financial performance, debt-paying capacity, and relevant indicators are chosen from the four aspects of profitability, operation ability, and development ability to design the financial performance assessment system.	[65, 66]
7.	E-commerce	Network flaws in the existing e-commerce operating paradigm, such as network chaos and unequal network distribution, impede economic growth and advancement. Through independent screening and an artificial intelligence system improves and analyses the assembly of e-commerce websites and merges the internet economics with online website theory.	[4]
8.	New product innovation	Currently, there is a growing tendency in enterprises to look at artificial intelligence and nonartificial intelligence for new product innovation and success. The goal of the continuing research is to look into the function of artificial and nonartificial intelligence in new product success, as well as the moderating effect of new product innovation in Chinese manufacturing companies. The findings revealed that both artificial and nonartificial intelligence had a favourable and substantial relationship with new product success.	[61]
9.	Accounting	The continued growth of AI has provided humanity with a plethora of new and unique experiences, as well as a variety of potential future services. Artificial intelligence is an unavoidable scientific and technical outcome of human civilization, as well as a future trend in human growth. In human civilization, accounting is an important financial analytical	[67]

Table 5: Continued.

S. no	Types of impacts	Description	References
		work. Accounting's intelligentization is a microcosm of societal progress. Artificial intelligence can be used to improve financial accounting and support societal development with quicker and smarter services.	
10.	Financial management	The linked contents of AI and big data, extensively examines the growth of the financial industry, and demonstrates the application of AI and big data in the area of finance and big data. In the context of big data, a risk evaluation approach for financial information management systems. This approach creates logical nodes based on the system module and then creates a risk estimate model by looking for logical relationships between data.	[68]
11.	Financial crisis	Artificial intelligence is a technological advancement that involves the use of computer systems to do tasks that would normally need human intelligence. This was credited to artificial intelligence management's capacity, as a computer technology, to create, process, and analyze vast amounts of data at once, as opposed to when people are utilized, to assist managers in making speedy decisions because the analysis findings are accessible in real time. According to the study, financial management has a critical role in reducing risks, financial crises, and improving financial performance efficiency in a company or organization.	[69, 70]
12.	Banking	For operational and marketing factors, the present banking business is strongly reliant on technical artifacts backed by intelligent systems. However, the characteristics that enable practice between such technical interfaces and management acceptance have lagged, resulting in a knowledge gap. The paper discusses the influence of AI in financial innovation and the information safety management system (ISMS) in bank financial innovation in the span of AI. Big data, cloud computing, and other technologies have become extensively employed in business and life as a result of the continual development of numerous new internet technologies. The advancement of artificial intelligence technologies has been aided by the expansion of data size and processing capabilities.	[6, 34, 38, 48, 70–74]
13.	Financial sector	A macro view is desperately needed to examine the general nature of AI implementations and how enforcement should be handled within the new frontier of AI technology. The main parameters of the service robotics market include growth rates, volumes, and the scope of service robots, key players are identified. Researchers want to introduce the service of robots to the financial sector.	[6, 75–78]
14.	Governance framework	Because of the widespread use of robots and artificial intelligence (AI) in a variety of industries, including autodriving, healthcare, military, mass media, service sector, large sets of information searching (legal records), financial services, and new business models, both developed and emerging market economies place a high value on AI development. The revealed scientific governance-based system will be constructed under the premise of responsible research innovation, with the researcher's objective being to establish a governance framework for AI.	[79, 80]
15.	Internal audit	Artificial intelligence (AI) is a technology discipline that stands out for what it can do and the benefits it can bring to a variety of industries. Internal auditing might benefit from incorporating AI into its activities, namely, through the automation of audit procedures that make them faster and more efficient, allowing internal auditors to take on more complicated jobs. Financial fraud and economic losses have paved the way for the development of trustworthy financial big data audit methods. It will assist internal auditors in deducing frauds in a systematic manner while also improving their skills. Internal auditors must adapt to AI's new innovation in order to help firms without losing sight of their goals.	[48, 81, 82]
16.	Education sector	Some study subjects appear to have lasted the test of time as sophisticated technologies in education grow over time, while others have seen peaks and troughs. The goal of the study is to create an international standard-based cyber security system for university education. Each doctrine is recommended to be constructed as a workflow for a certain application area, consisting of modules reflecting the necessary fields of knowledge, based on the ideology of knowing areas and application areas. Through so-called adaptive learning systems, it is possible to significantly improve education by introducing dynamic principles and customization in the curriculum. Furthermore, the management of adaptation may be accomplished using artificial intelligence technologies, which the authors have expertise with in the field of cybersecurity.	[18, 83]
17.	Financial services	The current and potential consequences of artificial intelligence- (AI-) based applications, as well as technical difficulties linked to behavioral finance, are the subject of this research.	[2, 76, 84]

Table 5: Continued.

S. no	Types of impacts	Description	References
		However, the financial services industry has seen tremendous progress in the field of AI-based applications, particularly in behavioral finance.	
18.	Validation for quality of service	Based on the input data, a genetic programming-based model is recommended to assure improved customer satisfaction with services. Customers are frequently exploited and subjected to other disruptions in conventional banking and other financial institutions. To address this issue, the authors have presented an effective method for providing and ensuring high-quality services	[85]
19.	Business	Artificial intelligence (AI) is a broad category of technologies that may provide enterprises with a variety of benefits in terms of increased economic value. Following a deluge of data and a significant growth in computing capability, companies have increasingly turned to AI to create commercial value during the last several years. Business process optimization based on artificial intelligence (AI) has a substantial influence on a country's economic progress. We contend that the deployment of artificial neural networks in business processes will aid in optimizing these processes and guaranteeing the appropriate degree of functionality and compliance with the foundations of sustainable development.	[8, 86]
20.	Antimoney laundering	The state-of-the-art AI methodologies for AML, and then propose a framework for next-generation AML solutions that incorporates advanced natural language processing and deep-learning algorithms. Our methodology uses unstructured external data to help domain specialists, with the goal of reducing the human investigator's burden. The study demonstrates the disparity between traditional AML approaches and cutting-edge AI. It emphasizes fresh AI directions that can aid in the development of the AML pipeline, as well as an accessible solution with a lower false positive rate and greater flexibility.	[87, 88]
21.	Product life cycle	Artificial intelligence (AI) technology has recently received a lot of interest in the industrial industry. It attracts a lot of attention as a crucial technology in smart manufacturing and the industry 4.0 agenda. Product lifecycle management (PLM) encompasses a wide range of technical, business, and management operations that occur throughout the lifespan of a product, from the conception of an intangible notion through the disposal of a completed product.	[89]
22.	Investment in firm	Artificial intelligence (AI) has lately acquired traction and attention, resulting in a surge in interest and investment in the field. In comparison to other businesses, nonmanufacturing enterprises and firms with limited information technology skills or low credit ratings incur a more unfavourable impact. The data imply that the majority of investors consider AI investment announcements to be unpleasant news. Following that, the characteristics influencing shareholders' reactions to AI adoption are discussed.	[90]
23.	Business forecasting	The methods and tactics used to forecast company trends such as sales, expenditures, and profits are referred to as business forecasting. The goal of business forecasting is to make better strategies based on these accurate forecasts. Many firms believe that gathering knowledge about the future is critical to ensuring future organizational performance. Managers may make better judgments through improving forecasting progression. A recommendation system including graphical services, database function, reporting, interface, mathematics, and cosmological constants was created for connection recognition.	[91]
24.	Corporate governance	Corporate governance (CG) is important in a company's commitment to and adoption of ethical standards across the board, as well as in interactions with workers, customers, creditors, shareholders, and regulators. The influence of artificial intelligence's continual advancement and adaption on corporate governance. It evaluates the appropriateness, practicality, and responsibility of automating board-level decision-making to guarantee successful corporate governance using three lenses—the business, technology, and society lenses. AI can assist in freeing up government labour by automating repetitive operations, resulting in faster transactions in the delivery of government services and more correctly analyzing the effects of policy alternatives.	[60, 66, 77, 92–94]
25.	Marketing	A growing body of research on intelligent systems/artificial intelligence (AI) in marketing has revealed that AI can imitate people and perform tasks in an 'intelligent' manner. The paradigm provides systematic guidelines for how human marketers and consumers might collaborate with AI in marketing, which has substantial consequences for retailing, which serves as the interface between marketers and customers. For informed consumption decisions, marketers should optimize the mix and timing of AI-HI marketing teams, consumers should comprehend the complementarity between AI and HI capabilities, and	[95, 96]

Table 5: Continued.

S. no	Types of impacts	Description	References
		researchers can examine creative methods to and boundary conditions of collaborative intelligence.	
26.	Financial statement	Identifies the danger of severe financial irregularities occurring in the firm based on the yearly financial accounts. These anomalies might be related to many sorts of fraud that do not always influence the yearly financial accounts. The fact that anomalies are large-scale and will have a significant influence on the company's reputation is a distinguishing attribute of them.	[97]
27.	Commercial bank	In both business and society, artificial intelligence (AI) is gaining traction. The earliest uses of AI in banking were effective; nevertheless, AI is mostly used in investment banking and backend services that do not interact with customers. Using an AI-based system in commercial banks to decrease loan losses, enhance payment processing security, organize compliance-related labour, and boost customer happiness.	[88, 98]
28.	Supply chain	Quality client experiences, cost control, and a company's agility in the face of market possibilities and uncertainties are all dependent on supply chains. Companies desire speed, dependability, and traceability while keeping in mind budgetary constraints, deadlines, and inventory management. Supply chains today are substantially different from those of only a few years ago, and they are still evolving in a highly competitive environment. Technology that can cope with the rising complexity of dynamic supply chain operations is required.	[99]
29.	Data governance	Big data algorithmic systems (BDAS), which are frequently based on machine learning, neural networks, and other kinds of artificial intelligence, are made possible by the advent of big, open, and linked data (BOLD) (AI). When a result, as systems are increasingly asked to make decisions that affect individuals, communities, and society as a whole, failures cannot be allowed, and they must adhere to strict legal and ethical criteria. They all, however, rely on data that is not just large, open, and interconnected, but also diverse, dynamic, and transmitted at high rates in real time.	[100]
30.	Business and economics	The industrial age, which mankind began long ago with the invention of steam power, resulted in rudimentary automation in manufacturing. Electronics, nanotechnology, breakthroughs in medicine, health, and digital applications, among other things, have all accelerated mechatronics research in recent years. The study demonstrates that altering the way businesses are conducted via the use of innovative technologies will have new effects on day-to-day operations as well as the export of these nations' economies to the global economy. As AI and robotics improve, many substances and services related to business and economics will face serious threats, exposures, hits, change, and opportunities, such as performance, jobless ratio, management, customer relationship management, sales, strategic planning, mass production, CRM analytics GDP, purchasing power parity, inflation, money, central banks, banking system, training, accounting, taxes, coaching, and so on	[101]
31.	Cash flow	Cash flow is currently one of the most essential notions in financial analysis. Large commercial banks' financial strategy relies heavily on cash flow forecasting. Forecasting cash flow is an essential aspect of the region's cash flow management process. In the event of a forecasting error, there may be a cash shortage in one of the currencies or an overflow of bank branch vaults, necessitating additional charges for strengthening or exporting money. Many variables impact money movement, including political, economic, and geographical considerations	[102]
32.	Open data	The goal of this study is to assess the adoption of OD technology in Kuwait and to obtain company owners' perspectives on the concept's capacity to be adopted. Our strategy for getting various opinions and points of view concerning this technology was to create an online and hardcopy survey. We aimed to concentrate on the private sector, and we targeted individuals who operate a business and want to provide better services to their clients.	[103]
33.	Earnings equity	The impact of corporate social responsibility disclosure (CSRD) on earnings quality (EQ) in Gulf Cooperation Council member nations is investigated in this study (GCC). Corporate social responsibility (CSR), which has gotten a lot of attention in accounting and finance, has piqued the interest of accounting scholars. CSR has always combined social and corporate operations.	[72]
34.	Annual reports	Academics and scholars have been paying close attention to business sustainability and social responsibility in recent years. It has long been recognized that corporate financial performance is linked to, among other things, long-term corporate economic growth. All firms are encouraged to voluntarily report all aspects of their sustainability in order to	[72]

Table 5: Continued.

S. no	Types of impacts	Description	References
		improve the accountability and transparency of their operations and assist investors in properly valuing them.	
35.	Firm financing	The majority of equity issuances occur in local markets, whereas bonds and loans are typically issued globally, have long maturities, and have minimal credit risk. In comparison to worldwide norms, the Arab region's issuing corporations are quite substantial. While the sums raised in the stock and credit markets (as a percentage of GDP) are high by international standards, bond issuance activity is low. Bond finance, on the other hand, has grown in importance over time.	[73, 104]
36.	Stock market	The stock markets in the Middle East are expanding at a breakneck speed. The goal is to identify the stock markets of Bahrain, Kuwait, Oman, Qatar, Saudi Arabia, and the United Arab Emirates' market dynamics and real-time interactions. While return behavior is certainly not uniform, there is evidence of growing market integration.	[105, 106]
37.	IRFS	Recent advancements and changes in corporate governance (CG), as well as the ongoing discussion in the international accounting literature over the implementation of IFRS, have revealed a number of major deficiencies that have yet to be addressed. Many issues concerning the role of CG in the implementation of IFRS, particularly in Gulf member nations, remain unaddressed. Almost all prior research on the influence and link between CG and IFRS adoption was conducted in wealthy nations.	[94, 107]
38.	IT governance	Advancements in information and telecommunications technologies, information technology (IT) governance has become increasingly important in enterprises and organizations. IT governance has evolved into a valuable asset for every business, and it is now seen as a key to success and profit generation.	[34]
39.	Human resources management	Artificial intelligence is a true corporate innovation that will have a significant influence on how workers operate, particularly in the human resources and employment departments.	[108]

Springer Link, IEEE Xplore, and ScienceDirect. A total of 126 most relevant research articles are finalized for assessment and evaluation purposes. The description regarding final database development and relevant articles selection is descripted in Table 2.

A total of 126 research articles are finalized for the assessment and evaluation purposes. The number of articles contributed in this final pool from the selected different peer-reviewed online repositories is depicted in Figure 2.

With the passage of time, artificial intelligence has become a fascinating and appealing area for researchers all around the world. The researchers used artificial intelligence and machine learning techniques extensively in a variety of disciplines, including healthcare, tracking and navigation, internet security, and business and lucrative sectors and organizations. Based on these applications researchers used these models in financial firms to assure strong security and integrity of their personnel. Figure 3 shows the annual contribution of various research publications in the suggested subject depending on the research questions selected.

After evaluating the results shown in Figure 3, it is concluded that with passage of time, the number of research articles exponentially increases that reflects the interest of researchers in the proposed domain. After 2019, the number of publication increased abruptly that shows the interest of the organizations for ensuring high security and safety for its employees and other assets.

4. Quality Assessment

After the development of a final selection of relevant articles, the next critical step is to evaluate all of the relevant articles using the criteria that have been established [13]. For the assessment purposes in this research work, a quality criterion (QC) has defined given below:

(i) If an article fully satisfies an inevitable selected research question, then that particular paper is assigned a weighted value of 1

(ii) While if a paper fails to satisfy to answer any particular research question, it was awarded a weighted value of 0

5. Results and Analysis

The findings of this SLR study are summarized in this portion of the publication. The relevant papers, as well as their emphasized descriptions in relation to each study topic, are detailed below.

5.1. What Are the Various Types of Organizational Security Risks Faced by Employees Working within the GCC Region? This research question has outlined different security threats typically faced within the financial sectors in the GCC region [14]. In this modern technological age, dangers and consequences vary from types of threats and organizations. The prime objective of this research question is to outline

different threats reported in the extant and find out what type of new threats are available, or we face in common. Table 3 represents the list of security threats most reported in the literature.

5.2. By Utilizing AI Capabilities as Evidence, How Many Proactive Approaches Are Proposed to Counter Organizational Security Risks in the GCC Region? This research question has offered a variety of ways for securing systems within an organization by utilizing AI capabilities. The major goal of this research topic is to describe the many proactive techniques to reducing security risk. Table 4 shows a list of several sorts of security risk mitigation techniques that have been recommended for use within businesses.

5.3. Based on the Extant Findings, How Can We Improve the Capabilities of the Available Authentication Systems in the GCC Organizations? Most firms compete not only in their field of competence but also in being the leaders and innovators in the use of new applications and innovative technology. This fast growth in reliance on technology and its usage to process meaningful data has become a key audit problem for any firm [48]. In our current technology age, artificial intelligence and machine learning models have been widely proposed for a variety of research topics spanning from healthcare [49] to navigation systems [50, 51], face recognition to object detection and recognition [52, 53], and many others. The usage of mobile devices with access to vital resources is increasing, which increases the attack surface of digital assets. A smartphone or laptop can now be used to access a private company's network or data. The goal is to identify the many technologies involved in the implementations of continuous authentication, as well as the assessment methodologies and application cases [54]. This study attempts to present the recommended ways in the field of financial organization to ensure high security and authenticity, taking into account the varied applications of AI and machine learning techniques. Researchers throughout the world have presented several ways based on both deep and shallow architectures to assure high security and resist unauthorized access to security systems within businesses, and overall identification and recognition rates are comparably much better.

To tackle the low accuracy rates of multiclass issues while also reducing simulation time, the researchers focused on hybrid models (deep-deep architectures, deep-shallow architectures, and so on), in which one architecture/classifier does one task while the other performs another. This cuts down on simulation time while ensuring excellent recognition rates. Using data fusion-based hybrid deep learning models, such models are presented for face verification [55], and many others. Given the importance of hybrid models, integrating sophisticated hybrid and AI models within financial institutions is the greatest way for providing high security for clients and investors.

5.4. What Are the Social and Economic Impacts of AI on Financial Bodies Operating in the GCC Region? Artificial intelligence has a wide range of effects on our lives and has a wide range of cutting-edge applications in a variety of fields. It has reduced human labour in numerous research disciplines, such as text recognition, by offering automated applications [56, 57], network security [57], and healthcare domain [51, 58]. Table 5 represents the list of social and economical impacts of the artificial intelligence in different financial organizations.

6. Limitations

This research article has outlined 126 most relevant articles by analyzing the techniques developed to restrict unauthorized access in the organizations. Besides some key advantages, the following are the limitations of this systematic mapping:

(i) Only four most peer-reviewed research libraries are selected for the articles accumulation and downloading purposes. Though there are a massive number of online repositories exist. Still, our prime concern was to select only those extensively searched and reviewed libraries by most researchers

(ii) This SLR work is executed only for ten years, but the papers are published daily in artificial intelligence

(iii) Only published research work is selected for assessment and analysis purposes. No under-review or the work under simulations in the labs is considered for evaluation and analysis purposes

(iv) The papers are accumulated using keywords and formulated queries. So, if an article has no synonym matching the keywords, that paper was skipped during the article accumulation process. Also, if a paper has only a word relevant to artificial intelligence or machine learning, that paper was also skipped (if it fails to satisfy the selected research question or has no content pertinent to financial organizations)

7. Conclusions

AI has demonstrated exceptional skills in a variety of disciplines, including the financial and regulatory industries. Financial sectors in GCC countries are facing serious issues in terms of security, safety, and fraudulent activities as a result of the rise of information technology and smart apps. These challenges are significant roadblocks to financial companies' success, and in most situations, they result in significant losses in the form of cash loss, information theft, and so on. This work gives a systematic analysis by assessing the most relevant research publications gathered from peer-reviewed online repositories in order to address these challenges and present new future research paths for assuring high security, privacy, and safety. These articles were assessed for (1) recognizing the difficulties facing or faced by financial sector of GCC region most typically, (2) to describe the many strategies offered to address these

difficulties, as well as where these solutions fall short, (3) how artificial intelligence-based solutions have been used to handle these problems and how they may be enhanced to ensure high levels of security and authenticity, and (4) what are the social and economic importance of AI on our lives and other sectors. Based on this systematic analysis, new research directions are proposed to ensure a safe and secure environment within the organizations for both employees and the owners.

8. Implications

This article has a lot of consequences in the financial sector of GCC region. The effectiveness of many processes will be improved by applying artificial intelligence skills in financial industry. Artificial intelligence, hybrid technology, and protocols can be used to safeguard data access for employees and financial institutions. Financial businesses should make data access control a solid policy decision that supports employee honesty, justice, and equality.

Data Availability

All related data is available in the paper.

Conflicts of Interest

The authors declare that they have no conflicts of interest

Acknowledgments

The Qatar University Internal Grant no. QUHI-CBE-21/22-1 funded this publication.

References

[1] S. M. C. Loureiro, J. Guerreiro, and I. Tussyadiah, "Artificial intelligence in business: state of the art and future research agenda," *Journal of Business Research*, vol. 129, pp. 911–926, 2021.

[2] J. Lee, "Access to finance for artificial intelligence regulation in the financial services industry," *European Business Organization Law Review*, vol. 21, no. 4, pp. 731–757, 2020.

[3] M. Lu, P. Corriveau, L. Koons, and D. Boyer, "Information technology service delivery to small businesses," in *International Conference on HCI in Business*, pp. 60–67, Springer, 2014.

[4] S. Li, "Structure optimization of e-commerce platform based on artificial intelligence and blockchain technology," *Wireless Communications and Mobile Computing*, vol. 2020, 8 pages, 2020.

[5] K. AlJemy, M. AlAnazi, M. AlSofiry, and A. Baig, "Improving IoT security using blockchain," in *2019 IEEE 10th GCC Conference & Exhibition (GCC)*, pp. 1–6, Kuwait, Kuwait, 2019.

[6] I. A. Kruglova and V. A. Dolbezhkin, "Objective barriers to the implementation of blockchain technology in the financial sector," in *2018 International Conference on Artificial Intelligence Applications and Innovations (IC-AIAI)*, pp. 47–50, Nicosia, Cyprus, 2018.

[7] M. Al-Azawi, Y. Yang, and H. Istance, "Human attention-based regions of interest extraction using computational intelligence," in *2015 IEEE 8th GCC Conference & Exhibition*, pp. 1–6, Muscat, Oman, 2015.

[8] I. M. Enholm, E. Papagiannidis, P. Mikalef, and J. Krogstie, "Artificial intelligence and business value: a literature review," *Information Systems Frontiers*, pp. 1–26, 2021.

[9] M. Riikkinen, H. Saarijärvi, P. Sarlin, and I. Lähteenmäki, "Using artificial intelligence to create value in insurance," *International Journal of Bank Marketing*, vol. 36, no. 6, pp. 1145–1168, 2018.

[10] S. AlSheibani, C. Messom, and Y. Cheung, "Re-thinking the competitive landscape of artificial intelligence," in *Proceedings of the 53rd Hawaii international conference on system sciences*, Hawai, USA, 2020.

[11] S. Ransbotham, D. Kiron, P. Gerbert, and M. Reeves, "Reshaping business with artificial intelligence: closing the gap between ambition and action," *MIT Sloan Management Review*, vol. 59, 2017.

[12] T. Fountaine, B. McCarthy, and T. Saleh, "Building the AI-powered organization," *Harvard Business Review*, vol. 97, pp. 62–73, 2019.

[13] H. U. Khan, M. K. Alomari, S. Khan et al., "Systematic analysis of safety and security risks in smart homes," *CMC-Computers Materials & Continua*, vol. 68, no. 1, pp. 1409–1428, 2021.

[14] M. Al-Saidi, "Cooperation or competition? State environmental relations and the SDGs agenda in the Gulf Cooperation Council (GCC) region," *Environment and Development*, vol. 37, article 100581, 2021.

[15] H. M. Farooq and N. M. Otaibi, "Optimal machine learning algorithms for cyber threat detection," in *2018 UKSim-AMSS 20th International Conference on Computer Modelling and Simulation (UKSim)*, pp. 32–37, Cambridge, UK, 2018.

[16] R. Trifonov, O. Nakov, and V. Mladenov, "Artificial intelligence in cyber threats intelligence," in *2018 International Conference on Intelligent and Innovative Computing Applications (ICONIC)*, pp. 1–4, Mon Tresor, Mauritius, 2018.

[17] J. Link, K. Waedt, I. B. Zid, and X. Lou, "Current challenges of the joint consideration of functional safety & cyber security, their interoperability and impact on organizations: how to manage RAMS+ S (reliability availability maintainability safety+ security)," in *2018 12th International Conference on Reliability, Maintainability, and Safety (ICRMS)*, pp. 185–191, Shanghai, China, 2018.

[18] R. Trifonov, O. Nakov, S. Manolov, G. Tsochev, and G. Pavlova, "Possibilities for improving the quality of cyber security education through application of artificial intelligence methods," in *2020 International Conference Automatics and Informatics (ICAI)*, pp. 1–4, Varna, Bulgaria, 2020.

[19] B. Thuraisingham, "The role of artificial intelligence and cyber security for social media," in *2020 IEEE International Parallel and Distributed Processing Symposium Workshops (IPDPSW)*, pp. 1–3, New Orleans, LA, USA, 2020.

[20] I. H. Sarker, M. H. Furhad, and R. Nowrozy, "Ai-driven cybersecurity: an overview, security intelligence modeling and research directions," *SN Computer Science*, vol. 2, no. 3, pp. 1–18, 2021.

[21] M. Dhingra, M. Jain, and R. S. Jadon, "Role of artificial intelligence in enterprise information security: a review," in *2016 fourth international conference on parallel, distributed and grid computing (PDGC)*, pp. 188–191, Waknaghat, India, 2016.

[22] Y. XIao-yang, "Study on development of information security and artificial intelligence," in *2011 Fourth International Conference on Intelligent Computation Technology and Automation*, pp. 248–250, Shenzhen, China, 2011.

[23] N. Mavridis, G. Pierris, C. BenAbdelkader, A. Krstikj, and C. Karaiskos, "Smart buildings and the human-machine cloud," in *2015 IEEE 8th GCC Conference & Exhibition*, pp. 1–6, Muscat, Oman, 2015.

[24] Y. Zhen, A. Khan, S. Nazir, Z. Huiqi, A. Alharbi, and S. Khan, "Crowdsourcing usage, task assignment methods, and crowdsourcing platforms: a systematic literature review," *Journal of Software: Evolution and Process*, vol. 33, no. 8, article e2368, 2021.

[25] B. Kitchenham, "Guidelines for performing systematic literature reviews in software engineering," Tech. Rep. EBSE-2007-01, 2007, Softw. Eng. Group School Comput. Sci. Math. Keele Univ., Keele, U.K. and Dept. of Comput. Sci. Univ. Durham, Durham, U.K, 2007.

[26] A. Mishra and P. Yadav, "Anomaly-based IDS to detect attack using various artificial intelligence & machine learning algorithms: a review," in *2nd International Conference on Data, Engineering and Applications (IDEA)*, pp. 1–7, Bhopal, India, 2020.

[27] B. Daya, *Network Security: History, Importance, and Future*, vol. 4, University of Florida Department of Electrical and Computer Engineering, 2013.

[28] J. H. Li, "Cyber security meets artificial intelligence: a survey," *Frontiers of Information Technology & Electronic Engineering*, vol. 19, no. 12, pp. 1462–1474, 2018.

[29] B. Alhayani, H. J. Mohammed, I. Z. Chaloob, and J. S. Ahmed, "Effectiveness of artificial intelligence techniques against cyber security risks apply of IT industry," *Materials Today: Proceedings*, 2021.

[30] B. D. Deebak and A.-T. Fadi, "Privacy-preserving in smart contracts using blockchain and artificial intelligence for cyber risk measurements," *Journal of Information Security and Applications*, vol. 58, article 102749, 2021.

[31] Y. Peng and Q. Wu, "Secure communication and access control for web services container," in *2006 Fifth International Conference on Grid and Cooperative Computing (GCC'06)*, pp. 412–415, Hunan, China, 2006.

[32] A. K. Alharam and W. Elmedany, "The effects of cybersecurity on healthcare industry," in *2017 9th IEEE-GCC Conference and Exhibition (GCCCE)*, pp. 1–9, Manama, Bahrain, 2017.

[33] P. Xie, J. H. Li, X. Ou, P. Liu, and R. Levy, "Using Bayesian networks for cyber security analysis," in *2010 IEEE/IFIP International Conference on Dependable Systems & Networks (DSN)*, pp. 211–220, Chicago, IL, 2010.

[34] Y. Alansari and A. M. A. Musleh Al-Sartawi, "IT governance and E-banking in GCC listed banks," *Procedia Computer Science*, vol. 183, pp. 844–848, 2021.

[35] H. Sato, "A new formula of security risk analysis that takes risk improvement factor into account," in *2011 IEEE Third International Conference on Privacy, Security, Risk and Trust and 2011 IEEE Third International Conference on Social Computing*, pp. 1243–1248, Boston, MA, USA, 2011.

[36] S. Erokhin, "Artificial intelligence for information security," in *2020 Systems of Signals Generating and Processing in the Field of on Board Communications*, pp. 1–4, Moscow, Russia, 2020.

[37] Y. A. Basallo, V. E. Senti, and N. M. Sanchez, "Artificial intelligence techniques for information security risk assessment," *IEEE Latin America Transactions*, vol. 16, no. 3, pp. 897–901, 2018.

[38] X. Hu and K. Wang, "Bank financial innovation and computer information security management based on artificial intelligence," in *2020 2nd international conference on machine learning, Big Data and Business Intelligence (MLBDBI)*, pp. 572–575, Taiyuan, China, 2020.

[39] A. Guzman, S. Ishida, E. Choi, and A. Aoyama, "Artificial intelligence improving safety and risk analysis: a comparative analysis for critical infrastructure," in *2016 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM)*, pp. 471–475, Bali, Indonesia, 2016.

[40] U. Kose and P. Vasant, "Fading intelligence theory: a theory on keeping artificial intelligence safety for the future," in *2017 International Artificial Intelligence and Data Processing Symposium (IDAP)*, pp. 1–5, Malatya, Turkey, 2017.

[41] S. Srivastava, A. Bisht, and N. Narayan, "Safety and security in smart cities using artificial intelligence—a review," in *2017 7th International Conference on Cloud Computing, Data Science & Engineering-Confluence*, pp. 130–133, Noida, India, 2017.

[42] K. Rindell and J. Holvitie, "Security risk assessment and management as technical debt," in *2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*, pp. 1–8, Oxford, UK, 2019.

[43] D. Dai and S. Boroomand, "A review of artificial intelligence to enhance the security of big data systems: state-of-art, methodologies, applications, and challenges," *Archives of Computational Methods in Engineering*, vol. 29, no. 2, pp. 1291–1309, 2022.

[44] E. V. Odisho and D. Truong, "Applying machine learning to enhance runway safety through runway excursion risk mitigation," in *2021 Integrated Communications Navigation and Surveillance Conference (ICNS)*, pp. 1–10, Dulles, VA, USA, 2021.

[45] W. Abbass, A. Baina, and M. Bellafkih, "Improvement of information system security risk management," in *2016 4th IEEE International Colloquium on Information Science and Technology (CiSt)*, pp. 182–187, Tangier, Morocco, 2016.

[46] M. Amini, S. Salimi, F. Yousefinejad, M. J. Tarokh, and S. M. Haybatollahi, "The implication of business intelligence in risk management: a case study in agricultural insurance," *Journal of Data, Information and Management*, vol. 3, no. 2, pp. 155–166, 2021.

[47] X. Shang and C. Zhao, "Research on the application of artificial intelligence in computer network technology," in *2020 5th international conference on mechanical, Control and Computer Engineering (ICMCCE)*, pp. 1107–1110, Harbin, China, 2020.

[48] A. A. Lawati and S. Ali, "Business perception to learn the art of operating system auditing: a case of a local bank of Oman," in *2015 IEEE 8th GCC Conference & Exhibition*, pp. 1–6, Muscat, Oman, 2015.

[49] R. Alshamsan, H. Leslie, A. Majeed, and M. Kruk, "Financial hardship on the path to universal health coverage in the Gulf states," *Health Policy*, vol. 121, no. 3, pp. 315–320, 2017.

[50] K. Zhu and T. Zhang, "Deep reinforcement learning based mobile robot navigation: a review," *Tsinghua Science and Technology*, vol. 26, no. 5, pp. 674–691, 2021.

[51] S. P. Singh, L. Wang, S. Gupta, B. Gulyas, and P. Padmanabhan, "Shallow 3D CNN for detecting acute brain hemorrhage from medical imaging sensors," *IEEE Sensors Journal*, vol. 21, no. 13, pp. 14290–14299, 2021.

[52] W. AbdAlmageed, Y. Wu, S. Rawls et al., "Face recognition using deep multi-pose representations," in *2016 IEEE winter conference on applications of computer vision (WACV)*, pp. 1–9, Lake Placid, NY, USA, 2016.

[53] M. Yasir, M. S. Hossain, S. Nazir, S. Khan, and R. Thapa, "Object identification using manipulated edge detection techniques," *Science*, vol. 3, no. 1, pp. 1–6, 2022.

[54] J. Junquera-Sánchez, C. Cilleruelo, L. De-Marcos, and J.-J. Martinez-Herráiz, "Access control beyond authentication," *Security and Communication Networks*, vol. 2021, 11 pages, 2021.

[55] Y. Sun, X. Wang, and X. Tang, "Hybrid deep learning for face verification," in *Proceedings of the IEEE international conference on computer vision*, pp. 1489–1496, Sydney, NSW, Australia, 2013.

[56] D. Coquenet, C. Chatelain, and T. Paquet, "End-to-end handwritten paragraph text recognition using a vertical attention network," *Institute of Electrical and Electronics Engineers transactions on pattern analysis and machine intelligence*, p. 1, 2022.

[57] J. H. Lee, T. Ernst, and N. Chilamkurti, "Performance analysis of PMIPv6-based network mobility for intelligent transportation systems," *IEEE Transactions on Vehicular Technology*, vol. 61, no. 1, pp. 74–85, 2012.

[58] H. Chen, S. Khan, B. Kou, S. Nazir, W. Liu, and A. Hussain, "A smart machine learning model for the detection of brain hemorrhage diagnosis based internet of things in smart cities," *Complexity*, vol. 2020, Article ID 3047869, 2020.

[59] D. Choi and K. Lee, "An artificial intelligence approach to financial fraud detection under IoT environment: a survey and implementation," *Security and Communication Networks*, vol. 2018, Article ID 5483472, 2018.

[60] H.-A. N. Al-Malkawi, R. Pillai, and M. I. Bhatti, "Corporate governance practices in emerging markets: the case of GCC countries," *Economic Modelling*, vol. 38, pp. 133–141, 2014.

[61] H. Jianjun, Y. Yao, J. Hameed et al., "The role of artificial and nonartificial intelligence in the new product success with moderating role of new product innovation: a case of manufacturing companies in China," *Complexity*, vol. 2021, Article ID 8891298, 2021.

[62] H. Jia, "Deep learning algorithm-based financial prediction models," *Complexity*, vol. 2021, Article ID 5560886, 2021.

[63] J. Zhang, "Development of internet supply chain finance based on artificial intelligence under the enterprise green business model," *Mathematical Problems in Engineering*, vol. 2021, Article ID 9947811, 2021.

[64] W. Xie, "Interbank offered rate based on artificial intelligence algorithm," *Mathematical Problems in Engineering*, vol. 2021, Article ID 9931539, 2021.

[65] Z. Chen, "Research on accounting intelligence system modeling of financial performance evaluation," *Security and Communication Networks*, vol. 2021, Article ID 5550382, 2021.

[66] W. M. Al-ahdal, M. H. Alsamhi, M. I. Tabash, and N. H. S. Farhan, "The impact of corporate governance on financial performance of Indian and GCC listed firms: an empirical investigation," *Research in International Business and Finance*, vol. 51, article 101083, 2020.

[67] Z. Li, "Analysis on the influence of artificial intelligence development on accounting," in *2020 International conference on big data, Artificial Intelligence and Internet of Things Engineering (ICBAIE)*, pp. 260–262, Fuzhou, China, 2020.

[68] N. Wang, Y. Liu, Z. Liu, and X. Huang, "Application of artificial intelligence and big data in modern financial management," in *2020 International Conference on Artificial Intelligence and Education (ICAIE)*, pp. 85–87, Tianjin, China, 2020.

[69] V. K. Shah, "Artificial intelligence management in financial crisis," in *2015 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC)*, pp. 1–6, Madurai, India, 2015.

[70] F. Alqahtani and D. G. Mayes, "Financial stability of Islamic banking and the global financial crisis: evidence from the Gulf Cooperation Council," *Economic Systems*, vol. 42, no. 2, pp. 346–360, 2018.

[71] R. Arjun, A. Kuanr, and K. Suprabha, "Developing banking intelligence in emerging markets: systematic review and agenda," *International Journal of Information Management Data Insights*, vol. 1, article 100026, 2021.

[72] M. K. Al Ani, "Corporate social responsibility disclosure and financial reporting quality: evidence from Gulf Cooperation Council countries," *Borsa Istanbul Review*, vol. 21, pp. S25–S37, 2021.

[73] R. Al-Khouri and H. Arouri, "The simultaneous estimation of credit growth, valuation, and stability of the Gulf Cooperation Council banking industry," *Economic Systems*, vol. 40, no. 3, pp. 499–518, 2016.

[74] S. Srairi, "Transparency and bank risk-taking in GCC Islamic banking," *Borsa Istanbul Review*, vol. 19, pp. S64–S74, 2019.

[75] A. V. Bataev, N. Dedyukhina, and M. N. Nasrutdinov, "Innovations in the financial sphere: performance evaluation of introducing service robots with artificial intelligence," in *2020 9th International Conference on Industrial Technology and Management (ICITM)*, pp. 256–260, Oxford, UK, 2020.

[76] M. Shanmuganathan, "Behavioural finance in an era of artificial intelligence: longitudinal case study of robo-advisors in investment decisions," *Journal of Behavioral and Experimental Finance*, vol. 27, article 100297, 2020.

[77] A. A.-N. Abdallah, M. K. Hassan, and P. L. McClelland, "Islamic financial institutions, corporate governance, and corporate risk disclosure in Gulf Cooperation Council countries," *Journal of Multinational Financial Management*, vol. 31, pp. 63–82, 2015.

[78] A. Maghyereh and H. Abdoh, "The effect of structural oil shocks on bank systemic risk in the GCC countries," *Energy Economics*, vol. 103, article 105568, 2021.

[79] H. Zhang and L. Gao, "Shaping the governance framework towards the artificial intelligence from the responsible research and innovation," in *2019 IEEE International Conference on Advanced Robotics and its Social Impacts (ARSO)*, pp. 213–218, Beijing, China, 2019.

[80] P. G. R. de Almeida, C. D. dos Santos, and J. S. Farias, "Artificial intelligence regulation: a framework for governance," *Ethics and Information Technology*, vol. 23, pp. 1–21, 2021.

[81] B. Couceiro, I. Pedrosa, and A. Marini, "State of the art of artificial intelligence in internal audit context," in *2020 15th Iberian Conference on Information Systems and Technologies (CISTI)*, pp. 1–7, Seville, Spain, 2020.

[82] Z. Zhang and Z. Wang, "Design of financial big data audit model based on artificial neural network," *International Journal of Systems Assurance Engineering and Management*, pp. 1–10, 2021.

[83] C. Guan, J. Mou, and Z. Jiang, "Artificial intelligence innovation in education: a twenty-year data-driven historical analysis," *International Journal of Innovation Studies*, vol. 4, no. 4, pp. 134–147, 2020.

[84] J. Y. Huang, A. Gupta, and M. Youn, "Survey of EU ethical guidelines for commercial AI: case studies in financial services," *AI and Ethics*, vol. 1, no. 4, pp. 569–577, 2021.

[85] M. Castelli, L. Manzoni, and A. Popovič, "An artificial intelligence system to predict quality of service in banking organizations," *Computational Intelligence and Neuroscience*, vol. 2016, Article ID 9139380, 2016.

[86] K. A. Rashedi, M. T. Ismail, N. N. Hamadneh, S. A. Wadi, J. J. Jaber, and M. Tahir, "Application of radial basis function neural network coupling particle swarm optimization algorithm to classification of Saudi Arabia stock returns," *Journal of Mathematics*, vol. 2021, Article ID 5593705, 2021.

[87] J. Han, Y. Huang, S. Liu, and K. Towey, "Artificial intelligence for anti-money laundering: a review and extension," *Digital Finance*, vol. 2, no. 3-4, pp. 211–239, 2020.

[88] M. Turki, A. Hamdan, R. T. Cummings, A. Sarea, M. Karolak, and M. Anasweh, "The regulatory technology "RegTech" and money laundering prevention in Islamic and conventional banking industry," *Heliyon*, vol. 6, no. 10, article e04949, 2020.

[89] L. Wang, Z. Liu, A. Liu, and F. Tao, "3D printing of aluminum alloys using laser powder deposition: a review," *The International Journal of Advanced Manufacturing Technology*, vol. 116, no. 1-2, pp. 1–37, 2021.

[90] A. K. Lui, M. C. Lee, and E. W. Ngai, "Impact of artificial intelligence investment on firm value," *Annals of Operations Research*, vol. 308, no. 1-2, pp. 373–388, 2022.

[91] B. Li, C. Yao, F. Zheng, L. Wang, J. Dai, and Q. Xiang, "Intelligent decision support system for business forecasting using artificial intelligence," *Arabian Journal for Science and Engineering*, pp. 1–11, 2021.

[92] M. Hilb, "Toward artificial governance? The role of artificial intelligence in shaping the future of corporate governance," *Journal of Management and Governance*, vol. 24, no. 4, pp. 851–870, 2020.

[93] G. D. Sharma, A. Yadav, and R. Chopra, "Artificial intelligence and effective governance: a review, critique and research agenda," *Sustainable Futures*, vol. 2, article 100004, 2020.

[94] F. A. Almaqtari, A. A. Hashed, and M. Shamim, "Impact of corporate governance mechanism on IFRS adoption: a comparative study of Saudi Arabia, Oman, and the United Arab Emirates," *Heliyon*, vol. 7, no. 1, article e05848, 2021.

[95] M.-H. Huang and R. T. Rust, "A framework for collaborative artificial intelligence in marketing," *Journal of Retailing*, 2021.

[96] B. Vlačić, L. Corbo, S. C. e Silva, and M. Dabić, "The evolving role of artificial intelligence in marketing: a review and research agenda," *Journal of Business Research*, vol. 128, pp. 187–203, 2021.

[97] J. Wyrobek, "Application of machine learning models and artificial intelligence to analyze annual financial statements to identify companies with unfair corporate culture," *Procedia Computer Science*, vol. 176, pp. 3037–3046, 2020.

[98] F. Königstorfer and S. Thalmann, "Applications of artificial intelligence in commercial banks - a research agenda for behavioral finance," *Journal of Behavioral and Experimental Finance*, vol. 27, article 100352, 2020.

[99] Y. Riahi, T. Saikouk, A. Gunasekaran, and I. Badraoui, "Artificial intelligence applications in supply chain: a descriptive bibliometric analysis and future research directions," *Expert Systems with Applications*, vol. 173, article 114702, 2021.

[100] M. Janssen, P. Brous, E. Estevez, L. S. Barbosa, and T. Janowski, "Data governance: organizing data for trustworthy artificial intelligence," *Government Information Quarterly*, vol. 37, no. 3, article 101493, 2020.

[101] C. Dirican, "The impacts of robotics, artificial intelligence on business and economics," *Procedia-Social and Behavioral Sciences*, vol. 195, pp. 564–573, 2015.

[102] K. Dadteev, B. Shchukin, and S. Nemeshaev, "Using artificial intelligence technologies to predict cash flow," *Procedia Computer Science*, vol. 169, pp. 264–268, 2020.

[103] N. Alawadhi, I. Al Shaikhli, A. Alkandari, and S. K. Chab, "Business owners' feedback toward adoption of open data: a case study in Kuwait," *Journal of Electrical and Computer Engineering*, vol. 2021, Article ID 6692410, 2021.

[104] J. J. Cortina, S. Ismail, and S. L. Schmukler, "Firm financing and growth in the Arab region," *Economic Systems*, vol. 42, no. 2, pp. 361–383, 2018.

[105] J. Bley and K. H. Chen, "Gulf Cooperation Council (GCC) stock markets: the dawn of a new era," *Global Finance Journal*, vol. 17, no. 1, pp. 75–91, 2006.

[106] N. T. Hung, "Financial connectedness of GCC emerging stock markets," *Economic Review*, vol. 11, no. 4, pp. 753–773, 2021.

[107] M. Abdelqader, K. Nimer, and T. K. Darwish, "IFRS compliance in GCC countries: do corporate governance mechanisms make a difference?," *International Journal of Disclosure and Governance*, vol. 18, no. 4, pp. 411–425, 2021.

[108] M. M. Abdeldayem and S. H. Aldulaimi, "Trends and opportunities of artificial intelligence in human resource management: aspirations for public sector in Bahrain," *International Journal of Scientific and Technology Research*, vol. 9, pp. 3867–3871, 2020.