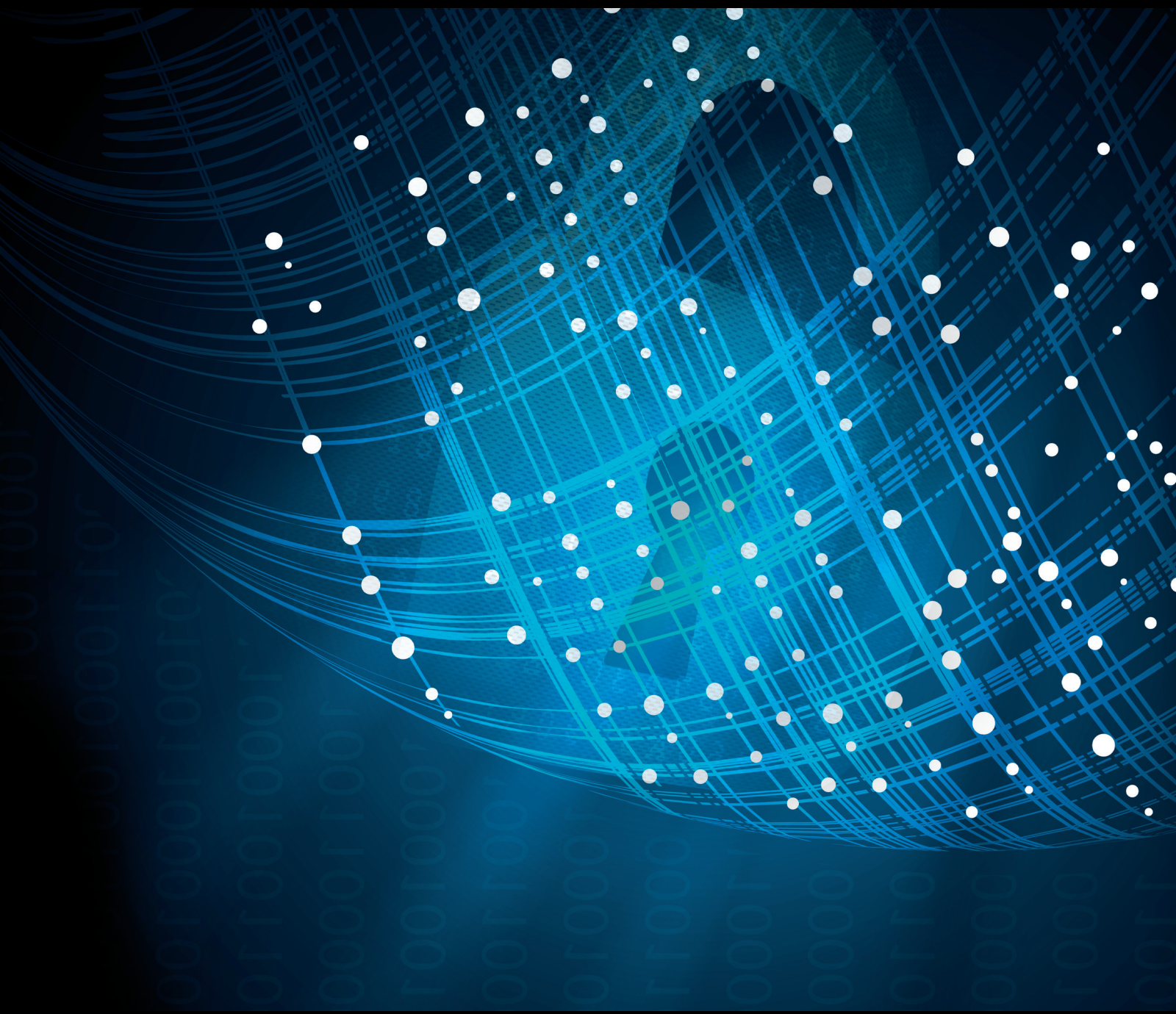
Security and Communication Networks

Blockchain-Assisted Secure Smart Cities Communication

Lead Guest Editor: Rabie A. Ramadan
Guest Editors: Bhisham Sharma, Rashid Ali, and Sung W. Kim



Blockchain-Assisted Secure Smart Cities Communication

Security and Communication Networks

Blockchain-Assisted Secure Smart Cities Communication

Lead Guest Editor: Rabie A. Ramadan
Guest Editors: Bhisham Sharma, Rashid Ali, and Sung W. Kim

Contents

Hindawi
Security and Communication Networks
Volume 2024, Article ID 9826070, 1 page
https://doi.org/10.1155/2024/9826070

Retraction

Retracted: An IoT-Enabled Intelligent and Secure Manufacturing Model Using Blockchain in Hybrid Cloud Communication System

Security and Communication Networks

Received 8 January 2024; Accepted 8 January 2024; Published 9 January 2024

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope

(2) Discrepancies in the description of the research reported

(3) Discrepancies between the availability of data and the research described

(4) Inappropriate citations

(5) Incoherent, meaningless and/or irrelevant content included in the article

(6) Manipulated or compromised peer review

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] S. Bhattacharyya, S. Athithan, S. Pal et al., "An IoT-Enabled Intelligent and Secure Manufacturing Model Using Blockchain in Hybrid Cloud Communication System," *Security and Communication Networks*, vol. 2023, Article ID 7556728, 12 pages, 2023.

Hindawi
Security and Communication Networks
Volume 2023, Article ID 9763845, 1 page
https://doi.org/10.1155/2023/9763845

Retraction

Retracted: Practical Research on College English Teaching Mode Reform Based on Computer Multimedia

Security and Communication Networks

Received 8 August 2023; Accepted 8 August 2023; Published 9 August 2023

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope
(2) Discrepancies in the description of the research reported
(3) Discrepancies between the availability of data and the research described
(4) Inappropriate citations
(5) Incoherent, meaningless and/or irrelevant content included in the article
(6) Peer-review manipulation

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] Z. Yang, "Practical Research on College English Teaching Mode Reform Based on Computer Multimedia," *Security and Communication Networks*, vol. 2022, Article ID 7110400, 9 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2024, Article ID 9826070, 1 page
https://doi.org/10.1155/2024/9826070

Retraction

Retracted: An IoT-Enabled Intelligent and Secure Manufacturing Model Using Blockchain in Hybrid Cloud Communication System

Security and Communication Networks

Received 8 January 2024; Accepted 8 January 2024; Published 9 January 2024

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope

(2) Discrepancies in the description of the research reported

(3) Discrepancies between the availability of data and the research described

(4) Inappropriate citations

(5) Incoherent, meaningless and/or irrelevant content included in the article

(6) Manipulated or compromised peer review

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] S. Bhattacharyya, S. Athithan, S. Pal et al., "An IoT-Enabled Intelligent and Secure Manufacturing Model Using Blockchain in Hybrid Cloud Communication System," *Security and Communication Networks*, vol. 2023, Article ID 7556728, 12 pages, 2023.

Hindawi
Security and Communication Networks
Volume 2023, Article ID 7556728, 12 pages
https://doi.org/10.1155/2023/7556728

Research Article

An IoT-Enabled Intelligent and Secure Manufacturing Model Using Blockchain in Hybrid Cloud Communication System

Sudipto Bhattacharyya,[1] **Senthil Athithan**,[2] **Souvik Pal**,[3,4] **Bikramjit Sarkar**,[5] **D. Akila**,[6] **Subrata Chowdhury**,[7] **Karthik Chandran**,[8] **and Saravanakumar Gurusamy**[9]

[1]*Department of Computer Science and Engineering, Global Institute of Management and Technology, Krishnagar, India*
[2]*Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Andhra Pradesh, India*
[3]*Department of Computer Science and Engineering, Sister Nivedita University, Kolkata, India*
[4]*Sambalpur University, Sambalpur, India*
[5]*Department of Computer Science and Engineering, JIS College of Engineering, Kalyani, India*
[6]*Department of Computer Applications, Saveetha College of Liberal Arts and Sciences, SIMATS Deemed University, Chennai, India*
[7]*Department of Computer Science and Engineering, Sreenivasa Institute of Technology and Management Studies, Chittoor, Andra Pradesh, India*
[8]*Department of Robotics and Automation, Jyothi Engineering College, Thrissur, Kerala, India*
[9]*Department of Electrical and Electronics Technology, Federal TVET Institute, Addis Ababa, Ethiopia*

Correspondence should be addressed to Subrata Chowdhury; subratachowdhury@svcet.in and Saravanakumar Gurusamy; saravanakumar.gurusamy@etu.edu.et

Received 27 July 2022; Revised 8 September 2022; Accepted 18 April 2023; Published 1 June 2023

Academic Editor: Andrea Michienzi

The smart manufacturing system can become a linked network with the help of the Internet of Things (IoT). Devices connected to the IoT are susceptible to various attacks and assaults. An effective protection plan is needed to ensure that the billions of IoT nodes are protected from these hazards. The security mechanisms on IoT devices are ineffective due to resource limitations. As a result, the academic community has recently paid attention to the cloud-, fog-, and edge-based IoT systems. A robust cloud provider is in the cloud or fog to perform computationally demanding activities, including safety, data analysis, decision-making process, and monitoring. Hash identities and upgraded Rivest–Shamir–Adleman (RSA) have been used to secure the IoT device's data. A four-prime integer of 512 bits makes up the proposed security algorithm. A hash signature is used to provide device authentication. An effective clustering method for sensing devices based on the node level, separation from the clusters, remaining energy, and fitness has been presented for long network life. The suggested swarm-based method determines the sensor nodes' fitness. A deep neural network- (DNN-) based resource scheduling algorithm (DNN-RSM) is meant to reduce the delay and communications overhead for IoT components in the hybrid cloud system. For optimum resource allocation, all queries originating from the cluster head are categorised using DNN based on their storage, processing, and bandwidth needs. The suggested structure delivers better outcomes, particularly regarding energy use, delay, and safety level. The results of the simulation provide credence to the concept that the proposed strategy is superior to the current system. The suggested scheme includes stringent security, decreased energy usage, decreased latency, and efficient resource utilization.

1. Introduction to Smart Manufacturing

The emergence of new generation storage innovations, such as cloud computing (CC), the Internet of Things (IoT), big data analytics (BDA), artificial intelligence (AI), and cyber-physical systems (CPS) has a significant impact on the industry and helps to drive improvements in productivity, cost-effectiveness, and production intellect [1]. A smart factory strives for greater intelligence through low-cost, omnipresent sensing, cutting-edge computation and computational modelling, and cyber-physical connectivity. Smart factories inevitably involve the fusion of numerous advanced and networked machines and gadgets.

In addition, the growing prevalence of IoT offers exciting chances to develop robust industrial software and applications [2]. This connected equipment, sensor, etc., produce a significant amount of varied information content [3]. This data must be cleansed, saved, and processed to create the data and insights that serve as the foundation for a smart factory [4]. However, the continuous explosion of digital exceeds users' typical processing capacities. In many situations, considerable systems have to cope with the information explosion addressed by cloud technology [5]. With the support of industry clouds, businesses may digitally transform by gaining access to prebuilt tools, workflows, and data models designed to address the unique challenges faced by their sector. Cloud technology is Internet computation where available resources (such as software, information, services, and storing and computing capacity) can be accessed and utilised as needed in a simple "pay-as-you-go" fashion [6]. Users receive high-quality solutions at a lower cost in the cloud computing environment.

This computing architecture is known as cloud computing, and it aims to increase the cloud's capacity for storing, processing, and networking at the network's periphery. When a network is in use and sophisticated traffic is transported to a data centre, time delays are minimised through cloud computing.

The virtualised thin layer, situated among end customers and the environment of cloud data centres, is a component of fog computing [7]. The cloud and fog-based approaches have many benefits, including decreased latency, networking congestion, and energy efficiency. The distribution of wealth and job scheduling are significant benefits [8]. Cloud computing enables the processes to match the needs of the clients with some of the best-suited resources [9]. The technologies can be regulated in the optimum way to hit assets for the duties of the application because they are involved in task assignment; this would not go far beyond the minimal defined times aimed at fulfilling the quality of service (QoS) requirements of the IoT device [10, 11]. This enhances the effectiveness of cloud computing and helps to implement the scheduling and load balancing tasks. Making sure that technology is around for a long time allows you to get the most use out of your products and services by keeping them in production for as long as possible. Because of our worldwide reach, companies are able to offer technical help during normal business hours, shorten delivery times, and cater to individual client needs.

Fog computing distributes the assets to benefit the devices due to the wide range of demands put on IoT nodes [12]. Its goal is to find the best resources for IoT nodes so that the most important planning goals can be met, such as reducing process delays and using resources better. In addition, this necessitates the development of reliable and secure systems in IoT nodes. So, getting real-world results from the computer system of the cloud network about how resources are used and how simulations work is of the utmost practical importance. Here, the experimental setup and tools were implemented using JAVA and NS3 to test and evaluate the model.

The following are the achievements of this job:

(i) First, the IoT's data protection has been ensured using enhanced RSA and hashing signature.

(ii) The second method is for grouping embedded sensors, predicated on efficiency, remaining energy, sensor network degree, and proximity from the member nodes.

(iii) With (DNN-RSM), the hybrid cloud's IoT parts will have less latency and connectivity burden.

(iv) The third method is the area and bandwidth categorisation using SoftMax-DNN for optimal resource planning based on storage and processing.

(v) The simulation's outcomes support the idea that using the suggested technique is preferable to using the current methods. The proposed plan features strict protection, reduced energy consumption, reduced latency, and effective resource utilisation.

The remainder of the article is listed as follows: the background to intelligent manufacturing and IoT is illustrated in Section 2. Section 3 proposes and creates a deep neural network-based resource scheduling algorithm (DNN-RSM) system, and the mathematical relations are shown. The simulation outcomes, the findings, and comparison study of the proposed method are illustrated in Section 4. Section 5 indicates the conclusion and the future study of the proposed system.

2. Background to the Intelligent Manufacturing and IoT Systems

Numerous researches have been conducted to provide adequate resources for an organisation's networking and safety. For example, Porkodi et al. have concentrated on identifying duplicate jobs capable of lowering the cloud server's memory space and delay [13]. Information has been encrypted using the edge cloud computing-based management method to increase data security. Research on scheduling algorithms in a cloud environment is also presented. The investigators have suggested the optimization method for grouping the resources in the cloud to suit the source. The best aspects of fuzzy clustering and swarm optimisation are combined to guarantee that allocating resources is optimal. The simulation's outcome shows an adequate distribution of resources.

To enable the exchange of information in Distributed systems, Bu et al. devised and modelled a secure and trustworthy model [14]. The IoT devices are collaboratively retrieving the data via threshold-based ciphertext, separating the information into portions to be saved on the Internet. Task scheduling in the cloud environment has been proposed by

Bhatia et al. in a different work as a quantised system [15]. The node processing index was a node-specific indicator for gauging the fog system's amount of computation. The authors' work has been compared to existing algorithms and is superior, according to their analysis. Fog nodes are the building blocks of a fog network and are comprised of one or more physical devices that can perform processing and sensing tasks.

With the use of a hashed Needham–Schroeder (HNS) cost-optimized deep machine learning (CODML) method, Alzubi et al. have developed a plan to provide safety for IoT data transmission via cloud services, demonstrating the necessity of delivering IoT security [16]. To eliminate long operational latencies and measure expenses while staying within the constraints of money and workforce, Gazori et al. have provided a task scheduling system for IoT applications [17]. For scheduling algorithm strategies, the authors developed a dual deep Q-learning. The assessment shows that the proposed algorithm has outperformed other basic methods in terms of delay, measurement expenses, energy usage, and task accomplishment. It also handles single-point failure together with issues of task scheduling.

In addition, Sun et al. created a fog-cloud-enabled Internet of Things architecture that takes advantage of the most significant aspects of both fog and edge nodes [18]. An efficient method has been used to reduce energy usage and finish applications. The authors have presented numerical simulations that can reduce energy consumption and fast response. However, there is no mention of data protection in this study. In a different study, Wang et al. aggregated the shared resources of fog devices into a group with enough computing power to manage the distribution of a challenging task [19]. Authors have implemented a multichannel information planning technique to reduce real-time network congestion and improve system reliability. Simulation findings show that the ideal data routing approach for performance gains can be made in different situations.

2.1. Problems and Shortages. The cloud-based manufacturer frees producers and consumers from many details while allowing for increased utilisation without raising costs or performance degradation. However, the growth of smart factories is still constrained by several issues.

(1) A bandwidth overflow. Data produced by diverse manufacturing assets that are dispersed worldwide are expanding rapidly. The cloud, where information processing is carried out, receives these data across the network [20]. High infrastructure is required because of the rising volume and speed of information, which is quite expensive. Some accidental deletions are possible when the connection is severely congested.

(2) Unavailability. The user is significantly dependent on the supply of a network connection and the computers, even though the data saved in the clouds can be viewed anywhere at any time [21]. The capacity of the cloud is useless if the information collected from the network is down.

(3) Latency. Time synchronisation is necessary for specific real-time and simultaneous settings, which causes real-time problems [22]. Unacceptable online round-trip delay, spanning tens to several hundred milliseconds, occurs during data transfer between endpoints and the clouds.

(4) Validity of the data. Many useless data, such as redundant information, background noise, and transient data are sent to the cloud, wasting resources [23]. In addition, specific locally used data does not require transmission to the cloud. However, the ability to filter data has not received enough attention.

(5) Privacy and security. Various security challenges arise from the ongoing emergence of new threat vectors (such as those originating from messaging services and denial-of-service (DoS) assaults) [24]. In addition, when all the information is sent to the network, they also include private information, which raises the possibility of user privacy being compromised [25].

(6) Ineffective communication. The flexibility and effectiveness of connection and active messaging are limited by cloud-based communications between producers, customers, and nearby machines [26]. Some businesses have communication problems, which lead to tension, hostility, and confusion between workers. When there is a breakdown in communication, it can lead to an uncomfortable atmosphere where no one wants to work together or contribute.

The lack of supply chain monitoring and risk management is a contributing factor to the lack of preparedness of organizations to deal with the supply chain problem. Companies can gain insight into their supply chains and be better prepared for slowdowns by strengthening relationships with their suppliers and working together with them. In recent years, smart manufacturing technologies have assisted several companies in meeting the ongoing challenge of supply chain monitoring. The Internet of Things (IoT) and other sensors are being used to create a more intelligent supply chain.

Dwivedi et al. [27] introduced the scalable blockchain distributed network, and the use of such platforms has presented new difficulties for actual deployment, such as the viral transmission of unfounded material with harmful purposes. By identifying the source of false information being disseminated online, this innovative approach has the potential to reduce the epidemic.

Dhar et al. [28] invented advanced security model for multimedia data sharing in Internet of Things resolving the privacy and scalability concerns while increasing the delay experienced by users. Finally, they conduct a security analysis of the proposed system and find that it has the ability to address the majority of vulnerabilities observed in existing systems.

Srivastava et al. [29] proposed blockchain technology in the security of Internet of Things (IoT). The article outlines the advantages of employing IoT devices for remote patient

monitoring and the challenges that blockchain-based security solutions face in practice. The study also provides an assessment of many cryptographic systems that may be useful for IoT implementation.

Because of these inherent issues, some applications that require a real-time, sensitive, and exact reaction to things cannot rely only on the cloud, given the extensive use of cloud technology in smart factories. Some latest innovations are anticipated, considering the current state of industrial automation.

3. Deep Neural Network-Based Resource Scheduling Algorithm (DNN-RSM)

This research suggests using SoftMax and an enhanced RSA method to schedule bandwidth, group sensor networks securely, and securely transmit IoT data. At the moment, cloud-based manufacturing (CBM) technology is the foundation of the majority of industrial automation. This architecture allows users to quickly configure and manage assets with the least effort and third-party contact. Users can use the shared resource of production resources from anyone at any time. The centralised architecture is highly vulnerable. In other words, all operations are stopped once the significant factor is broken. Therefore, this research aims to create a decentralised system where nodes mutually supervise one another.

The suggested architecture comprises five layers: the application server, the memory layer, the software layer, the administration layer, and the sensor layer. The following is a complete description of every layer: IoT layer for sensing layer. Devices and networks have been deployed to detect the data supplied to the cloud tops via the gateways and fog. To prevent unwanted entry to the IoT information at this level, the IoT equipment must first be registered before any login procedures can be carried out. The device connects to the remote server when the cloud layer successfully authenticates. To even build the clusters, the root node is chosen using the node degree (N), the distance between nodes (D), residual power (R), and their fitness (F). The salp swarm algorithm (SSA) is used to evaluate fitness. The member nodes' information is combined and sent to the cloud environment via the gateways layer.

Gateway layer: the gateway division is in charge of connection aggregation, allowing diverse heterogeneous smart objects to communicate with one another. Interoperability between various standards, methods, and platforms is another feature of this layer.

A layer of fog differs from a cloud, which is centralized, in that fog is diffuse. Queries from the cluster formation are constantly generated in the cloud environment in the form of tasks. The SoftMax deep learning models and machine learning technique assigns these received jobs to a remote server.

In other words, three categories, memory resources, broadband resources, and storage infrastructure, initially created from the tasks that have been received. Utilising resource task scheduling, these assets are safely assigned to the remote server (cloud layer). The suggested solution uses the SHA-512 and enhanced RSA algorithm to avoid information deduplication and boost security. The authentication of devices, storage systems, database management, and decision-making are all handled by this end-user level. Through this level, users and decision-makers communicate.

The logical architecture of the DNN-RSM system is shown in Figure 1. The DNN-RSM system has five layers: application, storage, management, firmware, and sensing layer. The sensing layer consists of numerous sensing devices and, at minimum, one microprocessor with a specified amount of processing power, which learns about various hardware items and pre-processes the information taken. Routers' primary roles are to determine the best path across networks and to safely forward data packets along that path. The fundamental building blocks of IP addressing are hosts and networks. On the one side, the administration hub layer decrypts, packages, and saves the database after parsing the uploaded data. On the other side, the administration hub layer must combine and control many pieces of machinery by the production planning plan and react to user demands in real-time to offer tailored services. Blockchain recordings and encoded and tamper-resistant files are stored in the storage system, which functions as a data centre. These records are distributed, stored, and periodically synced.

The research suggests the firmware surface, which includes the underlying execution innovations to link up each stack, such as the data capture, dispersed methodologies, and digital storage techniques, to allow the sensor, the managerial hub layer, and the storing layer to supplement one another successfully. Firmware is software that comes preinstalled on hardware and contains instructions for getting it up and running, communicating with other devices, and handling basic input and output. Users can access various services from the application layer, including real-time surveillance and failure predictions.

3.1. Device Authentication. As the installed devices receive the sensor readings sent to the cloud server connected via the pervasive computing level, device identification is a crucial responsibility in the IoT context. Device identification is suggested using 3 phases: enrolment, access, and validation, to prevent unwanted entry to IoT data sources. The linear cypher-based SHA 512 method is used for every step of verification, and it works as follows:

Step 1: device data including unique identifier (D_{ID}), device password (D_{PW}), device type (D_T), device MAC address (D_{MAC}), and device location (D_p) are used to complete the registration stage. Here, the identification code is initially generated using the affine cypher. Combining the item ID and gadget passcode yields the reference number, which is then encrypted using the following equations:

$$E_f = \langle M \rangle, \tag{1}$$

$$D_f = \langle M \rangle. \tag{2}$$

Here, M is denoted as the identification code. Coprime/key integers are denoted as p, q, the encrypting function is represented as E_f, and decrypting function is expressed as D_f. The hash function (f) for that code

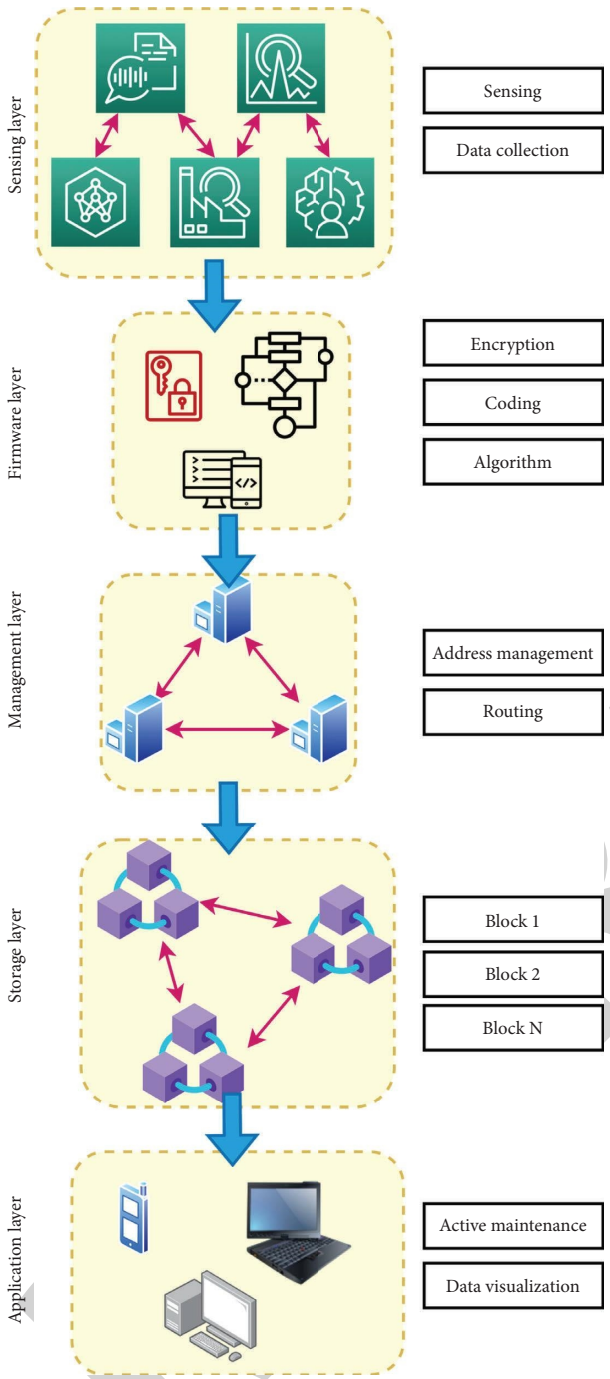


Figure 1: Logical architecture of the DNN-RSM system.

system is then generated using the SHA-512 method. A blockchain model is used in this research. The biasing part is denoted as b. Finally, the computer at the cloud tier stores the transformed hash value H_f and it is expressed in the following equation:

$$H_f = \mathrm{SHA}\left[\langle D_{\mathrm{PW}} \rangle\right]. \tag{3}$$

The encrypted data are denoted as $E_{D_{\mathrm{ID}}}$, and the decrypted data with the password (PW) are expressed as D_{PW}.

Step 2: after registering, the device must use a login method to establish a connection to the server to obtain sensor data. The device D and passwords (PWs) for the authentication scheme are sent to the remote server after login. The activation code is then created using the device (D) and passcode. The SHA-512 technique is then used to generate the hash value for this registration.

Step 3: the cloud server conducts the verification phase, which compares the received item value's hash code to the hashing value created during registering. If so, the web server receives the data while the IoT sensing machine is powered. If not, the validation phase is transferred to the login stage.

3.2. Task Scheduling. The cluster members combine the information in the group nodes after group formation. It is then brought to the layer of fog. The cluster heads send a tonne of information or queries to the cloud environment. As a result, it is crucial to plan the data analysis for transfer to the following layer. To achieve the most use of the resource allocated, the task scheduler must arrange user requests in a specific way. Here, processing activities like data standardisation and normalisation can be developed to enhance the accuracy rate before the preprocessed jobs are segmented into subtasks to perform optimisation techniques.

The assignment must be delivered to the task manager present in the cloud environment. The task scheduler collects scheduling information in the network nodes, monitoring, and cloud. The relevant fog node is subsequently given these duties to do. The categorised resources are tested for data processing using SHA-512 to save storage capacity and safely schedule the assets to clouds. After that, the enhanced RSA technique is used to complete the encryption before scheduling it to the virtual servers.

Let us use the numbers G for tasks and K for resources. The set of jobs can be expressed as $R = \{r_0, r_1, \cdots, r_G\}$, and the set of supplies for the fog as $V = \{v_0, v_1, \cdots, v_G\}$. The 1-dimensional representation of the characteristics of task x by the following equation:

$$R_x = \left[r_{ID}, r_L, r_c, r_q, r_s, r_D\right]. \tag{4}$$

The assignment ID (r_{ID}), task duration (r_L), computation needs (r_c), network needs (r_q), storage necessity (r_s), and task information (r_D) are used for task computation. By abstracting material assets from virtualised resources, cloud computing is made possible. The xth resources can be represented by Q_x as in equation (5) if the number of components in the xth set equals G of fog components.

$$Q_x = \left[q_{\mathrm{ID}}, q_c, q_G, q_s\right]. \tag{5}$$

$q_{\mathrm{ID}}, q_c, q_G$, and q_s, stand for resource identity, computing capabilities, resource throughput, and access, respectively. The following sections provide more information on job processing, categorisation, encrypting, and rescheduling. The following set in equation (5) determines the equal set.

3.2.1. Data Normalisation. In cloud computing, when unprocessed processing takes place directly, the effect on classification performance would be unevenly influenced by numerous assessments of fog project environment. Therefore, the resource matrix information is standardised by the standard error to address the adverse impacts of this circumstance. The matrices in equation (6) are made up of N components, and the collection of fog supplies $F = \{f_0, f_1, \cdots, f_G\}$ denotes the G vertices of the cloud source.

$$F = [f_{11}\, f_{12} \cdots f_{1G}\, f_{21}\, f_{22} \cdots f_{2G} \vdots f_{N1} \vdots f_{N2} \cdots\cdots \vdots f_{\mathrm{NG}}]. \tag{6}$$

The fog element is denoted as f_{xy}, and the number of cloud sources is denoted as N and the vertices are denoted as G. The mean resource is denoted in the following equation:

$$\underline{f}_{\mathrm{xy}} = \frac{1}{G} \prod_{y=0}^{N} f_{\mathrm{xy}}. \tag{7}$$

The fog element is represented as f_{xy}, and the number of cloud source is expressed as G. The fog element is denoted as f_{xy} when utilized on industries, the fogging system reduces environmental drying out time and gives them the water they need. The standard deviation is shown in the following equation:

$$w_y = \frac{1}{G} \sqrt[2]{\prod_{y=0}^{N} \left(f_{\mathrm{xy}}\right)^2 - \left(\underline{f}_y\right)^2}. \tag{8}$$

The fog element is denoted as f_{xy}, and the mean fog element is expressed as $\underline{f}_y$. The total cloud element is represented as G. The normalized value is expressed in equation.

$$f_{\mathrm{xy}} = \underline{f}_{\mathrm{xy}} - \left(\underline{f}_{\mathrm{xy}}\right) \times \left(\frac{1}{\left(\underline{f}_{\mathrm{xy}}\right)} - \frac{1}{\left(\underline{f}_{\mathrm{xy}}\right)}\right). \tag{9}$$

The mean resource is shown as $\underline{f}_{\mathrm{xy}}$ and the normalised value is expressed as f_{xy}. Data processing must be standard. It consequently has an average of 0 and SD 1. As a result, the matrix's information is normalised between 0 and 1.

3.2.2. Neural Network Model. After pretreatment, the preprocessed jobs are classified using the deep neural network-(DNN-) based SoftMax function. DNN is a multilayered, sophisticated neural network.

The neural network structure is shown in Figure 2. The system consists of multiple layers such as input layers, hidden layers, and output layers to produce optimum results. Input, outputs, and hidden units are all parts of the DNN. The resulting neural network is complex as a neuron's input rises, accompanied by a rise in the hidden state. In addition, while the quality decreases, the running time grows. The DNN is confined to the global minimum, which reduces time. To maintain a high rate of calculation and forecasting, the suggested method uses the SoftMax function using a corrected input signal in the output nodes. Incorporating a nonlinearity into a model is a direct approach to represent a nonlinear situation. Every element of the hidden layer can be connected to a nonlinear function. In the model depicted by the accompanying graph, the value of each node in the hidden layer is changed by a nonlinear function before being passed on to the weighted sums of the next layer. The activation function is a term used to describe this type of nonlinear function. The variety of output possibilities offered by SoftMax is a key benefit. The sum of all problem-solving talents falls between 0 and 1. SoftMax function-based DNN is the title of the suggested resource classification algorithm.

The SoftMax-DNN method is described as follows:

Step 1: the collected precompiled assignments of the clustered heads are first provided as an input in the input nodes.

Step 2: create weighting factors for every input information in the neural network, then attach each hidden and output surface neuron to a particular input data. Lastly, assure that the value of each input data neuron is preserved. The input data to the hidden layers of a neural network are transformed by a parameter called "weight." An array of cells called "neurons" make up a neural network. Each node incorporates its own inputs, weight, and bias. The node takes an input, multiplies it by some weight value, and then either stores the result for later use or sends it on to the next layer of the neural network. Most of the time, a neural network's weights are stored in its hidden layers.

Step 3: for resource categorization, the suggested method employs three hidden levels. The functions of the hidden layers are expressed in the following equations:

$$C_{1x} = w_{1x} + \prod_{x=0}^{N} G_x \times b_{1x}, \tag{10a}$$

$$C_{2x} = w_{2x} + \prod_{x=0}^{N} C_{1x} \times b_{2x}, \tag{10b}$$

$$C_{3x} = w_{3x} + \prod_{x=0}^{N} C_{2x} \times b_{3x}, \tag{10c}$$

where C_{1x}, C_{2x}, and C_{3x} specify the results of the 1st, 2nd, and 3rd layers; w_{1x}, w_{2x}, and w_{3x} and b_{1x}, b_{2x}, and b_{3x} signify the bias and weighting values of the 1st, 2nd, and 3rd layers; and N indicates the input feature elements from the grouping unit. An activation function is used as the output of a neural network, which has a hidden layer in between its input and output. The function applies weights to the inputs. In a nutshell, the hidden layers conduct nonlinear modifications on the network's inputs.

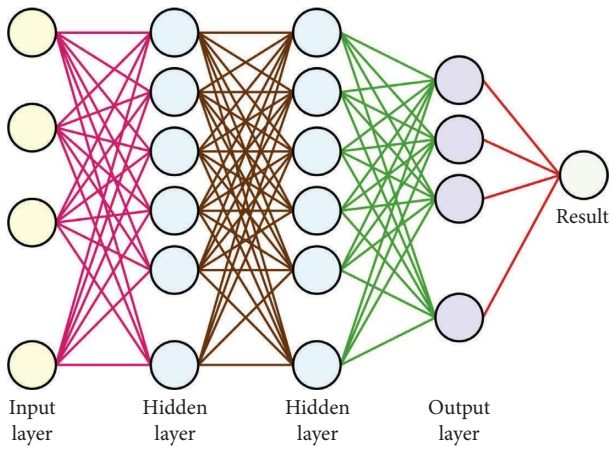


Figure. 2: Structure of the neural network.

The mathematical view of the three hidden layer functions C_{1x}, C_{2x}, and C_{3x} are displayed in Figure 3. The different biasing conditions of three hidden layers are shown as w_{1x}, w_{2x}, and w_{3x}, and the scaling factors at three layers are expressed as b_{1x}, b_{2x}, and b_{3x}.

Step 4: in this case, the SoftMax layers are employed as output nodes to calculate the winner output unit. It does this by computing the weight quality of the end concealed layer using the activation function. The network can fast converge thanks to the rectifier. The following is how the SoftMax activating algorithm for DNN is demonstrated in the following equation:

$$S_x = \frac{C_{3x} + W_x}{S_f(k)}, \tag{11}$$

where W_x stands for the current hidden layer's load and bias settings and S_x stands for the SoftMax output's $S_f(k)$ end price. Here, the operational amplifier is used to determine the weight quality of the end hidden state. The SoftMax layer output is expressed in the following equation:

$$S_f(k) = \frac{\text{maximum}\{0, i\}}{\widehat{b}_x}. \tag{12}$$

$S_f(k) = i$ for positive values of k, $S_f(k) = 0$ for negatives values of x, and $\widehat{b}_x$ stands for the weighting factor. The SoftMax layer effectively categorises the capabilities as a store, memory, and computational resources. After scheduling algorithms, and SHA-512 method is used to find duplicate activities. Neural network models that forecast a multinomial probability distribution use the SoftMax function as the activation function in the output layer. As an activation function, SoftMax is typically employed in situations requiring the classification of more than two classes. The cloud server generates the ciphertext for receiving device queries using SHA-512. The hash function is then verified to see if it is stored in a cloud computer's database. If so, the server routes the filename to be saved; otherwise, information storage is encrypted.

3.2.3. Enhanced RSA Model. Even if the attacker can sneak past the authentication, it would not be able to decode the data during this phase, adding another layer of complexity. Here, the suggested solution encrypts data using improved RSA encryption techniques. In RSA, two main numbers are first taken into account. Those two prime values are multiplied during the necessary generating procedure. As a result, the security feature drops if the invader can discover these factors utilising different sorts of attacks. Blockchain-based security model is suggested in this research.

To boost the system's safety, the RSA technique is supplemented here with four different prime integers. To lengthen the attack window, the RSA method uses four-prime factors. Consequently, enhanced RSA delivers solid outcomes by raising secure communication with a modest key size. Three steps make up the enhanced RSA. Essential creation, encryption, and decoding are these three. The following is a detailed description of enhanced RSA (Table 1).

3.2.4. Resource Allocation. Any system's capacity planning is a crucial component. The right resource categorisation and the device requirements are linked with the assets in the course. Following are the steps to finish the dynamic resource using superficial weight similarity. The weight similarity is expressed in the following equation:

$$Q = \frac{\prod_{x=0}^{N} \text{Rq}_x - \prod_{x=0}^{N} \text{Rs}_x}{\prod_{x=0}^{N} b_x}. \tag{13}$$

Rq_x is the request characteristics, Rs_x is the resource characteristics, and b_x is the weight attributes. Varying gadgets have various resource needs. As a result, they could be divided into processing, memory, and limited bandwidth for different task preferences. The expression determines the attributes and capacity attribute needed by the device based on the resource schedule outcome with the most incredible score.

3.3. Data Interaction Model. But fundamentally, the IoT is where the proposed design gets its inspiration. As a result, it uses the temperature collecting method to discuss how to build the architect's information interplay to fend against potential risks and attacks such as permission leaks, DoS or cyber-attacks, network sniffing, and compromised-key assassination attempts and invasions.

Collected data should be accomplished using the suggested architecture, which depends on the minicomputers. Typically, a microprocessor can link to one control hub and control one or more senses. The microprocessors must file a unique number after the data have been collected, which is added to the blocklist in the linked control hub. Each administrative corner contains a copy of the allow list. The linked microprocessor can opt to go into standby mode or modify its network configuration to move to another administration hub if one crashes.

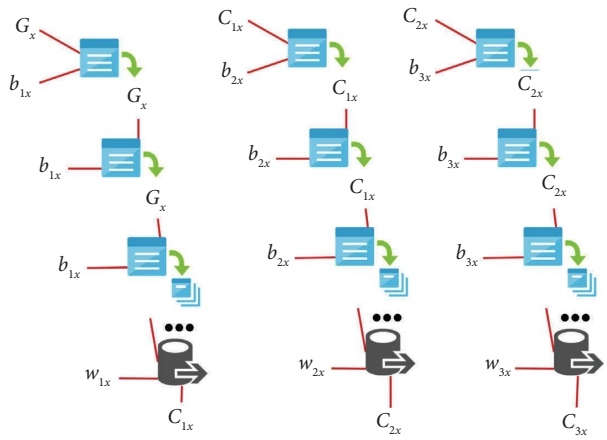


Figure 3: The mathematical view of the hidden layer functions.

Table 1: Description of enhanced RSA.

Select 512 bit numbers as x, y, k, l
Calculate $m = x * y/k * l$
$\propto = x + 1/k - 1 * (y - 1) * (l + 1)$
Compute GCD $(n, \propto)$
Calculate $x = n * k/l$
Compute $b = 1/x \bmod \propto$
Encrypt the data $E_f = \langle M \rangle$
Decrypt the data $D_f = \langle M \rangle$

It considers theft and misuse of node privileges as attacks in this procedure (mainly the control hub level and the sensor layer). It creates two-defence systems as a result. To stop the malicious activity and the insertion of false data, it combines the allow list system, the dynamic validation mechanism, and the key agreement method in the sensor surface. On the other side, as a multicentre solution is designed, the invaded control hub could be rapidly found, rejected, and rebuilt under the oversight of the other administration hubs. These two protection mechanisms can ensure the stable functioning of the operating platform.

The information is first placed into the buffer cache after being granted permission via the allow list validation. The administration hub computes the characteristics and contrasts them with the predetermined values once it has reached a specific amount of information, which is how the power of words (PoWs) is achieved. Blockchain-based system enhances the system outcomes. If the conditions are met, the information in the buffer cache is added to the system; the transferred data can temporarily be transported straight to the dataset, and all actions that fall under the equipment node's authorisation are permitted; if not, the permit application is denied, and the data obtained in the data cache are deleted. It should be remembered that the certificate authority must convert any data sent to the system into an encrypted message. For every authorisation request, the administration hub creates a new block record. The block recording is then transmitted to the other administration hubs, who record it after the second verification round. However, the adaptive validation method demands reauthentication after a given amount of time. Therefore, the system must repeat steps 1–6. The procedure for accessing and controlling requests is the same, and the diagram illustrates how to request storing permission.

DoS assaults frequently happen because the management centre is linked to the network. As a result, the ethernet cable is set up with the allow list system, dynamic verification method, and asymmetric critical method. The Internet's filtering and blocking of harmful traffic are carried out via the same blocklist and active validation mechanisms used on the network. The asymmetric cryptographic protocols were created expressly for the extranet to prevent illegal access.

The administration hub is a records node in the suggested design. Each administration hub has a copy of every block and piece of equipment's information. When block recordings are complete, the limited management centre creates a partnership to capture all access requests for that period. The blocks are formed, stored in the data store, and synchronised with the other administration hubs. It adds dual Merkel foundations to the block records to safeguard the data besides these defensive methods. The first is carried out on the block track's buffer cache information, while the other is given to the unit header's lead in the block bodies. This nesting ensures that the data would not be snooped on and that hostile intrusion is challenging to accomplish.

The suggested DNN-RSM method is designed in this section for security enhancement. The DNN-RSM with DNN and SoftMax layer provides higher security features in intelligent manufacturing with an advanced RSA algorithm. The impact of the DNN-RSM system is analysed and showcased in the next section.

4. Comparison Analysis and Impact of the DNN-RSM System

Using SoftMax-DNN and enhanced RSA algorithms, resource planning and secure information transfer of IoT information are suggested in this study. The simulation was carried out utilising the JAVA and NS3 technologies to verify and assess the model. Quantifiable metrics are examined in the simulated performance of the suggested and existing methodologies. End-to-end delay, energy usage, and security effectiveness are the measurement variables employed for the study.

The end-to-end delay and energy consumption analysis of the DNN-RSM system are shown in Figures 4(a) and 4(b), respectively. The software outcome of the DNN-RSM is evaluated by varying the IoT devices from rarer to denser conditions. As the number of IoT devices increases, the respective intermediate nodes increase, resulting in higher delay and energy consumption. The DNN-RSM with DNN and advanced RSA model enhances the security and thus reduces the unwanted intrusion of other data. The optimum result is obtained using the request and response functions Rq_x and Rs_x.

The software verification of the DNN-RSM system is carried out, and the findings such as sensitivity, F measure, accuracy, coverage probability, mean square error, and mean absolute error are computed for the DNN-RSM system. The results are compared with the existing convolutional neural

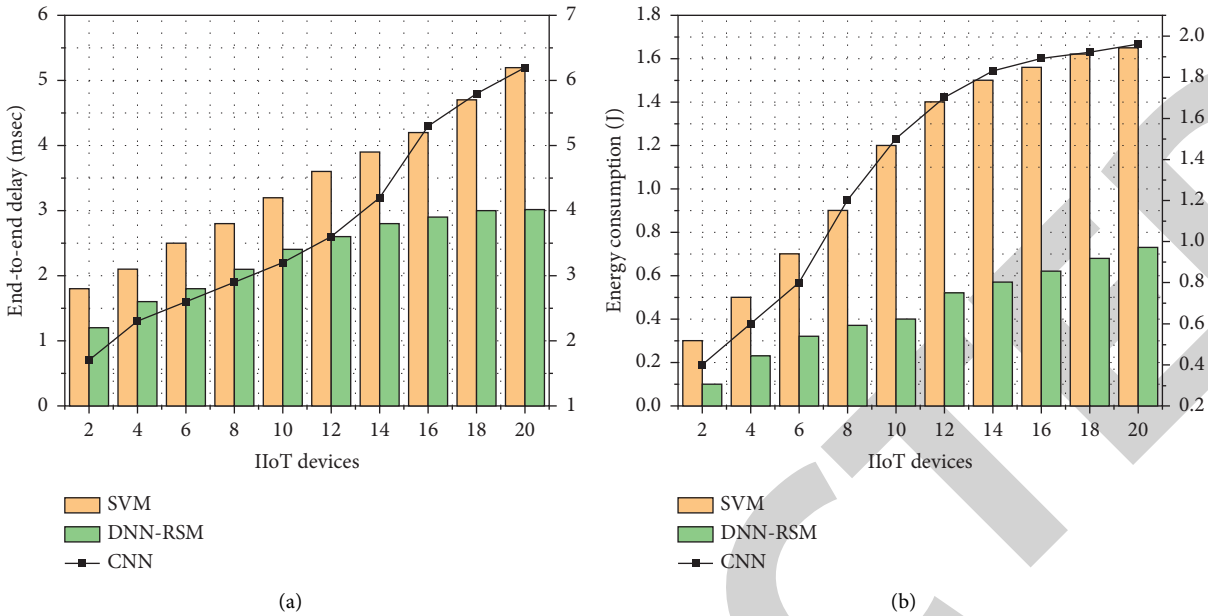


Figure 4: (a) End-to-end delay analysis. (b) Energy consumption analysis.

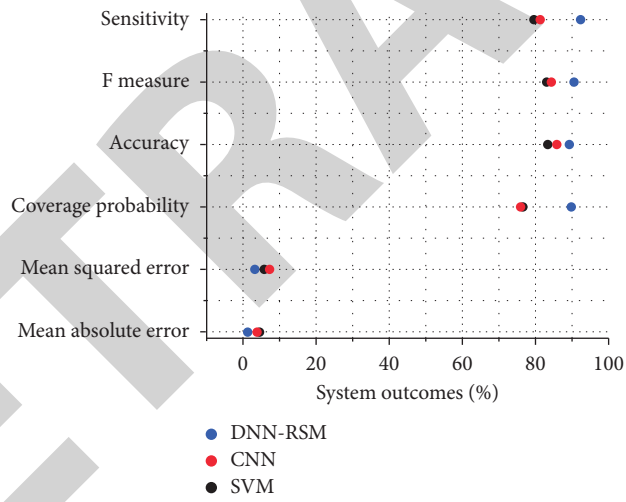


Figure 5: System performance analysis.

network (CNN) and support vector machine (SVM). The software results comparisons are depicted in Figure 5. The encrypted fog data E_f, and the decrypted fog data D_f with the public and private password PW, enhance the overall security of the DNN-RSM system with an advanced RSA algorithm. Performance analysis is a straightforward method for pinpointing the features of a good or service that may be enhanced for greater efficiency and productivity, or where costs can be reduced without substantially lowering standards.

The consumer satisfaction index and makespan analysis of the DNN-RSM system are analysed and displayed in Figures 6(a) and 6(b), respectively. The software outcomes of the DNN-RSM system are analysed, and the results are measured concerning the number of jobs. As the number of jobs increases, the system complexity is also increased. The security thread of the system also increases concerning the tasks. The normalised fog function $\underline{f}_{xy}$ and the average fog function $\overline{\overline{f}}_{xy}$ are used to compute and find better encryption results. The SoftMaxfunction $S_f(k)$ is directly linked to makespan and produces accurate and faster results.

The DNN-RSM system is designed in this section with DNN and SoftMax layer. The system's security is enhanced with the proposed advanced RSA encryption algorithms, and the outcomes are verified with the software findings and compared with the existing models.

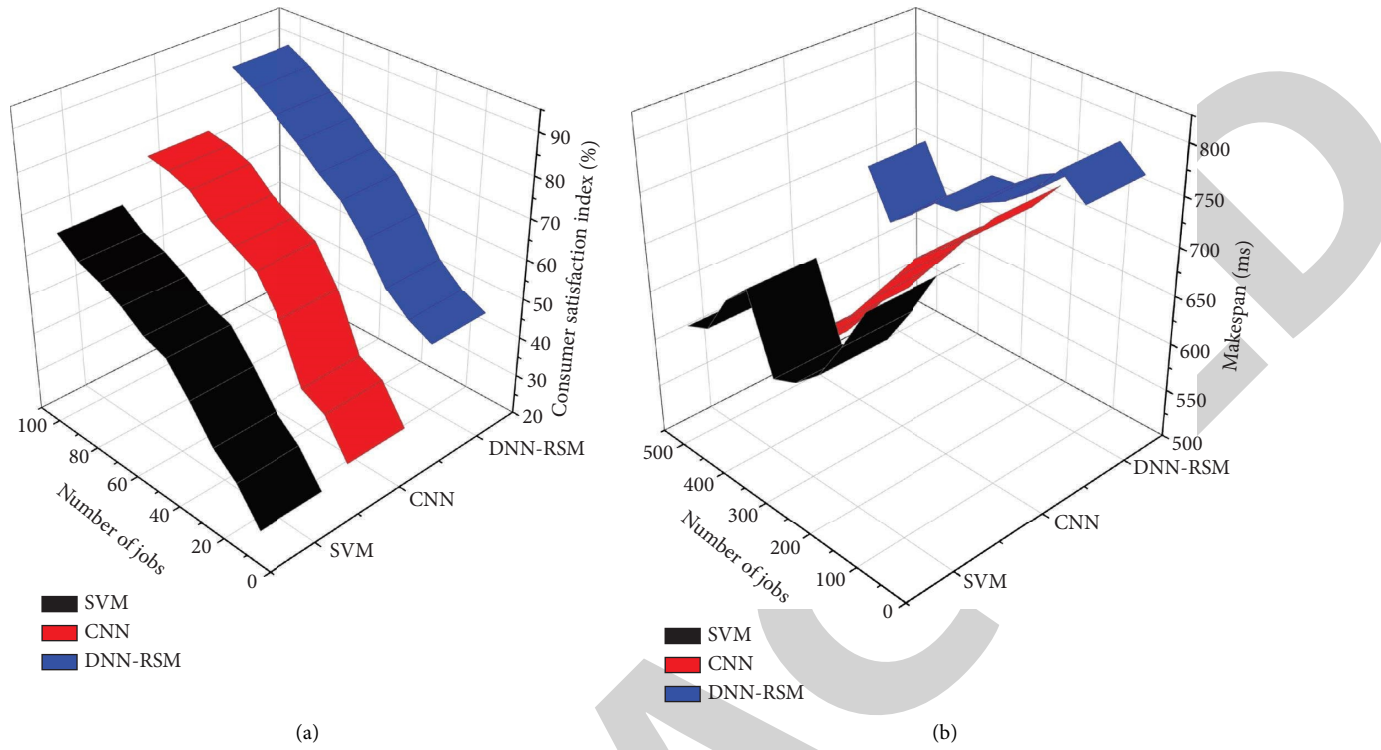


Figure 6: (a) Consumer satisfaction index analysis. (b) Makespan analysis.

5. Conclusion and the Future Scope of the Model

As a replacement to the previously used methods, a secure job scheduling method has been highlighted in this research for the hybrid cloud system. For IoT scenarios, the suggested method computes the use of another SoftMax-DNN and enhanced RSA algorithms. The suggested scheduling method adds the SHA-512 algorithm for quick networking infrastructure and information deduplication. By contrasting the proposed method's results with those of the existing process, its evaluation was carried out. The suggested approach achieves the best network life, minor energy usage, and shortest end-to-end delay.

The suggested upgraded RSA achieves the best security when conducting both encryption algorithms, while the current model achieves the lowest level of protection compared to the conventional one's efficiency. In addition, the suggested SoftMax-DNN resource categorisation technique performs better than others. When contrasted to SVM, the SoftMax-DNN achieves the highest levels of sensitivities (87), accuracy (93.2), and coverage (87.4), as well as the nominal error rates for measurements like mean squared error (3.2) and mean absolute error (4.3). As a result, the suggested method delivers more desirable outcomes, particularly regarding information transmission rate and energy savings. The system can be improved in future by using blockchain and a big data analytics model.

The anonymous characteristic of blockchain is the most cost-effective way to keep vehicle IDs concealed while protecting privacy in the IoV network. Furthermore, the availability of quantum computing machines at the adversary end may enhance future issues in blockchain security for IoVs [30–32]. The digital twin of any item, alive or nonliving, is an exact reflection of that object. Digital twin and cyber-physical system (CPS) and blockchain usher in a new age for businesses, particularly in the healthcare industry, which monitors the health data of individuals in order to deliver on-demand services that are lightning quick and highly effective to their customers is very challenging [33, 34]. Customers are able to acquire access to a vast array of manufacturing nodes through cryptographically sound networks with the help of blockchain-based, decentralized cloud manufacturing-as-a-service platforms. With the rise of decentralized cloud manufacturing-as-a-service, the Ethereum network has become a preferred blockchain platform for enabling provenance and traceability of proprietary manufacturing data. Organizations can digitize physical assets and create a decentralized immutable record of all transactions using blockchain technology, allowing for more transparent and accurate end-to-end tracking in the supply chain. This includes tracking assets from the point of production all the way through delivery or use by the end user.

Data Availability

The data used to support the study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] F. Tao, Q. Qi, L. Wang, and A. Y. C. Nee, "Digital twins and cyber-physical systems toward smart manufacturing and industry 4.0: correlation and comparison," *Engineering*, vol. 5, no. 4, pp. 653–661, 2019.

[2] A. Solanki and A. Nayyar, "Green internet of things (G-IoT): ICT technologies, principles, applications, projects, and challenges," in *Handbook of Research on Big Data and the IoT*, pp. 379–405, IGI Global, Hershey, PA, USA, 2019.

[3] A. H. Mohd Aman, E. Yadegaridehkordi, Z. S. Attarbashi, R. Hassan, and Y. J. Park, "A survey on-trend and classification of Internet of things reviews," *IEEE Access*, vol. 8, pp. 111763–111782, 2020.

[4] F. Tao, Q. Qi, A. Liu, and A. Kusiak, "Data-driven smart manufacturing," *Journal of Manufacturing Systems*, vol. 48, pp. 157–169, 2018.

[5] Q. Qi and F. Tao, "A smart manufacturing service system based on edge computing, fog computing, and cloud computing," *IEEE Access*, vol. 7, pp. 86769–86777, 2019.

[6] X. Li, Z. Zheng, and H. N. Dai, "When services computing meets blockchain: challenges and opportunities," *Journal of Parallel and Distributed Computing*, vol. 150, pp. 1–14, 2021.

[7] R. Casadei, G. Fortino, D. Pianini, W. Russo, C. Savaglio, and M. Viroli, "A development approach for collective opportunistic Edge-of-Things services," *Information Sciences*, vol. 498, pp. 154–169, 2019.

[8] S. Sharma and H. Saini, "Fog assisted task allocation and secure deduplication using 2FBO2 and MoWo in cluster-based industrial IoT (IoT)," *Computer Communications*, vol. 152, pp. 187–199, 2020.

[9] T. Choudhari, M. Moh, and T. S. Moh, "Prioritised task scheduling in fog computing," in *Proceedings of the ACMSE 2018 Conference*, pp. 1–8, New York, NY, USA, March, 2018.

[10] B. M. Nguyen, H. Thi Thanh Binh, T. The Anh, and D. Bao Son, "Evolutionary algorithms to optimize task scheduling problem for the IoT based bag-of-tasks application in cloud–fog computing environment," *Applied Sciences*, vol. 9, no. 9, p. 1730, 2019.

[11] G. Li, Y. Liu, J. Wu, D. Lin, and S. Zhao, "Methods of resource scheduling based on optimized fuzzy clustering in fog computing," *Sensors*, vol. 19, no. 9, p. 2122, 2019.

[12] H. Zhang, "Secure routing protocol using salp-particle swarm optimisation," *Algorithm—Journal of Networking and Communication Systems*, vol. 3, no. 3, 2020.

[13] V. Porkodi, A. R. Singh, A. R. W. Sait et al., "Resource provisioning for cyber–physical–social system in cloud-fog-edge computing using optimal flower pollination algorithm," *IEEE Access*, vol. 8, pp. 105311–105319, 2020.

[14] L. Bu, M. Isakov, and M. A. Kinsy, "A secure and robust scheme for sharing confidential information in IoT systems," *Ad Hoc Networks*, vol. 92, Article ID 101762, 2019.

[15] M. Bhatia, S. K. Sood, and S. Kaur, "Quantumized approach of load scheduling in fog computing environment for IoT applications," *Computing*, vol. 102, no. 5, pp. 1097–1115, 2020.

[16] J. A. Alzubi, R. Manikandan, O. A. Alzubi et al., "Hashed Needham schroeder industrial IoT based cost optimized deep secured data transmission in cloud," *Measurement*, vol. 150, Article ID 107077, 2020.

[17] P. Gazori, D. Rahbari, and M. Nickray, "Saving time and cost on the scheduling of fog-based IoT applications using deep reinforcement learning approach," *Future Generation Computer Systems*, vol. 110, pp. 1098–1115, 2020.

[18] H. Sun, H. Yu, G. Fan, and L. Chen, "Energy and time-efficient task offloading and resource allocation on the generic IoT-fog-cloud architecture," *Peer-to-Peer Networking and Applications*, vol. 13, no. 2, pp. 548–563, 2020.

[19] W. Wang, G. Wu, Z. Guo, L. Qian, L. Ding, and F. Yang, "Data scheduling and resource optimisation for fog computing architecture in industrial IoT," in *Proceedings of the International Conference on Distributed Computing and Internet Technology*, pp. 141–149, Springer, Heidelberg, Germany, January, 2019.

[20] A. Atieh, P. Nanda, and M. Mohanty, "Context-aware fog computing implementation for industrial internet of things," in *Proceedings of the 2021 International Wireless Communications and Mobile Computing (IWCMC)*, pp. 598–603, IEEE, Harbin, China, June, 2021.

[21] F. A. Khan, A. Rahman, M. Alharbi, and Y. K. Qawqzeh, "Awareness and willingness to use PHR: a roadmap towards cloud-dew architecture based PHR framework," *Multimedia Tools and Applications*, vol. 79, no. 13-14, pp. 8399–8413, 2020.

[22] M. de Brito, S. Hoque, R. Steinke, A. Willner, and T. Magedanz, "Application of the fog computing paradigm to smart factories and cyber-physical systems," *Transactions on emerging telecommunications technologies*, vol. 29, no. 4, p. 3184, 2018.

[23] I. Mistry, S. Tanwar, S. Tyagi, and N. Kumar, "Blockchain for 5G-enabled IoT for industrial automation: a systematic review, solutions, and challenges," *Mechanical Systems and Signal Processing*, vol. 135, Article ID 106382, 2020.

[24] Q. Qi and F. Tao, "A smart manufacturing service system based on edge computing, fog computing, and cloud computing," *IEEE Access*, vol. 7, pp. 86769–86777, 2019.

[25] M. Serror, S. Hack, M. Henze, M. Schuba, and K. Wehrle, "Challenges and opportunities in securing the industrial Internet of things," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 5, pp. 2985–2996, 2021.

[26] X. Deng, Z. Sun, D. Li, J. Luo, and S. Wan, "User-centric computation offloading for edge computing," *IEEE Internet of Things Journal*, vol. 8, no. 16, pp. 12559–12568, 2021.

[27] A. D. Dwivedi, R. Singh, S. Dhall, G. Srivastava, and S. K. Pal, "Tracing the source of fake news using a scalable blockchain distributed network," in *Proceedings of the 2020 IEEE 17th International Conference on Mobile Ad Hoc and Sensor Systems (MASS)*, pp. 38–43, IEEE, Delhi, India, December, 2020.

[28] S. Dhar, A. Khare, and R. Singh, "Advanced security model for multimedia data sharing in Internet of Things," *Transactions on Emerging Telecommunications Technologies*, p. 4621, 2022.

[29] G. Srivastava, J. Crichigno, and S. Dhar, "A light and secure healthcare blockchain for iot medical devices," in *Proceedings of the 2019 IEEE Canadian conference of electrical and computer engineering (CCECE)*, pp. 1–5, IEEE, Edmonton, AB, Canada, May, 2019.

[30] M. Gupta, R. B. Patel, S. Jain, H. Garg, and B. Sharma, "Lightweight branched blockchain security framework for

Hindawi
Security and Communication Networks
Volume 2023, Article ID 8168075, 13 pages
https://doi.org/10.1155/2023/8168075

Research Article

A Blockchain-Oriented Framework for Cloud-Assisted System to Countermeasure Phishing for Establishing Secure Smart City

Narendra Kumar,[1] Vikas Goel,[2] Raju Ranjan,[3] Majid Altuwairiqi,[4] Hashem Alyami,[4] and Simon Atuah Asakipaam[5]

[1]*VPLearning Closet Pvt. Ltd., Noida, Uttar Pradesh, India*
[2]*Department of IT, Kiet Group of Institutions, Ghaziabad, India*
[3]*School of Computing Science and Engineering, Galgotias University, Greater Noida, India*
[4]*Department of Computer Science, College of Computers and Information Technology, Taif University, Taif, Saudi Arabia*
[5]*Department of Electrical and Electronics Engineering, Tamale Technical University, Tamale, Ghana*

Correspondence should be addressed to Simon Atuah Asakipaam; simonasakipaam@gmail.com

Received 3 July 2022; Revised 23 July 2022; Accepted 9 August 2022; Published 21 April 2023

Academic Editor: Rabie Ramadan

The information that is saved in the cloud about users is protected by a number of different safeguards in order to facilitate the development of smart cities. Phishing and other forms of social engineering are two examples of misleading tactics that may be used by hostile actors to get sensitive information about users. Phishing is still the first step of a multistage assault, despite the significant technological advancements that have been made to it in recent years. Phishing kits have evolved to become attack tools that are much simpler, more user-friendly, and more readily available as time has gone. Indicators of a successful phishing assault include using foreign characters in the URL, typosquatting of prominent domain names, reserved characters in redirections, and multichain phishing. When papers with these types of phishing URLs are uploaded to cloud storage, hackers get a helping push in the right direction. The use of cloud servers in the commission of these assaults is becoming more common. The currently available software to disallow list phishing URLs does not provide sufficient protection against multilevel phishing and instead places the onus of safety on the user to protect themselves. In addition, the immutability of blockchain data and the avalanche effect both demonstrate their effectiveness as crucial safety measures. In view of the recent advances in technology, we suggest an implementation of filtering that is based on blockchain technology to safeguard the cloud-based data of users. The Phish Block that has been presented is able to recognize homographic phishing URLs with an accuracy of 91 percent, thus ensuring the security of cloud storage.

1. Introduction

The bulk of technology users, including financial services, have shifted their focus to cloud resources as the demand for these services has increased. It is possible that this may encourage the attackers and turn cloud servers into a target for security breaches. Because other cloud users sometimes upload stuff that is both dishonest and harmful, the papers that are stored in the cloud could not be completely secure. There are numerous different methods in which phishing assaults might occur. Emails are the primary vector for phishing attacks. Phishing may also take place via the use of a technique known as angler phishing. Social media is a relatively new attack vector, and it provides a lot of different options for perpetrators of attacks to deceive victims. To trick users into divulging private information or downloading malware, imposter URLs, cloned websites, postings, tweets, and instant messaging is one of the tactics that are used. Attackers are able to build highly targeted assaults by making use of the data that users voluntarily provide on social media platforms. The use of phishing URLs, which may mislead or misdirect users of cloud computing environments, is the primary kind of attack that is feasible in a cloud computing environment. Because the primary purpose of phishing is to

steal the data of the user, the perpetrators of the assault make an effort to get access to the user's information without the user's awareness. The vast majority of phishing assaults begin with a URL that has been carefully constructed. Phishing URLs, when clicked on, take users to fake websites, download malicious software, or request login credentials from users. The user is tricked into accessing these websites because the false URL seems remarkably similar to the actual URL. Cloud computing, in its most basic form, refers to the practice of accessing and storing data across a linked network rather than on the hard disc of a computer.

The data and information that are saved in the cloud are protected from the majority of potential threats. The user who creates the data that is stored in the cloud is the one who is responsible for its creation, but the cloud service provider (CSP) has complete authority over the contents of the cloud. People like the cloud not only because it can store data, but also because utilizing cloud services enables them to exchange files and documents with other people. This is one of the main reasons why people favor the cloud. The cloud service may also be used for the purpose of generating backups of the data in order to safeguard vital documents and other data. The data may be retrieved from the cloud storage facility in the event that anything catastrophic occurs to the local computer. Sharing data via cloud computing makes it possible for several participants to freely share the data of a group. This not only increases the productivity of work done in collaborative settings but also offers a broad range of potential applications [1]. Despite the development of a number of different encryption methods, maintaining the cloud storage's level of security continues to be challenging. A blockchain is a list that is constantly being added to. It is a record kept in digital format of transactions. It gets its name from its structure, which consists of individual entries being connected together in a single list known as a chain. These individual records are called blocks. Transactions that are done using cryptocurrencies are recorded using a technology called blockchain. The term "cryptocurrency" refers to any digital asset that may be traded like traditional currency. It keeps track of and maintains a ledger or record in a digitally computerized database that contains the ownership records of individual coins. For the purposes of protecting, creating, and verifying transaction records as well as their respective ownership, the database is encrypted using robust encryption. As a result, they are referred to as distributed ledgers since no centralized authority is responsible for their issuance or approval.

Figure 1 shows the structure of block. The avalanche effect is a characteristic of cryptography that describes what happens when a little change is made to the input but results in a significant change to the output. If the information included in a single block of the blockchain was altered in any way, the hash value of that block would be subject to significant revision. Because the hash value that is created in each subsequent block contains the hash value of the block that came before it, any change in the content of a single block results in a change in the hash value of all of the blocks. As a result, the blockchain is resistant to modifications and updates, which helps to ensure that the integrity of the

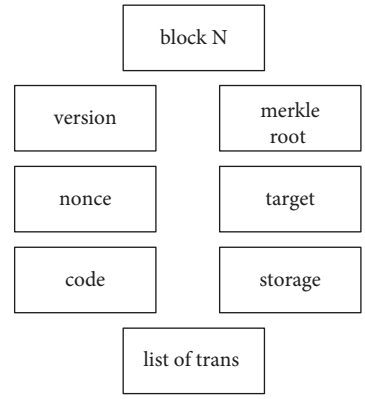


Figure 1: Structure of a block.

recorded data is maintained. Horst Feistel was the first person to adopt the phrase "avalanche effect," despite the fact that Shannon's diffusion was already using the notion. It is one of the most important goals of the design process for a hash function that makes advantage of the "butterfly effect." Through repeated uses of the hash algorithm, it enables even very little changes to have a significant impact in a short amount of time. Due to the avalanche effect, which makes the blockchain totally resistant to alterations, anything that has been entered as a block can only be read after it has been added, and it cannot be modified once it has been added. The user may begin the upload after they have successfully navigated the security system that is given by the cloud provider. The credentials of the user, which are maintained inside the blockchain, once again adhere to the avalanche effect, which guarantees that non-repudiation will occur. Modeling the data access and acquisition operations of the service provider as a series of access records that offer information about the data created and consumed for the service is one way to represent these activities. However, access records [2] are of no value if they cannot be relied upon, and it is not a good idea to place your faith on access records if you are not being provided with the appropriate protection. It is of the utmost importance to ensure that access records are both accurate and impossible to falsify.

Because of these many security considerations, blockchain technology has been selected as the platform of choice for safeguarding cloud servers. A Blockchain-as-a-Service (BaaS) platform can provide developers with convenient, high-performance blockchain ecosystems [3] and related services by embedding the blockchain framework into the cloud computing platform. This allows the platform to leverage the deployment and management advantages of cloud service infrastructure. There has not been any implementation of a phish-detecting blockchain yet. The currently available methods for preventing phishing URLs are carried out on the browser level utilizing domain certifications. In addition, there are several tools available, which enable client programs to verify URLs against continually updated lists of risky online sites. This helps to protect cloud users from falling victim to phishing scams. The usage of blockchain technology to preserve phishing information might be helpful in identifying the perpetrator

of the crime. Together, the non-repudiation feature of the cloud and the integrity of the documents stored in the blockchain are helpful in determining whether users are engaging in malevolent activity. Users will be able to protect themselves against phishing attacks if the content of fraudulent documents is exposed and made transparent. Criminals can then no longer hide their tracks. It will be less important for users to make sure they are using secure browsers if the proposed Phish Block is implemented. It functions as a utility between the users of the cloud and the storage while insertions and updates are being made, hence eliminating the need for a twofold check when accessing data from the cloud.

The objective of the Phish Block solution that has been developed is to distinguish safe homographic URLs from harmful homographic URLs inside the data that is being saved in the cloud environment. Adding a blockchain service to a cloud environment provides an additional degree of security, which will be to the users' advantage. The deployment of blockchain-based document filtering that has been suggested would guarantee that only valid documents are saved to cloud storage. By identifying phishing methods that are URL-based, the Phish Block technology prevents uploaded harmful documents from accessing the cloud and so protects users.

2. Literature Review

The blockchain technology is becoming an essential component of many different systems. In fog computing, a scalable blockchain may be created using a structure called groupchain that consists of group blocks and vice blocks. The transactions that take place in the environment that was formed are checked and authorized by a leader group using a round robin process. This helps to lower the confirmation latency while simultaneously increasing the transaction throughput. Through this solution, both selfish mining and unnecessary expenditure may be avoided [4]. Concerns relating to privacy, reputation systems, and transaction negotiation may be amenable to resolution using a platform like blockchain-based CloudEx [5]. Policy driven permissioned blockchain network has been designed for transport systems with a set of policies which contain the signing key of each user, and these signing keys are associated with a policy set [6]. In order to guarantee the integrity of the huge data throughout the process of controlling the Internet of Things, a permissioned blockchain that uses decentralized administration was used. A blockchain-based token incentive system has also been implemented in order to improve the overall quality of the data that has been provided. This particular blockchain architecture may potentially be practicable for very large amounts of data [7]. NutBaaS is a Blockchain-as-a-Service platform that has been designed as a layered architectural design. It has the capability of providing blockchain services to cloud computing environments. The development of blockchain ecosystems also includes the provision of various security services. Using a multilayered strategy, blockchain technology may offer security for the Internet of Things (IoT) and answer concerns about the confidentiality, integrity, and availability of IoT data. In order to guarantee the system's safety, the SHA-2 hashing algorithm is often implemented using Merkle trees and hash tables [8]. Blockchain taxonomies such as consensus protocols, smart contracts, and forks have been used to ensure the safety of cryptocurrencies, in addition to the Internet of Things (IoT) security. The immutable blockchain enables authorized access to the whole transaction history as well as multi-token trades [9]. For the purpose of bolstering the safety precautions taken by the wireless sensor nodes, a hybrid blockchain model has been developed to provide mutual authentication. Integrity, non-repudiation, and flexibility are provided by the hybrid model [10], which is comprised of base stations, cluster head nodes, and ordinary nodes. A blockchain-based smart contract that ensures fair remuneration may take the role of an independent auditor and help make auditing more safe. Storage protects private information and guarantees that parties do not have to communicate with one another during audits [11]. Blockchains are a well-known method used in cloud settings for the purpose of maintaining security. It is possible for the blockchain, which contains the data, to be stored on the cloud. When data is stolen in this cloud computing environment, a "block and respond" request is sent to the cloud owner. This helps to verify that data integrity is maintained. Hash trees and encryption algorithms were used to offer this security in order to ensure that cryptographic transactions are both quick and safe [12]. There have been several efforts that have focused on the smart contracts with the purpose of tailoring blockchain for certain purposes. Along with the explanation of a full overview of smart contracts by using Ethereum and Hyperledger blockchain frameworks, [13] also includes a suggestion of a six-layered framework that covers the essential parts of smart contracts. This framework covers the major features of smart contracts.

There has been development of a smart contract architecture that includes access control contracts (ACC), judge contracts (JC), and register contracts (RC). There are a variety of methods that may be used to identify and foil phishing scams. A SAFE-PC (Semiautomated Feature Generation for Phish Classification) model that carries out keyword extraction, feature engineering, and natural language processing in order to filter phishing attacks that come through the Internet and electronic mails is a method that can be utilized to protect against these types of attacks. SAFE-PC addresses real-world issues with a portable feature selection and uses the fastest boosting algorithm (RUSBoost) as a classifier. Its performance is superior to that of other filtering applications such as Sopho and SpamAssassin [14]. In order to identify instances of phishing on the Internet, an Adaptive Neuro-Fuzzy system was developed. This system takes a layered approach, integrating aspects of text, images, and frames. Phishing websites may be identified as having hybrid traits by the use of ANFIS feature classification, SVM, and KNN [15]. A fog network has to be established in order to identify and delete the phishing URLs. The phishing URLs are located by this fog network via the use of feature extraction, which is performed on online traffic characteristics. The WHOIS identification tool and the Google API open the

system up to massive amounts of real-time data and provide it with a higher quality of service [16]. The prediction of phishing is based on a generally used collection of 12 indicators that are collected from research conducted by third parties. These characteristics are a collection of URL patterns that are used by respectable websites with the goal of phishing the site [17].

Carrying out a phishing assault provides additional opportunities for learning about the aftermath of the attack as well. Extreme phishing attacks that look and feel nearly exactly like the genuine websites that are being targeted have been developed and exhibited to assess how successful they are. It was determined that 92 percent of the subjects did not exhibit any suspicious behavior [18]. There have been discussions on the creation of a variety of updated URLs and updated contents with the intention of tricking people. It has been said that not only URLs but even logos and visuals are phished in spam emails, which makes it exceedingly difficult to identify the existence of phishing since it makes it more difficult to tell what is being impersonated. Phishing is being addressed using a solution that consists of three stages: prevention, detection, and training for stakeholders [19]. Along with a comprehensive examination of the distinguishing traits that set spear phishing apart from regular phishing, a comprehensive description of the absence of preventative actions that can be taken against spear phishing is also provided [20]. There are ideas floating about with various detection methods for the many kinds of phishing, such as studies on the various kinds of phishing and spear phishing assaults. These ideas have been proposed [21].

3. Proposed Phish Block

The usage of blockchain technology to preserve phishing information might be helpful in identifying the perpetrator of the crime. Finding the malicious user is made easier because of the non-repudiation aspect of the cloud, which, when paired with the integrity of the documents stored in the blockchain, makes it possible to identify the user. The consumers have a better chance of becoming more knowledgeable about the phishing tactics that the crooks may utilize as the content of the fraudulent papers becomes more transparent. It will be less important for users to make sure they are using secure browsers if the proposed Phish Block is implemented. It functions as a utility between the users of the cloud and the storage while insertions and updates are being made, hence eliminating the need for a twofold check when accessing data from the cloud. The papers that are uploaded to cloud storage are screened for legitimacy by the Phish Block method that has been suggested. A homographic phishing URL detector is used by the employed framework of smart contract algorithms to identify documents that include phishing material. Once identified, these documents are withheld on the blockchain, which has the feature of the avalanche effect. The improved Proof-of-Work algorithm is used in the process of selecting the block miner from among the cloud users. After the block has been mined, the contents of the block are made available to all of the users of the cloud. Users who are authorized to utilize the cloud will now be aware of phishing. When the process of screening has been finished, any papers that have been left over but have not been uploaded to the blockchain will be regarded as secure. The framework of the smart contract will begin to operate on the most recent block of Phish Block as soon as an input has been identified. If the compilation of the contracts is successful, the block that contains the content of the malicious input document is mined via the Enhanced Proof-of-Work into the Phish Block. The remaining papers are now being uploaded to the server in the cloud. The Phish Block module will initially use the smart contract architecture in order to identify potential phishing URLs. Blocks are made out of any papers that are discovered to include phishing URLs, and these may then be removed. The Enhanced Proof-of-Work algorithm makes it possible for users to mine blocks based on whether or not a smart contract is legitimate. Only once a phishing URL has been successfully identified and removed is the assembled contract regarded to be legitimate. The deployment of a contract that is not legitimate does not result in the mining of the block. During this phase of the mining process, one participant will be chosen to take on the role of miner. That participant will be responsible for adding the document that contains the harmful code to the blockchain.

Figure 2 shows the phish detection architecture. The safe documents are encrypted using SHA-3 and sent to the respective cloud storage centers. As shown in Figure 2, the input documents are obtained from cloud users.

Once the document is added to the blockchain, its block contents are made visible to all the users. The documents that were identified as safe are for encryption. A user-friendly interface is created to communicate with the blockchain and display the content of the documents that were added to the blockchain in the enhanced PoW process. The safe documents are encrypted and sent to the cloud servers. Figure 3 shows the flow of functionalities incorporated by the modules of detection inside the contract framework. Check homograph is responsible for checking whether the given URL is a homographic phishing URL or not. Three strategies of homographic URL detection are considered, namely, Internationalized Domain Name in Applications (IDNA), typosquatting, and Reserved Character Usage (RCU). If any of the URL detection techniques returns true, the URL is directly considered to be phishing; otherwise, it is sent for detecting chained phishing.

(i) Internationalized Domain Name in Applications (IDNA). It extracts the domain name from the given URL and checks for homographs using multilingual characters.

(ii) Typosquatting. It extracts the domain name from the given URL and checks for homographs using deceptive spellings.

(iii) Reserved Character Usage (RCU). It searches for the reserved characters on a URL that can be used as an escape for redirections.

Web crawling is done with the URLs detected from the documents for the web page content to find the possible

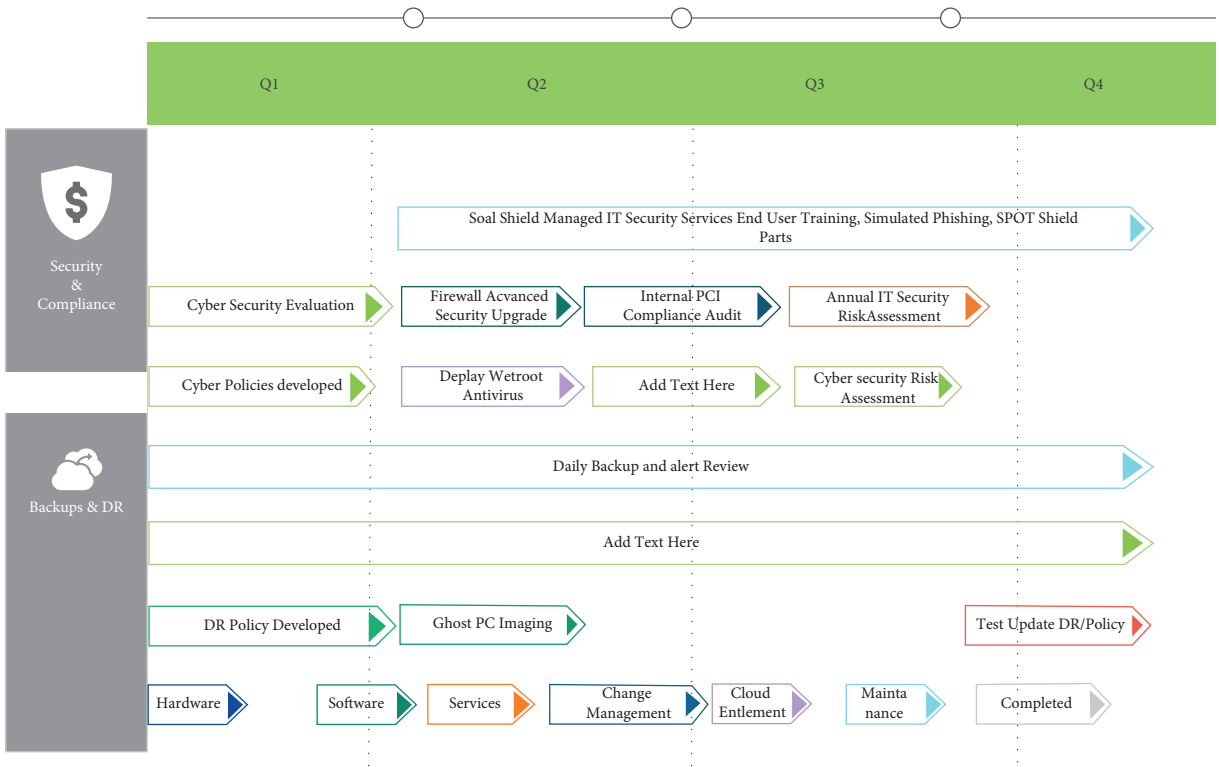


Figure 2: Proposed phish detection blockchain architecture.

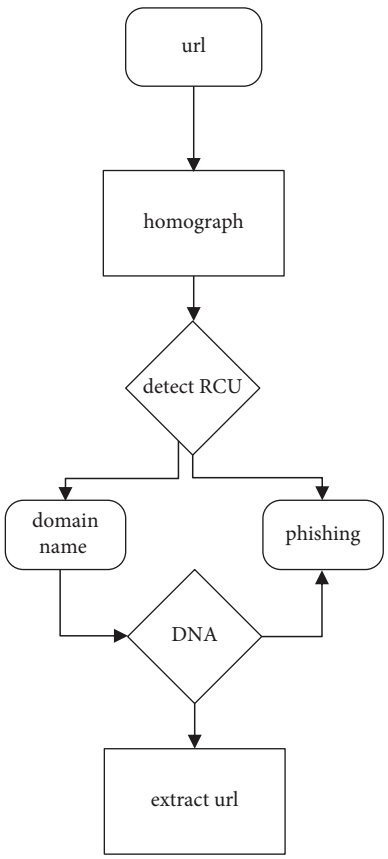


Figure 3: Flow of detection by the proposed Phish Block smart contract.

hyperlinks. The found hyperlink URLs are checked for homographs recursively until no more hyperlink is found.

As shown in Algorithm 1, the Phish Block algorithm takes a random list of documents as input from the dataset. The dataset contains 200 documents with and without phishing URLs. Phishing URLs are coined or referred from Wandera and Phishbank for creating .txt files. The input documents in the list are considered as those the cloud users try to upload to the cloud. The list is traversed to obtain each document. The document is scanned for the presence or absence of a phishing URL. The presence of phishing URL confirms the validity of the contract and deploys the same for creating a block with the document content as the entry. Each block contains a nonce value, hash value, difficulty, coin base, timestamp, file data, gas limit, and configuration details as fields. The content found to have the phishing URL is placed as the file data of the block. The count of blocks in the Phish Block increases as the number of malicious documents in the input list increases. Once the block is created, the Proof-of-Work employed by the Ethereum blockchain chooses the miner for Phish Block and the block gets mined.

The input list is traversed again to remove the documents corresponding to the created blocks from the list. The entire process is repeated until the list reaches the end. All the malicious documents are removed from the list after the completion of these iterations, causing the list size to either remain the same or decrease. The list size remains the same if there are no malicious documents among the list of selected documents. The list size gets reduced according to the respective number of malicious documents in the randomly

```
//n represents the number of documents, doc represents the list containing the n documents, a block is the genesis block
Input:
List of documents (LD)
Output:
Phish Block
Procedure:
input "n" documents in a list "doc"
initialize i = 0
initialize j = 1
do
Scan doc[i]
if (doc[i].CHECK_HOMOGRAPH() = = TRUE) then
   create_block()
   block[j] = doc[i]
   increment j
   PhishBlock_PoW
end
if (User_solves_PoW AND user_details IS VALID) then
   user ←minercreate_block()
   if (add_block == TRUE) then
   initialize k = i
   for k in n − 1:
   doc[k] = doc[k + 1]
   increment k
   end
end
increment i
while (doc.next! = NULL)
display Block Contents
initialize x = 0
do:
   encrypt_doc = Encrypt doc[x]
   add encrypt_doc to cloud
   increment x
   while (doc.next! = NULL)
end
```

Algorithm 1: Phishing detection blockchain.

selected input list. The documents remaining in the list are safe to upload to the cloud. An encrypted version of these files is ready for cloud storage. Algorithm 2 shows the traversal of each and every inputted document to check the presence of phishing URL. The code converter is used to convert the analog to digital values in the proposed work with the help of the boyer Moore algorithm. Punycode convertor has been incorporated by various browsers for phish detection and is the conversion tool that can be incorporated in Python. It is a simple and efficient transfer coding syntax designed to be used with IDNA [24]. Under auto correction using Python, models like error model and candidate model are available. Error model sticks to the proximity of the characters in the keypad for suggesting auto correction whereas candidate models use distance calculation of the words against a dictionary. Under text distance calculation, there are several categories like edit-based, token-based, sequence-based, and phonetic-based. Taking into consideration computational efficiency, Jaccard distance algorithm, a token-based technique, has been used [25]. Reserved characters like ";", ",", and "@" are used in URLs for redirection and are considered as escape characters. A URL with any other domain name followed by reserved characters can be a phishing URL. A naive pattern search algorithm can detect the same [25].

As shown in Algorithm 3, the multichain phishing is implemented using recursive calls. An empty list is given as the input for web crawling, and web contents are stored as .txt files into the list if hyperlinks are detected [26]. The items in the returned list are appended to scan for homographic phishing URLs again and again, until no such URLs are found. Web crawling uses Beautiful Soup, a web crawling framework in Python. Beautiful Soup enables the detection of multichain phishing. It also enables extracting URLs from web pages. It is used to visit web pages corresponding to the extracted URL and crawl through them for retrieving other available hyperlinks [27].

The proposed mathematical procedure aims at materializing the efficiency of the selected features for phish detection. The features used by Phish Block have been selected based on the ability to integrate with blockchain [28]. The rate of error detection can be found from the system's phish

```
Input: Document, D with x lines
Output: Boolean value
Procedure:
initialize i = 0
do:
if (D[i].is_URL == true) then
    RCU = pattern_search(URL, reserved characters)
  if (RCU == true)
    return true
  end
  DN = extract_domain_name(URL)
  IDNA = verify_punycode(DN)
  if (IDNA == true) then
    return true
  end
  TS = autocorrection_probability(DN)
  if (TS ≥ 0.4) then
    return true
  end
  MC = Multichain_Phishing(URL)
  if (MC is_not_null) then
    D.append(MC)
  end
end
  while (i is_lesser_than x)
  return false
```

Algorithm 2: Check_homograph.

```
//href_list represents the list of hyperlinks obtained from the source code of the web content corresponding to the extracted URL, EU
Input: Extracted URL, EU from Document, D
Output: href_list
Procedure:
  initialize href_list = empty
  crawl the HTML source code of EU
  extract hyperlinks
  href_list.add(hyperlinks)
  return href_list
```

Algorithm 3: Multichain_phishing.

block and logical parameters. This set of mathematical equations is used to prove the same.

Let w be the document that needs classification as safe or phishing [29]:

$$wX \longrightarrow \{\text{safe}, \text{phishing}\}. \tag{1}$$

Then, X is the anti-phishing Phish Block system that considers features $f_i \in w$, such that

$$w = \sum_{i}^{n} x f_i, \quad n > 0. \tag{2}$$

w is a non-empty set.

Table 1: Terms and description.

Terms	Description
PSR	Phish success rates
PFR	Phish failure rates
SSR	Safe success rates
SFR	Safe failure rates
P_P	Phishing sites classified as phishing
P_s	Phishing sites classified as safe
S_P	Safe sites classified as phishing
Ss	Safe sites classified as safe
P	Total number of phishing sites
S	Total number of safe sites

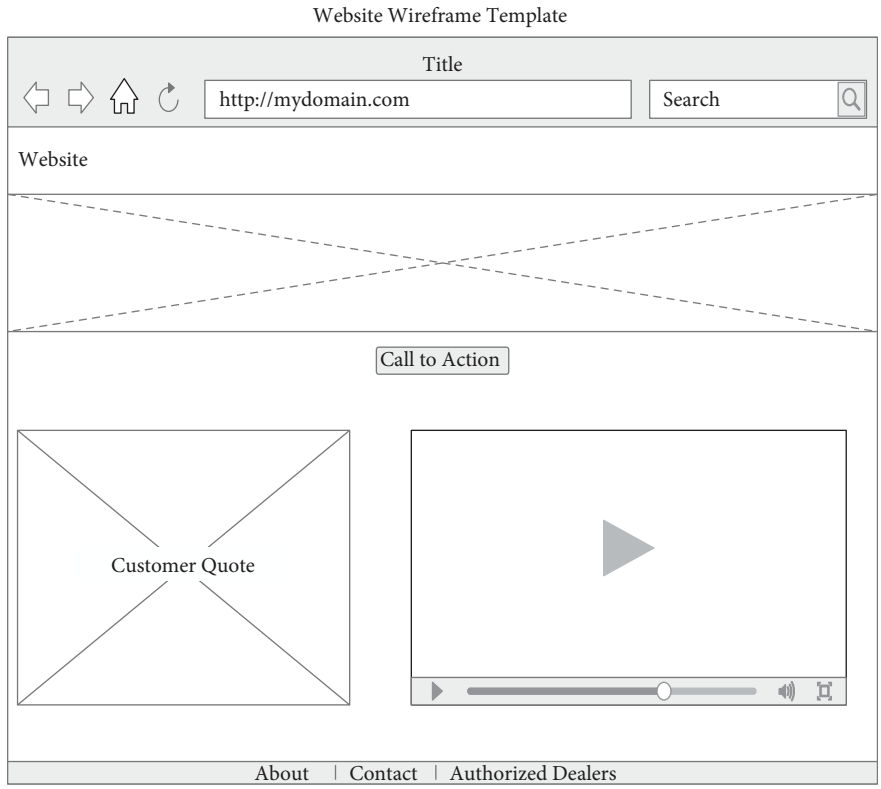


Figure 4: Ethers transferred to the accounts of the private blockchain.

The standards of classifications are applied to the system to analyze the accuracy. The used terms are shown in Table 1.

$$\begin{aligned} \text{PSR} &= \frac{P_P}{P} \times 100, \\ \text{PFR} &= \frac{P_S}{P} \times 100, \\ \text{SFR} &= \frac{S_P}{S} \times 100, \\ \text{SSR} &= \frac{S_S}{S} \times 100. \end{aligned} \tag{3}$$

Accuracy of detection is calculated by the following equation:

$$A = \frac{P_P + S_S}{S + P} \times 100. \tag{4}$$

The reliability of the Phish Block is calculated using Matthews Correlation Coefficient (MCC). When the chosen MCC approaches the value 1, the detection is considered chosen to perfection.

$$\text{MCC} = \frac{P_P \times S_S - P_S \times S_P}{\sqrt{(P_P + P_S)(P_P + S_P)(P_S + S_S)(S_P + S_S)}}. \tag{5}$$

The standards of classifications are applied to the system to analyze the accuracy. The used terms are shown in Table 1.

4. Implementation

4.1. Experimental Setup. The experimental setup for the implementation of the proposed Phish Block involves MetaMask, Rinkeby, Remix, Truffle, and Go Ethereum. MetaMask acts as a gateway to access Phish Block through Firefox browser. Rinkeby is a test network used to collect ethers for compiling the contracts in Phish Block [30], accessed via MetaMask. Remix is the Integrated Development Environment used to run and deploy the Phish Block smart contract. Truffle framework is used to integrate the driver code in Python with the Ethereum smart contract in solidity. Go Ethereum is the client where the accounts can be created and smart contracts for Phish Block can be implemented through Truffle suite. Web3.py library is used for interacting with the blocks [31]. SHA-3 algorithm is used for encrypting the safe documents. It is connected to MetaMask to interact with the private Ethereum blockchain. The interaction with the console is tested [32].

Rinkeby test network is used for collecting ethers. Figure 4 shows that the collected ethers are then transferred to the MetaMask account. Web3 is used to call Ethereum smart contracts [33] using Python. The web interface uses Python, JSON, JS, and Google scripts API.

4.1.1. Dataset. The dataset has been generated with and without URLs. Documents containing URLs consist of safe and phishing URLs. Phishing URLs are framed as homographs belonging to all the three strategies [34] for detection.

```
RandomForestClassifier(bootstrap=True, class_weight=None, criterion='gini',
                       max_depth=None, max_features='auto', max_leaf_nodes=N
one,
                       min_impurity_decrease=0.0, min_impurity_split=None,
                       min_samples_leaf=1, min_samples_split=2,
                       min_weight_fraction_leaf=0.0, n_estimators=1, n_jobs=
-1,
                       oob_score=False, random_state=None, verbose=0,
                       warm_start=False)
                                                                        Out[341]:
RandomForestClassifier(bootstrap=True, class_weight=None, criterion='gini',
                       max_depth=None, max_features='auto', max_leaf_nodes=N
one,
                       min_impurity_decrease=0.0, min_impurity_split=None,
                       min_samples_leaf=1, min_samples_split=2,
                       min_weight_fraction_leaf=0.0, n_estimators=2, n_jobs=
-1,
                       oob_score=False, random_state=None, verbose=0,
                       warm_start=False)
                                                                        Out[341]:
RandomForestClassifier(bootstrap=True, class_weight=None, criterion='gini',
                       max_depth=None, max_features='auto', max_leaf_nodes=N
one,
                       min_impurity_decrease=0.0, min_impurity_split=None,
                       min_samples_leaf=1, min_samples_split=2,
                       min_weight_fraction_leaf=0.0, n_estimators=4, n_jobs=
-1,
                       oob_score=False, random_state=None, verbose=0,
                       warm_start=False)
                                                                        Out[341]:
RandomForestClassifier(bootstrap=True, class_weight=None, criterion='gini',
                       max_depth=None, max_features='auto', max_leaf_nodes=N
one,
                       min_impurity_decrease=0.0, min_impurity_split=None,
                       min_samples_leaf=1, min_samples_split=2,
                       min_weight_fraction_leaf=0.0, n_estimators=8, n_jobs=
-1,
                       oob_score=False, random_state=None, verbose=0,
                       warm_start=False)
                                                                        Out[341]:
RandomForestClassifier(bootstrap=True, class_weight=None, criterion='gini',
                       max_depth=None, max_features='auto', max_leaf_nodes=N
one,
                       min_impurity_decrease=0.0, min_impurity_split=None,
                       min_samples_leaf=1, min_samples_split=2,
                       min_weight_fraction_leaf=0.0, n_estimators=16, n_jobs
=-1,
                       oob_score=False, random_state=None, verbose=0,
                       warm_start=False)
```

Figure 5: Compiling smart contracts using Truffle.

Phishing URLs are coined or referred from Wandera and Phishbank for creating .txt files.

Total documents generated: 200 (safe: 50, phishing: 150).

Documents with no URL: 25.

Documents with safe URL: 15.

Documents with multiple safe URLs: 10.

Documents with phishing URL (IDNA): 25.

Documents with phishing URL (typosquatting): 25.

Documents with phishing URL (RCU): 25.

Documents with multiple phishing URLs (IDNA): 25.

Documents with multiple phishing URLs (typosquatting): 25.

Documents with multiple phishing URLs (RCU): 25.

4.1.2. Implementation of Phish Block. As shown in Figure 5, the Geth client is accessed via Truffle framework. When the complete set of 200 documents are given as input, the files with safe content are encrypted and those with phishing content are added as blocks [35]. The block content and type of phishing as well as the block times are displayed as shown in Figure 6.

```
BaggingClassifier(base_estimator=DecisionTreeClassifier(class_weight=None,
                                                        criterion='gini',
                                                        max_depth=None,
                                                        max_features=None,
                                                        max_leaf_nodes=None,
                                                        min_impurity_decreas
e=0.0,
                                                        min_impurity_split=N
one,
                                                        min_samples_leaf=1,
                                                        min_samples_split=2,
                                                        min_weight_fraction_
leaf=0.0,
                                                        presort=False,
                                                        random_state=None,
                                                        splitter='best'),
                  bootstrap=True, bootstrap_features=False, max_features=1.0
,
                  max_samples=1.0, n_estimators=500, n_jobs=None,
                  oob_score=False, random_state=8, verbose=0, warm_start=Fal
se)
```

Figure 6: Classification of 200 safe and phishing files by Phish Block.

Table 2: Accuracy of Phish Block.

Test cases (files)	Input documents		Detection by Phish Block		Accuracy (%)
	Phishing	Safe	Phishing	Safe	
Test case 1 (50 files)	37	13	34	16	91.89
Test case 2 (100 files)	75	25	68	32	90.67
Test case 3 (150 files)	113	37	103	47	91.15
Test case 4 (200 files)	150	50	132	68	88
Average accuracy:					90.42 = ~ 91

An Ethereum interface has been developed for the interaction with the front end. It allows the safe documents to get uploaded to Google Drive (considered as cloud).

The proposed Phish Block system is tested through 4 test cases. The number of the input documents is increased gradually for each case [31]. Test case 1 takes 50 documents as input, test case 2 takes 100 documents as input, test case 3 takes 150 documents as input, and test case 4 takes 200 documents as input. These documents are randomly chosen by the driver program from the generated dataset containing 200 documents. For evaluating the system, two different measures have been considered. The first measure to be calculated is the accuracy of phish detection by Phish Block, which is shown in Table 2, for each test case [32]. The Phish Block system gives approximately 91% accuracy upon the generated dataset as an average. Figure 7 also clearly shows the misclassification of 9% of the actual files.

The block time is the other measure that has to be computed. It is the amount of time that passes between successive blocks being mined and added to the blockchain [33]. The duration of a block in Phish Block is determined by subtracting the timestamps of its predecessors from those of its successors as they are added to the blockchain in sequence. A function call to the smart contract is made in order to retrieve the timestamp of the newly inserted block. The smart contract then sends the timestamp of the currently active block to the driver application [34]. The total amount of time required to complete the most recent addition of Phish Block is 327 seconds. The result that was obtained is equal to the difference in the timestamps of the first block and the final block that was inserted in test case number 4.

5. Result Analysis

Figure 8 presents the findings, which indicate the inputs that were incorrectly identified for each test scenario. Test case number four has been shown to have the highest amount of incorrect classifications, while test case number one has been shown to be the most accurate of the four. The severely misspelt URLs that were identified by the typosquatting detection system led to the misclassification that occurred. Because our typosquatting detection relies on an auto correction technique, it is not possible to identify large degrees of variance in the text. Despite this, the efficiency of the system has not been compromised in any way since URLs with significant misspellings are easy for human eyes to see. Phish Block has achieved a maximum accuracy of 91.89 percent in test case 1 and a minimum accuracy of 88 percent in test case 4. This is due to the number of misclassifications, as well as the quantity of documents that were supplied as input in each of the relevant test cases. When evaluated with 100 files, the system demonstrates an accuracy of 90.67 percent, whereas in test case 2, it shows an accuracy of 91.15 percent.

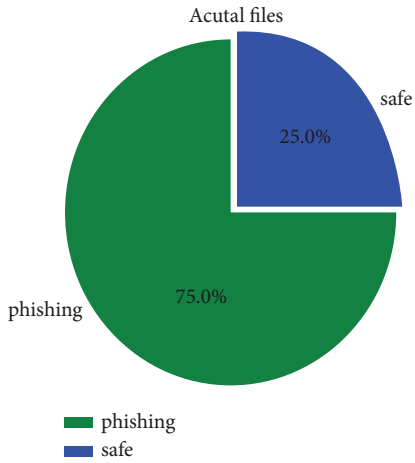


Figure 7: Displaying the ratio of the phishing files and safe files.

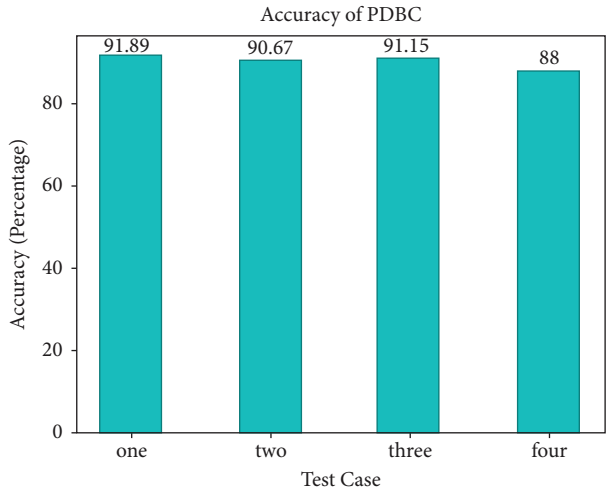


Figure 8: Accuracy shown by Phish Block for different test cases.

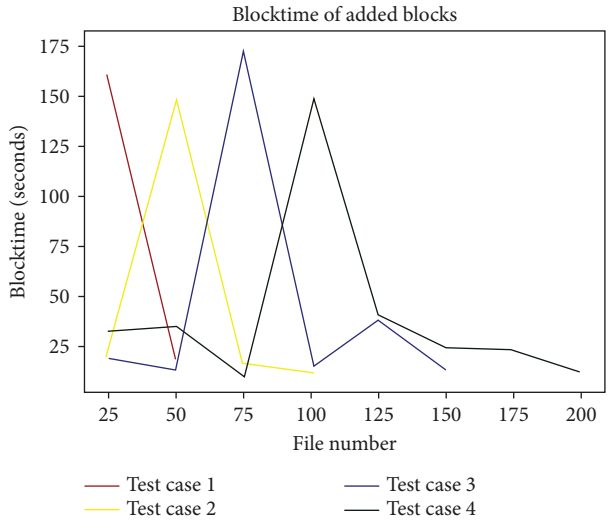


Figure 9: Graph representing the block time for different test cases.

In each of the test cases, the block timings of the subsequent blocks that were appended to the Phish Block are shown in Figure 9. Recordings of the block timings were taken at regular intervals of every 25 files that were provided as input. The files are mapped to the times at which their individual blocks were created in order to ensure that they are successfully mined into the Phish Block. When the succeeding blocks are added to the Phish Block at the same timestamp or when the accompanying files are not added to the chain, the block time is recorded as zero seconds. The blockchain does not include the files that do not include phishing URLs, and the block time values for such files are set to zero seconds. It is abundantly clear that the block timings of the blocks that were added in test case 1 suffered highest volatility among values that were not zero. This might be the explanation for the successful first run of the deployed contracts as well as the high level of accuracy achieved while identifying phishing files. The recording time of case 2 and case 4 is 147 seconds and 148 seconds which is taken as input in the system. In addition, the minimum block timings for test cases 2 and 4 are comparable, being 11 seconds and 10 seconds for 25 files, respectively. Case 3 reaches its maximum point with a block time of 175 seconds, which makes it the most successful of the tests. The first test case takes 20 seconds, which is the maximum time among the lowest block timings. Because succeeding blocks have identical timestamp values, the block duration has been cut down, which may be ascribed to this fact. At the conclusion of test case 4, it became apparent that the blocks were being mined to Phish Block at a quicker rate. According to the detected pattern, the blocks are mined slowly at first but then quickly pick up the pace as they get closer to the finish, which causes the block time values to fall. It has come to our attention that test case 3 has required the greatest amount of time for processing files, which ranges from 50 to 75 seconds. It is possible to draw the conclusion that the 25 files were either an examination of multichain phishing or alternative safe files. The system has shown signs of becoming more consistent as the test cases continue to be carried out. Both test case 2 and test case 4 have maintained a constant block time for blocks mined within the intervals of 25–50 and 75–100 seconds, respectively. It would seem that test case 1 has reached its maximum block time while processing the first batch of 0–25 files. It has been observed that the maximum value always happens up to the first 100 files in each of the four scenarios; beyond that point, the system begins to operate at a quicker pace. After conducting a thorough examination of the patterns, it has been deduced that the block duration of a newly added block may rapidly increase after an extended period of mining inactivity. In any case, the existence of harmful files in the inputs collected from cloud users is not playing the major role in real time, and as a result, the block timings of the blocks are anticipated to be quite high.

6. Conclusion and Future Work

The proposed Phish Block has been implemented on a private Ethereum blockchain, and it has been effective in keeping the homographic phishing URLs (about 91 percent). On the other hand, papers that were unnoticed included various sorts of phishing URLs (around 9 percent). The

phishing filter that has been suggested also includes a few restrictions. The default difficulty level designed for the Ethereum platform has been an overhead in block time. This is changeable when the Phish Block algorithm is applied on a self-configured private blockchain that the CSP could afford, and the modification leads to improved block time. Not only would the addition of the Phish Block system as a utility offer safety for cloud storage and cloud users, but it would also provide an additional value as a trust element in the service level agreement (SLA) that is supplied by the cloud service provider (CSP). Therefore, the suggested phishing block has the potential to bring about a significant influence on the customer's choice of cloud services among the several CSPs that are competing. In upcoming projects, we will be working to make the Phish Block more resistant against documents that include phishing content by including detection of various forms of phishing and providing sufficient compensation for the cost involved.

Data Availability

The data used to support the findings of this study can be obtained from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest to report regarding the present study.

Acknowledgments

This research was supported by Taif University researchers supporting project no. TURSP-2020/306, Taif University, Taif, Saudi Arabia.

References

[1] J. Shen, T. Zhou, D. He, Y. Zhang, X. Sun, and Y. Xiang, "Block design-based Key agreement for group data sharing in cloud computing," *IEEE Transactions on Dependable and Secure Computing*, vol. 16, no. 6, pp. 996–1010, 2019.

[2] J. Xue, C. Xu, and Y. Zhang, "Private blockchain-based secure access control for smart home systems," *KSII Transactions on Internet and Information Systems*, vol. 12, no. 12, pp. 6057–6078, 2018.

[3] W. Zheng, Z. Zheng, X. Chen, K. Dai, P. Li, and R. Chen, "NutBaaS: a blockchain-as-a-service platform," *IEEE Access*, vol. 7, Article ID 134433, 2019.

[4] J. Mahatpure, M. Motwani, and P. K. Shukla, "An electronic prescription system powered by speech recognition, natural language processing and blockchain technology," *International Journal of Science & Technology Research (IJSTR)*, vol. 8, no. 8, pp. 1454–1462, 2019.

[5] K. Lei, M. Du, J. Huang, and T. Jin, "Groupchain: towards a scalable public blockchain in fog computing of IoT services computing," *IEEE Transactions on Services Computing*, vol. 13, no. 2, pp. 252–262, 2020.

[6] S. Xie, Z. Zheng, W. Chen, J. Wu, H. N. Dai, and M. Imran, "Blockchain for cloud exchange: a survey," *Computers & Electrical Engineering*, vol. 81, Article ID 106526, 2020.

[7] A. Patel, N. C. Debnath, and P. Kumar Shukla, "SecureOnt: a security ontology for establishing data provenance in semantic web," *Journal of Web Engineering*, vol. 21, no. 4, pp. 1347–1370, 2022.

[8] Y. Mu, F. Rezaeibagha, and K. Huang, "Policy-driven blockchain and its applications for Transport systems," *IEEE Transactions on Services Computing*, vol. 13, no. 2, pp. 230–240, 2020.

[9] S. B. Goyal, N. Pradeep, P. K. Shukla, M. M. Ghonge, and R. V. Ravi, *Utilizing Blockchain Technologies in Manufacturing and Logistics Management*, IGI Global, PA, USA, 2022.

[10] M. Zhaofeng, W. Lingyun, W. Xiaochang, W. Zhen, and Z. Weizhe, "Blockchain-enabled decentralized trust management and secure usage control of IoT big data," *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 4000–4015, 2020.

[11] D. Minoli and B. Occhiogrosso, "Blockchain mechanisms for IoT security," *Internet of Things*, vol. 1–2, pp. 1–13, 2018.

[12] P. K. Shukla, L. Sharma, K. Raj Bhatele, P. Sharma, and P. Shukla, K. I. Lakhtaria, Design, architecture, and security issues in wireless sensor networks," in *Next Generation Wireless Network Security and Privacy*, pp. 211–237, IGI Global, Hershey, PA, 2015.

[13] Z. Cui, F. Xue, S. Zhang et al., "A hybrid BlockChain-based identity authentication scheme for multi-WSN," *IEEE Transactions on Services Computing*, vol. 13, no. 2, pp. 241–251, 2020.

[14] P. Rani, P. N. Singh, S. Verma, N. Ali, P. K. Shukla, and M. Alhassan, "An implementation of modified blowfish technique with honey bee behavior optimization for load balancing in cloud system environment," *Wireless Communications and Mobile Computing*, vol. 2022, Article ID 3365392, 14 pages, 2022.

[15] H. Wang, H. Qin, M. Zhao, X. Wei, H. Shen, and W. Susilo, *Blockchain based fair payment smart contract for public cloud storage auditing*, Elseiver - Information Sciences, vol. 519, pp. 348–362, 2020.

[16] K. S. Khan, K. Saleem, M. M. Hazzazi, M. Alotaibi, P. K. Shukla, and M. Aqeel, "Human psychological disorder towards cryptography: true random number generator from EEG of schizophrenics and its application in block encryption's substitution box," *Computational Intelligence and Neuroscience*, vol. 2022, Article ID 2532497, 20 pages, 2022.

[17] P. C. Wei, D. Wang, Z. Yu, S. K. S. Tyagi, and N. Kumar, "Blockchain data based cloud data integrity protection mechanism," *Future Generation Computer Systems*, vol. 102, pp. 902–91, 2020.

[18] S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han, and F. Y. Wang, "Blockchain-enabled smart contracts: architecture, applications, and future trends," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 49, no. 11, pp. 2266–2277, 2019.

[19] Y. Zhang, S. Kasahara, Y. Shen, X. Jiang, and J. Wan, "Smart contract based access control for the internet of things," *IEEE Internet Of Things Journal*, vol. 6, no. 2, pp. 1594–1605, 2019.

[20] C. N. Gutierrez, T. Kim, R. D. Corte et al., "Learning from the Ones that got away: detecting new forms of phishing attacks," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 6, pp. 988–1001, 2018.

[21] M. A. Adebowale, K. T. Lwin, E. Sanchez, and M. A. Hossain, "Intelligent Web Phishing Detection and protection scheme using integrated features of images, Frames and Text," *Elsevier- Expert Systems with Applications*, vol. 115, pp. 300–313, 2019.

[22] M. Kaur and D. Singh, "Multiobjective evolutionary optimization techniques based hyperchaotic map and their applications in image encryption," *Multidimensional Systems and Signal Processing*, vol. 32, no. 1, pp. 281–301, 2021.

[23] C. Pham, L. A. T. Nguyen, N. H. Tran, E. N. Huh, and C. S. Hong, "Phishing – aware: A Neuro – Fuzzy approach for anti – phishing on fog networks," *IEEE Transactions on Network and Service Management*, vol. 15, no. 3, pp. 1076–1089, 2018.

[24] C. M. R. D. Silva, E. L. Feitosa, and V. C. Garcia, "Heuristic based strategy for Phishing prediction: A survey of URL - based approach," *Elsevier- Computers and Security*, vol. 88, 2020.

[25] R. Zhao, S. John, S. Karas et al., "Design and Evaluation of the highly insidious extreme phishing attacks," *Elsevier- Computers and Security*, vol. 70, 2017.

[26] I. Vayansky and S. Kumar, "Phishing - challenges and solutions," *Elsevier - Computer Fraud and Security*, vol. 2018, no. 18, 2018.

[27] M. Kaur, D. Singh, V. Kumar, B. B. Gupta, and A. A. Abd El-Latif, "Secure and energy efficient-based E-health care framework for green internet of things," *IEEE Transactions on Green Communications and Networking*, vol. 5, no. 3, pp. 1223–1231, Sept. 2021.

[28] S. Gupta, K. K. Gupta, P. Kumar Shukla, and M. Kumar Shrivas, "Blockchain-based voting system powered by post-quantum cryptography (BBVSP-pqc)," in *Proceedings of the 2022 Second International Conference on Power, Control and Computing Technologies (ICPC2T)*, pp. 1–8, IEEE, Raipur, India, March 2022.

[29] A. Aldaej, T. A. Ahanger, M. Atiquzzaman, I. Ullah, and M. Yousufudin, "Smart cybersecurity framework for IoT-empowered drones: machine learning perspective," *Sensors*, vol. 22, no. 7, p. 2630, 2022.

[30] L. Allodi, T. Chotza, E. Panina, and N. Zannone, "The need for new antiphishing measures against spear-phishing attacks," *IEEE Security & Privacy*, vol. 18, no. 2, pp. 23–34, 2020.

[31] J. B. Awotunde, S. Misra, O. B. Ayoade, R. O. Ogundokun, and M. K. Abiodun, "Blockchain-based framework for secure medical information in internet of things system," in *Blockchain Applications in the Smart Era. EAI/Springer Innovations in Communication and Computing*, S. Misra and A. Kumar Tyagi, Eds., Springer, Cham, Switzerland, 2022.

[32] T. Ahamed Ahanger, A. Aldaej, M. Atiquzzaman, I. Ullah, and M. Yousuf Uddin, "Securing consumer internet of things for botnet attacks: deep learning approach," *Computers, Materials & Continua*, vol. 73, no. 2, pp. 3199–3217, 2022.

[33] S. Khezr, M. Moniruzzaman, A. Yassine, and R. Benlamri, "Blockchain technology in healthcare: a comprehensive Review and directions for future research," *Applied Sciences*, vol. 9, no. 9, p. 1736, 2019.

[34] P. Ratta, A. Kaur, S. Sharma, M. Shabaz, and G. Dhiman, "Application of blockchain and internet of things in healthcare and medical sector: applications, challenges, and future perspectives," *Journal of Food Quality*, vol. 2021, Article ID 7608296, 20 pages, 2021.

[35] S. S. Kushwaha, S. Joshi, D. Singh, M. Kaur, and H.-N. Lee, "Systematic Review of security vulnerabilities in ethereum blockchain smart contract," *IEEE Access*, vol. 10, pp. 6605–6621, 2022.

[36] A. Ghosh, S. Gupta, A. Dua, and N. Kumar, "Security of Cryptocurrencies in Blockchain Technology: State-Of-Art, Challenges and Future Prospects," *Journal of Network and Computer Applications*, vol. 163, Article ID 102635, 2020.

Hindawi
Security and Communication Networks
Volume 2023, Article ID 9763845, 1 page
https://doi.org/10.1155/2023/9763845

Retraction

Retracted: Practical Research on College English Teaching Mode Reform Based on Computer Multimedia

Security and Communication Networks

Received 8 August 2023; Accepted 8 August 2023; Published 9 August 2023

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope
(2) Discrepancies in the description of the research reported
(3) Discrepancies between the availability of data and the research described
(4) Inappropriate citations
(5) Incoherent, meaningless and/or irrelevant content included in the article
(6) Peer-review manipulation

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] Z. Yang, "Practical Research on College English Teaching Mode Reform Based on Computer Multimedia," *Security and Communication Networks*, vol. 2022, Article ID 7110400, 9 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2022, Article ID 7110400, 9 pages
https://doi.org/10.1155/2022/7110400

Research Article

Practical Research on College English Teaching Mode Reform Based on Computer Multimedia

Zhao Yang

Institute of Foreign Languages, Hunan University of Humanities, Science and Technology, Loudi 417000, Hunan, China

Correspondence should be addressed to Zhao Yang; drm@bbc.edu.cn

Received 5 July 2022; Revised 15 August 2022; Accepted 29 August 2022; Published 10 September 2022

Academic Editor: Rabie Ramadan

The fastest development of technologies encourages computer multimedia-oriented education. Nowadays, information technologies create human basic abilities. College English teaching mode reform based on computer multimedia is the aim of the paper. Generally, computer multimedia technologies oriented college English education merging pictures, videos, audio, vocabulary, and animation. We described the development of multimedia in English teaching mode, applications of college English teaching, a novel model of foreign language teaching in the classroom and a computer, computerized English language teaching method TPACK design, and the latest architecture of college English language teaching based on computers in this paper. We are discussing face-to-face teaching, language lab autonomous learning room, network teaching area in multimedia, and network teaching circumstances in this paper. This paper evaluated wireless communication's range, challenges facing college English teaching, comparative analysis of attitude, comparative analysis of curriculum, and comparative analysis of technology. We express that, from the year 2000 to the present, the technologies in wireless communications with computer multimedia are developing in the range of wireless communication.

1. Introduction

The English major is comprised of three aspects, language learning theory, the technology of foreign language teaching, and the theory of foreign language teaching. These aspects have to be agreed out fairly, in that time be completely developing. The present college course is one of the fundamental courses of the University [1]. The eagerness in English learning is undoubtedly linked with the advantages English could provide to its learners. On a national level, English is considered as playing an important role in national advancement and modernization. On an individual level, English is considered a passport for career development and flourishing personal advancement [2]. More English talents are required for society along with the advancement of the economy, technology, science, and cultural exchange. So the necessity for college English teaching is put forward. All universities should reform college English Teaching, according to the particular situation of University and college English teaching [3].

The teaching of English plays a vital role in college education by enhancing the level of students' English. Also, it is a crucial basis for the pupil to integrate into the development trend of the globe. Still, there are various issues in college English teaching, and the effect of teaching is not clear. The reform of college English is essential for making teaching conform to the advancement of the new education atmosphere and also for making the teaching practice more connected with modern education's standards [4]. The advancement in computer and global technology pave the way for the revolution and enhancement of college English teaching. Application skills and English knowledge, intercultural communication and learning strategies are the main contents utilized by the College English teaching, and the guidance of linguistic and foreign language teaching theory is being used. Also, it is concerned with a system of teaching that holds various teaching methods. To unite the methods of traditional classroom teaching and modern teaching, the enhanced teaching model must be used. Reforming the traditional teaching model is the

keystone of the college English model reforming. The network teaching model is comprised of plenty of operational and practical importance to college English teaching, and the coordination of students and teachers is essential to the effective use of the model [5].

The computer multimedia technology-based college English classrooms combine images, words, animation, video, and audio. The core of teaching is broken by the intuitive and vivid computer multimedia technology factors, and it has the human-computer interaction which is not in traditional teaching. Utilizing a task-focused teaching method under multimedia conditions is recommended to develop college English multimedia teaching and to improve the language consciousness and capability of students [6]. The college English teaching reform in private universities and colleges is a big responsibility for educators. In private universities and colleges, there is still a long way to go in the college English teaching reform [7]. An essential subject in fundamental teaching is college English teaching. A key role is played by college English teaching in enhancing the basic knowledge and quality of English of students [8]. The limitations in the present college English teaching can be overcome by the utilization of multimedia computer technology [9]. With the advancement of technology and science, computer multimedia has been utilized broadly in all phases, particularly in English teaching. The mixture of English teaching and computer multimedia makes the English class teaching interesting. The multimedia-assisted English teaching could encourage pupils' eagerness of learning English and improves the atmosphere of English class. Also, it could improve students' listening and speaking ability and encourages students' eagerness for communication. The distinct teaching features, and the teaching atmosphere of computer multimedia, assisted English teaching has been accepted by the greater part of students and teachers for the improvement of students' ability in learning English [10]. Thus, this paper explores the college English teaching mode reform based on computer multimedia. The major contribution of the paper is expressed in the following:

(i) The newness of the paper is English teaching mode with multimedia and modifications of the conventional teaching design to the latest method.

(ii) This paper described the Information Communication Technology of English language teachers and wireless communication in multimedia.

2. Related Works

Tan [11] expressed that China's education department is publishing educational information 2.0, which is to execute an action plan. Integrate information technology to get innovative in teaching. FiF smart learning (FiF-SL) is introduced by Leshan Normal University. iFLYTEK Co., Ltd improved the intelligent learning platform. To improve oral and broad English ability, FiF smart teaching platform presented the perfect role in a positive manner that was presented by this research.

Shu [6] expressed that this article utilizes English translation for the use of multimedia-oriented teaching. To improve students' curiosity, online translation software, online English translation, and multimedia sources are utilized. The application of multimedia-oriented teaching sources creates actual English learning circumstances. It concentrates to make strong college English translation training. Through this, pupils realized English translation and grammatical knowledge. This article said college English multimedia classroom has to improve learning with the awareness of language and capabilities.

Chen [12] expanded from music teaching data and cross-border relations optimizing (CBRO) relationships. The features of computer multimedia music teaching analysis were achieved from the relationship among computer multimedia, and the music teaching classrooms, and the improvement of computer multimedia techniques. In basic music teaching, computer technologies use was investigated, by analytics the optimization of music teaching techniques. Also, in music teaching, the positive effect of computer technology was expressed.

Li [13] expressed that instructors' use of multimedia, growth, and the use of media sources were considered in this article. The proposed way to resolve these issues by utilizing the latest technologies of information merged with conventional teaching techniques (CTT) is expressed. The major importance positioned on the technique is to connect the latest information technologies into the teaching model. The outcome of the paper is the plentiful teaching content strength by the latest teaching which means that the English classroom person is bringing a brand new empire.

Zhiyong et al., [14] investigated the College English Language Teaching Reform, English Foreign Language lecturer views, and CELTR's improving the EFL lecturer's teaching practice, affecting the effects and implementations of CELTR. In China's Nanyang city, from the newly enhanced university, ninety-two English Foreign Language lecturers participated in this research. Overall, the outcomes indicate that the English Foreign Language lecturer had a moderate stage of understanding and knowledge about College English Language Teaching Reform and that the teaching practice of lecturers has been satisfactorily improved due to the implementation of College English Language Teaching Reform.

Kanellopoulou et al., [15] expressed that this paper is based on the theoretical basis of dual-code and multimedia learning principles for creating a highly successful digital tool utilizing movies and scripts. Bilingual coding is providing indirect access from a particular language to another, and various kinds of subtitles are explored for their effectiveness. At last, this paper looks into a few latest alternative audiovisual apparatuses which actively engaged learners in an active manner with subtitles and movies, framed towards vocabularies learning.

Al-Ajmi and Aljazzaf, [16] expressed that this article came to recognize the aspects influencing the usage of multimedia technology in English language teaching in Kuwait. To investigate this proposed design, questionnaires and empirical data are gathered. There are seven factors to

using multimedia for learning the English language. The factors are motivating, facilitating, behaviors, community, effective factors, and teaching. Also, the outcome of the paper is that the lecturers have a positive concept of technology. But need more support and supplements.

Zhang and Lin [17] developed the author of this dissertation takes the university-oriented ESP course, International Textile Business English as a case study, and uses the key concept of the four schools of structuralism as a lead to streamlining the teaching process. In China, there is no permanent teaching content or structure to follow. Most instructors do not have a background in textile engineering. To some extent, complete qualification is required to teach courses such as those having an engineering background. The most important thing is that the instructor without a textile engineering education background is completely incompetent to teach a course with an engineering background. But its originality expressed that language letters. It has to follow language teaching and learning rules without a doubt. Next, the teacher has to be ready to learn. And through learning, the teacher has to take an effort to share.

3. Proposed Methodology

Computer multimedia technology utilizes a computer to deal with the information of graphics, text, pictures, animation, video, and sound to start logical relationships and communication among computers and human beings. Computer multimedia teaching indicated the teaching procedure of selecting correct designs and utilizing the latest teaching media based on the teaching object and the student's qualities via the teaching model and merging along with conventional instruction designs. Computer multimedia teaching denoted the teaching procedure of selecting appropriate designs and utilising the most recent teaching media based on the teaching object and the student's characteristics via the teaching model and combining them with traditional instruction designs with a large amount of media details to structure a realistic teaching procedure. Excellent teaching outcomes will be acquired. Computer multimedia instruction designs graphics, animation, audio, other media signal, and text combined into a single thing with a sequence of bendable communication among computers and human beings which is based on the application of the utilization. And communication is clear and amicably, with ignoring capability. But, this highly developed teaching design cannot perform out that is the correct performance with correct utilization. The computer multimedia teaching method developed the instinct of teaching and inspired the learning eagerness of the pupils, and computer multimedia teaching expands the teaching time of the lecturers, and these are considered the advantage of computer multimedia teaching. There are some methods to develop computer multimedia teaching. They know instruction schedules exactly, create good computer multimedia course content, and along with conventional teaching, colleges should increase the investment in computer multimedia teaching [18]. Figure 1 expresses the development of computer multimedia in English teaching mode.

3.1. Applications of College English Teaching. College English teaching is considered the most difficult of English teaching. Nevertheless, these circumstances express chances to execute daring reforms. Many pupils, and lecturers, are concerned with the practical investigation and theoretical research of teaching reforms. In the new teaching model, the effect of the reforms contains some features and trends. The most indicated and leading thing is the constructivism teaching concept. It stresses English's instrumental nature and emphasizes language's meaning is more than language's form. Humans considered English as the shortest view of the subject. But, the reality is English is considered essential communication equipment, which is utilized to develop the pupil's language in a very good manner and which will recover the English communication equipment. To accomplish this target, the English language application is considered the center. People have to provide full effect to achieve unity of teaching targets from sentence teaching to cultural beauty's transmission and content teaching. English is considered a tool language so pupils have the capability to communicate. After learning, they have to do work [19].

3.2. English Teaching Mode with Multimedia. In recent years, China's foreign language standards have been too poor when compared globally; they are long-term and contain some errors, suggesting that dump english has a good relationship with traditional english teaching. Generally, English-teaching classes focus on the teachings such as grammar, finding the answer, and vocabulary. But, this way of teaching declines the learners' ability. With the growth of technologies in the twenty-first century, the English teaching mode has begun as the latest method which is relevant to classrooms and computers, which was expressed in Figure 2. When utilizing classroom and computer-oriented English teaching models, colleges get more advantages from the latest information technologies. It is very important to establish the solo teaching model, in which the instructor is the central focus, through the use of computer multimedia. English learning and teaching will not be restricted to place and time which is directed towards learning by self and personalizing. Teaching model changing is not considered a change that change has to be in philosophical teaching, which is a great change. It executes the changes from teacher-centered, easiest teaching, and learning language knowledge to a new learning model which is related to student-centered. Languages change learning by self-skills and language realistic that has to be expressed that the latest teaching model execution is a world-shattering transformation of the conventional English teaching model.

Figure 3 expresses the computerized English language teaching method has taken shape. When discussing the connection between English language teaching and the computer, the think of computer-assisted language learning is very usual. Computer skill is considered an important thing. But, with the great growth of computer science, we have to understand the position of computers in the English language. The pupil can have a lot of microcomputers.

Figure 1: Development of computer multimedia in English teaching mode.

Anyone can get learning sources anywhere from networks. Also, they can gain more knowledge based on their requirements.

3.3. Multimedia and Network Teaching Circumstance

(i) Multimedia classroom with face-to-face teaching

In the English hypothetical knowledge class, face-to-face interaction has to be improved, because of the aspects of the English subject. But boring grammar, and hypothetical knowledge class, is like a difficult part for all the pupils every time. To overcome these issues, these classes have to be assembled in computer multimedia classrooms. Through the utilization of computer multimedia equipment, teachers can help with lecturing, and they can change the difficult part into an eye-catching part. Also, they will develop the quality of lecturing.

(ii) English interactive lecturing with language lab

In foreign language teaching, language skills are the most significant especially like speak and listening. While comparing conventional classrooms, they cannot provide the perfect language practice and circumstances. So, nowadays, English speaking and listening are provided in language labs. Pupils, and lecturers, can realize the easiest communication, role-play, and discussion through pronunciation design, which improves practice and ability results.

(iii) Networks based on autonomous learning with autonomous learning room

Improving and teaching language utilization skills is considered a long-term process. But pupils' practice time in the computer multimedia classroom is being too decreased. This realism demanded that pupils will get good favorable language learning circumstances. According to the local area network and the campus network, they framed the English network autonomous learning method. They will see foreign language network sources through the campus network.

(iv) Online learning with network teaching area

Nowadays, on university campuses, lecturers, and pupils, face-to-face interaction is decreased. Colleges are making campus networks in college English teaching platform which creates English teaching skill that is more bendable and unlimited. Lecturers, and pupils, will be organizing dissimilar networks of teaching actions in the area including online class appointments, online FAQs, online classes, discussions on online, online examinations, and a lot [20].

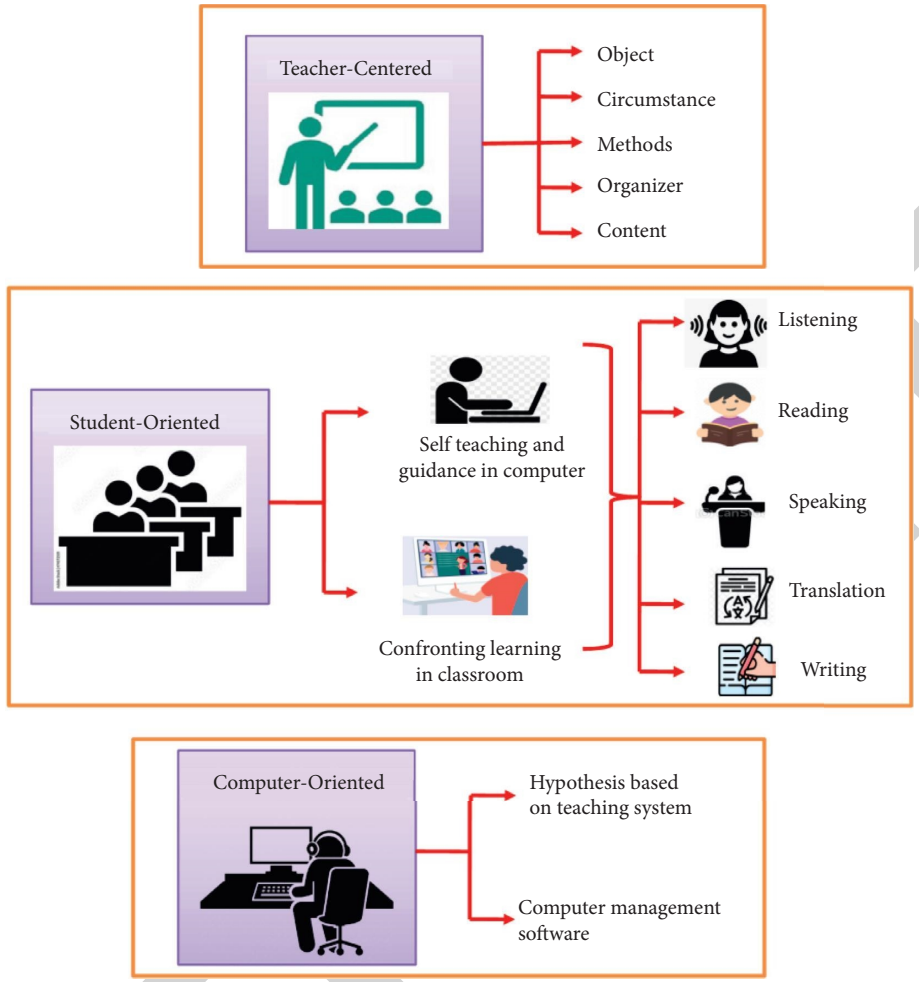


Figure 2: Novel model of foreign language teaching in the classroom and computer.

3.4. Modifications of the Conventional Teaching Design to the Latest Method. The latest computer multimedia English learning is connected with the traditional textbook and a classroom learning method. There, lecturers provide knowledge through textbooks and computer presentations. Nowadays, pupils provide attention to their self-learning. Lecturers also do not guide conventional teaching. New English teaching methods view modification as a thing that develops the student's knowledge. Therefore, computer multimedia assists modification in teaching the conventional teaching circumstances leading to a basic modification in the teaching architecture [21]. Figure 4 represents the latest architecture of college English language teaching.

3.5. Information Communication Technology Literacy of English Language Teachers. In most of the research, the researcher mentioned the specialty of English language learning and teaching. The function of learning activities such as connecting students and their interests enhances learning-based instruction. The advantage enhances and expands under technical advancements that are expressed devices like tablets and smartphones to English language teaching framework. Learning and teaching the English language enables us to cross space and time limits and create extra communication and amusement [22]. The efficiency, mobility, and expediency of mobile learning contain create clearly [23]. The advantages of mobile learning have to be extensible, to the English as a Foreign Language framework. The assimilation of mobile technologies in English language learning, and teaching, helps the growth of pupils' language capabilities. Lecturers' guidance is an essential thing all the time, but more than instructors, mobile learning is the central thing to learners. Teaching with technologies will be a problematical job for a few instructors under the impact of circumstances and social causes. Thus, instructors have to learn the knowledge of teaching knowledge and technology. TPACK design helps to know the understanding ability of teachers and taking actions based on that. Schulman's actual work expressed the concept of an instructor's knowledge through his pedagogy content knowledge model, and by Kohler and Mishra, the TPACK design was improved, as the method of describing connections. Figure 5represents teachers' knowledge of technology, content, and education. In this figure, instructor's technology knowledge, content knowledge, and pedagogy knowledge are linked and a guide to the three latest knowledge structures such as pedagogy content knowledge, technology pedagogy knowledge, and

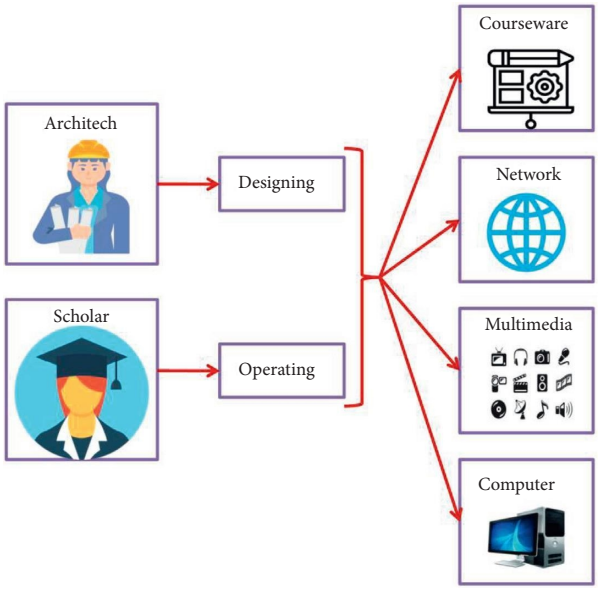


Figure 3: Computerized English language teaching method.

technology content knowledge. These three types of knowledge connections create TPACK. This is considered the central theme of TPACK. The word TPACK categorizes through teaching, technology knowledge, and the teaching of content knowledge. The concept of TPACK attracts the researcher's attention. But, there is a little explanation for its relevance in particular subjects like language learning as well as teaching. Informative and communicative technologies on literacy of universities and English language instructors was rarely investigated as a structure of TPACK in the COVID-19 platform of secondary English language teaching or foreign language learning [24].

3.6. Wireless Communication in Multimedia. Multimedia is a structure of computer science, which indicates two or three media mixtures. Multimedia is considered the media's unity [10]. Wireless broadcast technologies and computer multimedia technologies are considered the latest trend, with the fastest growth in information technologies. The fame of the Internet has hurried the consolidation of these dual technologies. Also, the fastest growth of mobile connections has expressed a better command for wireless remote transmission. The wireless remote transmission will send pictures, video, and audio. Velocity, several service channels, and media support are the features of wireless transmission data. According to the transmission velocity, it is not lower than conventional data transmission design. Also, it will be explained other businesses. While comparing the conventional data with other transmission methods, distant wireless communication contains broad application chances. With the arrival of the 5G, that will be capable to present utilizers with effective transmission velocity and great quality multimedia service. One of the main wireless networks technology is considered Bluetooth technology. This allows for different communicative devices and home gadgets to link wirelessly. Due to the frequency hopping technologies, its

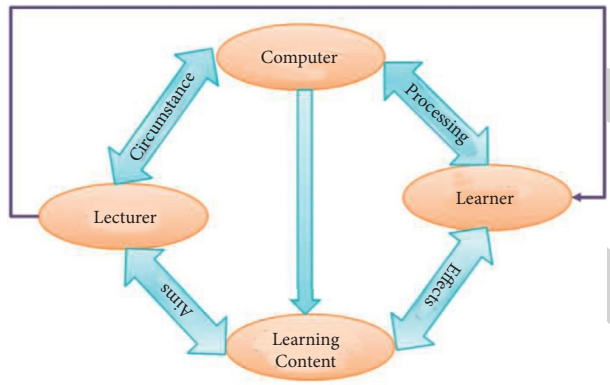


Figure 4: Latest architecture of college English language teaching based on computers.

battery life will be available for some days. The scale of Bluetooth is not well. Also, it accepts some gadgets only. One of the most comfortable technologies is considered as wifi technology. While comparing other technologies, it is being too faster. And its benefits are noticeable. But, its battery life is not to believe. It may fail within one hour, and it will not meet up humans' needs for less power low amount and consumption. According to UWB, wireless USB technology was created, which is dissimilar from Bluetooth and wifi, which is the class of noncarriers communications. The factors of wireless USB technology are extensive battery life and the low amount, which is accurately fitting for long-distance transmissions. It also needs scalability and safety. One of the trustworthy technologies is considered ZigBee technology. But, transmission remoteness is too short, and transmission rates are too slow. So, it is not apt to the remoteness transmissions. NFC technology is the change in radiofrequency recognition technologies and interconnected technologies. 13.56 MHz is considered the operating frequency. While comparing various communication technologies which are dependable transmissions remoteness is shorter, its permanence and velocity are improved than infrared [25]. Overall, wireless communication technologies support multimedia in various ways.

4. Results and Discussion

This section analyzes the wireless communication's range, challenges facing college English teaching, comparative analysis of attitude, comparative analysis of curriculum, and comparative analysis of technology. Figure 6 presents the range of wireless communication in computer multimedia from 2000 to 2020. This graph expresses the years and the percentage of wireless communication's range. The results are in 2000 (63%), 2004 (69%), 2008 (76%), 2012 (88%), 2016 (90%), 2021 (95%). From 2000 to the present, wireless communications with computer multimedia technologies have advanced. While comparing it in 2000, wireless communication performance is improving. This result supports to find the growth of the technologies.

Figure 7 represents the challenges facing college English teaching in computer multimedia-based. The challenges are

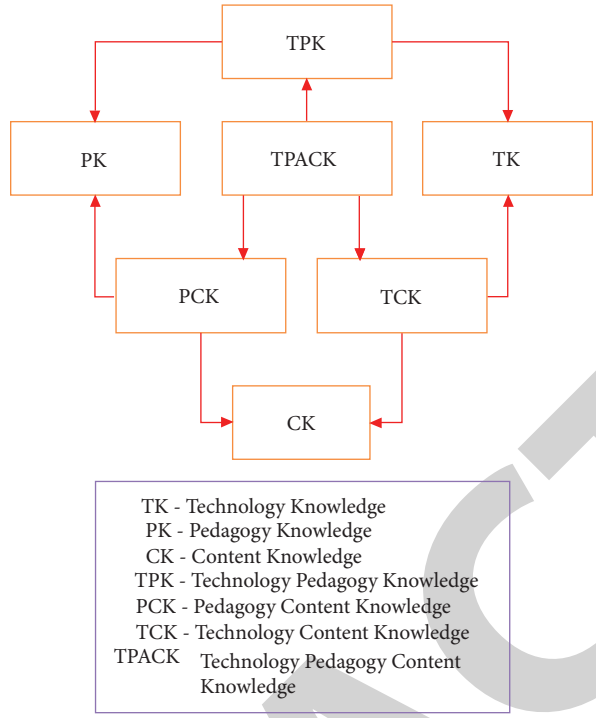


Figure 5: TPACK design.

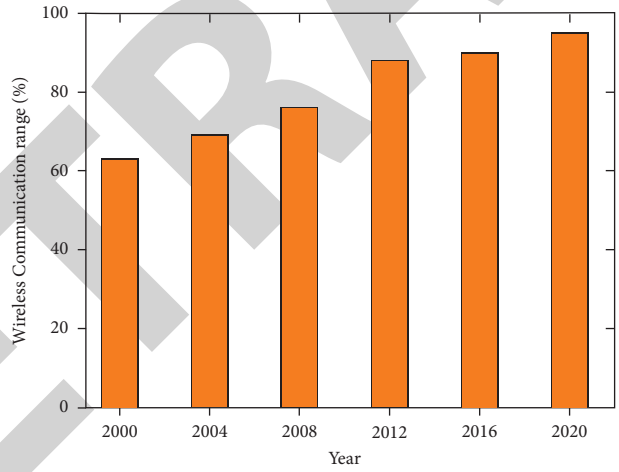


Figure 6: Wireless communication's range.

utilizing various languages in the classroom, infrastructure lacking, in-person interaction lacking, and discipline lacking. This graph plotted the challenge rate and challenges facing college English teaching computer multimedia-based. The result is utilizing various languages in the classroom (75%), infrastructure lacking (85%), in-person interaction lacking (25%), and discipline lacking (65%). While comparing other challenges, infrastructure lacking (85%) is considered a very difficult challenge. In-person interaction lacking (25%) is too low.

In this section (Figure 8), the techniques such as FiF- SL, CBRO, CTT, and proposed methods are utilized for comparative analysis of attitude. The proposed method is high. Attitude level is compared with other methods. Here, FiF-SL is 35%, CBRO is 45%, CTT is 65%, and the proposed method is 95%.

In the coming section (Figure 9), the methods such as FiF- SL, CBRO, CTT, and proposed techniques are used for comparative analysis of the curriculum. The curriculum level is greater when compared with various techniques. In this analysis, FiF-SL is 45%, CBRO is 65%, CTT is 57%, and the proposed method is 94.5%.

In the following section (Figure 10), the techniques such as FiF-SL, CBRO, CTT, and proposed techniques are applied for comparative analysis of the technology. The technology level is greater when compared with other methods. In this,

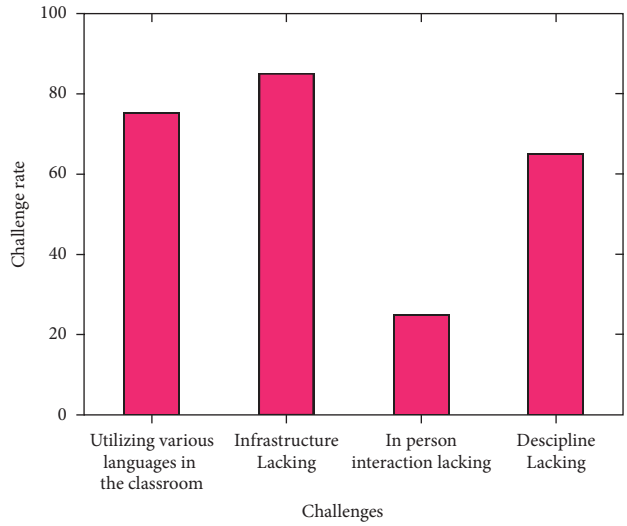


Figure 7: Challenges facing college English teaching.

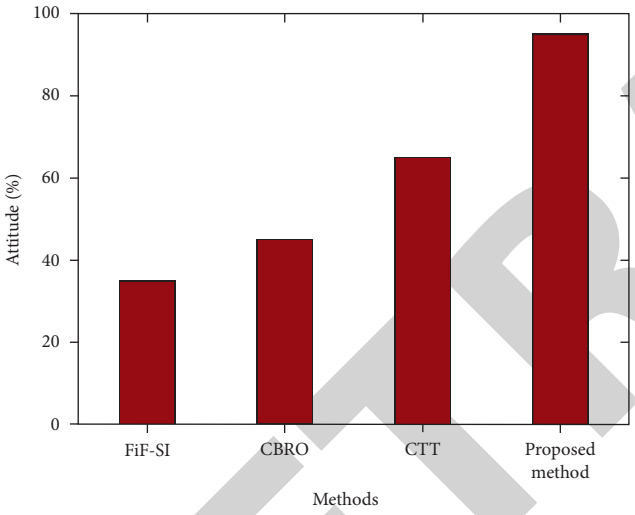


Figure 8: Comparative analysis of attitude.

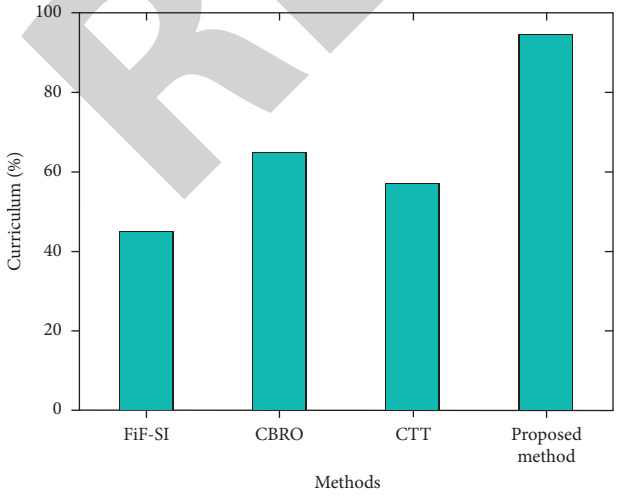


Figure 9: Comparative analysis of curriculum.

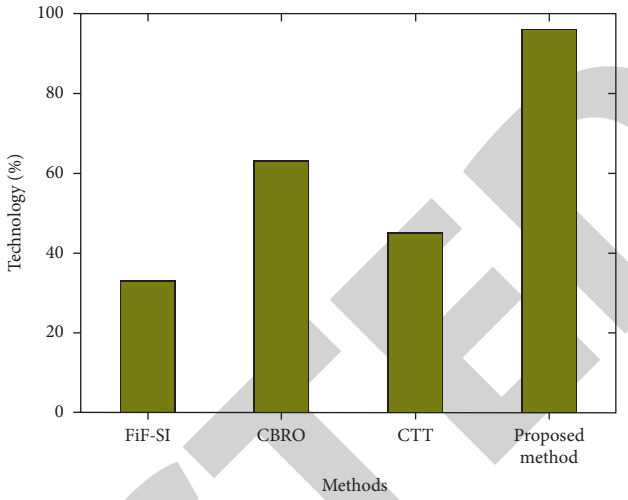


Figure 10: Comparative analysis of technology.

FiF-SL is 35%, CBRO is 45%, CTT is 65% and the proposed method is 95%.

5. Conclusion

This paper expresses the college English teaching mode reform based on computer multimedia. Here, the development of computer multimedia in English teaching mode, a novel model of foreign language teaching in the classroom and a computer, computerized English language teaching method TPACK design, and the latest architecture of college English language teaching based on computers are presented in this paper. This paper analyzes wireless communication's range, applications of college English teaching, challenges facing college English teaching, comparative analysis of attitude, comparative analysis of curriculum, and comparative analysis of technology. In the wireless communication range, we express that, from 2000 to the present, the technologies in wireless communications with multimedia have developed. Infrastructure lacking (85%) is considered a very difficult challenge in this paper. While comparing FiF-smart learning, cross-border relations optimization, and conventional teaching techniques, the proposed model is greater. And we are focusing on face-to-face teaching, language lab autonomous learning room, network teaching area in multimedia, and network teaching circumstances in this paper. Thus, computer multimedia makes a more positive influence on college English Teaching mode reform.

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 known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.