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This article has been retracted by Hindawi following an investigation undertaken by the publisher [1].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 preprocesses 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

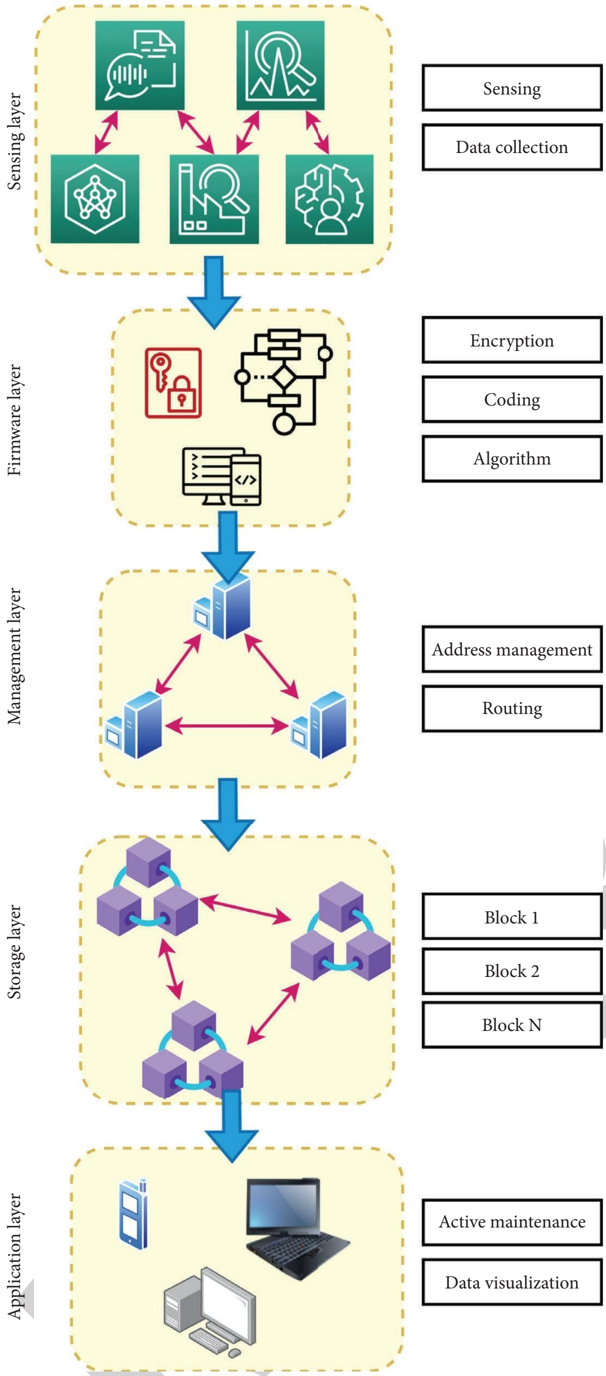


FIGURE 1: Logical architecture of the DNN-RSM system.

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:

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

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:

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

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.

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

$q_{\mathrm{ID}}, q_c, q_G,$ andq_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.

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

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:

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

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:

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

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.

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

The mean resource is shown as $\underline{f}_{xy}$ 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.

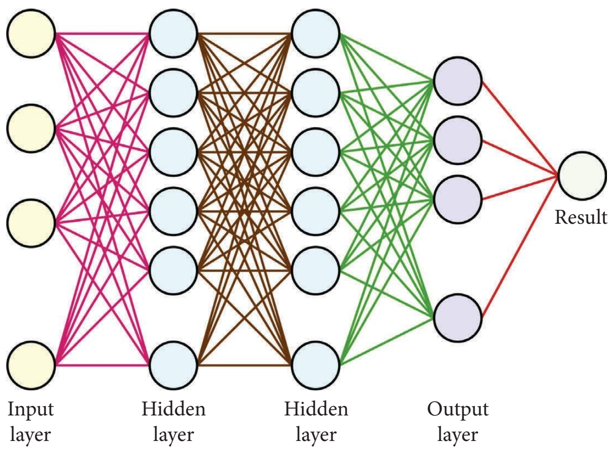


Figure. 2: Structure of the neural network.

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:

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

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:

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

$S_f(k) = i$ for positive values of k, $S_f(k) = 0$ for negatives values of x, and $\hat{b}_x$ 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:

$$Q = \frac{\prod_{x=0}^{N} \mathrm{Rq}_x - \prod_{x=0}^{N} \mathrm{Rs}_x}{\prod_{x=0}^{N} b_x}. \qquad (13)$$

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 mini-computers. 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.

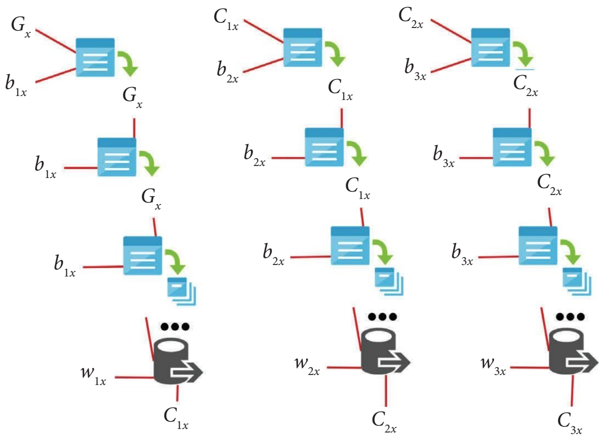


Figure 3: The mathematical view of the hidden layer functions.

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.

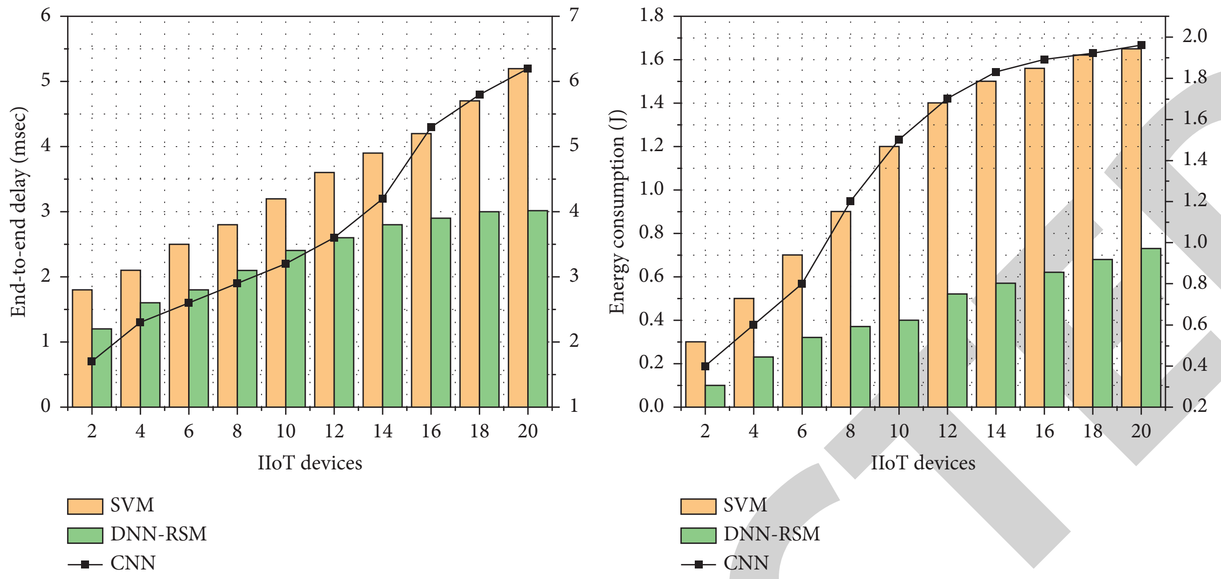
The suggested DNN-RSM method is designed in this section for security enhancement. The DNN-RSM with DNN and SoftMax layer provides higher security features in intelligent manufacturing with an advanced RSA algorithm. The impact of the DNN-RSM system is analysed and showcased in the next section.

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



(a)

(b)

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

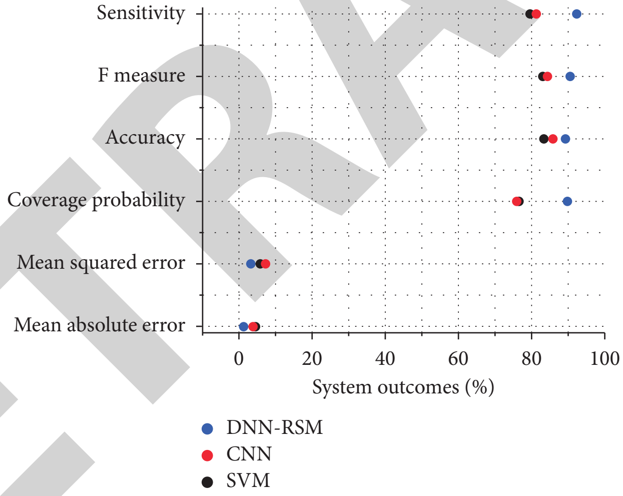
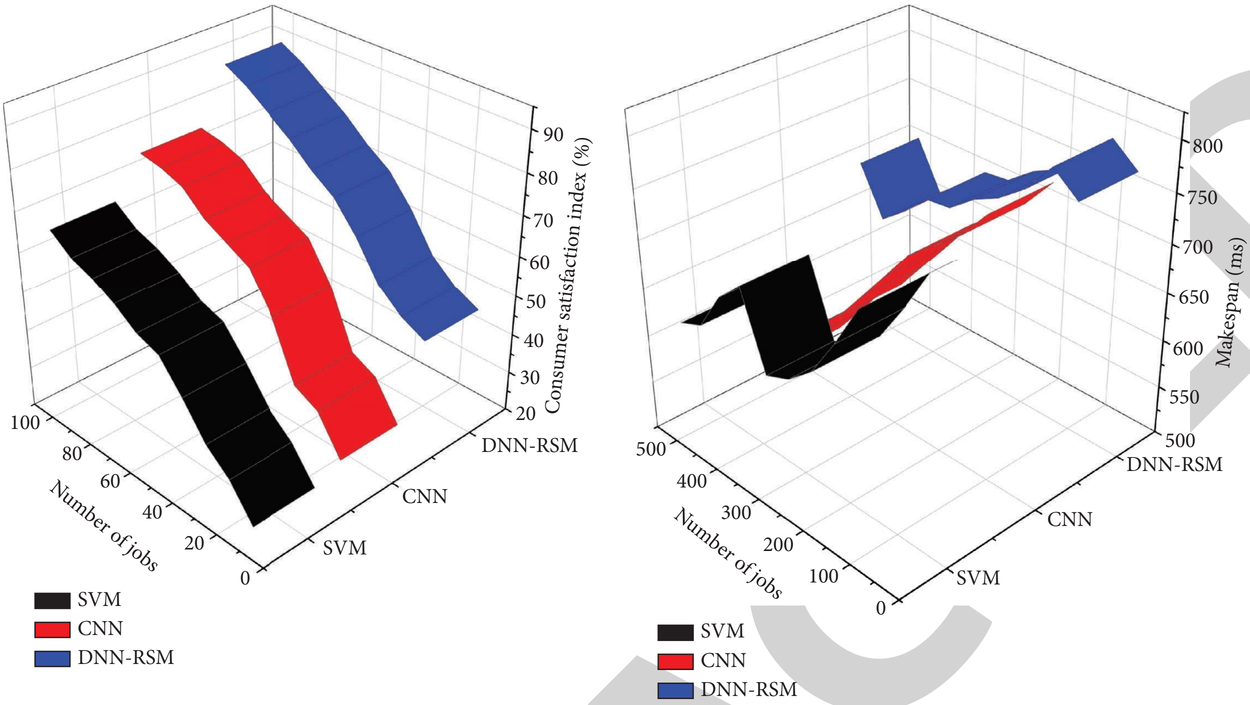


Figure 5: System performance analysis.

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 $\overline{f}_{xy}$ 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.



(a)

(b)

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

Internet of Vehicles," *Transactions on Emerging Telecommunications Technologies*, p. 4520, 2022.

[31] M. Gupta, R. Kumar, S. Shekhar et al., "Game theory-based authentication framework to secure internet of vehicles with blockchain," *Sensors*, vol. 22, no. 14, p. 5119, 2022.

[32] M. Gupta, B. Sharma, A. Tripathi et al., "n-Player stochastic duel game model with applied deep learning and its modern implications," *Sensors*, vol. 22, no. 6, p. 2422, 2022.

[33] H. Garg, N. Gupta, R. Agrawal, S. Shivani, and B. Sharma, "A real time cloud-based framework for glaucoma screening using EfficientNet," *Multimedia Tools and Applications*, vol. 81, no. 24, pp. 34737–34758, 2022.

[34] H. Garg, B. Sharma, S. Shekhar, and R. Agarwal, "Spoofing detection system for e-health digital twin using EfficientNet Convolution Neural Network," *Multimedia Tools and Applications*, vol. 81, no. 19, pp. 26873–26888, 2022.