Computers, Materials & Continua
DOI: 10.32604/cmc.2022.026513
Article

Tech Science Press

An Efficient Security Solution for Industrial Internet of Things Applications

Alaa Omran Almagrabi*

Department of Information Systems, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, Kingdom of Saudi Arabia
*Corresponding Author: Alaa Omran Almagrabi. Email: aalmagrabi3@kau.edu.sa
Received: 29 December 2021; Accepted: 02 March 2022

Abstract: The Industrial Internet of Things (IIoT) has been growing for presentations in industry in recent years. Security for the IIoT has unavoidably become a problem in terms of creating safe applications. Due to continual needs for new functionality, such as foresight, the number of linked devices in the industrial environment increases. Certification of fewer signatories gives strong authentication solutions and prevents trustworthy third parties from being publicly certified among available encryption instruments. Hence this blockchain-based endpoint protection platform (BCEPP) has been proposed to validate the network policies and reduce overall latency in isolation or hold endpoints. A resolver supports the encoded model as an input; network functions can be optimized as an output in an infrastructure network. The configuration of the virtual network functions (VNFs) involved fulfills network characteristics. The output ensures that the final service is supplied at the least cost, including processing time and network latency. According to the findings of this comparison, our design is better suited to simplified trust management in IIoT devices. Thus, the experimental results show the adaptability and resilience of our suggested confidence model against behavioral changes in hostile settings in IIoT networks. The experimental results show that our proposed method, BCEPP, has the following, when compared to other methods: high computational cost of 95.3%, low latency ratio of 28.5%, increased data transmitting rate up to 94.1%, enhanced security rate of 98.6%, packet reception ratio of 96.1%, user satisfaction index of 94.5%, and probability ratio of 33.8%.

Keywords: Industrial internet of things (IIoT); blockchain; trusted third parties; endpoint verification

1 Introduction

The Industrial Internet of Things (IIoT) has gained popularity as it enables contemporary industrial operations and applications to increase efficiency and effectiveness [1]. The IIoT combines industry and network connection worlds by connecting, controlling, and monitoring everything in industry [2]. New business models such as the proactive maintenance that keeps machinery and

This work is licensed under a Creative Commons Attribution 4.0 International License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

equipment down to a minimum require further data interchange between manufacturing systems and other types of equipment [3]. Because of this continuous digitization, a higher level of networking is essential in industrial facilities and the manufacturing business [4]. Smart sensors are linked to systems that enable Industrial Internet of Things (IIoT) applications, using especially low-cost edge node devices [5]. The increasing interconnections and equipment increase the attachment area and lead to new safety challenges [6]. Due to its potential for quicker and better decision making, the IIoT is significant. The IIoT can provide an insight into the wider supply chain, allowing enterprises to coordinate and achieve further efficiencies. Endpoint authentication is an authentication method used to validate an external or remote network connector [7]. This approach guarantees that the network is mainly linked to legitimate or authorized endpoint devices.

Smartphones, tablets, and servers are included among such gadgets [8]. Endpoint security is the technique of safeguarding terminal devices or access points from hostile players and campuses such as PCs, laptops, and mobile devices [9]. Security endpoint systems safeguard these endpoints against cybersecurity attacks on a network or in the cloud [10]. Endpoint safety has developed from standard antivirus software to provide complete protection against advanced malware and developing zero-day threats [11]. Hacktivists, organized crime, and intentional and unintentional insider threats are endangering organizations of all sizes [12]. The IIoT can help firms better understand their business operations by delivering incredibly detailed data in real-time. Analyzing data from sensors can make their processes more efficient and offer up new sources of income. The IIoT can provide an insight into the wider supply chain, allowing enterprises to coordinate and achieve further efficiencies. Safety at endpoints is frequently viewed as the forefront of cybersecurity, and the endpoint is one of the top locations in which companies seek to safeguard corporate networks [13]. For several reasons, an endpoint platform for protection is important to business cybersecurity [14]. Data collection is sometimes the most relevant asset a company has in today's economic climate and the loss of data or access to such data may jeopardize the entire organization [15]. These include direct sales, subscriptions, premiums, and the franchise. Depending on the business, one of these income-generating strategies is likely to be the most appropriate approach to manage the organization. Companies have never had to face such an increasing number of endpoints [16]. Endpoint safety is a practice where endpoints or entry points of end-user products such as desktops, laptops, and mobile devices are secured from malicious actors or campaigns. Today's endpoint protection solutions are designed swiftly to identify, analyze, block, and contain ongoing assaults. This makes it harder for business safety by distant operational and network rules, progressively making perimeter protection insufficient and creating vulnerabilities [17]. Add to the cost of redistributing resources from company objectives to address risks, the cost of a major reputation infringement, and the actual financial impact of compliance violations and it is easy to see why platforms are considered essential for safeguarding contemporary businesses [18,19]. Endpoint security management is the policy that is developed to guarantee the safety and security of all the endpoint devices in a network [20]. It is part of an extensive cybersecurity program, a modern need for small local companies and big multinationals [21]. There is limited guidance and management of IoT devices for the life cycle, and limited best practice is available for IoT developers. In addition, the authentication and permission standards for IoT edge devices are lacking. Endpoint security is a technique of protecting the information and workflows of the devices connected to the network [22]. The EPP works by looking at files while entering the networks. Modern EPPs leverage the power of the cloud to maintain a continuously increasing database of information about threats, to unbundle endpoints involved with keeping all this information locally and to maintain them [23]. More speed and scalability can sometimes be achieved by accessing this information via the cloud [24].

The EPP provides a single dashboard that allows cybersecurity professionals to remotely regulate security for each device for system administrators on a network gateway or server. The monitoring of endpoints concerns tracking activity and risk on all the mobile network devices. It represents the process of continual and continuous management of a dynamic range of endpoints in a corporate network. This article introduces the notion that the IIoT based on blockchain technology has been trusted and used in several industries to ensure anonymity. The IIoT is concerned with the IoT branch that specially deals with the production and agriculture industries. It likewise involves linking gadgets and making them considerably more intelligent and available, and on a far larger scale. The end objective in industry is to improve speed and safety to enhance the smooth operation of manufacturing sites at a lower cost.

1.1 Limitations of the Work

As a result, blockchain is a guaranteed solution, with a decentralized structure and distributed approach, and is a helpful approach to IIoT situations. The blockchain used is a block chain that tracks and coordinates transactions and stores data for millions of IIoT devices on distributed blocks. However, endpoint security software examines the whole corporate network and may provide visibility for all connected endpoints from a single location. Legacy antivirus solutions depend on the user for manual updating or updating the databases in advance. EPPs offer integrated security, which transfers management duties onto IT companies or cybersecurity staff. An important initial step requires all devices to use an authorized operating system and a virtual private network (VPN). If a device does not comply, access to essential data might be restricted. Users may now remotely manage or even automate security programs to ease the procedure.

2 Related Works Based on IIoT Secure Authentication

Xu et al. [25] described the Novel Blockchain Framework (NBF) to edge computing in the IIoT. This report offered a Layered Lightweight Blockchain Framework (LLBF) and implementation method restricted by resources. The framework comprises a resource-restricted blockchain layer and an extended resource layer in the IIoT. A lightweight consensus method and a dynamic trust algorithm are created to enhance blockchain performance and minimize verified transactions in fresh blocks.

Khan et al. [26] suggested the Blockchain-Based Secure Image Encryption Scheme (BCSIES) for the IIoT. The cryptographic pixel values of a picture are recorded on the blockchain to ensure data privacy and security. Encrypted findings demonstrate that the method presented is very successful in preventing and ensuring data leakage.

Arachchige et al. [27] explored the PriModChain for industrial IoT systems. This article offered a PriModChain architecture that promotes data confidentiality and confidence via mixing differential privacy, ML, Ethereum blockchain, and intelligent contracts. PriModChain was tested with the help of simulations created in Python using socket programming on a general purpose computer in terms of privacy, security, dependability, security, and resilience.

FASTEN IIoT for the end-to-end integration of the Industrial Internet of Things was expressed by Costa et al. [28]. The aim was to give a flexible, configurable, and open solution to the FASTEN IIoT Platform. The platform works as an interface of 4.0 advanced applications and solutions between the shop floor and the industry. These efforts include administration, provision, optimization, and simulation by harmonizing diverse data source features while fulfilling real-time needs.

A hinge classification algorithm based on mini-batch gradient descent with an adaptive learning rate and momentum (HCA-MBGDALRM) was described by Yan et al. [29]. In contrast to standard neural networks, decision trees, and retrograde logistic measures, the method significantly increases the performance of deep network training. In the shuffle phase, they have solved the data skew problem, and they are implementing a parallel HCA-MBGDALRM framework to increase the processing speed of very large data sets.

The node degree (N), distance from the cluster (D), residual energy (R), fitness (NDRF), and salp swarm algorithm (SSA) for a secure Industrial Internet of Things was deliberated by Abuhasel et al. [30]. The sensor nodes' accuracy is calculated using the SSA. SoftMax's deep-neuronal network is recommended to minimize latency and overhead communication for IIoT devices. In all cluster head applications, optimal resource planning is dependent on the demand for storage, computation, and bandwidth.

A cybersecurity framework (CF)-based power system connected for the IIoT was discussed by Jang et al. [31]. A suitable cybersecurity directive must thus be developed to allow effective answers to risks posed by cybersecurity due to the misuse of such flaws. Unfortunately, developing an effective cybersecurity guideline for each organization is not straightforward.

A deep-learning feature extraction based semi-supervised model (DLFE-SSM) for IIoT networks was introduced by Hassan et al. [32]. In addition, they presented an adaptive IIoT network for confidential border security utilizing a DLFE-SSM. The technique described requires no manual effort to upgrade the attack databases. The quickly changing nature of unknown attack models may be learned through unmonitored learning and unlabeled wild data. A BlockEdge model is proposed in [33], which combines blockchain and edge computing to address a few of the critical issues faced by the current IIoT networks. The authors validate the possibility of BlockEdge in terms of latency, power consumption, and network usage. In [34], the authors propose a blockchain-based model along with fog computing (FC), which inserts a blockchain with a yet-another-consensus protocol creating a safety structure into FC for storing and transmitting IoT data.

The main contribution of this paper:

- ➢ Designing the proposed BCEPP to enhance cybersecurity with secure end-to-end communication.
- ➢ The proposed method, BCEPP, utilized the virtual network function for optimized network output.
- ➢ The experiment has been performed based on the proposed BCEPP to achieve a high data transmission rate, packet reception, security, and user satisfaction index.

The overall paper structure is as follows: Section 1 discusses the importance of endpoint node verification for the IIoT; Section 2 explores the related works based on IIoT secure authentication; Section 3 demonstrates the BCEPP for reducing the network latency; Section 4 presents the results and discussion; and Section 5 concludes the paper.

3 Blockchain-based Endpoint Protection Platform (BCEPP)

This paper discusses the Industrial Internet of Things (IIoT) for endpoint authentication. A novel idea, termed the industrial relationship between IIoT devices, will be based in the first part of this paper's architecture. The model to monitor IIoT nodes in the architecture is suggested in the trust metrics. Compared to the conventional IIoT network design of automotive plants, the simulation results have demonstrated the energy efficiency of our BCEPP architecture. The manufacturing

industry concentrates on converting tangible goods, such as raw materials, into final products, while the production process includes non-tangible items. Both procedures aim to develop finished items that are sold for profit by firms. The first part of this paper's architecture will be built on a unique notion known as the industrial interactions between IIoT devices. In the confidence metrics, the model for monitoring IIoT nodes in the architecture is suggested. The simulation results showed the energy efficiency of our BCEPP architecture compared to the standard IIoT network design of manufacturing plants. The essential distribution and security of IIoT applications in practice involve the intelligent placement of services in physically distinct areas that directly influence latency and an appropriate policy enforcement system that ensures dependability, security, and services security. This article addresses these concerns by presenting a new VNF solution for the IIoT that reduces the overall latency while verifying that network-wide rules such as connection or isolation exist between the endpoints. Networking enables individuals to access opportunities that may not be found alone. The network can give information on what possible employers are searching for and recommendations on developing a network professionally.

The IIoT infrastructure schemes are shown in Fig. 1. Various possible approaches for secured communication and control in the IIoT via a cloud platform or at the leading level around Fig. 1 have been suggested. Authors have introduced technology for understanding the IoT, controlling access, downloading, and identifying viruses for data protection. If an assault breaches cloud-based security measures effectively, few documented solutions to assure the safety of a CPS are available. The local safety of a CPS is not responsible operationally for these works. The closest work the author could detect shows that the primary part of the middleware layer is an IoT name resolution service. The technique to detect and minimize safety hazards initially requires specific CPS limits for the IIoT. Workplace safety can be related to both physical and mental security. In both circumstances, it indicates a reasonably safe workplace for all employees and actively avoids insecurity in the workplace.

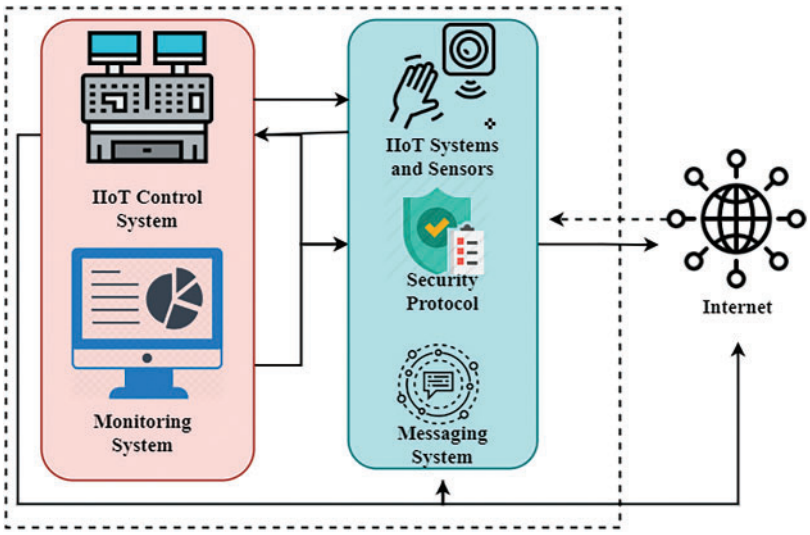

Figure 1: IIoT architecture

Network connection management is then set to these criteria by the CPS. Fig. 1 illustrates the position of the heating fan sensor and refrigeration ventilators, as described in the above paragraph, in the IIoT system and external sensor system (the scattered-line box). The microcontroller Raspberry Pi is the feature of every block with a dotted line. The detection of endpoints and reactions, often

known as endpoint threat detection and response, is the integrated endpoint security solution, combining continuous monitoring and data gathering in real-time with automated response and analysis capabilities based on rules. The IIoT control system controls cooling and heat supply, as indicated in the above section. The monitoring device identifies all uneven CPS activities. The protocol of the security system provides appropriate web security protocols based on tracking system data. The messaging platform transmits important messages to the users based on the IIoT control system; the IIoT covers industrial applications, including robotics, medical devices, and manufacturing processes with software definition. The IIoT extends beyond regular consumer gadgets and physical IoT-associated internet activities. The last part of the normal surgery is stated in the circumstances that follow. If the target temperature is not stabilized for at least 30 s, the messaging system will produce a message announcing uneven operation on the IIoT gateway. When the temperature within the target environment has not stabilized within 50 s, all network connections with the IIoT gateway are terminated by the protocol frame.

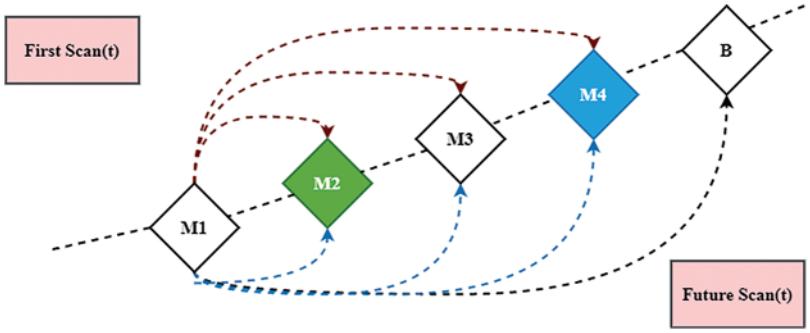

Figure 2: Mapping network node

This study provides a method based on edge nodes that examines the network environment from each smart sensor. The example of mapping from a network node device is shown in Fig. 2. There are four nodes (M1–M4) in this sample network, and M1 periodically scans the network pseudo-randomly. The first scanning findings of four devices (M1–M4) are shown in the dashed arrows. This first scan will be used as a reference and this network must be kept safe. After then, the network enters a new edge node device (A). The second (dotted) scan finds the expected equipment on the one hand and the new equipment on the other (A). This may suggest an intruder or other activities that cause the network to change maintenance. The following settings can be used for the network scanning and mapping in which the connections of the hosts are analyzed. The following classes include the standard port scan techniques and extra possibilities. These groups are divided into two classes. Activated hosts in the network can be discovered with an internet control message protocol (ICMP) ping sweep. SYN detects and connects scanning of open ports and services. The detection of redirection might utilize time. The approaches provided here incorporate these as a safety component for devices with IIoT edge nodes. No network scanner for low-power MCUs is currently available to the best knowledge of the authors.

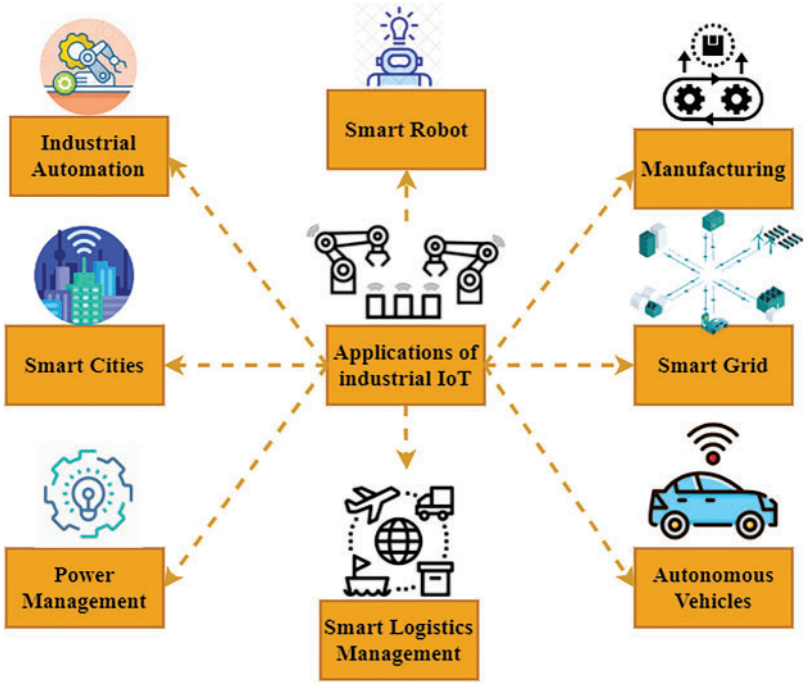

Figure 3: IIoT blockchain-based architecture

The preceding section presented an IIoT blockchain-based architecture that considers the importance of the IIoT network to provide confidence and privacy. There are several advantages to the IIoT, as shown in Fig. 3. Predictive maintenance is one of the primary advantages of the IIoT, using sensors that can anticipate machine faults in real-time from the IIoT. It moreover leads to better on-site servicing by helping to spot possible equipment problems. Asset management, customer satisfaction, and facility management are all of the IIoT's benefits, and all this is achievable provided the network runs without any problems. There can be confidence and privacy problems via the suggested design of the blockchain. In this section, various key blockchain architecture applications in the IIoT will be highlighted. Industrial automation can be revolutionized by blockchain technology. Blockchain can combine a large number of digital ledgers stored in various locations and process them as blocks. This results in improved governance of transactions. Process automation as well as transparency may be achieved by integrating technology and automating business operations. This might prove fabrication, as any transactions that follow depend on confirmation of the preceding transactions. Many factories are developing intelligent robotics systems. Intelligent robotics is concerned with the correct and efficient use of tools and resources. Smart robotic arms can be used to specify precise requirements. The design of the blockchain can make sure data are safe in intelligent robots. The smart robot can use sensor data directly for decision making without human intervention. The blockchain architecture cannot be responsible for data securement. It is important to protect the industrial process and ensure that AI choices are visible and traceable. The secure exchange of information within and outside the industrial walls is one of the major issues facing businesses. Blockchain technology may play a major role in IIoT manufacturing when it comes to data security and privacy. The technique is useful when there is no trust between parties needing to collect, store, and communicate vital information securely. Innovative business models may be developed using blockchain and production boundaries can be extended beyond standard plants. This would result in improved supply chain efficiency. It

can lead to greater order precision, product quality, and tracking. This would ensure that producers can fulfill delivery deadlines, increase the quality of the products, and sell more. The intelligent grids are simply electric networks, which operate and implement energy measures. Smart grids are subject to many security vulnerabilities because of interconnection, data sharing, authorization, and blockchain technology. Their safety is essential because of automation and remote access. Blockchain can help prevent unauthorized access to power systems and harmful assaults. Intelligent cities are based on data and technology, improving the quality factor for living standards and improving sustainability and economic development. Since the intelligent city has many components, blockchain is individually applicable. Blockchain-technology-based remote employee payment solutions can help securely transfer funding to anybody without incurring additional transaction fees for third parties. Blockchain technology with the assistance of intelligent contracts for diverse tasks may define a better governance scenario. In addition, it provides support for digital signatures in place of a conventional password-based method for managing and tracing digital identities. This can help improve the management of the supply chain. Moreover, greater transparency may be introduced between manufacturers and customers. Due to its decentralized ledger, it may store personal user data in different businesses about healthcare and banking. It would exclude any manipulation of data. To allow improved trash management, blockchain may be interfaced with smart and AI sensors. All papers and transactions must be transparent for the logistics sector. This can be addressed by blockchain technology and eventually enhance the supply chain's productive route. Blockchain technology can help to resolve inefficiencies in logistics by supervising the process of transferring products from start to finish in the supply chain or logistical business. Blockchains are suitable for streamlining complicated and fragmented procedures frequently seen within the supply chain and logistics business. Blockchain technology can monitor transactions, track assets, and establish a system of transparency to manage all sorts of key documents. Blockchain technology can be incorporated with its digital business transactions in vehicles. In various instances, it can be utilized. It can provide improved interconnection using smart sensors to avoid vehicle involvement and drive smoothly away from incoming traffic without breaking. This can lead to quick transactions on the road, such as e-wallets, and will simplify these transactions and protect information. Everything that might be handled can be done so securely and effectively via blockchain. Insurance agencies may utilize blockchain. Payments can thus be issued if the sensors of the vehicle identify a contravention. Due to blockchain information stored in the number of accessible servers, it may be hard to achieve illegal access to data on such systems. Electric power networks face safety challenges and blockchain might be one of the most effective methods to respond. Blockchain technology is sufficient to turn the intelligent grid into a peer-to-peer trade network. In addition, grid balancing through dispersed energy resources is sufficiently effective. The wholesale market, in particular, establishes the energy price based on client demand and the necessary quantity. Blockchain technology, in particular for electricity, enables storing and exchanging for sustainability. Transforming migration services from the public chain to business logic would need blockchain technology amalgamation and virtualization. Over the years, several designs and business requirements have emerged in virtualization logic. Enterprise virtual machines deal with performance, scalability, verification, upgradable intelligent contracts, and confidentiality regulations that are mostly achievable with blockchain technology. The future of industry-ready VMs may be blockchain technology coupled with virtual machines.

3.1 Virtual Network Function

The proposed method has Boolean input variables X_i and $Y_{j,i}$ to formally address the VNE problem that takes the actual value when the substratum node m_i^t is used and when VNF m_j^u is hosted

at the substratum node m_i^t. The latter predicate is referred to as $m_j^u \uparrow m_i^t$. A service request is mapped to two functions: N_m, which maps the service request to substitute nodes meeting their resource needs, and N_f, which maps endpoints. This is the mapping of the services request. The following can be defined explicitly as N_m. For all, $m^u \in M^u$.

$$N_m\left(m^u\right) = m^t \tag{1}$$

Eq. (1) determines the mapping function, subject to $m^t \in M^t$, and $m^u \uparrow m^t$, and for every i such that $m_i^t \in m^t$.

$$\left(\sum_{\forall_j \left| m_j^u \right| m_i^t} storage\left(m_j^u\right) * Y_{j,i}\right) \leq storage\left(m_i^t\right) * X_i \tag{2}$$

The storage requirement has been calculated in Eq. (2). It assumes that the actual value of $Y_{j,i}$ and X_i is the false value of 0. Eq. (2) stipulates that all storage necessary for VNFs allotted to a substrate node must be lower or equal to the available storage in that node. Here it is assumed that VNFs from the same service application may use the same node of substrates used to minimize latency on NFV systems.

In light of this formalization, the following phrases have been developed to represent N_m. First of all, this paper incorporates disparities as hard clauses (2). The BCEPP has to explain in addition to these inequalities that N_m is a function and that each VNF is mapped to precisely one node. The restriction stated in the following equation is for any occurrence that $M_j^u \in M^U$

$$\sum_{\forall_j \left| m_j^u \right| m_i^t} Y_{j,i} = 1 \tag{3}$$

The virtual network function is expressed in Eq. (3). To appropriately link variable X_i with variables $Y_{j,i}$, the proposed method adds the implications for each i that m_i^t is M_t,

$$X_i \Rightarrow \bigvee_j Y_{j,i} \tag{4}$$

Eq. (4) calculates and discusses the bind variable. At least one VNF is deployed in this node while the f_0^u substratum is in use. The endpoint VNF f_m^u routing table is drawn up as a soft clause with the negative shape of the delay in the connection being weighted. This reduces the total latency of the chosen infrastructure path in the MaxSAT solver to a minimum f_0^t. As the position of f_0^u is set to 0, the following soft constraint is generated for every potential substratum node m_l^t, which may be allocated to m_{adj}^u (near VNF neighbor in SG).

$$soft\left(\left(route\left(f_0^u,\ m_{adj}^u, k_{0,l}^t\right) \Rightarrow\ Y_{adj,l}\right) - latency\left(k_{0,l}^t\right)\right) \tag{5}$$

The routing tables have been described in Eq. (5), where a soft clause d with weight z is specified by notation $soft\ (d, z)$. In reality, the endpoint VNF routing table sets out to which node, L, of a packet is sent dependent on the next VNF assignment in the SG.

The remaining $VNF\ m_j^u \in M^v$ in the SG, with $j > 0$, have identical soft-clause provisions:

$$soft\left(\left(route\left(m_j^u, m_{adj}^u, k_{0,l}^t\right) \Rightarrow\ Y_{j,i} \wedge Y_{adj,l} - latency\left(k_{0,l}^t\right)\right)\right) \tag{6}$$

Identical soft-clause provisions have been evaluated in Eq. (6). When VNF j forwards the packets in the neighboring VNF_{adj} chart via link $K_{i,l}$, the Boolean variables $Y_{j,i}$ and $Y_{adj,l}$ that indicate where

VNFs are located must be true. If the same substrate node has two VNFs $i = l$ and a *latency* $\left(k_{0,l}^{t}\right) = 0$, the set is appended with a soft clause equal to zero weight.

VNF settings allow us to simulate a fixed processing time for each VNF. This is the latency (m^{u}) function that may be used to calculate the overall latency to incorporate the processing delay in the supplied VNF. If the BCEPP has a general end-to-end latency upper bond with an extra hard constraint, the system must guarantee that.

As many services as feasible should be mapped to the substratum network, using substrate network resources efficiently from the network infrastructure perspective. In the industrial context, too, the propagation of connections between endpoints is normally minimized. Consequently, our method has two objectives: to decrease the quantity and the latency of substrates in use.

The soft provisions with route predicates reduce the latency of the solver. Add an extra soft clause for each substratum node ns to decrease the number of substratum nodes using $m_{i}^{t} \in m^{t}$:

$$Soft\left(-X_{j}, L\right) \tag{7}$$

Eq. (7) estimates a soft clause for each substrate node, where L is determined based on the prioritization of latency minimization, a smaller L, or several substratum nodes in use depreciation, a bigger L. To reduce the penalty for incorrect provisions in the current model, the MaxSAT solver seeks to assign fake values to the Boolean variable X_{j}, decreasing the number of nodes in use.

3.2 Probability Occurrence

The likelihood of a mistake in the door test is a maximum of $\frac{2s(\varepsilon)g_{2}(\varepsilon)}{P}$. If each door test is a correct T then N environment is perfectly simulated until N has made a static key reveal ($\hat{a}$). T sets $\left(U, \frac{tQ}{\partial U}\right)$ to the public key $\hat{a}$ at least $1/m(\varepsilon)$, where $\hat{a}$ is an honest entity and N queries $g_{1}(*, a_{1}, a_{2})$ before a static key disclosure to the public key $\widehat{a}$. The chance of success of T is as follows:

$$Q(T) \geq \frac{Q_{1}(\varepsilon)}{m(\varepsilon)} - \frac{2s(\varepsilon)\, g_{2}(\varepsilon)}{P} \tag{8}$$

where $Q_{1}(\varepsilon)$ is the probability of occurrence.

The probability of error occurrence has been estimated in Eq. (8). If M wins, the forgery attack g_{2} must be requested to resolve the elliptic-curve Diffie–Hellman (ECDH) problem, whereas T may solve the problem. It must evaluate if N can differentiate between actual settings and simulations. If it can discriminate between them, users must make a G_{1} query of $\left(\check{y}, b_{1}, b_{2}\right)$ or $\left(\check{x}, b_{1}, b_{2}\right)$. Public key encryption is used to encode and decode data using a pair of keys to guard against unwanted access or use. The certifying authorities will give users public and private key pairs. If additional users desire to encrypt data, a general directory provides the intended receiver with the public key. Since it is a current meeting, N does not query the private short- and long-term keys of $\check{B}$ (or $\check{A}$) concurrently. N will not search when N requests the short-range private key (or) through static key reveal (.). It is unable to obtain information (or), because (or) is utilized in one session, without a static key reveal (.) query. The chance of success for T is as follows:

$$Q(T) \geq \frac{2Q_{2}(\varepsilon)}{\left(T(\varepsilon)^{2} g_{2}(\varepsilon)\right)} \tag{9}$$

where $Q_{2}(\varepsilon)$ is the probability of occurrence.

Session two probability occurrence is evaluated in Eq. (9). Because of freshness, N does not perform a static key reveal ($\check{A}$) query and cannot simultaneously query the private long-term key and short-term private key $\check{B}$. At that moment N can differentiate between the actual atmosphere, i.e., a $G_1(\check{y}, b_1, b_2)$ search and a $V = G_1(\check{y}, b_1, b_2)\, Q$ check, and the simulated environment. This occurrence is probable. $(L + G_1(\varepsilon))/2^{\varepsilon} - 1$ is the probability for this event. The likelihood of the success of S is the following:

$$Q(T) \geq \frac{1}{T(\varepsilon)\, m(\varepsilon)^2 g_2(\varepsilon)} Q_3(\varepsilon) \left(1 - \frac{L + G_1(\varepsilon)}{2^{\varepsilon} - 1}\right) - \frac{2T(\varepsilon)\, g_2(\varepsilon)}{P} \tag{10}$$

where $Q_3(\varepsilon)$ is the probability of the occurrence. The probability of success in session three has been described in Eq. (10).

3.3 Trust Model

To assess their members S_n, the IIoT server provides all required information to every DK_i. DK_i is based on the three performance measures known as cooperation, direct honesty, and indirect honesty, essential for updating the confidence meter. With an initial trust metric, each node integrates the network. In the interval [0, 1] the values S_n and S_0 vary. As seen in the transition diagram in Fig. 2, the Tm of a monitored node will rise, drop, remain steady, or descend to zero. The transitions rely on three confidence performance measurements and the present condition of the NM_j node monitored.

The proposed method utilizes a state transition diagram in $F + 1$ states as illustrated in Fig. 4 to officially transition S_n. Each state matches a certain value of S_n. State 0 matches a degree of non-trust and State F matches a high level of trust. The interval [0, 1] of S_n is divided into $F + 1$ states. Each is a step (1 mod $\varphi = 0$). The transition matrix that corresponds to our suggested approach's state transitional diagram is as follows:

$$Q = \left(Q_{j,i}(s)\right)_{0 \leq j,i \leq F} \tag{11}$$

As shown in Eq. (11), the transition matrix has been performed. When $Q_{j,i}$ is likely to go from State j to State i, it is as follows:

$$Q_{j,i}(s) = Q(X_t = i | X_{t-1} = j) \tag{12}$$

The probability of the transition state has been deliberated in Eq. (12). The altered variable X_t is the actual IIoT device's S_n at time t. The chance for being in State j at time t may be determined as follows from the transition matrix stated in Eq. (9), provided that the starting node status is $X_0 = 1$:

$$Q_j(s) = \sum_{Zin[1 \ldots F]} Q_{1,W}(s_W) * Q_{1,W}(s) \tag{13}$$

The probability has been described in Eq. (13). DC utilizes information from the IIoT server to create three performance metrics that describe the behavior of the monitored NM_j nodes with time to assess different transitional probabilities, allowing the update of $s_{W,Z}$ member nodes.

The rate of collaboration assesses the behavior of the monitored NM_j in connection with its network cooperation. The D_{NM_j} cooperation rate is the number of successful messages delivered divided by the NF total of messages transmitted by the NM_j cooperation rate. The NM_j node cooperation rate

is determined as follows:

$$D_{NM_j} = \left(\frac{\sum_{j=1}^{ME} (D_{nj})}{ME} \right) \tag{14}$$

The collaboration rate has been estimated in Eq. (14), where D_{nj} equals 1 if the message mi is transmitted properly or 0 when the message M_j is not transmitted. The likelihood of the NM_j working on the network is as follows:

$$QD = DNM_j * QMFS \tag{15}$$

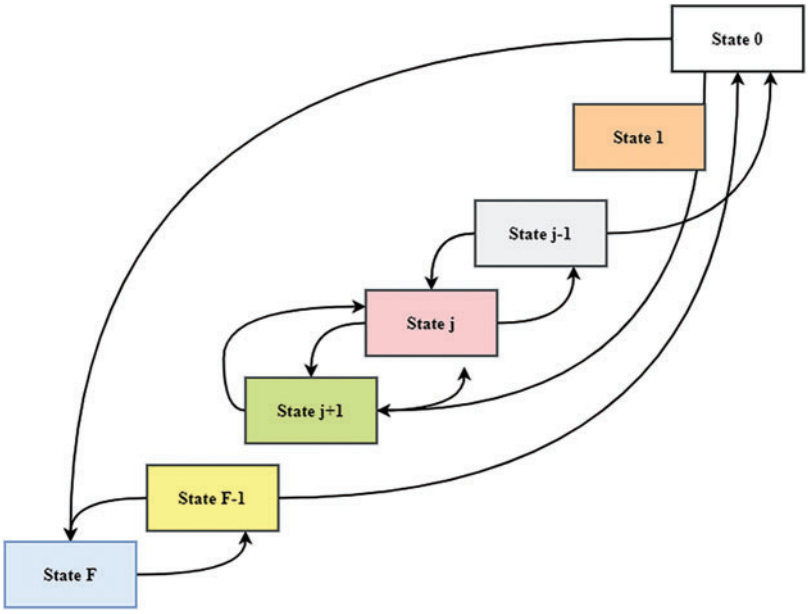

Figure 4: Transition diagram

The wireless network constraints have been formulated in Eq. (15), where $QMFS$ reflects the limitations of the nature of wireless networks: congestion, retransmission, barriers, and connection quality between the transmitter and the receiver. Each environment is supposed to have a well-known $QMFS$ of probability measured by the number of transmissions and by the number of incorrect bits. The aim of introducing this probability is to take the limitations of the monitoring environment into account in the final trust assessment.

The straightforward honesty assesses the compatibility with and profiling of the actions done in the network by the NM_j node. The node that monitors a production machine to transmit reports to the production system each hour is regarded as a dishonest node; when carrying out this duty every four hours, the source of this behavior needs to be separated from the network. This kind of harmful action and behavioral modification caused by MNI nodes can be detected in direct honesty.

A set of hashed activities that the NM_j node must execute in the network will be sent to DK_j, a node in list $B(NM_j)$. In the IIoT server and the DK_j node, the hashes contained in list $B(NM_j)$ are saved. The activities are delivered in a hatched manner to DK_j nodes to guarantee that data leakage is not exposed in the case of DK_j penetration, due to the likely interception of monitoring messages by hostile nodes. To evaluate the C_{NM_j} direct honesty rate of an NM_j node, the DK_j calculates a similarity

ratio for the set of hashes included in both $B\left(NM_j\right)$ and $BE\left(NM_j\right)$ lists:

$$D_{NM_j} = \left(\frac{B\left(NM_j\right) \cap BE\left(NM_j\right)}{B\left(NM_j\right) \cup BE\left(NM_j\right)}\right) \tag{16}$$

As shown in Eq. (16) the similarity ratio has been derived. Qch is likely to be honest with the NM_j node monitored and is computed as follows:

$$Qch = C_{NM_j} * QMFS \tag{17}$$

The monitored probability has been evaluated in Eq. (17). The $BE\left(NM_j\right)$ list consists of the NM_j node hashed feeds. To execute comparisons, the hashes are produced via the NM_j node and are transmitted to the DK_j node. After the comparisons, the DK_j node automatically removes the set of hashing included in the $BE\left(NM_j\right)$ list to minimize the memory space. The indirect rate of honesty reflects the MNi's reputation in its community. The community nodes that have already experienced NM_j have to be assigned a score based on their conduct in the network. The nodes that offer excessive scores (either too big or too little) over the other nodes are malicious, which aim to carry out voting assaults or mistreatment. DK_j contacts its nodes to comment on the NM_j node. The list of nodes that create spam will be sent to the IIoT server for punishment. As an average of the scores supplied by community members when removing spam, DK_j determines the indirect honesty rate of node NM_j:

$$J_{NM_j} = \left(\frac{\sum_{NM_{j,}=1}^{M} O_{NM_{j,}}, NM_j}{M}\right) \tag{18}$$

As shown in Eq. (18), the average score has been determined. In $O_{NM_{j,}} NM_j$ is the reputation of member node $NM_{j,}$ for NM_j, $NM_j \neq NM_{j,}$. NM_j does not offer a score to prevent assaults on itself. M is the total number of nodes after the spam nodes have been deleted. The likelihood of a positive reputation for the monitored NM_j node is determined as follows:

$$Qjg = J_{NM_j} * QMFS \tag{19}$$

Positive reputation has been explored in Eq. (19). To achieve the transitional matrix Q of Eq. (19), the probability of stay $Q_{j,j+1(s)}$, the probability of remain in the trusted state F, $Q_{F,F(s)}$, and the probability of transition into State o, $Q_{j,0(s)}$ is calculated by DK_j in the same way, as in our earlier work (s). The state transition diagram in Fig. 2, which shows that the trust status of an NM_j node will be known in time $s-1$, shows that the state has five options only: $State\ +1$, $State\ 1$ remains the same, reaching a trusted $State\ F$ or $State\ 0$.

Each probability is determined using an equation in State S_n (11). At s, S_n of a monitored NM_j is the trust value corresponding to the condition in which the probability computed by Eq. (11) is at its highest level. Each state is equivalent to a specific value of S_n; State o is equivalent to $S_n = 0$ and State F to $S_n = 1$.

Fig. 5 explores the proposed BCEPP. The paper analyzes the typical IIoT scenario consisting of a Key Generation Center (KGC) cloud-string, providing the storage of IIoT users, data proprietors, and generally not data proprietors, magenta and IIoT sensors. The following four companies are the enhanced IIoT community leader scheme. The KGC creates public and partial-private key (PPK) system parameters for cloud servers and users' data owners. The server of the cloud is accountable for user owners' data processing. It then connects with users to transmit and calculate data. The data owner generates a certificate-free signature scheme with its own private signing key produced using

KGC's partial-private key. For signature verification, the appropriate public key will be given to the data user. On the cloud server, the CLS data are saved and hence the data user may be checked. The data user obtains their KGC PPK and the public key for verifying a CLS system from the information owner. They can produce their private key and its equivalent public key with their partial-private key. Its communication flows can be signed with the cloud for authentication. As a network administrator, users of KGC are first required to be registered for the proposed IIoT system.

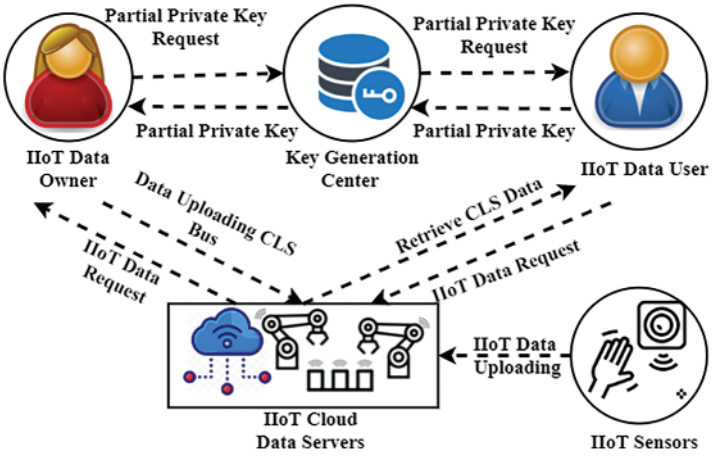

Figure 5: Proposed BCEPP

KGC makes public parameters and partial-private key publications and publishes them; users transmit their identity and partial-private keys to the KGC for registration. Data owners and data consumers then establish and utilize their private signing keys to generate community leaders of IIoT data. The users' keys are saved on intelligent IIoT devices. Data from the IIoT sensor are stored on the cloud server and collected, signed, and retained as CLS data by the data owner. Finally, data consumers can obtain stored IIoT cloud data and verify them using the public key of the data proprietor. The internet security of IoT devices and the networks with which they are associated is the securing act. IoT devices in the business environment include industrial machinery, smart energy grids, construction automation, and personal IoT devices that employees use. This then suggests an entirely new CLS that provides comprehensive security safety with the standard security model against all identified threats and complete security proof (without random oracles). Currently, it redefines industries such as energy, manufacturing, transport, and healthcare. This new wave is the Industrial Internet of Things (IIoT): an Internet of things, machines, computers, and people that enables intelligent industrial operations to achieve transformative business results utilizing advanced data analytics.

As mentioned above, this paper intends to modify the existing IIoT network design in the car industry to simplify confidence administration. The IIoT network will thus be subdivided into clusters known as industrial communities, as shown in Fig. 6. It consists of L community leaders and K nodes of members. Let the groups DK_i and NM_i be the nodes of the community. Community leader DK_i administers the Tm trust in its community with each member node NM_i in three performance measures: collaboration, honesty, and indirect honesty. DK is a particular node that requires high confidence, sufficient processing capacity, storage, and energy resources to execute surveillance duties. A request must be sent to the IIoT server to any node that wishes to join the network. A single identifier is assigned to the nodes and a profile is created for the IIoT server. The profile is saved to the IIoT node and the IIoT server databases. It sets forth the activities that the IIoT node may carry out and the

measurements, operations, and data that each node in the network can exchange. It specifies the sorts of industrial connections between two nodes. Every node may create, update, or end any relationship with a different node based on these defined rules. To be authorized, any node that wishes to be a *DK* must interact with the server. According to several criteria described in Phase I below, the server provides the authorization to lead a certain node or not. When a node becomes a *DK* its community will be established. The *DK* will either give the server the monitoring findings or gather the necessary data to assess the S_n of its members. The first step involves the multi-parametric identification of *DK*. The second step creates, based on the geographical distances and industrial linkages, industrial communities surrounding the designated *DK*. The last step is the monitoring procedure in which the DK_i node monitors the confidence metric S_n of its communities to detect suspicious behaviors. The proposed BCEPP method has a high computational cost, a low latency ratio, an increased data transmitting rate, and an enhanced security rate, packet reception ratio, user satisfaction index, and probability ratio.

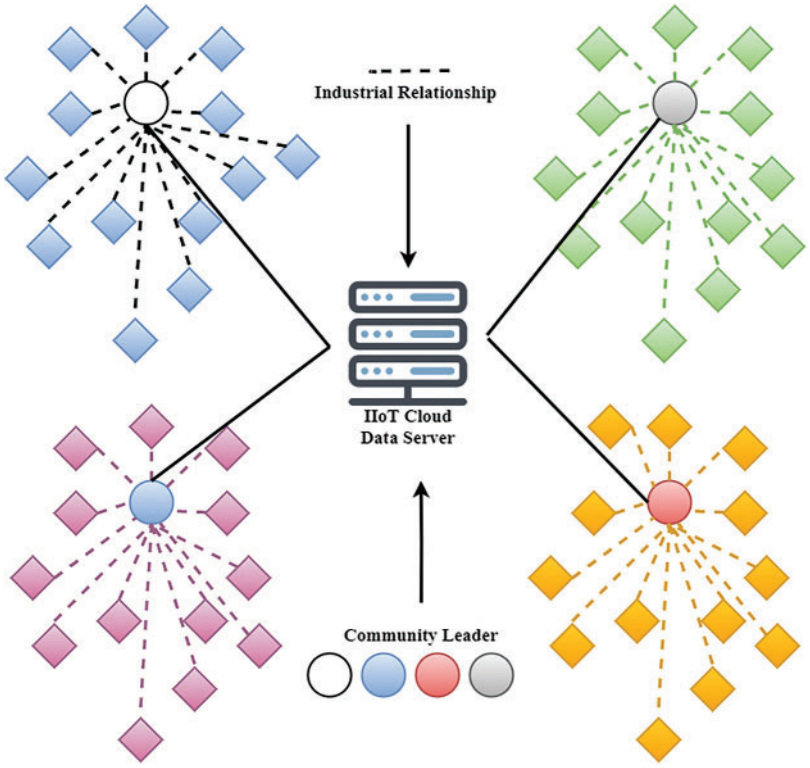

Figure 6: IIoT data communication

4 Results and Discussion

In the industrial situation, these blockchain technologies may be used to build a network functional chain guaranteed by latency, jitter, loss of packets, and redundancy, with tight latency and reliability requirements for important events. In addition, network virtualization real-time monitoring techniques assist in mitigating important occurrences, which may be tested by changing the service diagram and enforcing new network regulations. IIoT applications require an intelligent positioning of services across physically isolated sites, directly affecting latency, and a proper policy enforcement

mechanism to ensure dependability, security, and safety. This study takes these factors into account by offering a VNF placement solution for the IIoT to minimize overall latency and, in addition, to verify that policies throughout the network, such as connection or isolation, are maintained across these endpoints.

4.1 Probability Ratio

Considering the network topology and security vulnerabilities, the likelihood of choosing distinct security flaws as attack entry points has been analyzed. An analysis has been carried out on the assault and defense strategy, for this is the basis of the security model. By solving the security model, probable attack nodes in the next phase may be anticipated. Finally, by evaluating the importance of various vulnerabilities to security, the safety level of the power network vulnerabilities may be assessed and evaluated. The likelihood is high that hostile attackers will target them. The protocol can be extended to ensure long-term sustainability and the availability of encryption. The suggested protocol is based on the study of probability, which ensures that the system designer has a common key among all IoT devices in predefined likelihood. The execution demonstrates the viability of our proposed IoT network security protocol. Tab. 1 shows the probability ratio.

Table 1: Probability ratio

Number of data	DLFE-SSM	CF	NDRF-SSA	BCSIES	BCEPP
10	42.1	53.1	62.5	45.3	32.9
20	48.3	44.4	61.6	46.6	35.6
30	49.7	57.3	59.1	47.8	37.3
40	47.8	58.6	58.3	48.6	39.6
50	48.5	62.9	61.4	42.5	31.5
60	49.4	61.2	64.6	46.4	33.2
70	54.3	68.4	65.8	41.8	36.7
80	56.6	51.1	66.5	47.3	37.5
90	58.8	53.6	67.8	44.5	38.1
100	59.4	57.5	68.7	48.6	33.8

4.2 Latency Ratio

This article offers the common NFV and SDN-enabled IIoT network service model for optimization and verification. This allows us to monitor network service transmission behavior and ensure optimum latency positioning in the network architecture. The encoded model is given to a solver as an input. Network features are optimally positioned in the infrastructure network as an output if the included VNFs meet the network features. The result ensures minimum cost for the end-to-end service, including latency issues and network latency. The findings shown reflect latency reduction issue calculations under different situations, reductions in the number of substratum nodes in use and reductions in network latency. Tab. 2 expresses the latency ratio.

Table 2: Latency ratio

Number of data	DLFE-SSM	CF	NDRF-SSA	BCSIES	BCEPP
10	43.1	52.2	42.2	45.3	32.4
20	49.4	58.5	41.5	46.7	35.3
30	42.7	57.4	49.2	47.9	37.2
40	45.8	58.7	48.4	48.2	39.5
50	48.4	52.8	40.3	52.4	36.2
60	42.3	59.1	44.5	56.6	35.1
70	46.4	51.5	45.7	51.7	36.6
80	56.7	54.2	43.2	57.9	37.4
90	51.9	52.5	47.5	54.6	33.3
100	49.1	47.3	41.8	58.8	28.5

4.3 Data Transmission Rate

When the customer receives the request, the node will not execute a transaction but will put it together and pass it on to the check node. The member services administration module issues certificates, transactions, transmissions, and encryption keys in the blockchain. The system uses the participation technique immediately. The data collection and consensus modules are employed to manage power nodes for the sharing method. During the transaction process, these lead to achieving the broken book. In these cases, if the transaction information is altered, the rogue node should occupy numerous computer resources. Compared to unlawful collusion attacks, the proposed technique performs better. Therefore, the suggested system can enhance the packet receipt and transmission rate if significant warning information is found in the blockchain-based network. Fig. 7 depicts the data transmission rate.

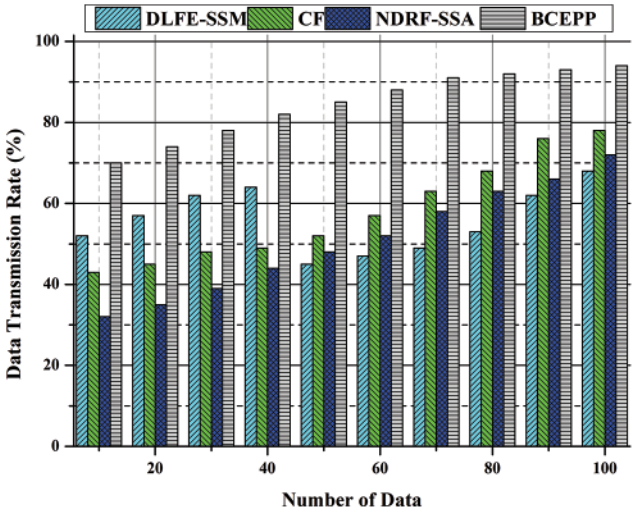

Figure 7: Data transmission rate

4.4 Packet Reception Rate

Illegal attackers may acquire information from power users using system vulnerabilities in the energy-based blockchain network to transfer data. This impacts the confidentiality of data and the stability of the network throughout the whole network. The experimental findings are displayed in Fig. 8. The recommended secure data transmission system based on blockchains provides a mechanism for data exchange. Because of the decentration communication technique, the system will not communicate data to other power nodes. In blockchain networks, data transmission delays check the security and the reliability of the transfer of data. The results reveal that the technique calculates the blockhead hash value by changing the random integer in the blockhead of the power node. In this instance, if the malicious node wants to manipulate transaction data, it should use many calculation resources.

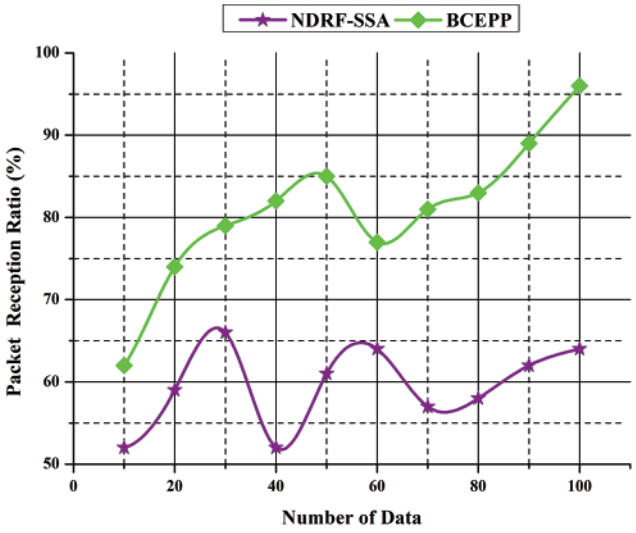

Figure 8: Packet reception rate

In comparison to unlawful collusion attacks, the proposed technique performs better. Consequently, the suggested regime may enhance packet reception and transmission speeds when significant warning information is available in the blockchain-based network. Fig. 8 demonstrates the packet reception rate.

4.5 Computational Costs

The calculation costs of the various data packets are assessed in this section. The outcome is shown in Fig. 9. The computational costs of the proposed system are low because of the usage of the decentration-based secure transmission model with the increase of transmitted and received data packages. The overhead communication of data transmission is minimized efficiently. Compared to the suggested method, the overall performance is superior. Enabling dynamic power node add-ons by initiating data transactions across nodes offers a very efficient and trustworthy data consensus process. The safety consensus approach works at the price of additional computation resources. The consensus time in the data transfer can be shortened by adding the additional node dynamically. The proposed approach is appropriate for a network based on a blockchain system. The compatibility of the running system should be increased further. Fig. 9 shows the computational costs.

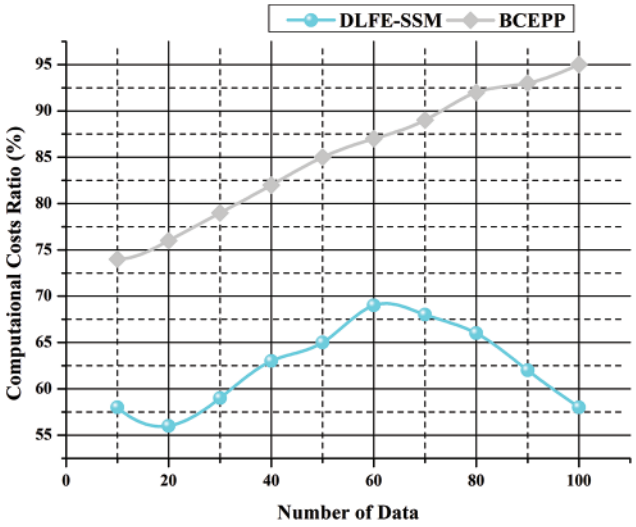

Figure 9: Computational costs

4.6 Security Rate

The experiments indicate that the technique for data consensus decreases system costs significantly. The spread of malicious applications in the industrial blockchain network is regulated. By addressing the security model, the suggested system creates an optimal control strategy. The method provides a mechanism for data consensus that can increase the data transfer success rate. The consensus method can dynamically pick a security approach when the malicious software stores the total power nodes. Fig. 10 shows the security rate.

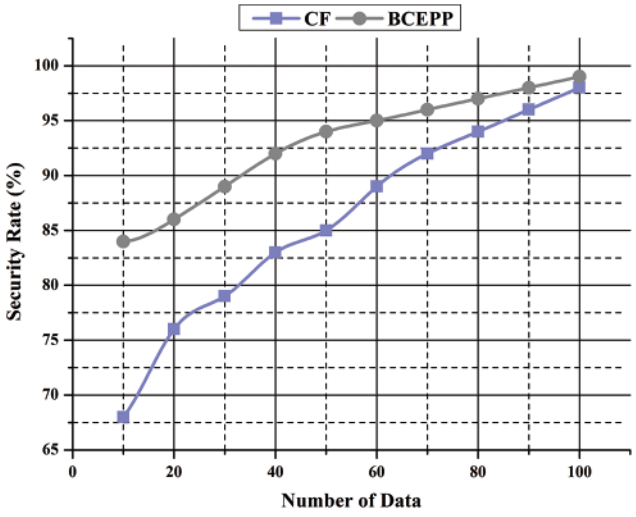

Figure 10: Security rate

4.7 User Satisfaction Index

For the classification of the fog resources, the encryption is carried out and the resource size required is determined. The user requirements can be split into many classes. Provided they are available, relevant resources are identified and adapted to user demands. Because users have various resource needs, the computer, bandwidth, and storage requirements are combined. The system includes all three sorts of conditions with different resources, measures user and resource needs, and awards the user the maximum score. Fig. 11 illustrates the user satisfaction index.

$$V_t = \left(\frac{\delta\left(T_{com}\right) + \gamma\left(T_a\right) + \sigma\left(T_t\right)}{g_{com} + g_a + g_t} \right) \tag{20}$$

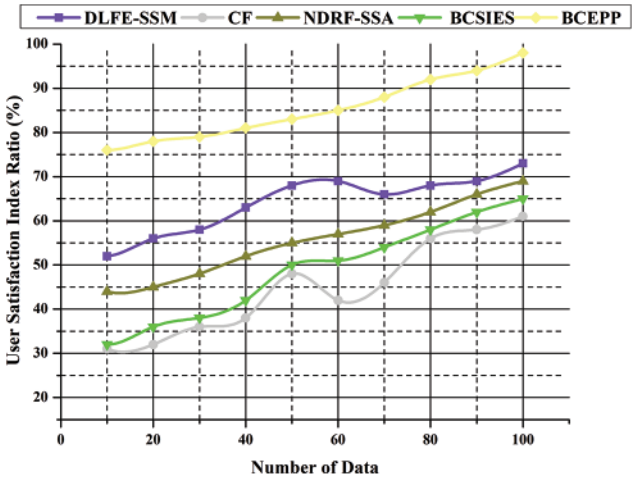

Figure 11: The user satisfaction index

Eq. (20) and Fig. 11 show the user satisfaction index. V_t is calculated to examine the essence of resource planning. In contrast, the satisfaction index of the user is determined by T_{com}, T_a, and T_t, which reflect the demands, storage, and attributes of the bandwidth of the job. In addition, g_{com}, g_a, and g_t indicate the computer, bandwidth, and storage characteristics. The coefficients of the characteristics are δ, γ, and σ. The above-proposed BCEPP-based analysis shows the high computational cost, low latency ratio, increased data transmitting rate, enhanced security rate, packet reception ratio, user satisfaction index, and probability ratio when compared to the Blockchain-Based Secure Image Encryption Scheme (BCSIES), node degree (N), distance from the cluster (D), residual energy (R), fitness (NDRF), salp swarm algorithm (SSA), deep-learning feature extraction based semi-supervised model (DLFE-SSM), cybersecurity framework (CF), and other methods.

5 Conclusion and Future Scope

These technologies may be employed in the industrial environment to construct the delay, vibration, data loss, and redundancy networks guaranteed to ensure that key events demand strict latency and dependability. Furthermore, real-time network virtualization approaches help minimize significant events, which may be evaluated by altering the service design and applying new network rules. In reality, IIoT applications require a clever positioning of services across physical isolation locations that directly impact latency and an appropriate policy enforcement mechanism to guarantee service safety, reliability, and security. To reduce overall latency and ensure that policies such as the

link or isolation throughout the network are maintained across those endpoints, the survey considers these aspects by giving a VNF placement solution for the IIoT. Thus, the experimental results show our proposed BCEPP method to have the following: high computational cost of 95.3%, low latency ratio of 28.5%, increased data transmitting rate up to 94.1%, enhanced security rate of 98.6%, packet reception ratio of 96.1%, user satisfaction index of 94.5%, and probability ratio of 33.8%.

Acknowledgement: The authors extend their appreciation to the Deputyship for Research & Innovation, Ministry of Education in Saudi Arabia for funding this research work through the Project Number IFPHI-218-611-2020." and King Abdulaziz University, DSR, Jeddah, Saudi Arabia.

Funding Statement: The authors received funding as stated in the acknowledgment.

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

References

[1] K. Seyhan, T. N. Nguyen, S. Akleylek, K. Cengiz and S. H. Islam, "Bi-GISIS KE: Modified key exchange protocol with reusable keys for IoT security," *Journal of Information Security and Applications*, vol. 58, pp. 102788, 2021.

[2] G. Manogaran, M. Alazab, V. Saravanan, B. S. Rawal, P. M. Shakeel *et al.,* "Machine learning assisted information management scheme in service concentrated IoT," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 4, pp. 2871–2879, 2020.

[3] D. T. Do, M. S. Van Nguyen, T. N. Nguyen, X. Li and K. Choi, "Enabling multiple power beacons for uplink of noma-enabled mobile edge computing in wirelessly powered IoT," *IEEE Access,* vol. 8, pp. 148892–148905, 2020.

[4] G. Manogaran, M. Alazab, P. M. Shakeel and C. H. Hsu, "Blockchain assisted secure data sharing model for internet of things based smart industries," *IEEE Transactions on Reliability*, vol. 71, no. 1, pp. 348–358, 2022. https://doi.org/10.1109/TR.2020.3047833.

[5] T. G. Nguyen, T. V. Phan, D. T. Hoang, T. N. Nguyen and C. So-In, "Efficient SDN-based traffic monitoring in IoT networks with double deep Q-network," in *Proc. Int. Conf. on Computational Data and Social Networks (CSoNet 2020), Lecture Notes in Computer Science*, vol. 12575. Cham, Springer, pp. 26–38, 2020.

[6] Y. Zhao, Y. Yu, P. M. Shakeel and C. E. Montenegro-Marin, "Research on operational research-based financial model based on e-commerce platform," *Information Systems and e-Business Management*, pp. 1–17, 2021. https://doi.org/10.1007/s10257-021-00509-4.

[7] M. Abdel-Basset, G. Manogaran and M. Mohamed, "Internet of things (IoT) and its impact on supply chain: A framework for building smart, secure and efficient systems," *Future Generation Computer Systems*, vol. 86, pp. 614–628, 2018.

[8] R. Gad, M. Talha, A. A. Abd El-Latif, M. Zorkany, E. S. Ayman *et al.,* "Iris recognition using multi-algorithmic approaches for cognitive internet of things (CIoT) framework," *Future Generation Computer Systems*, vol. 89, pp. 178–191, 2018.

[9] Z. Lv, Y. Han, A. K. Singh, G. Manogaran and H. Lv, "Trustworthiness in industrial IoT systems based on artificial intelligence," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 2, pp. 1496–1504, 2020.

[10] A. A. Abd El-Latif, B. Abd-El-Atty, S. E. Venegas-Andraca, H. Elwahsh, M. J. Piran *et al.,* "Providing end-to-end security using quantum walks in IoT networks," *IEEE Access*, vol. 8, pp. 92687–92696, 2020.

[11] J. Gao, H. Wang and H. Shen, "Task failure prediction in cloud data centers using deep learning," in *Proc. 2019 IEEE Int. Conf. on Big Data (Big Data)*, Los Angeles, CA, USA, pp. 1111–1116, 2019. https://doi.org/10.1109/BigData47090.2019.9006011.

[12] J. I. R. Molano, J. M. C. Lovelle, C. E. Montenegro, J. J. R. Granados and R. G. Crespo, "Metamodel for integration of internet of things, social networks, the cloud and industry 4.0," *Journal of Ambient Intelligence and Humanized Computing*, vol. 9, no. 3, pp. 709–723, 2018.
[13] J. Gao, H. Wang and H. Shen, "Smartly handling renewable energy instability in supporting a cloud datacenter," in *Proc. 2020 IEEE Int. Parallel and Distributed Processing Symp. (IPDPS)*, New Orleans, LA, USA, pp. 769–778, 2020.
[14] D. Ezhilmaran and M. Adhiyaman, "Soft computing method for minutiae-based fingerprint authentication," *International Journal of Industrial and Systems Engineering*, vol. 30, no. 2, pp. 237–252, 2018.
[15] S. VE, C. Shin and Y. Cho, "Efficient energy consumption prediction model for a data analytic-enabled industry building in a smart city," *Building Research & Information*, vol. 49, no. 1, pp. 127–143, 2021.
[16] V. E. Sathishkumar, J. Lim, M. Lee, K. Cho, J. Park *et al.,* "Industry energy consumption prediction using data mining techniques," *International Journal of Energy, Information and Communications*, vol. 11, no. 1, pp. 7–14, 2020.
[17] M. Abdel-Basset, R. Mohamed, M. Elhoseny, A. K. Bashir, A. Jolfaei *et al.,* "Energy-aware marine predators' algorithm for task scheduling in IoT-based fog computing applications," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 7, pp. 5068–5076, 2020.
[18] F. Farivar, M. S. Haghighi, A. Jolfaei and M. Alazab, "Artificial intelligence for detection, estimation, and compensation of malicious attacks in nonlinear cyber-physical systems and industrial IoT," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 4, pp. 2716–2725, 2019.
[19] B. Bera, D. Chattaraj and A. K. Das, "Designing secure blockchain-based access control scheme in IoT-enabled internet of drones deployment," *Computer Communications*, vol. 153, pp. 229–249, 2020.
[20] T. Sultana, A. Almogren, M. Akbar, M. Zuair, I. Ullah and N. Javaid, "Data sharing system integrating access control mechanism using blockchain-based smart contracts for IoT devices," *Applied Sciences*, vol. 10, no. 2, pp. 488, 2020.
[21] Y. Gao, Y. Chen, X. Hu, H. Lin, Y. Liu *et al.,* "Blockchain based IIoT data sharing framework for SDN-enabled pervasive edge computing," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 7, pp. 5041–5049, 2020.
[22] S. Latif, Z. Idrees, J. Ahmad, L. Zheng and Z. Zou, "A Blockchain-based architecture for secure and trustworthy operations in the industrial internet of things," *Journal of Industrial Information Integration*, vol. 21, pp. 100190, 2021.
[23] J. Sengupta, S. Ruj and S. D. Bit, "A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT," *Journal of Network and Computer Applications*, vol. 149, pp. 102481, 2021.
[24] Y. Wu, H. N. Dai and H. Wang, "Convergence of blockchain and edge computing for secure and scalable IIoT critical infrastructures in industry 4.0," *IEEE Internet of Things Journal*, vol. 8, no. 4, pp. 2300–2317, 2020.
[25] X. Xu, Z. Zeng, S. Yang and H. Shao, "A novel blockchain framework for industrial IoT edge computing," *Sensors*, vol. 20, no. 7, pp. 2061, 2020.
[26] P. W. Khan and Y. Byun, "A blockchain-based secure image encryption scheme for the industrial internet of things," *Entropy*, vol. 22, no. 2, pp. 175, 2020.
[27] P. C. M. Arachchige, P. Bertok, I. Khalil, D. Liu, S. Camtepe *et al.,* "A trustworthy privacy preserving framework for machine learning in industrial iot systems," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 9, pp. 6092–6102, 2020.
[28] F. S. Costa, S. M. Nassar, S. Gusmeroli, R. Schultz, A. G. Conceição *et al.,* "FASTEN IIoT: An open real-time platform for vertical, horizontal and end-to-end integration," *Sensors*, vol. 20, no. 19, pp. 5499, 2020.
[29] X. Yan, Y. Xu, X. Xing, B. Cui, Z. Guo *et al.,* "Trustworthy network anomaly detection based an adaptive learning rate and momentum in iiot," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 9, pp. 6182–6192, 2020.
[30] K. A. Abuhasel and M. A. Khan, "A secure industrial internet of things (IIoT) framework for resource management in smart manufacturing," *IEEE Access*, vol. 8, pp. 117354–117364, 2020.

[31] J. W. Jang, S. Kwon, S. Kim, J. Seo, J. Oh *et al.,* "Cybersecurity framework for IIoT-based power system connected to microgrid," *KSII Transactions on Internet and Information Systems (TIIS)*, vol. 14, no. 5, pp. 2221–2235, 2020.

[32] M. M. Hassan, S. Huda, S. Sharmeen, J. Abawajy and G. Fortino, "An adaptive trust boundary protection for IIoT networks using deep-learning feature-extraction-based semisupervised model," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 4, pp. 2860–2870, 2020.

[33] T. Kumar, E. Harjula, M. Ejaz, A. Manzoor, P. Porambage *et al.,* "BlockEdge: Blockchain-edge framework for industrial IoT networks," *IEEE Access*, vol. 8, pp. 154166–154185, 2020.

[34] M. AI-Duhayyim, F. N. Al-Wesabi, R. Marzouk, A. I. A. Musa, N. Negm *et al.,* "Integration of Fog computing for health record management using blockchain technology," *Computers, Materials & Continua*, vol. 71, no. 2, pp. 4135–4149, 2022.