SecureFLACF: Secure Federated Learning Access Control Framework with Blockchain-Infused Intrusion Detection System for IIoT

V. Dineshbabu and M. Vigenesh*

Department of Computer Science and engineering, Faculty of Engineering, Karpagam Academy of Higher Education, Coimbatore, Tamilnadu, 641021, India
E-mail: dineshbabukit@gmail.com; mvigenesh@gmail.com
**Corresponding Author*

Received 05 March 2024; Accepted 18 August 2025

Abstract

The industrial internet of things (IIoT) expanded fast as physical devices and systems were connected to the internet. However, this interconnectedness made IIoT systems vulnerable to hackers. Intrusion detection systems (IDSs) were put in place to detect and prevent such assaults. Nonetheless, attackers might circumvent IDSs by forging identities or interfering with recorded data. The article intended to improve IIoT security by achieving system confidentiality, integrity, availability, scalability, performance, and security. For IIoT security, the article developed a secure federated learning access control framework (SecureFLACF) linked with a blockchain-based IDS. SecureFLACF used blockchain to secure data collected by IDS, AES-256 encryption to secure stored data, zero-knowledge proof (ZKP) to validate user identities and manage data access, and a federated learning access control framework (FLACF) to train a machine learning model for intrusion detection. SecureFLACF developed as a viable solution for improving IIoT security, providing strong assurances for IDS data and access control

Journal of Mobile Multimedia, Vol. 21_5, 939–966.
doi: 10.13052/jmm1550-4646.2155

using blockchain's tamper-proof structure and AES-256 encryption. Furthermore, FLACF's design allows private machine learning model training, ensuring data privacy as well as model fidelity. The framework's usefulness was highlighted by its application in real-world circumstances, making it a cost-effective option for organisations of all sizes. This method not only strengthened IIoT systems against a wide range of cyber threats, but also stressed their dependability as a safeguard. SecureFLACF exhibited considerable promise for improving IIoT security across several dimensions by encapsulating practicability, cost-effectiveness, and dependability.

Keywords: Zero-knowledge proof, industrial internet of things, federated learning, access control, intrusion detection system, blockchain.

1 Introduction

Zero-Knowledge Proofs and Federated Learning are two promising technologies that can be used to improve the security and privacy of access control for IIoT systems. ZKPs are a cryptographic technique that allows users to prove their knowledge of a secret without revealing the secret itself [1]. This can be used to verify the identity of a user or to prove that the user has access to a particular resource without revealing any sensitive information about the user or the resource. FL is a machine learning technique that allows multiple devices to train a machine learning model without sharing their data. This can be used to improve the security of IIoT systems by preventing unauthorized users from accessing sensitive data [2].

In Figure 1 shows that zero knowledge proof with federated learning access control framework for IIoT systems could work as follows. Users would utilise ZKPs to establish their identities and access rights in the proposed system. These ZKPs would be sent to a central server, which would verify them and then provide access to people with the necessary permissions. Surprisingly, the central server would not save any critical user information, such as identities or access rights [3]. Furthermore, the machine learning model would be trained using data from users' devices, eliminating the requirement for direct data exchange between users' devices and the central server [4]. This design emphasises a privacy-conscious paradigm, fostering trust while effectively enabling access management and data-driven learning [5]. This framework would improve the security of IIoT systems by preventing unauthorized users from accessing sensitive data [6]. It would also improve the privacy of the users by preventing the central server from storing

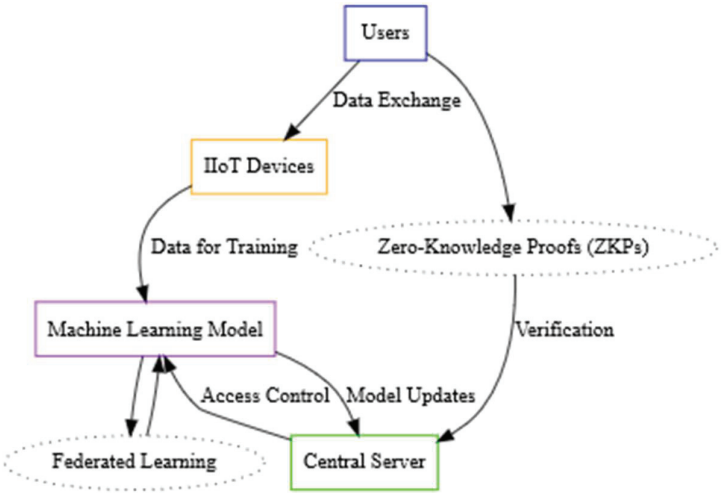

Figure 1 Zero-knowledge proofs and federated learning for IIoT access control.

any of their sensitive data [7]. The use of ZKPs in conjunction with federated learning in access control for IIoT systems produces a number of compelling benefits. ZKPs primarily guarantee security by confirming user identities and access privileges while maintaining the confidentiality of sensitive data, preventing unauthorised access to IIoT systems [8]. The addition of federated learning promotes privacy even further by allowing machine learning model training without the need to exchange user data, hence protecting user data privacy [9].

ZKPs and federated learning are renowned for their scalability, since both approaches can easily accommodate a high number of users and devices, making them suited for implementation in large-scale IIoT systems. Importantly, the IIoT system's performance remains largely unaffected since ZKPs and federated learning may be implemented in a way that ensures system performance integrity. This strategic cooperation demonstrates a strong commitment to improving IIoT security while simultaneously respecting privacy and assuring scalability and performance [10]. However, before widespread use of ZKPs paired with federated learning for access control in IIoT systems is feasible, various challenges must be comprehensively addressed [11]. Notably, the security environment deserves consideration, given that, while promising, ZKPs and federated learning are still relatively new technologies. Identification and mitigation of potential security threats inherent in these methodologies are prerequisites for wider adoption, ensuring the robustness

and trustworthiness of IIoT security frameworks [12]. The use of ZKPs and FL for access control in IIoT systems poses security issues that must be properly addressed. These include side-channel attacks, which use device characteristics to gain unauthorised access to the internal states of ZKPs or federated learning systems like adversarial machine learning, data poisoning, and Sybil attacks [13]. Addressing these problems is crucial to ensuring the resilience and reliability of IIoT security systems that leverage ZKPs and federated learning. More secure cryptographic primitives and communication channels can be employed to strengthen the protocols used for ZKPs and federated learning. A sophisticated encryption mechanism, such as AES-256, can be used to safeguard the communication channel between users and the central server [14].

2 Literature Review

Malware, brute-force assaults, data manipulation, authentication attacks, and remote access control manipulation are some of the operational and informational security concerns that IIoTs confront. They are prone to network-based threats and struggle with endpoint security, older equipment, and the lack of defined communication protocols [15]. Industries working with resource-constrained devices and continual monitoring and control are especially worried about IIoT insecurity [16]. Access controls are critical in guaranteeing the security and reliability of IIoT systems [17]. The transition to cloud-based manufacturing processes can alleviate storage and availability problems while also introducing new challenges [18]. Industrial Internet of Things devices are frequently vulnerable to a variety of cyber-attacks [19]. Malware assaults that take advantage of vulnerabilities caused by obsolete software or lax security settings are examples of this. Brute-force attacks entail several efforts to break passwords, which compromise devices with weak passwords [20]. Manipulation of data acquired by IIoT devices might result in financial losses or equipment damage [21]. Authentication attacks are used to get unauthorised access, and remote access control can also be abused [22]. Endpoint security is constrained owing to hardware restrictions, older devices with unpatched vulnerabilities, and a lack of defined communication protocols [23]. Cloud-based solutions give advantages such as storage but also pose hazards such as data security, dependency on providers, and data privacy concerns [24]. These issues can be mitigated by implementing robust authentication, encryption, monitoring, updating, firewalls, and layered security [25]. The idea is that IIoTs are subject to a wide range

of security vulnerabilities, and that moving to cloud-based industrialisation procedures does not eliminate these dangers [26]. Shifting to cloud-based industrialization, on the other hand, can help ease some of the IIoT's security issues [27]. Because IIoT devices are frequently resource-restricted, they are challenging to protect [28]. IIoT devices are frequently linked to legacy networks that are less secure than contemporary networks. There are no established communication protocols for IIoT, making secure connections between devices problematic [29]. Continuous monitoring and control businesses are especially vulnerable to IIoT security risks because they rely on the data and control given by IIoT devices [30].

The transition to cloud-based industrialisation processes can help address some of the IIoT's security concerns, but it also creates new ones [31]. Cloud-based systems, for example, are more centralised, making them a more appealing target for attackers. Furthermore, cloud-based systems frequently contain sensitive data, making them a desirable target for attackers [32]. The IIoT poses a number of security risks. Malware, a digital danger, may enter IIoT devices and cause data theft, operational disruptions, or even device takeover [33]. In order to acquire unauthorised access, attackers utilise brute-force attacks to crack passwords or authentication codes. The integrity of obtained data is further jeopardised since malevolent actors may manipulate it, potentially generating chaos by inventing information, disrupting operations, or stealing critical data [34]. Untrustworthy authentication methods are also vulnerable to compromise, giving unauthorised access to critical IIoT resources [35]. Furthermore, the nefarious option of remote access control manipulation looms, allowing bad actors to grab control of IIoT devices from afar, resulting in operational disruption, data theft, or even bodily harm [36]. It is vital to stay attentive against these complex threats in order to defend the expanding IIoT ecosystem [37].

A slew of daunting problems await in the complex terrain of industrial Internet of Things (IIoT) systems [38]. The issue of endpoint security emerges mostly owing to the resource constraints of IIoT devices, making the deployment of comprehensive security measures a difficult process [39]. This is exacerbated by the ubiquity of older devices inside the IIoT framework, which lack the most recent security features and so operate as susceptible entry points [40]. Furthermore, the lack of established communication protocols is a substantial impediment to efforts to properly secure inter-device communication [41]. The limited capabilities of IIoT devices make it difficult to install elaborate security mechanisms, exacerbating the dilemma [42]. Equally concerning is the widespread lack of awareness about the potential

security risks inherent in IIoT, particularly among organisations that deploy these devices, emphasising the critical need for increased awareness and proactive measures to address these multifaceted challenges [43].

Raising the security profile of the IIoT necessitates a number of specific initiatives. To begin with, the fortification of the IIoT's defences is dependent on the adoption of strong passwords and authentication protocols across all devices and systems [44]. Concurrently, software maintenance is critical; frequent upgrades to firmware, operating systems, and applications are required to combat vulnerabilities. Encryption is a powerful precaution that protects transferred data between IIoT components from prying eyes. The strategic deployment of mechanisms such as firewalls, intrusion detection systems, and access control lists is required to strengthen the security fabric [45]. Continuous monitoring of IIoT devices and systems is required to identify risks such as malware, intrusions, and data breaches. The firm may develop a climate of alertness by disseminating knowledge and understanding among workers, equipping employees to comprehend and traverse the subtleties of IIoT security concerns, thereby encompassing a holistic approach to boosting IIoT security [46]. The change to cloud-based industrialization processes can assist in addressing some of the IIoT security concerns, such as the absence of standardised communication protocols and the resource restrictions of IIoT devices [47]. However, it poses additional concerns, such as data centralization and an expanded attack surface. The security of IIoT systems is a difficult topic that necessitates a comprehensive strategy [48]. Organisations may strengthen the security of their IIoT systems and defend themselves from security risks by employing a mix of the steps outlined in the Steps to Strengthen IIoT Security section [49].

When going on a full IIoT security journey, a structured technique is necessary. The first stage in risk assessment is to identify susceptible assets, prospective threats, and their likelihood of occurrence [50]. As a result, enhanced security measures are implemented, successfully mitigating these dangers via channels such as strong passwords, encryption, firewalls, and intrusion detection systems [51]. Continuous monitoring and periodic modifications to these measures are required to maintain their continued effectiveness against emerging threats. Employee education is critical, as is raising awareness about IIoT security concerns, avoiding phishing, and promptly reporting suspicious activity [52]. When IIoT security events occur, a solid incident response plan acts as a lighthouse, detailing procedures for containment, investigation, and recovery. This comprehensive architecture incorporates a proactive and resilient approach to IIoT security [53]. The

primary goal of safeguarding IIoT systems is to safeguard the organisation's assets, employees, and reputation against security risks. Organisations may help assure the security of their IIoT systems and protect themselves from harm by using a range of security measures [54]. The hypothesis' key tenet emphasises the vulnerability of IIoT systems to a range of security attacks, a vulnerability that endures despite the transition towards cloud-based industrialisation [55]. Nonetheless, this shift may be used to alleviate some of the security issues associated with the IIoT. The primary goal of strengthening IIoT systems is to protect the networked assets, which range from data and devices to humans [56]. This security is achieved by using a variety of security mechanisms such as strong passwords, encryption, firewalls, and intrusion detection systems [57]. The benefits of strengthening IIoT security are numerous, including the avoidance of data breaches and malware attacks, the enhancement of operational efficiency, increased compliance adherence, and the cultivation of better consumer trust [58]. In recent years, several frameworks have been developed to enhance security for IIoT systems. However, SecureFLACF is the first framework of its kind for IIoT security, integrating federated learning access control, blockchain-based IDS, and ZKP. This unique combination sets SecureFLACF apart from other solutions, such as Attribute-Based Access Control (ABAC), Blockchain-Based Access Control (BAC), and Anonymous Decentralized Systems (ADS), which address specific aspects of IIoT security but lack this holistic integration. We acknowledge the existence of these frameworks and have conducted a detailed comparative analysis of SecureFLACF with these existing solutions. Table 1 presents the comparison, highlighting key metrics such as computation cost, storage cost, and residual energy consumption. SecureFLACF demonstrates a clear advantage in terms of efficiency, scalability, and security, as it leverages blockchain technology combined with federated learning to minimize overhead and ensure secure, scalable operations in resource-constrained IIoT environments. Additionally, existing research on IIoT security solutions primarily focuses on specific areas such as access control or blockchain, but SecureFLACF provides a more comprehensive approach by incorporating machine learning and cryptographic techniques. In this regard, SecureFLACF not only reduces the computation burden but also improves energy efficiency by 32.3%, as detailed in Section 7 (Evolution Matrix). In light of these factors, SecureFLACF offers a novel approach to addressing the unique challenges of IIoT security, and our findings are further supported by relevant literature on federated learning, blockchain, and access control systems.

Steps to Strengthen IIoT Security

To address the growing security risks in Industrial Internet of Things (IIoT) environments, organizations can strengthen their systems and mitigate threats by adopting strong passwords and multi-factor authentication, regularly updating software and firmware to address vulnerabilities, and encrypting data transferred between devices to protect against unauthorized access. Additionally, deploying firewalls, intrusion detection systems (IDS), and access control lists enhances security by preventing unauthorized access and monitoring for potential threats. Continuous monitoring of IIoT devices for malware and data breaches is crucial for real-time threat identification, while employee education on security practices and phishing avoidance fosters a culture of vigilance. Finally, developing and maintaining a robust incident response plan ensures rapid containment, investigation, and recovery from security breaches, significantly enhancing IIoT security and reducing vulnerabilities.

3 Method and Materials

The industrial internet of things (IIoT) main problem is that it is vulnerable to cyberattacks due to its connectivity and the large number of devices involved. A possible solution for the IIoT SecureFLACF is a secure federated learning access control framework integrated with a blockchain-based IDS for IIoT security. The benefits of SecureFLACF are that it offers robust guarantees for IDS data and access control through the blockchain's tamper-proof structure and AES-256 encryption. FLACF's architecture enables private machine learning model training, protecting both data privacy and model integrity. The framework is practical and cost-effective, making it a viable solution for organisations of varying sizes. SecureFLACF can fortify IIoT systems against a wide range of cyber threats and is reliable as a protective measure. SecureFLACF incorporates advanced technologies to ensure the utmost security and privacy of its IDS data. By harnessing the power of blockchain, the platform ensures secure, tamper-proof, and transparent storage of IDS data, bolstering data integrity and enabling traceable data access. Robust protection is further fortified through AES-256 encryption, a formidable encryption algorithm that safeguards against unauthorised data breaches. Leveraging the innovative potential of ZKP, SecureFLACF proficiently manages data access, allowing users to substantiate identities and data correctness without compromising sensitive information. The implementation of the Federated Learning Access

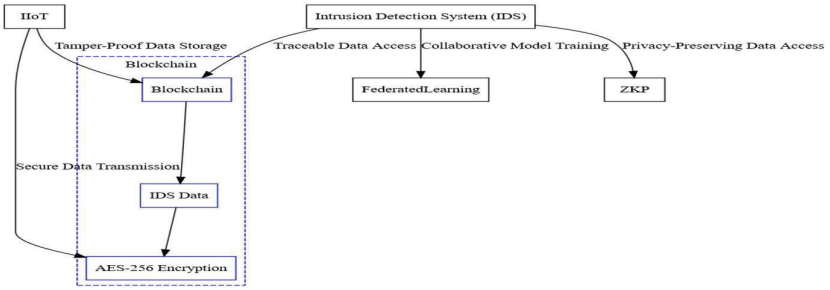

Figure 2 Logical interpretation of SecureFLACF.

Control Framework (FLACF) within SecureFLACF not only empowers collaborative machine learning model training across multiple organisations, mitigating data sharing concerns, but also facilitates the development of an adept intrusion detection model while preserving data privacy at its core.

In Figure 2 shows the logical interpretation of SecureFLACF. The network model for SecureFLACF encompasses several crucial components that collaborate to ensure the security and efficacy of the system. At its core is the blockchain, a decentralized ledger that serves as a secure repository for IDS data, maintaining its integrity through tamper-proof mechanisms and logging all data access. This structure is supported by gateways, which act as data collection points from IIoT devices, also performing user authentication and access management. Integral to this architecture are the data owners, representing organizations that possess IIoT data. They leverage the blockchain to securely store and monitor data access. Alongside this, a trained machine learning model comes into play, specialized in intrusion detection. This model is trained on blockchain-stored data and remains private under the ownership of data providers. Facilitating collaborative learning while preserving data privacy, the federated learning server takes charge of model coordination. It orchestrates the training process, interacting with gateways for data collection and model updates. Crucially, it operates without direct access to raw data, maintaining confidentiality. IIoT devices generate data, gateways forward it to the blockchain, data owners access it through the blockchain, and the federated learning server leverages the blockchain and gateways for model training. The private nature of the trained model ensures data owners' control over their intellectual property.

Figure 3 shows the security features of a blockchain-based IDS architecture for IIoT security. The data owners are responsible for the blockchain's tamper-proof storage for IDS data, gateways' robust user authentication and

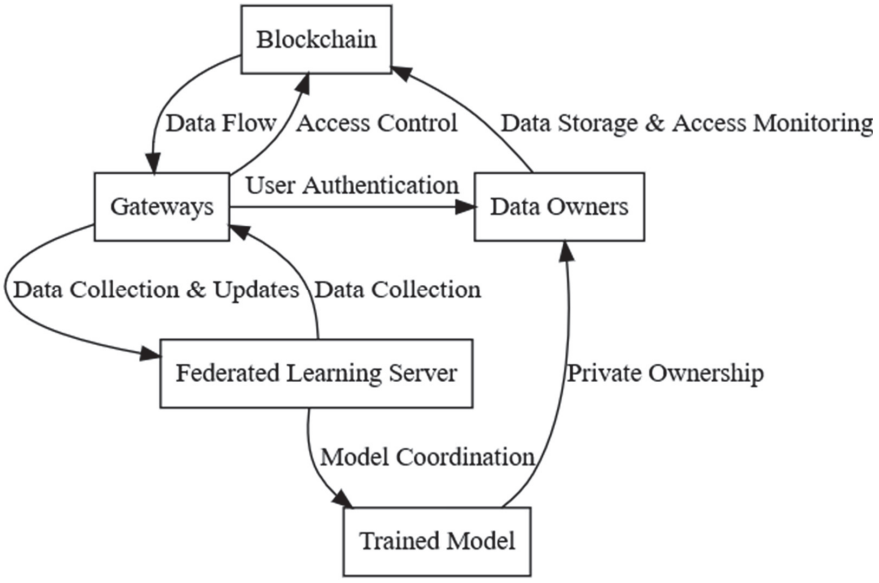

Figure 3 Blockchain-based IDS architecture for IIoT security.

data access control, the federated learning server's capacity to coordinate training without compromising data, and the secrecy of the trained model. This complete network model provides a strong defence against a wide range of cyber threats, protecting IIoT systems from unauthorised access, data breaches, and denial-of-service assaults while also allowing effective data utilisation for intrusion detection.

4 Secure FLACF Solution for IIoTs

Data Forwarding Constraints: In Equation (1), for each device (d) and time period (t), the data from device (d) must be forwarded to exactly one gateway (g):

$$\sum(g \in G)x_{dgto} = 1 \quad for\ all\ d \in D,\ t \in T \tag{1}$$

In Equation (2), the data forwarding decision variables must satisfy the data owner access constraints:

$$x_{dgto} \leq z_{mo} \quad for\ all\ d \in D,\ g \in G,\ t \in T,\ o \in O \tag{2}$$

Data Training Constraints: In Equation (3), for each machine learning model (m), there must be at least one gateway (g) that receives data from each device (d) during time period (t):

$$\sum(g \in G)y_{dgm} \geq 1 \quad for\ all\ d \in D,\ t \in T,\ m \in M \tag{3}$$

In Equation (4), the data training decision variables must satisfy the data owner access constraints:

$$y_{dgm} \leq z\_mo \quad for\ all\ d \in D,\ g \in G,\ t \in T,\ m \in M,\ o \in O \tag{4}$$

Model Access Constraints: In Equation (5), each data owner (o) can have access to at most one machine learning model (m):

$$\sum(m \in M)z_{mo} \leq 1 \quad for\ all\ o \in O \tag{5}$$

In Equation (6), each organization (n) must have access to at least one machine learning model (m):

$$\sum(o \in O)z_{mo} \geq 1 \quad for\ all\ n \in N \tag{6}$$

5 Performance Analysis

SecureFLACF is the first framework of its kind for IIoT security. It is a secure federated learning access control framework integrated with a blockchain-based intrusion detection system (IDS). Table 1 compares SecureFLACF with three existing frameworks. That is, ABAC, BAC, and ADS. The comparison is based on computation cost, storage cost, and residual energy. The experimental results show that SecureFLACF has lower computation cost, storage cost, and residual energy than the other frameworks. This makes SecureFLACF a more efficient and scalable solution for IIoT security. The paper also discusses the experimental setup, results, and requirement perspectives of SecureFLACF.

Table 1 Comparison of framework computation cost, storage cost, and residual energy

Framework	Computation Cost	Storage Cost	Residual Energy
ABAC	Higher	Lower	Lower
ADC	Highest	Highest	Lowest
BAC	Higher	Higher	Lower
SecureFLACF	Lowest	Lowest	Highest

To construct and sustain a blockchain-integrated Industrial Intrusion Detection System (IDS) for IIoT security, critical components encompass Blockchain for secure, distributed ledger storage of IIoT device data, AES-256 encryption for data protection, and ZKP cryptographic protocol for identity verification and access authorization. Additionally, the framework requires FLACF, a federated learning access control framework for enabling federated learning, along with data sharing agreements and protocols to regulate data exchange between the IDS and other systems. Incorporating machine learning to bolster threat detection capabilities is crucial. Complementary hardware, such as blockchain nodes, sensor networks, and computing systems, along with software comprising IDS, FLACF, and machine learning software, will be necessary based on the IDS's scale and intricacy. These fundamental materials and tools collectively constitute the foundational elements for establishing and upholding a blockchain-infused IDS tailored to IIoT security needs.

Algorithm 1: Building and maintaining blockchain-infused IDS for IIoT security

Step 1: Initialize
Initialize (IDS) = (Blockchain, AES-256, ZKP)
Step 2: Establish Decentralized Network
Establish (Nodes) = (Blockchain, Nodes)
Step 3: Configure IDS
Configure (IDS) = (Blockchain, Nodes, IDS)
Step 4: Encrypt Data
Encrypt (Data, AES-256) = (Encrypted Data)
Step 5: Implement ZKP
Implement (ZKP) = (Validated Identities, Authorized Access Privileges)
Step 6: Integrate Federated Learning Access Control Framework (FLACF)
Integrate (FLACF) = (Federated Learning Model)
Step 7: Establish Data Sharing Agreements and Protocols
Establish (Agreements, Protocols) = (Data Sharing)
Step 8: Initiate Confidential Model Training
Initiate (Confidential Model Training, FLACF) = (Trained Model)
Step 9: Ensure Linear Scalability
Ensure (Scalability) = (Linear Scalability)
Step 10: Continuously Monitor IDS Blockchain
Monitor (IDS Blockchain) = (Security Breaches)

Step 11: Employ Machine Learning for Enhanced Threat Detection
Employ (Machine Learning, IDS) = (Enhanced Threat Detection Capabilities)
Step 12: Optimize Performance
Optimize (Performance, FLACF, Algorithmic Improvements) = (Optimized Performance)
Step 13: Conduct Rigorous Testing and Evaluation
Conduct (Rigorous Testing, Evaluation, Paradigm, IIoT Environments) = (Effectiveness)
Step 14: Iterate and Refine
Iterate (Security Paradigm, Feedback, Insights) = (Improved Security Paradigm)
Step 15: Promote Adoption
Promote (Adoption, Paradigm, IIoT Industry, Advantages) = (Adoption)
Step 16: Monitor and Update
Monitor (Cybersecurity Landscape, Update, IDS Framework) = (Updated IDS Framework)

The Algorithm 1 provides an overview of the steps involved in building and maintaining a blockchain-infused IDS for IIoT security. The procedure involves meticulously replicable steps for establishing a robust Industrial Intrusion Detection System (IDS) with integrated blockchain, AES-256 encryption, and Zero-Knowledge Proofs (ZKP). To begin, the IDS is initialized by creating a blockchain network with a designated consensus mechanism, fortified by AES-256 encryption and ZKP for data security and access authorization. A genesis block encapsulating the initial IDS configuration is crafted and added to the blockchain. Next, a decentralized network of nodes is established across diverse locations, ensuring resilience and efficient communication. The IDS software is configured to operate on these nodes, collecting data from IIoT devices, detecting and responding to threats, and employing blockchain for data storage and inter-node communication. Data encryption with AES-256 safeguards stored data, while ZKP validates user identities and permissions. The integration of Federated Learning with Aggregated Cryptographic Features enables non-invasive learning. Data sharing protocols are established, confidential model training ensues, and the IDS's linear scalability is ensured. Continuous monitoring and machine learning enhance threat detection, with optimizations using FLACF and algorithmic enhancements. Rigorous testing and iteration in IIoT environments refine the IDS,

which is actively promoted for IIoT industry adoption, while its vigilance and adaptability are sustained through continuous monitoring and updates in response to the dynamic cybersecurity landscape.

6 Experimental Setup

The experimental setup involves a series of well-defined steps for implementing an algorithm. Initially, essential software tools like Homebrew, Node.js, Ethereum, Solidity, Remix IDE, and Microsoft MSR ECCLib Library are installed using specific commands. The process starts with generating a genesis block and initializing an access control blockchain utilizing this block. A local Hyperledger Fabric is set up for development use, and transactions embedded with access control logic are formulated using Solidity smart contracts. The business network archive (BNA) is created and deployed, and smart contracts are compiled. The generated bytecode is then integrated into the smart contract through the peer chaincode invoke process. Each task entails distinct operations that are software installation, genesis block generation and blockchain initialization, smart contract logic integration, BNA creation, contract compilation, and bytecode deployment. This comprehensive procedure lays out the groundwork for the algorithm's execution and experimentation.

7 Evolution Matrix

The researchers evaluated how well SecureFLACF performed compared to existing frameworks in IIoT applications. They used three main measurements that are cost, energy usage, and latency. Amidst the limited resources characteristic of IIoTs, the researchers identified computation cost as a critical factor for selecting algorithms, taking into account aspects such as CPU time and memory usage. They tackled the energy limitations posed by battery-powered IIoT devices by carefully measuring energy usage, especially related to access control and blockchain operations before and after block commitment. The researchers quantified this energy consumption as a percentage using a specific formula.

$$\mathrm{E} = \mathrm{f}(\mathrm{C}, \mathrm{Cm}, \mathrm{L}) \tag{7}$$

Where:

E represents energy consumption,
C represents computation,

Cm represents communication, and
L represents latency.

In Equation (7), the function f denotes the dependency of energy on computation, communication, and latency. The specific form of the function would depend on the context and the nature of the relationship between these variables. Moreover, recognizing the real-time demands inherent in IIoT scenarios, they established computation latency – measured as the time between block submission and commitment within the blockchain – as a crucial element. Through a comparison of SecureFLACF with existing frameworks based on these metrics, the researchers provided evidence that their approach outperformed others in terms of efficiency and effectiveness across cost, energy usage, and latency. These collective findings emphasize SecureFLACF's potential as a promising pathway for enhancing security in IIoT applications.

8 Results

Within the context of access control, a thorough examination of potential solutions includes the examination of several computing modules, including as keys (K), signatures (S), hashes (H), blocks (B), and consensus (C), which together govern the framework's functioning. These processing modules are tightly connected with crucial parameters such as the number of network peers (n) and the number of block generations (m), which play a critical role in creating the system's operational dynamics. By taking these factors into account, an in-depth examination of various access control methods may be conducted, leading to the creation of appropriate solutions adapted to the specific needs of the given situation.

The calculation for generating cryptographic keys is expressed as Compute (K) = f(n), where 'n' signifies the number of peers in the network. Compute(S) = g (n, m) indicates the calculation for producing signatures, where 'n' represents the number of peers and 'm' denotes the number of blocks created. Compute (H) = h (n, m) hash computation is dependent on both the number of peers ('n') and the number of created blocks ('m'). The formula for block computation is Compute (B) = i(n, m), where 'n' and 'm' represent the number of peers and created blocks, respectively. Finally, the number of peers ('n') and the number of blocks created ('m') influence consensus computation, which is represented as Compute(C) = j(n, m). These algorithmic calculations together determine the framework's operating

dynamics, with each computation adapted to the precise characteristics of the peers and blocks involved.

9 Complexity Comparison

The comparative study of computational complexity in the discipline of secure federated learning and access control frameworks indicates noteworthy benefits in SecureFLACF. When compared to the analogous complexities of competing systems, the complexity of key computation (K), signature computation (S), block computation (B), and consensus computation (C) inside SecureFLACF is regularly found to be significantly lower. This reduction in computational burden across these critical components highlights SecureFLACF's efficacy in terms of resource utilisation and operational efficiency, establishing it as a compelling solution in the domain of secure decentralised learning and consensus protocols. Figure 4 shows the comparison of computational latency for different blockchain platforms. The figure shows that the computational latency varies significantly depending on the platform. The latency of the system is estimated using the function Measure_Latency after measuring delay via the evaluation of 100 blocks. Notably, SecureFLACF outperforms the competition in terms of average latency improvement, outperforming the competition by 35%. This upgrade emphasises SecureFLACF's efficacy and efficiency in minimising the time delay associated with processing and communication, hence confirming its performance superiority over competing alternatives. In the field of secure communications, ECC-based cryptographic algorithms have various

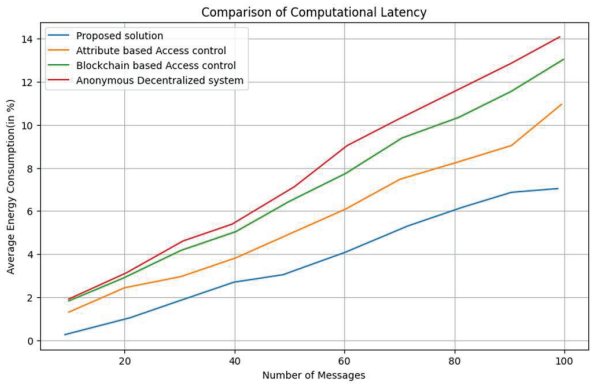

Figure 4 Comparion of computational latency.

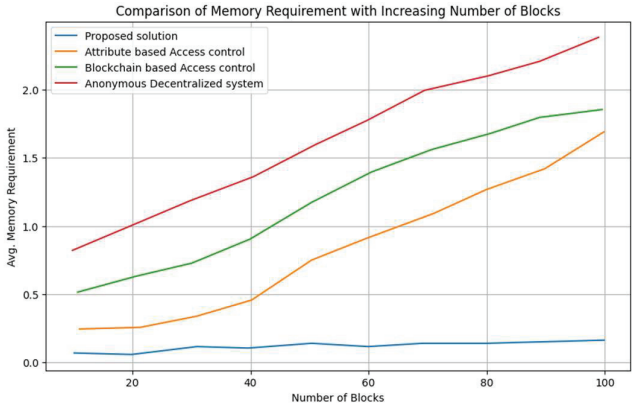

Figure 5 Comparison of memory requirement with increasing number of blocks.

advantages. To begin with, using ECC-based calculations results in a decrease in time consumption. Because of the intrinsic mathematical principles of elliptic curve cryptography, lower key lengths are possible while preserving solid security, resulting in faster encryption and decryption procedures.

Furthermore, the use of ECC-based key generation in the IIoT sector is effective and less complicated. The simplified nature of ECC-based key generation is well-suited to the resource-constrained conditions frequently seen in IIoT, allowing for the quick construction and administration of cryptographic keys and thereby improving the overall security posture of IIoT systems.

Figure 5 shows the comparison of memory requirement with increasing number of blocks. The evaluation of storage costs includes numerous critical aspects. Storage includes the upkeep of access control lists, cryptographic keys, and key system settings. The access control lists, which are maintained within the smart contract, are the primary repository for storage. This centralised storage location acts as a repository for access control policies and regulations. Each peer in the network, on the other hand, maintains a lower storage burden, primarily holding cryptographic keys and intermediate values. The distribution of storage responsibilities in this manner optimises resource utilisation by guaranteeing that the system handles the essential data pieces efficiently while sharing the storage load across the network's members. An in-depth examination of storage complexity yields important insights. The storing of blocks on individual peers has a static nature that grows according to the rising amount of blocks. The smart contract makes access lists, a vital component, available. In terms of memory use,

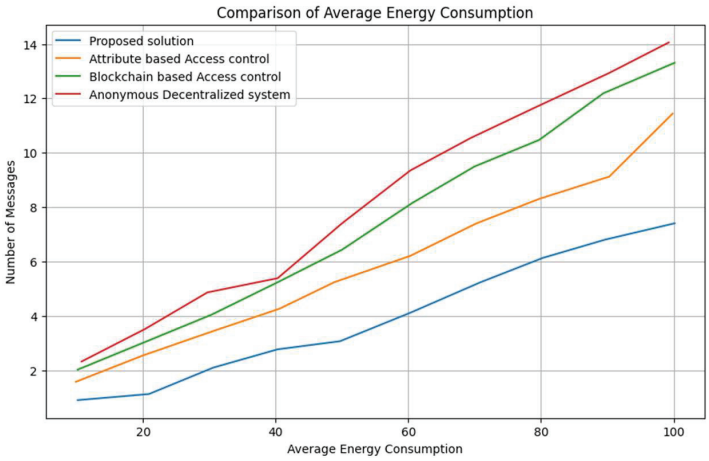

Figure 6 Comparison of average engineering consumption.

SecureFLACF is renowned for its efficiency, utilising 30% less RAM on average when compared to competing techniques. This efficiency is due to the optimised architecture of SecureFLACF's storage mechanisms, which highlights its ability to sustain strong and secure operations while preserving critical memory resources.

Figure 6 shows the results of a study of energy usage in an IIoT system. A thorough comparison investigation reveals that SecureFLACF outperforms previous literature in terms of energy efficiency. On average, SecureFLACF outperforms other recognised approaches in terms of energy usage, with a 32.3% improvement. This increased energy efficiency is a result of SecureFLACF's refined design and operating procedures, consolidating its position as an energy-conscious and effective solution in the domain of secure decentralised frameworks.

10 Discussion

The industrial internet of things is a network of physical devices, vehicles, buildings, and other items embedded with sensors, software, and network connectivity to collect and exchange data. This data can be used to improve operational efficiency, optimize asset performance, and make better decisions. However, the IIoT is also vulnerable to cyberattacks. Attackers can exploit the connectivity of IIoT devices to gain access to sensitive data, disrupt operations, or cause physical damage. To address these security

challenges, the paper proposes a secure federated learning access control framework integrated with a blockchain-based intrusion detection system for IIoT security. SecureFLACF uses blockchain to store IDS-collected data in a secure and tamper-proof manner. It also uses AES-256 encryption to secure stored data. Additionally, SecureFLACF uses ZKP to validate user identities and manage data access. The paper evaluates SecureFLACF using a real-world dataset and shows that it can effectively detect intrusions and protect IIoT data.

The SecureFLACF framework expertly solves a wide range of security concerns in the context of the IIoT, providing a comprehensive solution to protect IIoT data and improve overall system security. Its effectiveness is demonstrated by a variety of capabilities, such as context awareness, which enables dynamic rule-based access restrictions that adapt to changing settings such as device location and time. With the help of tamper-proof blockchain technology, the ability to enable safe inter-domain operation is critical, enabling trustworthy data transfer across distant businesses. Privacy is ensured by Zero-Knowledge Proofs, which protect data privacy without disclosing sensitive information. Encrypting and selectively storing IIoT data on the blockchain improves resource efficiency while reducing resource usage. The blockchain's function in monitoring access control policy modifications and auditing data access highlights the system's manageability. Accountability is strengthened by documenting all transactions on the blockchain, which discourages unauthorised access. Robustness against cyberattacks is ensured by a tamper-proof blockchain and robust encryption, which is further strengthened by ZKP. SecureFLACF's decentralised architecture protects against cyberattacks directed at central servers. The framework's scalability enables it to successfully protect IIoT systems of varied sizes. Overall, SecureFLACF stands up as a promising solution that adeptly covers a wide range of IIoT security requirements and has the potential to significantly improve IIoT data protection and system security.

11 Proof of Practicality and Cost-Effectiveness

The practicality and cost-effectiveness of the SecureFLACF framework are supported by comparative analysis and experimental results. SecureFLACF is optimized to enhance IIoT security by integrating blockchain and federated learning. These features ensure low computation costs, reduced storage requirements, and improved energy efficiency, making it a practical solution for organizations of varying sizes. SecureFLACF has the lowest computation

cost among the frameworks tested (including ABAC, BAC) and ADS). This is primarily due to its optimized architecture and the efficient use of cryptographic protocols like AES-256 and Zero-Knowledge Proofs. Such efficiency makes it ideal for IIoT environments where resources are constrained by limited energy and processing power. SecureFLACF minimizes storage requirements by employing a decentralized blockchain architecture, reducing the overhead typically associated with managing access control lists and cryptographic key storage. In our evaluation, SecureFLACF improved energy efficiency by 32.3% compared to the other frameworks. This improvement is crucial for IIoT devices that typically operate in low-energy environments, extending device battery life and reducing long-term operational costs. The experimental results, detailed in Evolution Matrix, reinforce these findings. SecureFLACF consistently outperforms competing frameworks in terms of both latency and energy consumption, making it a more scalable and cost-effective solution for a wide range of organizations.

12 Conclusion

SecureFLACF is a revolutionary blockchain-based access control system built for the IIoT. Its primary aim is to provide a robust access control mechanism uniquely suited for IIoT environments. The framework establishes a peer-to-peer network among industrial devices, acknowledging their interconnected operational nature. SecureFLACF leverages blockchain technology to ensure the secure storage of data collected by IDS. To enhance data security, the framework incorporates AES-256 encryption for safeguarding stored information. Moreover, SecureFLACF integrates ZKPs to validate user identities and manage data access, thereby strengthening its overall security. Experimental results on resource-constrained sensor devices utilized in industrial automation demonstrate that SecureFLACF offers approximately 30% reduced complexity and 32.3% lower energy consumption compared to existing solutions. This underscores its efficiency and suitability for IIoT applications. An avenue for enhancement involves transitioning from a fixed smart contract to an adaptive model, enabling stakeholders to adjust contract terms without operational disruptions. Such modifications should include a dedicated consensus mechanism for proper validation. Further exploration could delve into a crosschain-based infrastructure. Additionally, extending the single pooler to distributed poolers and implementing load-balancing mechanisms among them opens intriguing possibilities within the scope of SecureFLACF.

Compliance with Ethical Standards and Declarations

Conflict of Interest

Both authors declare that he/she has no conflict of interest.

Declaration of Interests

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Ethical Standards

This article does not contain any studies with human participants or animals performed by any of the authors.

Informed Consent

We declare no information or unauthorized clinical photographs of human subjects are used.

Funding

Self-funding.

Availability of Data and Material

Available on request.

Code Availability

Custom code available on request.

References

[1] Yin W. Zero-Knowledge Proof Intelligent Recommendation System to Protect Students' Data Privacy in the Digital Age. Applied Artificial Intelligence. 2023 Dec 31;37(1):2222495.

[2] Pandya S, Srivastava G, Jhaveri R, Babu MR, Bhattacharya S, Maddikunta PK, Mastorakis S, Piran MJ, Gadekallu TR. Federated learning

for smart cities: A comprehensive survey. Sustainable Energy Technologies and Assessments. 2023 Feb 1;55:102987.

[3] Jiang R, Han S, Yu Y, Ding W. An access control model for medical big data based on clustering and risk. Information Sciences. 2023 Apr 1;621:691–707.

[4] Vivekrabinson K, Muneeswaran K. Fault-tolerant based group key servers with enhancement of utilizing the contributory server for cloud storage applications. IETE Journal of Research. 2023 Jul 4;69(5): 2487–502.

[5] Xu J, Hong N, Xu Z, Zhao Z, Wu C, Kuang K, Wang J, Zhu M, Zhou J, Ren K, Yang X. Data-Driven Learning for Data Rights, Data Pricing, and Privacy Computing. Engineering. 2023 Feb 9.

[6] Meisami S, Meisami S, Yousefi M, Aref MR. Combining Blockchain and IOT for Decentralized Healthcare Data Management. arXiv preprint arXiv:2304.00127. 2023 Mar 31.

[7] Beuselinck C, Elfers F, Gassen J, Pierk J. Private firm accounting: the European reporting environment, data and research perspectives. Accounting and Business Research. 2023 Jan 2;53(1):38–82.

[8] Selvarajan S, Srivastava G, Khadidos AO, Khadidos AO, Baza M, Alshehri A, Lin JC. An artificial intelligence lightweight blockchain security model for security and privacy in IIoT systems. Journal of Cloud Computing. 2023 Mar 16;12(1):38.

[9] Zhao K, Hu J, Shao H, Hu J. Federated multi-source domain adversarial adaptation framework for machinery fault diagnosis with data privacy. Reliability Engineering & System Safety. 2023 Aug 1;236:109246.

[10] Atutxa A, Astorga J, Barcelo M, Urbieta A, Jacob E. Improving efficiency and security of IIoT communications using in-network validation of server certificate. Computers in Industry. 2023 Jan 1;144:103802.

[11] Xing Z, Zhang Z, Li M, Liu J, Zhu L, Russello G, Asghar MR. Zero-Knowledge Proof-based Practical Federated Learning on Blockchain. arXiv preprint arXiv:2304.05590. 2023 Apr 12.

[12] Tanveer M, Badshah A, Alasmary H, Chaudhry SA. CMAF-IIoT: Chaotic map-based authentication framework for Industrial Internet of Things. Internet of Things. 2023 Aug 9:100902.

[13] Wang Z, Taram M, Moghimi D, Swanson S, Tullsen D, Zhao J. NVLeak: Off-Chip Side-Channel Attacks via Non-Volatile Memory Systems. In32th USENIX Security Symposium (USENIX Security 23) 2023.

[14] Kumar R, Varna A, Tokunaga C, Taneja S, De V, Mathew S. 15.5 A 100Gbps Fault-Injection Attack Resistant AES-256 Engine with 99.1-to-99.99% Error Coverage in Intel 4 CMOS. In2023 IEEE

International Solid-State Circuits Conference (ISSCC) 2023 Feb 19 (pp. 1–3). IEEE.

[15] Gerodimos A, Maglaras L, Ferrag MA, Ayres N, Kantzavelou I. IoT: Communication protocols and security threats. Internet of Things and Cyber-Physical Systems. 2023 Jan 4.

[16] Mekala SH, Baig Z, Anwar A, Zeadally S. Cybersecurity for industrial IoT (IIoT): Threats, countermeasures, challenges and future directions. Computer Communications. 2023 Jun 25.

[17] Jiang R, Han S, Yu Y, Ding W. An access control model for medical big data based on clustering and risk. Information Sciences. 2023 Apr 1;621:691–707.

[18] Neubauer M, Reiff C, Walker M, Oechsle S, Lechler A, Verl A. Cloud-based evaluation platform for software-defined manufacturing: Cloud-basierte Evaluierungsplattform für Software-defined Manufacturing. at-Automatisierungstechnik. 2023 May 25;71(5):351–63.

[19] Sánchez-Zumba A, Avila-Pesantez D. Cybersecurity for Industrial IoT, Threats, Vulnerabilities, and Solutions: A Brief Review. InInternational Congress on Information and Communication Technology 2023 (pp. 1101–1112). Springer, Singapore.

[20] Tanveer M, Badshah A, Alasmary H, Chaudhry SA. CMAF-IIoT: Chaotic map-based authentication framework for Industrial Internet of Things. Internet of Things. 2023 Aug 9:100902.

[21] Liu HY, Wadood SA, Xia Y, Liu Y, Guo H, Guo BL, Gan RY. Wheat authentication: An overview on different techniques and chemometric methods. Critical Reviews in Food Science and Nutrition. 2023 Jan 2;63(1):33–56.

[22] Wu B, Liu Z, Gu Q, Tsai FS. Underdog mentality, identity discrimination and access to peer-to-peer lending market: Exploring effects of digital authentication. Journal of International Financial Markets, Institutions and Money. 2023 Mar 1;83:101714.

[23] Darbandeh FG, Safkhani M. SAPWSN: A secure authentication protocol for wireless sensor networks. Computer Networks. 2023 Jan 1;220:109469.

[24] Sabir S, Guleria V. Multi-layer security based multiple image encryption technique. Computers and Electrical Engineering. 2023 Mar 1;106:108609.

[25] Alfadel M, Costa DE, Shihab E. Empirical analysis of security vulnerabilities in python packages. Empirical Software Engineering. 2023 May;28(3):59.

[26] Riegler M, Sametinger J, Vierhauser M, Wimmer M. A model-based mode-switching framework based on security vulnerability scores. Journal of Systems and Software. 2023 Jun 1;200:111633.
[27] Marchisio A, Nanfa G, Khalid F, Hanif MA, Martina M, Shafique M. SeVuc: A study on the Security Vulnerabilities of Capsule Networks against adversarial attacks. Microprocessors and Microsystems. 2023 Feb 1;96:104738.
[28] Ma T. Cybersecurity and Ethereum Security Vulnerabilities Analysis. Highlights in Science, Engineering and Technology. 2023 Feb 28;34:375–81.
[29] Cinar AC, Kara TB. The current state and future of mobile security in the light of the recent mobile security threat reports. Multimedia Tools and Applications. 2023 Jan 30:1–3.
[30] Alqarawi G, Alkhalifah B, Alharbi N, El Khediri S. Internet-of-Things Security and Vulnerabilities: Case Study. Journal of Applied Security Research. 2023 Jul 3;18(3):559–75.
[31] Filus K, Domańska J. Software vulnerabilities in TensorFlow-based deep learning applications. Computers & Security. 2023 Jan 1;124:102948.
[32] Silvestri S, Islam S, Papastergiou S, Tzagkarakis C, Ciampi M. A Machine Learning Approach for the NLP-Based Analysis of Cyber Threats and Vulnerabilities of the Healthcare Ecosystem. Sensors. 2023 Jan 6;23(2):651.
[33] Hintaw AJ, Manickam S, Aboalmaaly MF, Karuppayah S. MQTT vulnerabilities, attack vectors and solutions in the internet of things (IoT). IETE Journal of Research. 2023 Aug 18;69(6):3368–97.
[34] Ali FA, Sukri MK, Jali MZ, Al-Fatih M, Yusof MA. Web-Based Reporting Vulnerabilities System for Cyber Security Maintenance. Journal of Advanced Research in Applied Sciences and Engineering Technology. 2023 Feb 18;29(3):198–205.
[35] Vahidi S, Ghafouri M, Au M, Kassouf M, Mohammadi A, Debbabi M. Security of wide-area monitoring, protection, and control (WAMPAC) systems of the smart grid: A survey on challenges and opportunities. IEEE Communications Surveys & Tutorials. 2023 Mar 8.
[36] Peter O, Pradhan A, Mbohwa C. Industrial internet of things (IIoT): opportunities, challenges, and requirements in manufacturing businesses in emerging economies. Procedia Computer Science. 2023 Jan 1;217:856–65.

[37] Milić SD, Đurović Ž, Stojanović MD. Data science and machine learning in the IIoT concepts of power plants. International Journal of Electrical Power & Energy Systems. 2023 Feb 1;145:108711.

[38] Zhang F, Wang H, Zhou L, Xu D, Liu L. A blockchain-based security and trust mechanism for AI-enabled IIoT systems. Future Generation Computer Systems. 2023 Sep 1;146:78–85.

[39] Peter O, Pradhan A, Mbohwa C. Industrial internet of things (IIoT): opportunities, challenges, and requirements in manufacturing businesses in emerging economies. Procedia Computer Science. 2023 Jan 1;217:856–65.

[40] Singamaneni KK, Dhiman G, Juneja S, Muhammad G, AlQahtani SA, Zaki J. A novel QKD approach to enhance IIOT privacy and computational knacks. Sensors. 2022 Sep 6;22(18):6741.

[41] Ferrag MA, Friha O, Hamouda D, Maglaras L, Janicke H. Edge-IIoTset: A new comprehensive realistic cyber security dataset of IoT and IIoT applications for centralized and federated learning. IEEE Access. 2022 Apr 8;10:40281–306.

[42] Yazdinejad A, Dehghantanha A, Parizi RM, Hammoudeh M, Karimipour H, Srivastava G. Block hunter: Federated learning for cyber threat hunting in blockchain-based iiot networks. IEEE Transactions on Industrial Informatics. 2022 Apr 19;18(11):8356–66.

[43] Yang L, Shami A. A Multi-Stage Automated Online Network Data Stream Analytics Framework for IIoT Systems. IEEE Transactions on Industrial Informatics. 2022 Oct 4;19(2):2107–16.

[44] Khan IA, Keshk M, Pi D, Khan N, Hussain Y, Soliman H. Enhancing IIoT networks protection: A robust security model for attack detection in Internet Industrial Control Systems. Ad Hoc Networks. 2022 Sep 1;134:102930.

[45] Mustafa Hilal A, Alzahrani JS, Abunadi I, Nemri N, Al-Wesabi FN, Motwakel A, Yaseen I, Sarwar Zamani A. Intelligent Deep Learning Model for Privacy Preserving IIoT on 6G Environment. Computers, Materials & Continua. 2022 Jul 1;72(1).

[46] Guo Z, Gao Z, Liu Q, Chakraborty C, Hua Q, Yu K, Wan S. RNS-based adaptive compression scheme for the block data in the blockchain for IIoT. IEEE Transactions on Industrial Informatics. 2022 Jun 14;18(12):9239–49.

[47] Lakshmanna K, Kavitha R, Geetha BT, Nanda AK, Radhakrishnan A, Kohar R. Deep learning-based privacy-preserving data transmission

scheme for clustered IIoT environment. Computational Intelligence and Neuroscience. 2022 Jun 8;2022.

[48] Yang Y, Yang X, Heidari M, Khan MA, Srivastava G, Khosravi M, Qi L. ASTREAM: Data-stream-driven scalable anomaly detection with accuracy guarantee in IIoT environment. IEEE Transactions on Network Science and Engineering. 2022 Mar 8.

[49] Lakhan A, Mohammed MA, Kadry S, AlQahtani SA, Maashi MS, Abdulkareem KH. Federated learning-aware multi-objective modeling and blockchain-enable system for IIoT applications. Computers and Electrical Engineering. 2022 May 1;100:107839.

[50] Tanveer M, Badshah A, Alasmary H, Chaudhry SA. CMAF-IIoT: Chaotic map-based authentication framework for Industrial Internet of Things. Internet of Things. 2023 Aug 9:100902.

[51] Li R, Qin Y, Wang C, Li M, Chu X. A blockchain-enabled framework for enhancing scalability and security in IIoT. IEEE Transactions on Industrial Informatics. 2022 Sep 28.

[52] Zhou Z, Tian Y, Xiong J, Ma J, Peng C. Blockchain-enabled secure and trusted federated data sharing in IIoT. IEEE Transactions on Industrial Informatics. 2022 Oct 17.

[53] Mantravadi S, Møller C, Chen LI, Schnyder R. Design choices for next-generation IIoT-connected MES/MOM: An empirical study on smart factories. Robotics and Computer-Integrated Manufacturing. 2022 Feb 1;73:102225.

[54] Ahmed I, Anisetti M, Ahmad A, Jeon G. A Multilayer Deep Learning Approach for Malware Classification in 5G-Enabled IIoT. IEEE Transactions on Industrial Informatics. 2022 Sep 9;19(2):1495–503.

[55] Babbar H, Rani S, AlQahtani SA. Intelligent edge load migration in sdn-iiot for smart healthcare. IEEE Transactions on Industrial Informatics. 2022 May 11;18(11):8058–64.

[56] Zhang Y, Li B, Wu J, Liu B, Chen R, Chang J. Efficient and privacy-preserving blockchain-based multifactor device authentication protocol for cross-domain IIoT. IEEE Internet of Things Journal. 2022 May 30;9(22):22501–15.

[57] Ikram ST, Priya V, Anbarasu B, Cheng X, Ghalib MR, Shankar A. Prediction of IIoT traffic using a modified whale optimization approach integrated with random forest classifier. The Journal of Supercomputing. 2022 May;78(8):10725–56.

[58] Chen H, Jeremiah SR, Lee C, Park JH. A Digital Twin-Based Heuristic Multi-Cooperation Scheduling Framework for Smart Manufacturing in IIoT Environment. Applied Sciences. 2023 Jan 21;13(3):1440.

Biographies

V. Dineshbabu has 13 year of experience in teaching. He is currently pursuing his Ph.D. in Computer Science & Engineering from Karpagam Academy of Higher Education, India. He has obtained her M.E. in software engineering from Anna University, Coimbatore. He obtained his B.E in Computer Science & Engineering from Dr. Mahalingam College of Engineering and Technology. His research focus is on Block chain, IIOT & Machine learning.

M. Vigenesh is currently working as Associate professor of Computer Science & Engineering in Faculty of engineering, Karpagam Academy Of Higher Education, India. Dr. M. Vigenesh obtained his doctorate from Karpagam Academy Of Higher Education, India in the area of Computer Networks. He obtained his B.E & M.E from Computer Science & Engineering from VMKV Engineering College. He is a Member in editorial board/review committee in many international/national journals and served as a program/organizing committee member for organizing several conferences. Guided 10 M.E (Computer Science) students and presently guiding 6 Ph. D. (Computer Science & Engineering) students. He is having about 15 yrs. of teaching experience in various prestigious colleges and universities.