Enhancing Aspects of IIoT Networks with Federated Learning Blockchain-Integrated Authentication Solution

by Ling Fang Ting

Submission date: 15-Jul-2024 10:51AM (UTC+0700)

Submission ID: 2416996019

File name: IJEEMCS_VOL_1_NO_3_SEPT_2024_Page_25-42.docx (242.15K)

Word count: 5694

Character count: 38083

IJEEMCS : International Journal of Electrical Engineering, Mathematics and Computer Science
Vol. 1, No.3 September 2024
e-ISSN: 3048-1945, p-ISSN : 3048-1910, Page 25-42
DOI: https://doi.org/10.62951/ijeemcs.v1i3.17
Available online at: https://international.arteii.or.id/index.php/IJEEMCS/==

Enhancing Aspects of IIoT Networks with Federated Learning Blockchain-Integrated Authentication Solution

Ling Fang Ting[1], Ng Hui Wen[1], Tsi Shi Ping[1], Vivian Bong Chiaw Cin[1], Yew Wei Yi[1], & Muhammad Faisal[2]

1 Faculty of Computer Science and Information Technology, Universiti Malaysia Sarawak, Kota
Samarahan 94300, Malaysia
2 Director HRIMS, Ministry of Human Right

75463@siswa.unimas.my, 76014@siswa.unimas.my, 73863@siswa.unimas.my, 77104@siswa.unimas.my, 77222@siswa.unimas.my, dr.faisalshabbir88@gmail.com

Address: Jln Datuk Mohammad Musa, 94300 Kota Samarahan, Sarawak, Malaysia
Author Correspredence : 75463@siswa.unimas.my

Abstract. *The Industrial Internet of Things (IIoT) faces various challenges in ensuring secure communication, authentication, and data integrity due to its distributed nature and evolving threat landscape. To address these issues, this paper proposes the integration of blockchain authentication as a robust solution to enhance security and reliability in IIoT networks. By leveraging Federated Learning with blockchain technology, the proposed solution aims to improve authentication mechanisms by training models across multiple edge devices, increasing fault tolerance, and adaptability while reducing the risk of single points of failure. The use of blockchain technology ensures a tamper-proof and transparent ledger for securely storing authentication data and model updates, enhancing security and integrity in IIoT networks. The results and analysis demonstrate that the integration of Federated Learning and blockchain technology effectively addresses interoperability issues, performance optimization concerns, and security vulnerabilities within IIoT networks, offering a more efficient, secure, and scalable authentication alternative.*

Keywords:*authentication;blockchain;complexities;decentralized;Industrial Internet of Things*

1. INTRODUCTION

In the dynamic landscape of Industrial Internet of Things (IIoT), the establishment of robust authentication mechanisms is paramount to ensuring the security of critical data, preserving operational integrity, and fostering trust among interconnected devices. As IIoT networks grow in complexity and scale, traditional centralized authentication systems struggle to keep pace with the escalating security demands and the heterogeneous nature of connected devices. In this context, blockchain technology emerges as a beacon of promise, renowned for its decentralized and distributed ledger architecture that inherently resists tampering and fraud.

Blockchain's decentralized nature ensures that no single point of failure exists, which significantly mitigates the risk of cyberattacks that could compromise an entire network. This

Received: Juni 09, 2024; Revised: Juni 21, 2024; Accepted: Juli 12, 2024; Online Available: Juli 15, 2024;
** Ling Fang Ting, 75463@siswa.unimas.my*

is particularly crucial in IIoT environments, where the integrity and availability of data are critical for maintaining operational continuity and safety. By distributing the authentication process across multiple nodes, blockchain enhances the resilience and reliability of IIoT networks, ensuring that even if some nodes are compromised, the overall system remains secure.

As demonstrated in [14], there have been at the forefront of pioneering advancements in this domain, introducing ingenious strategies for decentralized authentication through blockchain distributed ledgers. Their innovative authentication mechanism intricately orchestrates nodes into clusters, with each cluster possessing its authentication blockchain interconnected by another blockchain, as depicted below [14]. This intricate hierarchical structure heralds a new era of decentralized and scalable authentication, meticulously tailored to address the unique resource constraints of IIoT devices. By leveraging blockchain technology, Al Ahmed et al.'s approach underscores the indispensable role of decentralized authentication in fortifying the security and reliability of authentication mechanisms within industrial IIoT networks.

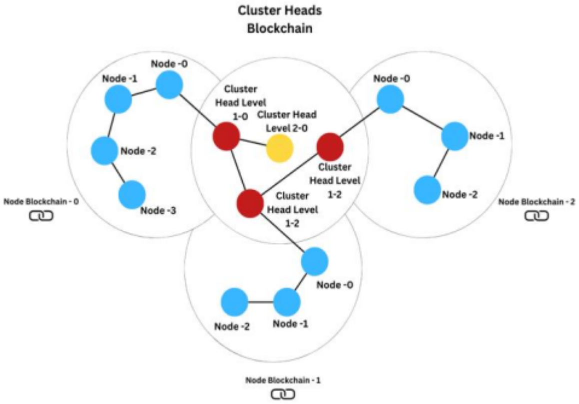

Fig. 1. The hierarchical structure of clusters with authentication blockchains connected by another blockchain.

The hierarchical clustering of nodes allows for efficient resource management, as each cluster can operate semi-independently, reducing the computational overhead and latency typically associated with blockchain operations. Furthermore, this structure facilitates seamless scalability, enabling the network to expand without compromising security or performance. However, challenges persist in seamlessly integrating blockchain technology for authentication purposes within IIoT networks. Issues such as interoperability, performance optimization, and security vulnerabilities are particularly pressing [15],[20]. Security attacks targeting public-key cryptography algorithms pose a significant threat to IIoT systems, while the overhead associated with trust computation and blockchain maintenance impacts system performance. Robust encryption, authentication mechanisms, and optimization of communication protocols are crucial to ensuring secure communication and preventing unauthorized access. Additionally, enhancing scalability and adapting to the distributed nature of IIoT environments are essential to effectively address these evolving challenges.

A myriad of scholarly endeavors has delved deeply into the multifaceted application of blockchain in IIoT authentication. These studies have proposed a diverse array of architectures and protocols, each offering unique contributions to the evolving landscape of IIoT security. To address these challenges, this paper proposes the integration of Federated Learning with blockchain technology as a novel solution. Federated Learning allows decentralized machine learning models to be trained across multiple devices without centralizing data, thereby enhancing privacy and reducing data transfer overhead. When integrated with blockchain, this approach not only enhances the security and reliability of authentication mechanisms but also optimizes the performance and scalability of IIoT networks.

2. RELATED WORKS

Based on the article titled ‘Integration of Hardware Security Modules and Permissioned Blockchain in Industrial IoT Networks’, In the realm of Industrial IoT (IIoT) security, the combination of Hardware Security Modules (HSM) and Permissioned Blockchains (PB) represents a significant advancement. HSMs, serving as hardware-based roots of trust, provide robust physical protection and enhance security within system architectures. However, prior research in this domain has highlighted several challenges. One prominent issue is the seamless integration of HSM and Blockchain technologies, particularly in the context of public-key cryptographic methods and protocols. While the theoretical benefits are evident, practical implementation hurdles remain, including interoperability and performance optimization. Proposed techniques often focus on establishing efficient communication protocols and ensuring compatibility between HSMs and Blockchain networks. However, weaknesses such as potential scalability limitations and increased complexity in deployment are acknowledged. Strengths of these proposed techniques lie in their potential to significantly enhance security in IIoT systems by leveraging the combined strengths of HSMs and Blockchains. By addressing authentication and data integrity concerns, they pave the way for more robust and reliable industrial networks. Future work in this area should concentrate on refining integration methods to mitigate identified weaknesses, optimizing performance, and extending applications to diverse IIoT scenarios. Additionally, exploring novel cryptographic approaches and further investigating the impact of these integrated solutions on specific industrial use cases will be crucial for advancing the field [15].

Based on the article titled 'Enabling Secure Authentication in Industrial IoT With Transfer Learning Empowered Blockchain', the Industrial Internet of Things (IIoT) landscape presents substantial opportunities for advancement, particularly within the framework of Industry 4.0. However, alongside these opportunities come significant challenges in ensuring the security and privacy of data collected and transmitted in real-time for industrial applications. Existing authentication mechanisms within IIoT often rely on single-factor authentication and struggle to adapt to the dynamic nature of user populations and their diverse roles within industrial environments. Addressing these challenges requires innovative approaches to authentication and privacy preservation. In response to these challenges, the article presents a fresh authentication mechanism called ATLB, which is empowered by Transfer Learning within Blockchain technology. ATLB represents a fusion of blockchain technology and transfer learning, tailored to enhance privacy preservation in industrial applications while improving authentication efficiency. By leveraging blockchain, ATLB ensures the integrity and privacy of data within IIoT systems, crucial for maintaining industrial safety and national security. Additionally, the integration of transfer learning enables the creation of trustworthy blockchain networks capable of adapting authentication models to varying user populations and regional contexts. Strengths of ATLB lie in its ability to provide accurate and efficient authentication for IIoT applications while maintaining low latency and high throughput. By employing transfer learning techniques, ATLB reduces model training time and enhances adaptability to diverse user environments, addressing the limitations of traditional authentication methods. However, challenges remain in optimizing the implementation of transfer learning within blockchain-based authentication systems and ensuring seamless integration with existing IIoT infrastructures. Subsequent research in this domain should focus on further refining the transfer learning mechanisms employed in ATLB to improve scalability and robustness [23].

Based on the article titled 'A Secure and Trusted Mechanism for Industrial IoT Network Using Blockchain', The realm of Industrial Internet-of-Things (IIoT) embodies a transformative influence on industrial operations, enabling seamless communication and data exchange across various components such as manufacturing units and packaging facilities. However, the distributed nature of IIoT architectures presents challenges in efficiently analyzing collected data, hindering the ability to derive meaningful insights. Moreover, the inherent security vulnerabilities within IIoT networks, including the risk of network anomalies and attacks, pose significant threats to the integrity and confidentiality of data. To address these challenges, this article introduces a secure mechanism leveraging both trust management and blockchain technology within IIoT networks. A central aspect of the proposed approach involves the election of a coordinator IoT device tasked with computing the trust factor (TF) of individual IoT devices, thereby preventing malicious devices (MDs) from compromising the network. Additionally, transparency and immutability of data are ensured through the integration of a blockchain-based data model, enabling secure transaction tracking and preventing unauthorized alterations. Strengths of this approach lie in its comprehensive approach to enhancing IIoT network security, combining trust management and blockchain to address both trustworthiness assessment and data integrity concerns. By computationally determining the legitimacy of IoT devices and maintaining a tamper-proof ledger of transactions, the proposed framework offers robust protection against various security threats. However, weaknesses may include potential overhead associated with trust computation and blockchain maintenance, which could impact system performance in large-scale deployments. Subsequent research in this area should focus on optimizing the computational efficiency of trust management algorithms and blockchain protocols to minimize overhead while maintaining security guarantees [20].

Based on the article titled ‘Data Security in Healthcare Industrial Internet of Things With Blockchain’, Within the healthcare sector of the Industrial Internet of Things (IIoT), the convergence of self-governing system configurations and interconnected applications has ushered in transformative opportunities, particularly evident in E-healthcare environments. These environments, leveraging medical sensors and real-time data processing, enable the seamless capture, analysis, and documentation of patient transactions. However, amidst the benefits lie significant data security challenges, particularly concerning the exchange of sensitive patient information over centralized server-based systems. Issues such as node connectivity, data sharing failures, and delivery-related concerns amplify risks to patient privacy and data integrity. To address these challenges, this article presents a multifaceted solution. It introduces BHIIoT which is blockchain hyperledger-enabled, an inventive and secure framework harnessing blockchain technology to fortify E-healthcare information security. BHIIoT employs a distributed ledger system to guarantee the integrity and confidentiality of patient documentation, mitigating risks associated with centralized systems. BHIIoT integrates a mechanism for threshold re-encryption provided by NuCypher within the blockchain to secure data, ensuring the protection of shared resources. Strengths of this approach lie in its comprehensive approach to enhancing data security in E-healthcare IIoT environments, addressing challenges related to authentication, record sharing, and privacy preservation. By leveraging blockchain technology and innovative encryption mechanisms, BHIIoT offers robust protection against unauthorized access and tampering of patient data. The weaknesses may include potential overhead associated with blockchain maintenance and the complexity of implementing distributed network architectures. Subsequent research in this area should focus on optimizing the efficiency of BHIIoT's resource consumption metrics and further enhancing its resilience against malicious attacks [16].

Based on the article titled 'Authentication-Chains: Blockchain-Inspired Lightweight Authentication Protocol for IoT Networks', the article introduces a blockchain-based authentication protocol that is decentralized and lightweight, addressing the centralized nature of key exchange servers in IoT networks, which pose security vulnerabilities and scalability issues. The study aims to decentralize authentication, ensuring security, reliability, and efficiency in IoT device authentication. "Authentication-Chains" introduces a decentralized and lightweight authentication protocol tailored for IoT networks, leveraging blockchain technology. It arranges nodes into clusters, each with its authentication blockchain interconnected via another blockchain. A Device Authentication Request (DAR) containing NodeID, CHID, and signature for network joining is introduced. The protocol utilizes a rapid and lightweight consensus algorithm, employing identity-based key pairs to sign authentication requests. Secure data communication is ensured through public key pairs and authentication block hashes. The strengths include decentralized authentication, lightweight design for IoT devices, faster response time, and scalability, while weaknesses involve reliance on simulations and informal security analysis, and complexity in managing multiple blockchain levels and authentication tables. The authors evaluated the protocol's performance on a Raspberry Pi network, conducted casual security evaluation, and utilized Verifpal for cryptographic protocol verification [14].

Based on the article titled 'Blockchain-Based IoT Access Control System: Towards Security, Lightweight, and Cross-Domain', The article highlights constraints within current access control systems for IoT based on blockchain, such as vulnerability to DDoS attacks due to repeated access requests from malicious users and constraints in distribution based on the proportion of entities. These limitations underscore the need for enhanced security measures and broader distribution in IoT access control systems. The system partitions the IoT environment into separate functional domains, creates individual blockchain ledgers for each domain, and empowers additional connected devices to function as specialized blockchain nodes. The use of HLF channel technology facilitates cross-domain access, while IBS filters legal access requests for each domain to prevent DDoS attacks. The strengths include enhanced security through decentralized access control, lightweight design for IoT devices, and cross-domain access facilitated by HLF channel technology. Weaknesses involve potential challenges in scalability and interoperability and complexity in managing multiple blockchain nodes. The authors evaluate the proposed system's practicality by implementing and testing it to demonstrate its effectiveness in enhancing security, lightweight design, and access control across multiple domains in IoT settings [22].

Based on the article titled ‘RRV-BC: Random Reputation Voting Mechanism and Blockchain Assisted Access Authentication for Industrial Internet of Things’, Within the context of Industry 4.0, the merging of the integration of Industrial IoT, AI technology, and cloud-based computing has ushered in a revolutionary epoch of transformative applications. However, alongside these advancements come significant security challenges, particularly exacerbated by the advent of the 5G era. The expanding scale of networks, increasing complexity of environments, and prominence of security risks, such as malicious attacks and privacy breaches, underscore the need for robust cybersecurity solutions. In response, this article introduces a hierarchical IIoT security mechanism based on blockchain technology., aimed at enhancing the dependability and safety of the digital realm. Strengths of this approach lie in its innovative use of blockchain technology and reputation-based consensus mechanisms to enhance data communication reliability and fault tolerance. By reducing communication overhead and improving fault tolerance compared to traditional methods such as the Practical Byzantine Fault Tolerance (PBFT) protocol, the proposed scheme offers improved security and efficiency in IIoT environments. However, weaknesses may include the potential storage costs associated with the ECDSA digital signature algorithm and scalability limitations of the PBFT consensus algorithm. Future studies in this field should aim to tackle these constraints while also bolstering the flexibility and scalability of the suggested approach [25].

The article titled ‘Hybrid blockchain-based many-to-many cross-domain authentication scheme for smart agriculture IoT networks’ addresses the necessity for secure collaboration among agricultural IoT devices across different domains, proposing a scheme based on a blended blockchain architecture. Existing centralized authentication methods struggle with multiple devices connecting to diverse data servers simultaneously. The proposed scheme introduces a many-to-many cross-domain authentication approach, allowing multiple devices to authenticate with various data service providers concurrently. A key feature is the groupable batch verification (GBV) algorithm, dynamically adjusting batch sizes for flexible cross-domain batch authentication, enhancing efficiency. Additionally, a pseudonym update mechanism safeguards device privacy and prevents illegal access. The scheme's security analysis and performance evaluation demonstrate its superiority, though complexities in blockchain implementation may arise. Future work focuses on refining the PBFT consensus algorithm for enhanced security and efficiency. Overall, the proposed scheme offers improved security, flexibility, and privacy protection, making it a promising solution for securing collaborative interactions in smart agriculture IoT networks across different domains [17].

Based on the article titled 'Hierarchical blockchain structure for node authentication in IoT networks': The integration of IoT devices in networks necessitates robust security measures, particularly in node authentication, often relying on centralized methods, which pose single points of failure. Blockchain technology emerges as a promising alternative due to its decentralized nature. However, conventional blockchain applications in IoT face challenges such as resource demands and potential single points of failure. To address this, the proposed hierarchical blockchain framework for node verification in IoT networks offers a decentralized, scalable solution. Authentication is decentralized by categorizing IoT devices into clusters based on their computational capacity and energy resources, and location. Each cluster creates a small blockchain for authentication, connected to a larger blockchain for scalability. A lightweight consensus algorithm validates nodes based on their public key and related cluster head public key, reducing computational load. Strengths include decentralization, efficiency, and scalability, mitigating potential single points of failure. Challenges may arise in managing the hierarchical structure and ensuring interoperability between clusters. Evaluation metrics encompass computational load, storage requirements, efficiency of the consensus algorithm, and resilience against attacks, with results showing reduced computational and storage needs compared to existing protocols, while maintaining decentralization and security. Further validation through comprehensive simulations with larger device networks is planned to enhance adaptability and validate the proposed approach [13].

Based on the article titled ‘Blockchain-Enhanced Data Sharing With Traceable and Direct Revocation in IIoT’, The industrial Internet of Things (IIoT) has emerged as a crucial enabler of data handling and informational offerings, especially within the realm of smart factories. With the proliferation of mature IIoT cloud platforms catering to these needs, ensuring secure storage, access control, and information integrity has become imperative. However, the semi-credibility nature of IIoT cloud platforms introduces challenges in addressing issues such as data security, access control, and user revocation. In response to these challenges, the article suggests a security access control scheme for IIoT in smart factories enhanced by blockchain technology. This scheme prioritizes traceability and revocability, ensuring robust security measures against malicious users throughout the data lifecycle. Through unified identity authentication and the storage of public keys, user attributes, and lists of revoked access on the blockchain, the proposed scheme enables seamless access control while providing mechanisms for tracking and revoking malicious users. Strengths of this approach lie in its comprehensive support for secure data sharing and access control, underpinned by traceability and revocability features. By embedding unique identity parameters in the private key generation phase and enabling direct revocation of malicious users, the proposed scheme enhances security and mitigates collusion attacks. Additionally, the scheme boasts smaller key sizes and reduced overhead time compared to alternative approaches, enhancing efficiency without compromising security. However, potential weaknesses may include the complexity of implementation and the need for robust governance mechanisms to manage access policies and revocation processes effectively. Future research avenues for this proposed technique include exploring partial revocation mechanisms to address diverse user behavior and implementing fine-grained access restrictions for more nuanced control over data sharing [24].

Several other researchers have also contributed in end-to-end security mechanism even with the assistance of the counter partners i.e. universities or industries for broaden implications [1]-[12]. This research article can act as the guidelines for future young researchers in end-to-end security measures in 6^{th} generation networks. This improved work (proposed solution) for the given problem statement is adopted from [5], which act as a benchmark for this research article.

3. PROPOSED SOLUTION

To address the challenges, our proposed solution integrates Federated Learning with Blockchain technology. Federated learning integrated with blockchain represents a novel fusion of two advanced technologies aimed at bolstering privacy, security, and transparency within machine learning systems. Federated learning, a distributed approach to machine learning, ensures that model training occurs across multiple devices or nodes without the need to exchange raw data. Instead, only model updates or gradients are shared between devices and a central server, safeguarding the privacy of individual data as sensitive information never leaves the device itself. In contrast, blockchain technology functions as a decentralized ledger system, providing a secure and transparent platform for recording transactions across a network of computers. This technology ensures the integrity of data through cryptographic links, decentralizing control and eliminating the need for a central authority [19].

Integration of federated learning with blockchain introduces several key advantages. Firstly, it enables secure record-keeping by recording each device's contribution to the federated learning process as a transaction on the blockchain, with cryptographic hashes of model updates maintaining data privacy. Additionally, blockchain facilitates transparent governance by providing a clear record of model updates, enhancing trust among participants. Furthermore, users maintain ownership and control over their data, as the raw data never leaves the devices. Blockchain mechanisms enable users to track how their data is utilized in model training and provide permissioned access. Lastly, the decentralized nature of blockchain enhances security and integrity, as any attempt to tamper with recorded model updates would require consensus among network participants, rendering it highly resistant to manipulation or fraud. In sum, the integration of federated learning with blockchain offers a robust solution for collaborative machine learning across various sectors, including healthcare, finance, and IoT, where ensuring data privacy and security is paramount [21].

To better understand the proposed solution, it is helpful to visualize how it enhances security and privacy in IIoT networks. Figure 2 depicts a system that combines federated learning with blockchain integration to enhance security and privacy in distributed machine learning. In this setup, each participant, such as Device A and Device B, keeps its data locally, ensuring that private data remains on the individual devices, significantly reducing the risk of data breaches. Instead of sharing raw data, only model updates or parameters derived from local data are sent to a central aggregator. This central aggregator is responsible for aggregating these updates to improve the global model.

Blockchain technology is integrated into this system to further enhance security. All transactions, including model updates, are recorded on a decentralized and immutable blockchain ledger. This ledger ensures that once a transaction is recorded, it cannot be tampered with, thereby maintaining the integrity of the model updates. Additionally, data transmission between the devices and the blockchain is encrypted, ensuring secure communication channels. This combination of federated learning and blockchain creates a robust framework that prioritizes data privacy and security while enabling collaborative machine learning.

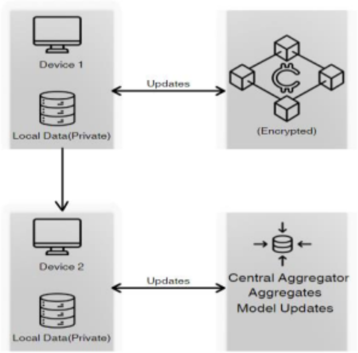

Fig. 2. The federated learning integrated with blockchain: enhanced security and privacy.

Furthermore, combining federated learning with blockchain technology not only boosts security and confidentiality but also enhances visibility and accountability. Figure 3 illustrates how integrating federated learning with blockchain technology enhances transparency and traceability. In this system, blockchain nodes (such as Blockchain Node 1 and Blockchain Node 2) are responsible for verifying updates and maintaining the integrity of the distributed ledger. These nodes communicate with each other to ensure that any changes or additions to the blockchain are valid and consistent. Model updates, generated by individual participants based on their local data, are formatted as transactions. Once verified, these transactions are added to the blockchain's immutable ledger, which records all transactions in a tamper-proof and transparent manner. This ledger provides a traceable record of all model updates, ensuring that any changes to the model can be audited and tracked back to their source, thus enhancing accountability. By integrating federated learning with blockchain technology, the system benefits from enhanced transparency, as every model update transaction is recorded on the blockchain, and improved traceability, as the immutable nature of the blockchain allows for detailed auditing and verification of the model's evolution. This integration ensures that the federated learning process is secure, transparent, and accountable, leveraging the strengths of both technologies to address common challenges in decentralized machine learning systems.

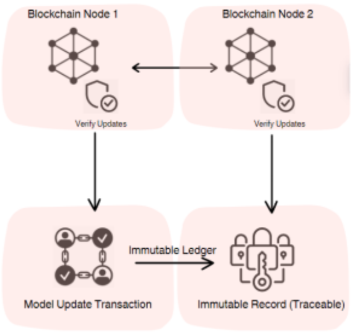

Fig. 3. The federated learning integrated with blockchain: enhanced transparency and traceability.

To better illustrate the effectiveness of the proposed solution, it is essential to compare it with existing authentication methodologies. Table I compares existing methods with the proposed integration of Federated Learning and Blockchain technology across several key aspects. Existing methods typically exchange raw data between devices and central servers, making them vulnerable to single points of failure and tampering, with limited transparency, fault tolerance, and scalability. Conversely, the proposed solution boosts data privacy by retaining raw data on devices and enhances security with blockchain's immutable ledger. It also offers high transparency with immutable and traceable records, increased fault tolerance by distributing training across devices, better scalability through decentralized model training, reduced latency with localized updates, and ensured data integrity via cryptographic hashes and consensus mechanisms.

TABLE I: Comparison of Existing Methods and Proposed Federated Learning with Blockchain Integration

Aspect	**Existing Methods**	**Proposed Solution (Federated Learning with Blockchain)**
Data Privacy	Raw data exchanged	Raw data remains on device

Security	Vulnerable to single points of failure	Enhanced with blockchain's tamper-proof ledger
Transparency	Limited	High, due to blockchain's immutable and traceable records
Fault Tolerance	Lower	Higher, as training is distributed across devices
Scalability	Limited	Improved, due to decentralized model training
Latency	Higher	Reduced, with localized model updates
Integrity	Susceptible to tampering	Ensured through cryptographic hashes and consensus

4. RESULT AND ANALYSIS

The integration of Federated Learning with blockchain technology presents a promising solution to the challenges facing authentication within Industrial Internet of Things (IIoT) networks. By combining the decentralized nature of blockchain with the privacy-enhancing capabilities of Federated Learning, this approach offers several notable benefits. Firstly, it addresses the pressing issue of security vulnerabilities inherent in IIoT systems, particularly those stemming from attacks on public-key cryptography algorithms. Federated Learning enables the training of machine learning models on various devices without the need to centralize data, thereby minimizing the risk of data breaches and unauthorized access.

Furthermore, by leveraging blockchain technology, this solution enhances the integrity and reliability of authentication mechanisms. The distributed ledger architecture of blockchain ensures that authentication data remains tamper-resistant and transparent, thereby bolstering the overall security posture of IIoT networks. Moreover, the integration of Federated Learning optimizes the performance of IIoT systems by reducing the overhead associated with trust computation and blockchain maintenance. This results in improved scalability and efficiency, critical factors for accommodating the dynamic nature of IIoT environments. The scalability can be modeled using the speedup equation from parallel computing [18]:

$$S = \frac{T_s}{T_p}$$

where T_s is the time to execute a task serially and T_p is the time to execute the task in parallel.

However, while the proposed solution offers significant advantages, challenges may still arise in its implementation. Interoperability remains a concern, as integrating Federated Learning with existing IIoT infrastructure and protocols may require careful coordination and standardization efforts. Additionally, ensuring the robustness of encryption and authentication mechanisms is paramount to preventing security breaches and unauthorized access. Moreover, while Federated Learning mitigates privacy risks by decentralizing data, careful consideration must be given to data governance and regulatory compliance to safeguard sensitive information.

In analysis, the proposed solution demonstrates a holistic approach to addressing the multifaceted challenges of IIoT authentication. By integrating Federated Learning with blockchain technology, it not only enhances security and reliability but also optimizes performance and scalability. However, successful implementation will require concerted efforts to overcome interoperability issues and ensure robust encryption and authentication mechanisms. Additionally, ongoing monitoring and adaptation to evolving threats and regulatory requirements will be essential to maintain the effectiveness of the solution over time. Overall, while the proposed solution holds great promise, its successful deployment will hinge on careful planning, collaboration, and ongoing vigilance.

Now, let's delve into how the proposed solution effectively resolves these challenges and enhances various aspects of current authentication mechanisms within Industrial Internet of Things (IIoT) networks. The solution's effectiveness lies in its ability to decentralize model training through federated learning, thereby minimizing data transfer and overhead while ensuring interoperability among diverse devices. This approach mitigates risks associated with centralized systems, reducing reliance on vulnerable infrastructure and enhancing overall security and reliability. For instance, it effectively addresses concerns about centralized vulnerabilities, as discussed in related works such as 'Authentication-Chains: Blockchain-Inspired Lightweight Authentication Protocol for IoT Networks,' by eliminating single points of failure and distributing authentication processes across multiple nodes [14].

Moreover, blockchain's decentralized ledger enhances security by securely recording transactions and ensuring data integrity. Robust cryptographic mechanisms protect against attacks on public-key cryptography algorithms, further bolstering the security of IIoT systems. Additionally, the immutable nature of the blockchain ledger and decentralized consensus mechanisms ensure the integrity of data, providing a robust framework for authentication mechanisms. This directly addresses the data integrity concerns highlighted in works like 'A Secure and Trusted Mechanism for Industrial IoT Network Using Blockchain,' where ensuring the immutability and transparency of data is crucial [20].

The solution also addresses scalability concerns by distributing trust computation and authentication processes across multiple nodes, offering scalability advantages over traditional methods. This scalability ensures that IIoT networks can accommodate increasing device populations and data volumes without compromising performance or security. For instance, the hierarchical blockchain approach discussed in 'Hierarchical blockchain structure for node authentication in IoT networks' is enhanced by the proposed solution, which further distributes computational tasks and improves the ability to scale efficiently [13].

Furthermore, the integration of federated learning with blockchain enhances privacy preservation by keeping sensitive data localized on individual devices. This diminishes the chance of data breaches and unapproved entry, thereby protecting the secrecy and reliability of information within IIoT networks. The privacy-preserving aspects are particularly significant in sectors such as healthcare, as discussed in 'Data Security in Healthcare Industrial Internet of Things With Blockchain,' where safeguarding patient information is paramount. By keeping data local and only sharing necessary updates, the solution enhances privacy without compromising on the efficiency of the system [16].

5. CONCLUSION

In conclusion, the integration of Federated Learning with blockchain technology presents a promising solution to the complex challenges facing authentication within Industrial Internet of Things (IIoT) networks. This innovative approach offers a multifaceted strategy to enhance security, reliability, scalability, and privacy within industrial settings.

By decentralizing model training through Federated Learning, the solution minimizes data transfer and overhead while ensuring interoperability among diverse IIoT devices. This not only mitigates risks associated with centralized systems but also reduces reliance on vulnerable infrastructure, thereby enhancing overall security and reliability. Additionally, the utilization of blockchain's decentralized ledger enhances security by securely recording transactions and ensuring data integrity, further bolstering the security of IIoT systems. Moreover, the solution addresses scalability concerns by distributing trust computation and authentication processes across multiple nodes, ensuring that IIoT networks can accommodate increasing device populations and data volumes without compromising performance or security. Furthermore, the integration of Federated Learning with blockchain enhances privacy preservation by keeping sensitive data localized on individual devices, thereby reducing the likelihood of data breaches and unauthorized access.

In summary, the proposed solution represents a holistic approach to addressing the multifaceted challenges of IIoT authentication. By integrating Federated Learning with blockchain technology, it offers a robust framework for enhancing security, reliability, scalability, and privacy within industrial settings. However, successful implementation will require concerted efforts to overcome interoperability issues and ensure robust encryption and authentication mechanisms. Additionally, ongoing monitoring and adaptation to evolving threats and regulatory requirements will be essential to maintain the effectiveness of the solution over time. Overall, while the proposed solution holds great promise, its successful deployment will hinge on careful planning, collaboration, and ongoing vigilance.

ACKNOWLEDGEMENTS

This research work is the outcome of class project of computer security at Faculty of Computer Science and Information Technology, Universiti Malaysia Sarawak, Malaysia.

REFERENCE

Abbasi, I. A., et al. (2018). Dynamic multiple junction selection based routing protocol for VANETs in city environment. *Applied Sciences, 8*(5), 687.

Abbasi, I. A., et al. (2018). A reliable path selection and packet forwarding routing protocol for vehicular ad hoc networks. *EURASIP Journal on Wireless Communications and Networking, 2018*, 1-19.

Abbasi, I. A., & Khan, A. S. (2018). A review of vehicle-to-vehicle communication protocols for VANETs in the urban environment. *Future Internet, 10*(2), 14.

Abbasi, I. A., et al. (2024). A lightweight and robust authentication scheme for the healthcare system using public cloud server. *PLOS ONE, 19*(1), e0294429.

Al Ahmed, M. T., Hashim, F., Hashim, S. J., & Abdullah, A. (2022). Hierarchical blockchain structure for node authentication in IoT networks. *Egyptian Informatics Journal, 23*(2), 345-361.

Al Ahmed, M. T., Hashim, F., Hashim, S. J., & Abdullah, A. (2023). Authentication-Chains: Blockchain-inspired lightweight authentication protocol for IoT networks. *Electronics, 12*(4), 867.

Cabrera-Gutiérrez, A. J., et al. (2022). Integration of hardware security modules and permissioned blockchain in industrial IoT networks. *IEEE Access, 10*, 114331-114345.

Ahmad, Z., et al. (2023). MS-ADS: Multistage spectrogram image-based anomaly detection system for IoT security. *Transactions on Emerging Telecommunications Technologies, 34*(8), e4810.

Khan, A. A., et al. (2023). Data security in healthcare industrial Internet of Things with blockchain. *IEEE Sensors Journal*.

Khan, A. S., Lenando, H., Abdullah, J., & Jambli, M. N. B. (2014). Lightweight message authentication protocol for mobile multihop relay networks. *International Review on Computers and Software, 9*(10), 1720-1730.

Khan, A. S., et al. (2015). Evaluating national innovation system of Malaysia based on university-industry research collaboration: A system thinking approach. *Asian Social Science, 11*(13), 45.

Khan, A. S., et al. (2015). An efficient evaluation model for the assessment of university-industry research collaboration in Malaysia. *Research Journal of Applied Sciences, Engineering and Technology, 10*(3), 298-306.

Khan, A. S., et al. (2015). Reinforcing the national innovation system of Malaysia based on university-industry research collaboration: A system thinking approach. *International Journal of Management Sciences and Business Research, 4*(1), 6-15.

Luo, F., Huang, R., & Xie, Y. (2024). Hybrid blockchain-based many-to-many cross-domain authentication scheme for smart agriculture IoT networks. *Journal of King Saud University-Computer and Information Sciences, 101946*.

Ngoko, Y., & Trystram, D. (2018). Scalability in parallel processing. In *Springer eBooks* (pp. 79–109).

Putra, M. A. P., et al. (2023, October). Blockchain-based federated learning for bearing fault detection in the Industrial Internet of Things. In *2023 14th International Conference on Information and Communication Technology Convergence (ICTC)* (pp. 1069-1074). IEEE.

Rathee, G., Ahmad, F., Jaglan, N., & Konstantinou, C. (2022). A secure and trusted mechanism for industrial IoT network using blockchain. *IEEE Transactions on Industrial Informatics, 19*(2), 1894-1902.

Salim, M. M., & Park, J. H. (2022). Federated learning-based secure electronic health record sharing scheme in medical informatics. *IEEE Journal of Biomedical and Health Informatics, 27*(2), 617-624.

Sun, S., Du, R., Chen, S., & Li, W. (2021). Blockchain-based IoT access control system: Towards security, lightweight, and cross-domain. *IEEE Access, 9*, 36868-36878.

Wang, X., et al. (2021). Enabling secure authentication in industrial IoT with transfer learning empowered blockchain. *IEEE Transactions on Industrial Informatics, 17*(11), 7725-7733.

Yu, K., et al. (2021). Blockchain-enhanced data sharing with traceable and direct revocation in IIoT. *IEEE Transactions on Industrial Informatics, 17*(11), 7669-7678.

Zhang, P., et al. (2023). RRV-BC: Random reputation voting mechanism and blockchain assisted access authentication for Industrial Internet of Things. *IEEE Transactions on Industrial Informatics*.

Enhancing Aspects of IIoT Networks with Federated Learning Blockchain-Integrated Authentication Solution

ORIGINALITY REPORT

19%	14%	16%	10%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	ir.unimas.my Internet Source	2%
2	www.mdpi.com Internet Source	1%
3	journals.plos.org Internet Source	1%
4	Submitted to National College of Ireland Student Paper	1%
5	www.opastpublishers.com Internet Source	1%
6	ksascholar.dri.sa Internet Source	1%
7	www.researchgate.net Internet Source	1%
8	Submitted to Loughborough University Student Paper	1%
9	doaj.org Internet Source	<1%

10	Submitted to Asia Pacific University College of Technology and Innovation (UCTI) Student Paper	<1 %
11	pureportal.coventry.ac.uk Internet Source	<1 %
12	Submitted to Hong Kong University of Science and Technology Student Paper	<1 %
13	Jun Yan, WeiFen Lin, Xi Tu, Qun Wu. "IoT-based interaction design of smart home products for elderly families", Applied Mathematics and Nonlinear Sciences, 2024 Publication	<1 %
14	Submitted to UIN Sunan Gunung DJati Bandung Student Paper	<1 %
15	dergipark.org.tr Internet Source	<1 %
16	www.maxwellsci.com Internet Source	<1 %
17	www.frontiersin.org Internet Source	<1 %
18	Nayeem Ahmad Khan, Adnan Shahid Khan, Hushmat Amin Kar, Zeeshan Ahmad, Seleviawati Tarmizi, Azlina Ahmadi Julaihi. "Employing Public Key Infrastructure to	<1 %

	Encapsulate Messages During Transport Layer Security Handshake Procedure", 2022 Applied Informatics International Conference (AiIC), 2022 Publication	
19	www.ijraset.com Internet Source	<1 %
20	Aya H. Allam, Ibrahim Gomaa, Hala H. Zayed, Mohamed Taha. "IoT-based eHealth using blockchain technology: a survey", Cluster Computing, 2024 Publication	<1 %
21	Mahmoud Tayseer Al Ahmed, Fazirulhisyam Hashim, Shaiful Jahari Hashim, Azizol Abdullah. "Hierarchical blockchain structure for node authentication in IoT networks", Egyptian Informatics Journal, 2022 Publication	<1 %
22	Submitted to University of Ulster Student Paper	<1 %
23	Yue Wang, Kai Zhang, Xiaohu Zhao, Xiaofei Hu. "BTIA-IME: A blockchain-based trusted interactive architecture for intelligent manufacturing equipment", Internet of Things, 2024 Publication	<1 %

24	P. Hemashree, V. Kavitha, S. B. Mahalakshmi, K. Praveena, R. Tarunika. "Chapter 7 Machine Learning Approaches in Blockchain Technology-Based IoT Security: An Investigation on Current Developments and Open Challenges", Springer Science and Business Media LLC, 2024 Publication	<1%
25	pubs2.ascee.org Internet Source	<1%
26	ebin.pub Internet Source	<1%
27	fastercapital.com Internet Source	<1%
28	Haoran Zhang, Shan Jiang, Shichang Xuan. "Decentralized federated learning based on blockchain: Concepts, framework, and challenges", Computer Communications, 2024 Publication	<1%
29	arxiv.org Internet Source	<1%
30	dblp.org Internet Source	<1%
31	digibug.ugr.es Internet Source	<1%

32	Amnah Hmoud, Ghada Ali, Rawabi Alanzi, Salim Elkhediri. "IoT and Blockchain Integration Security", 2023 6th International Conference on Advanced Communication Technologies and Networking (CommNet), 2023 Publication	<1 %
33	Submitted to Pathfinder Enterprises Student Paper	<1 %
34	"Blockchain and Deep Learning for Smart Healthcare", Wiley, 2023 Publication	<1 %
35	dokumen.pub Internet Source	<1 %
36	"Engineering Applications of Neural Networks", Springer Science and Business Media LLC, 2024 Publication	<1 %
37	online-journals.org Internet Source	<1 %
38	Aqsa Rashid, Asif Masood, Atta ur Rehman Khan. "ACS-IoT: Smart Contract and Blockchain Assisted Framework for Access Control Systems in IoT Enterprise Environment", Wireless Personal Communications, 2024 Publication	<1 %

39	Chenchen Li, Jiang Xiao, Xiaohai Dai, Hai Jin. "AMVchain: authority management mechanism on blockchain-based voting systems", Peer-to-Peer Networking and Applications, 2021 Publication	<1 %
40	Deepak, Preeti Gulia, Nasib Singh Gill, Mohammad Yahya, Punit Gupta, Prashant Kumar Shukla, Piyush Kumar Shukla. "Exploring the Potential of Blockchain Technology in an IoT-Enabled Environment: A Review", IEEE Access, 2024 Publication	<1 %
41	Gholam Reza Zargar, Hamid Barati, Ali Barati. "An authentication mechanism based on blockchain for IoT environment", Cluster Computing, 2024 Publication	<1 %
42	Kiran Ahuja, Sandeep Joshi. "chapter 22 Enhancing Security of IoT Systems Using Machine Learning-Based Blockchain Technology", IGI Global, 2024 Publication	<1 %
43	Saeed Hamood Alsamhi, Ammar Hawbani, Alexey V. Shvetsov, Santosh Kumar. "Advancing Pandemic Preparedness in Healthcare 5.0: A Survey of Federated	<1 %

Learning Applications", Advances in Human-Computer Interaction, 2023
Publication

44 link.springer.com
Internet Source
<1%

45 ouci.dntb.gov.ua
Internet Source
<1%

46 www.iieta.org
Internet Source
<1%

47 Fateh Bahadur Kunwar, Hitendra Singh, Rakesh Kumar Yadav. "Efficient Encryption using Quondam Signature Algorithm and Modified Lean Six Sigma for Sustainability with Supply Chain Management", Research Square Platform LLC, 2024
Publication
<1%

48 Shantanu Pal, Ali Dorri, Raja Jurdak. "Blockchain for IoT access control: Recent trends and future research directions", Journal of Network and Computer Applications, 2022
Publication
<1%

49 Turki Aljrees, Ankit Kumar, Kamred Udham Singh, Teekam Singh. "Enhancing IoT Security through a Green and Sustainable Federated Learning Platform: Leveraging Efficient
<1%

Encryption and the Quondam Signature Algorithm", Sensors, 2023
Publication

50 Antonio J. Cabrera-Gutierrez, Encarnacion Castillo, Antonio Escobar-Molero, Jose A. Alvarez-Bermejo et al. "Integration of Hardware Security Modules and Permissioned Blockchain in Industrial IoT Networks", IEEE Access, 2022
Publication
<1%

51 Fengting Luo, Ruwei Huang, Yuqi Xie. "Hybrid blockchain-based many-to-many cross-domain authentication scheme for smart agriculture IoT networks", Journal of King Saud University - Computer and Information Sciences, 2024
Publication
<1%

52 J. Chandra Priya, R. Praveen, K. Nivitha, T. Sudhakar. "Improved blockchain-based user authentication protocol with ring signature for internet of medical things", Peer-to-Peer Networking and Applications, 2024
Publication
<1%

53 Mahmoud Tayseer Al Ahmed, Fazirulhisyam Hashim, Shaiful Jahari Hashim, Azizol Abdullah. "Authentication-Chains: Blockchain-Inspired Lightweight Authentication Protocol for IoT Networks", Electronics, 2023
Publication
<1%

54 Xiaoyan Huo, Xuemei Wang. "Internet of things for smart manufacturing based on advanced encryption standard (AES) algorithm with chaotic system", Results in Engineering, 2023 <1%

Publication

55 Yutong Han, Chundong Wang, Huaibin Wang, Yi Yang, Xi Wang. "A study of blockchain-based liquidity cross-chain model", PLOS ONE, 2024 <1%

Publication

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	Off		

Enhancing Aspects of IIoT Networks with Federated Learning Blockchain-Integrated Authentication Solution

GRADEMARK REPORT

FINAL GRADE

/0

GENERAL COMMENTS

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6

PAGE 7

PAGE 8

PAGE 9

PAGE 10

PAGE 11

PAGE 12

PAGE 13

PAGE 14

PAGE 15

PAGE 16

PAGE 17

PAGE 18