SMDI
Digital Management Sciences Journal *Vol.1/ Issue2*

Received: 24-6-2024 Accepted:28-6-2024 Published: 30-6-2024

Research Article

Integrated Framework for Industrial Internet of Things Authentication Leveraging Block chain, Proxy Re-encryption, and AI Techniques

1. Andrea Xiao Xuan Ang
Faculty of Computer Science and Information Technology, Universiti Malaysia Sarawak
Kota Samarahan, Malaysia
Email: 76757@siswa.unimas.my
2. James Kin Hock Po
Faculty of Computer Science and Information Technology, Universiti Malaysia Sarawak Kota Samarahan, Malaysia
Email: 74905@siswa.unimas.my
3. Pikk Heang Lau
Faculty of Computer Science and Information Technology, Universiti Malaysia Sarawak Kota Samarahan, Malaysia
Email: 77363@siswa.unimas.my
4. Yuki Pei Ying Chung
Faculty of Computer Science and Information Technology, Universiti Malaysia Sarawak Kota Samarahan, Malaysia
Email: 76977@siswa.unimas.my
5. Zhi Hao Voon
Faculty of Computer Science and Information Technology, Universiti Malaysia Sarawak Kota Samarahan, Malaysia
Email: 77122@siswa.unimas.my
6. Shakeel Ahmed
Department of eLearning (ELC), Jazan University
Email: shakeel@jazanu.edu.sa

ABSTRACT

The digital evolution has fostered the rise of the Internet of Things (IoT) and its industrial counterpart, the Industrial Internet of Things (IIoT). While IoT is used to connect everyday devices for daily use, IIoT is responsible on optimizing the industrial processes. This paper first explores blockchain-enhanced authentication mechanisms in industrial settings, highlighting their benefits, challenges, and practical applications. In response to the challenges faced, we propose a novel framework that integrates and enhances upon the leading solutions. Our proposed solution is integrated with block chain and RFID technologies, proxy re-encryption, and a block chain authentication mechanism empowered with Transfer Learning (TL). This integrated approach aims to enhance security, efficiency, and adaptability in IIoT environments. Through comprehensive analysis, the paper aims to provide in-depth review into the potential applications and future directions of blockchain-enabled authentication methods in IIoT, contributing to the advancement of secure and efficient industrial operations.

Keywords: Authentication, Block chain, Industrial Internet of Things (IIoT), Proxy Re-encryption, Transfer Learning

Citation
Xin, S., S., T., Yong, G., Nee, T., J., Ying, T., L., Chao, W., T., Z., and Ahmad, S., (2024) The impact of Blockchain-Based System on Goods Tracking and management in Industrial Environment, *Digital Management Sciences Journal* , *1*(2), pp 13-29

1 Introduction

The digital advancement has given rise to the Internet of Things (IoT) and its specialized counterpart, the Industrial Internet of Things (IIoT), each with distinct applications and characteristics. While IoT encompasses a wide network of devices that are interconnected, which enables everyday objects to collect and exchange data for consumer-centric purposes, IIoT is tailored specifically for industrial settings, aiming to optimize processes, enhance efficiency, and improve decision-making.

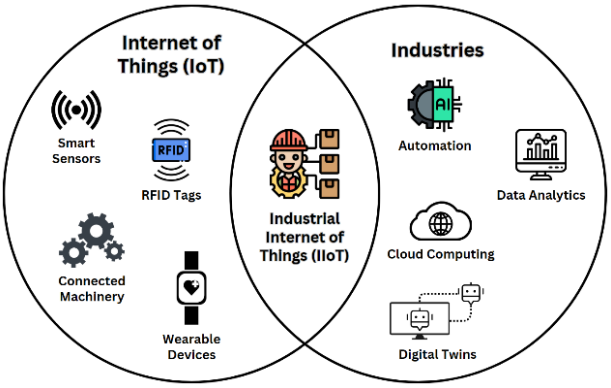

Fig. 1. Concept of IIoT.

Fig. 1 illustrates the concept of the IIoT as the combination of IoT technologies with industries principles within various industrial sectors. For instance, IoT may include smart home devices like thermostats and wearables, whereas IIoT extends to industrial sensors monitoring equipment performance or optimizing supply chain logistics. Despite their shared foundation of connectivity, IIoT diverges in its focus on industrial automation and optimization, catering to different fields, including agriculture, healthcare, manufacturing and more. In the field of IIoT, the benefits are profound, promising to revolutionize industrial operations through enhanced data-driven insights, predictive maintenance, and streamlined processes [1]. However, alongside these advantages, there are notable weaknesses to consider, including concerns over data security and privacy vulnerabilities in industrial applications [2].

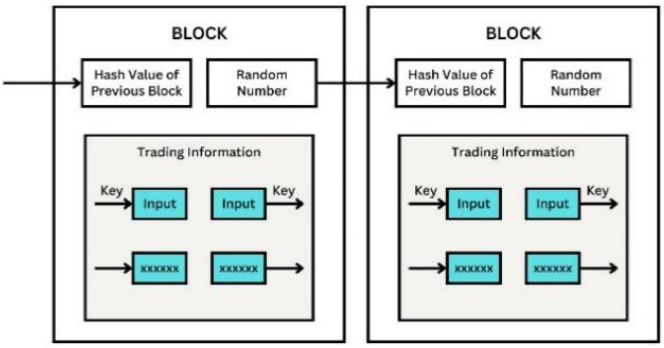

Fig. 2. Fundamental Data Structure of Blockchain.

Recent advancements in web technologies, particularly the emergence of Web 3.0, have ushered in a new era of decentralization and trustless interactions, epitomized by blockchain technology. Blockchain, a decentralized ledger system, ensures data integrity, transparency, and immutability by recording

transactions across a distributed network of computers [3]. As depicted in Fig. 2, blockchain has a fundamental data structure where blocks are interconnected by hashing and storing information from their preceding block. Its integration with IIoT holds immense potential, offering secure and tamper-proof solutions for data authentication and validation, especially in sectors where trust and security are paramount. This paper aims to delve into the intersection of IIoT and blockchain, focusing specifically on the various blockchain-enhanced authentication methods used in industrial settings. By exploring the synergies between these technologies, we seek to elucidate the benefits, challenges, and practical implications of leveraging blockchain to enhance the security and reliability of IIoT systems. Through comprehensive analysis, we aim to provide valuable insights into the potential applications and future directions of blockchain-enabled authentication methods in the context of IIoT, ultimately contributing to the advancement of secure and efficient industrial operations.

2 Problem statements

Industrial IoT (IIoT) systems are facing increasing security challenges due to several reasons as follows.

1) *Limited security of traditional authentication methods:* Existing methods, such as single-factor authentication, prove insufficient in safeguarding against evolving cyberattacks [1].
2) *Rapid growth of devices and users:* The exponential expansion of devices and user types within IIoT networks strains the traditional mechanisms, which struggle to adapt to the ever-growing landscape [2].
3) *Data privacy concerns:* With real-time data collection and monitoring becoming integral to industrial operations, protecting the sensitive industrial data privacy has emerged as an essential issue [1].

These vulnerabilities pose significant risks to data integrity, confidentiality, and overall system security, thereby potentially disrupting critical industrial operations. To mitigate these risks, several innovative solutions have been proposed as follows.

1) *Leverage Blockchain and RFID Technologies:* Implement a lightweight blockchain-based RFID identity authentication mechanism [4]. This solution would strengthen security between RFID readers and electronic tags while simultaneously minimizing communication and storage overhead. Techniques, including bitwise operations, cyclic shift operations, and hash arithmetic, can be employed to further improve both security and efficiency.
2) *Implement Proxy Re-encryption:* Implement proxy re-encryption scheme alleviate the storage demands on blockchain and employs data packing strategies to enhance efficiency [5]. This solution guarantees the authenticity and trustworthiness of data sources through secure storage and authenticated access mechanisms. Additionally, it implements efficient storage methods that reduce the strain on the blockchain's storage capacity.
3) *Implement Transfer Learning Empowered Blockchain:* Adopt a novel approach that utilizes both local and cross-region records for authentication, thus improving privacy and preventing collusion or Sybil attacks [1]. This solution involves training local authentication models with high accuracy using a G-DDPG-based algorithm, while Transfer Learning (TL) minimizes the training time. Inner and outer blockchains are employed to achieve robust privacy preservation.

3 RELATED WORKS

Lu *et al.* [6] explore the need for a secure and efficient data storage protocol tailored to the unique requirements of sensors operating within the Industrial Internet of Things (IIoT). With sensors grappling with limitations in storage capacity and computational power, ensuring secure and optimized data storage processes becomes critical. A proposed solution, as introduced by Lu *et al.* [6], is a novel group signature scheme, leveraging structure-preserving signatures on equivalence classes (SPS-EQ) and proof of knowledge (PoK), to authenticate sensors and employees anonymously. This scheme, coupled with smart contracts and proxy re-encryption techniques, aims to enhance security, privacy, and efficiency in data sharing within a blockchain-based cloud storage system designed specifically for IIoT environments. Strengths of the proposed technique include its efficient group signature scheme, which streamlines authentication processes, along with enhanced security measures and cost-effectiveness. These aspects ensure a robust and economical approach to secure data storage for sensors in IIoT environments. However, potential weaknesses include scalability challenges, as the system may struggle to efficiently handle a large volume of data and devices, along with complexity in implementation, which could pose obstacles for organizations lacking specialized expertise. Additionally, there are potential concerns regarding latency, which might affect real-time data access and responsiveness, particularly in time-sensitive industrial settings. Lu *et al.* [6] employed a rigorous set of evaluation metrics to thoroughly assess the proposed protocol's effectiveness in securing sensor data within IIoT ecosystems. These metrics included formal security models and proofs, ensuring the protocol's adherence to stringent security standards. Additionally, performance evaluations were conducted, focusing on computational overhead, communication overhead, and scalability. By analyzing these key aspects, Lu *et al.* [6] were able to provide a comprehensive evaluation of the protocol's robustness and efficiency in safeguarding sensor data in IIoT environments.

Similarly, Chen *et al.* [4] address the pressing need for a lightweight authentication mechanism in smart factories. The rise of Industry 4.0 has ushered in the era of smart factories, where digitally networked devices operate in increasingly automated and intelligent production environments. In such settings, ensuring data security and rapid authentication is paramount. Traditional authentication systems face challenges in meeting the demands of smart factories due to their complexity and high-load operations. The challenge lies in ensuring secure authentication while minimizing communication and storage overheads in the face of complex and high-load operations. The proposed solution introduces a lightweight blockchain-based radio-frequency identification (RFID) identity authentication mechanism. By the integration of RFID technologies and blockchain, the mechanism ensures security between RFID readers and electronic tags while requiring minimal communication and storage. Techniques such as hash arithmetic, cyclic shift operations, and bitwise operations are employed to enhance security and efficiency. The strengths of the proposed mechanism lie in its ability to guarantee security while minimizing communication and storage requirements. The integration of blockchain and RFID technologies enhances overall security and enables efficient authentication in smart factory environments. However, potential weaknesses may include the complexity of implementing blockchain and the need for ongoing optimization to address scalability issues. Chen *et al.* [4] employ formal analysis using BAN logic to confirm security guarantees provided by the protocol. Additionally, non-formal analysis, including performance comparisons, validates the efficiency of the mechanism in terms of reduced communication and storage overheads. Experimental results further validate the suitability of the protocol for smart factories, especially those operating under high load conditions. Overall, the proposed RFID lightweight authentication mechanism, as elucidated by Chen *et al.* [4], offers a promising solution to the authentication challenges faced by smart factories. Utilizing both RFID technologies and blockchain, the mechanism enhances security and efficiency, providing direction for

future research in the field of smart factory data security.

Next, Wang *et al.* [5] focus on data sharing in the Industrial Internet of Things (IIoT) and the challenges faced in ensuring security and efficiency within traditional cloud-based frameworks. The problem statement in the article highlights the limitations and deficiencies of existing blockchain-based data-sharing schemes in IIoT environments, particularly regarding data supervision, security vulnerabilities, and inefficiencies in data sharing [5]. Specific concerns include data trustworthiness, privacy protection, computational burden, and storage pressure on the blockchain. To counter these challenges, Wang *et al.* [5] propose a blockchain-enabled data-sharing scheme based on proxy re-encryption, incorporating storage and access authentication to ensure data trustworthiness and prevent misuse. This scheme utilizes on-chain and off-chain collaborative storage mechanisms to reduce blockchain storage pressure and supports data packing for improved efficiency [5]. The proposed solution offers several strengths, particularly ensuring the trustworthiness of data sources through storage and access authentication, along with implementing efficient storage mechanisms that alleviate the burden on the blockchain. Additionally, the scheme enhances data storage efficiency by supporting data packing and optimizing resource utilization [5]. However, implementing the technique may demand extra computational resources, potentially affecting resource-constrained IIoT devices. Furthermore, its complexity may hinder scalability, particularly in extensive IIoT environments, where increased system size and complexity could pose challenges to the performance of scheme [5]. Wang et al. [4] evaluate their scheme through security analysis to ensure the scheme meets security requirements and performance evaluation to measure its effectiveness and practicality in blockchain-enabled IIoT environments, focusing on computational overhead, data storage efficiency, security robustness, and system scalability. In summary, Wang *et al.* [5] presents a promising approach to addressing the security and efficiency challenges in IIoT data sharing through a blockchain-enabled proxy re-encryption scheme.

In addition, Wang *et al.* [1] propose a novel Transfer Learning (TL) empowered Blockchain (ATLB) authentication mechanism. While user authentication is a potential solution for the data privacy and security challenges that industrial applications have encountered when the data is collected and monitored automatically in real-time, the existing mechanisms have limitations such as single-factor authentication and lack of adaptability to handle increasing users and user categories. In contrast to traditional blockchain design, where authentication relies solely on local records, this proposed solution suggests employing both local and cross-region records for the authentication mechanism to achieve privacy preservation against collusion and Sybil attacks and integrated user's local and cross-regional credit into the mechanism [1]. A G-DDPG-based algorithm is developed for the training of high-accuracy local authentication models. TL is used to minimize the required time for authentication models training, build trustworthy blockchains and preserve privacy. This solution has achieved privacy preservation using inner and outer blockchains. The integration of local and cross-regional user credits improves authentication accuracy. ATLB is evaluated on the aspects of transaction latency, system throughput, and accuracy of authentication. ATLB presents an authentication model of IIoT applications that have high throughput and accuracy, and low latency.

The rise of 5G presents security challenges for IIoT systems like user privacy, data security, high concurrency, and resource constraints, as discussed by Zhang *et al.* [3]. With numerous devices and frequent data exchange, identity authentication and authorization become highly complex. Huge IoT systems that apply symmetric key mechanisms must deal with complicated key management. The conventional schemes depend mainly on third-party platforms that are centralized, which may result in more potential vulnerabilities. Existing authentication and authorization mechanisms lack the adaptability needed for the diverse communication scenarios in IIoT applications. Zhang *et al.* [3]

introduce a novel blockchain-based authentication mechanism to thwart unauthorized access and lighten the load on the blockchain system. Their proposed solution comprises a three-layer architecture that consists of the layers of entity, virtual node, and blockchain which aim at ensuring secure data transmission. Additionally, a random reputation voting mechanism and blockchain (RRV-BC) scheme based on verifiable random function (VRF) and reputation voting is presented to lessen the communication cost during consensus. In order to evaluate the node credit dynamically, a node credit scoring mechanism is also presented [3]. The strengths include the enhanced fault tolerance and data communication dependencies, effective reduction of malicious nodes' survival possibility through a grouping and credit mechanism, and resistance to several cyber-attacks. However, the PBFT consensus algorithm is not well scalable for large-scale scenarios and the use of ECDSA signatures has resulted in high storage costs [3]. The solution is evaluated through simulations. The performance of the solution against various cyber-attacks, fault tolerance, transactions per second (TPS) and communication cost is also compared to that of the traditional PBFT, DPBFT, and GPBFT protocols.

Although IIoT has revolutionized communication within smart systems, the proliferation of cyber threats poses significant risks, as highlighted by Rathee *et al.* [7]. While cybersecurity approaches for IIoT systems exist, identifying and addressing issues during data exchange is still nascent, prompting the need for efficient cybersecurity communication mechanisms. Rathee *et al.* [7] aim to address cybersecurity challenges in IIoT applications by proposing an efficient communication mechanism. It leverages device trust evaluation and blockchain-based monitoring to ensure secure communication, mitigating risks posed by malicious devices. Nonetheless, current approaches lack the capability to effectively detect and respond to cybersecurity threats during data exchange. The proposed solution introduces TrustBlkSys, which is a trusted communication mechanism for IIoT applications based on blockchain technology. By integrating device trust evaluation and blockchain-based monitoring, TrustBlkSys ensures secure and efficient communication. It evaluates the trust of each device to make informed decisions during communication, while blockchain-based monitoring enhances security and accountability. The proposed approach is validated against existing schemes, demonstrating superior performance across various security metrics. TrustBlkSys offers robust security and efficiency in IIoT communication, leveraging device trust evaluation and blockchain-based monitoring. It enhances security and accountability, outperforming existing approaches. However, potential weaknesses may include implementation complexity and scalability issues. Rathee *et al.* [7] validate TrustBlkSys against existing schemes using various security metrics, including device sensitivity, convergence time, and the probability of malicious devices affecting data delivery and authentication. Results demonstrate the superiority of TrustBlkSys in ensuring secure and efficient communication in IIoT applications. Overall, TrustBlkSys offers a promising solution to cybersecurity challenges in IIoT applications, leveraging device trust evaluation and blockchain-based monitoring to enhance security and efficiency. Future research efforts, as highlighted by Rathee *et al.* [7], will focus on refining the proposed approach to further enhance security and effectiveness in IIoT environments.

Next, Deebak *et al.* [2] delve into the realm of enhancing privacy and security in industrial applications enabled by IoT through a trust-aware blockchain-based authentication system, emphasizing the proliferation of sensory technologies in smart cities and the need for robust authentication mechanisms to ensure data integrity and privacy in industrial settings. The problem statement revolves around the lack of efficient trust-aware and privacy-preserving authentication solutions for industrial applications enabled by IoT, particularly in real-time and decentralized network scenarios. To address these challenges, Deebak *et al.* [2] proposed the TAB-SAPP system, which leverages lightweight cryptographic operations like one-way hashing and bitwise XOR for seamless authentication. The system utilizes identity management to enhance data traffic patterns, ensuring secure device management and

preventing denial-of-service attacks. This proposed technique minimizes computational and communication costs, maintain secure device identities, and improve packet delivery ratio in real-time environments, offering a comprehensive solution to the challenges of privacy-preserving and trust-aware authentication. However, potential weaknesses may include scalability issues with a growing number of IoT devices and the complexity of managing blockchain-based authentication systems. Deebak *et al.* [2] evaluated the TAB-SAPP system using various metrics to assess its performance. These evaluation metrics include computation efficiency, communication effectiveness, mobility speed, and packet delivery ratio. Through simulations and analysis, Deebak *et al.* [2] demonstrated the system's effectiveness in managing device identities securely, enhancing data transmission efficiency, and preventing potential security threats in industrial applications enabled by IoT. Overall, the TAB-SAPP system proposed by Deebak *et al.* [2] presents a promising solution to the challenges of trust-aware and privacy-preserving authentication in massive networks of IoT, providing a thorough method for improving privacy and security in industrial settings.

Furthermore, Li *et al.* [8] present a novel approach, the BLMA protocol, to address the challenges of device authentication in the context of the IIoT. They highlighted the limitations of traditional centralized public key infrastructure systems in ensuring secure and efficient device authentication in large-scale IIoT environments. Therefore, the necessity arises for a more lightweight, scalable, and decentralized authentication protocol capable of effectively verifying the identities of numerous devices without compromising security. The proposed solution, the BLMA protocol, leverages editable blockchain technology to enhance IIoT device authentication. The protocol introduces the Validate-Practical Byzantine Fault Tolerance (vPBFT) consensus algorithm, which eliminates the commit stage to reduce resource consumption during the signature process. Additionally, the protocol utilizes online and offline signature mechanisms for efficient authentication result synchronization and implements a chameleon hash function for secure certificate storage and revocation verification. The strengths of the BLMA protocol lie in its lightweight and distributed consensus algorithm, which ensures efficient authentication result synchronization and network-wide consensus. By combining editable blockchain technology, the protocol enables collaborative identity authentication while meeting the dynamic security requirements of IIoT environments. Furthermore, the protocol eliminates the need for a centralized trusted authority, enhancing scalability and reducing the risk of single point malfunctions and DoS attacks. However, the proposed technique may face challenges in terms of implementation complexity and the need for specialized cryptographic operations. The protocol's reliance on blockchain technology could introduce latency issues in highly dynamic IIoT environments. To evaluate the effectiveness of the BLMA protocol, Li *et al.* [8] used metrics such as communication overhead, energy consumption, privacy security, and authentication delay. Through simulation experiments and performance analysis, they had demonstrated the protocol's advantages in reducing computational resource consumption, improving authentication efficiency, and enhancing network scalability in large-scale IIoT deployments.

In the framework of the Multidomain Internet of Things (IoT), Tong et al. [9] offer a solution to problems relating to authorization and authentication (A&A). Currently, different domains implement their own A&A mechanisms, creating incompatibility issues between them. The proposed solution leverages blockchain technology to achieve flexible A&A that works seamlessly within a domain (intra-domain) and across different domains (inter-domain). To achieve decentralized trust and domain interoperability (DI), consortium blockchain is used as a foundation for the agreement to be built upon, allowing domain managers to control access permissions without relying on any central authority. To enable anonymous authentication for IoT devices seeking access to authorized domains, an authentication protocol that is both secure and confidential makes use of one-out-of-many proof approaches to allow for anonymous domain-to-domain access. Domain managers can use the blockchain to transparently

audit resource access using a voting-based protocol and threshold-based cryptosystem. The proposed scheme offers several security benefits, including DI, privacy protection, and accountability, addressing the pressing need for efficient cybersecurity communication mechanisms [9]. Additionally, Tong *et al*. [9] developed proof-of-concept prototypes to show how effective the approach is in terms of communication overhead and computation.

According to Wang et al. [10], IIoT raises unique challenges to network security since there are so many connected devices. Wang *et al.* [10] propose a scheme to addresses these challenges by leveraging blockchain and smart contracts to establish a reliable and efficient certificate-less signature system. The scheme's architecture includes a smart contract acting as a Key Generation Center (KGC) to securely distribute keys to users, ensuring data privacy and security in communication channels. The proposed scheme offers significant security enhancements compared to existing certificate-less signature schemes. By utilizing blockchain technology, the scheme mitigates centralized KGC compromised attacks and provides protection against privileged-insider attacks. Additionally, measures such as timestamp inclusion to prevent replay attacks, decentralized verification processes to thwart DDoS attacks, and ElGamal encryption for identity protection against MITM attacks are implemented to enhance overall security. Moreover, a comprehensive evaluation of the scheme's security features, communication costs, and computation costs has been conducted. The comparison with existing schemes highlights the proposed scheme's robust security measures and its ability to achieve higher security assurance with reduced communication and computation costs. Despite the scheme's communication cost being competitive with that of current protocols, it outshines them in terms of security features and efficiency. Overall, the proposed blockchain-based certificateless signature scheme presents a promising solution to enhance security in IIoT devices while minimizing operational costs. According to Wang *et al.* [10], the computation cost for the CLS scheme has significantly reduced compared to other existing schemes. In the signature verification aspect, the CLS scheme proves efficient and secure, defending against specific attacks. The comparison shows a notable decrease in signature costs, rendering superior security and functionality features. The proposed blockchain-based CLS scheme tackles persistent issues in IIoT applications, offering enhanced security against common attacks. Future work aims at exploring security enhanced CLS protocols for real-world applications. Various references highlight advancements in cryptographic protocols, security challenges, and efficient authentication schemes, emphasizing the continuous evolution towards more secure and efficient systems.

Several other researchers have also contributed in end-to-end security mechanisms even with the assistance of the counter partners i.e. universities or industries for broaden implications [11]-[22]. This research article can act as guidelines for future young researchers in end-to-end security measures in 6th generation networks. This improved work (Integrated Framework for IIoT Authentication Leveraging Blockchain, Proxy Re-encryption, and AI Techniques) for the given problem statement is adopted from [1], [4], [5], which act as a benchmark for this research article.

4 PROPOSED SOLUTIONS

In response to the authentication challenges faced by Industrial Internet of Things (IIoT) environments, this section presents a novel authentication framework that integrates and improves upon the three leading solutions identified in [1], [4], [5]. The proposed solution combines blockchain and RFID technologies, proxy re-encryption, and a Transfer Learning (TL) empowered blockchain authentication mechanism. This integrated approach aims to enhance security, efficiency, and adaptability in IIoT environments. Each solution addresses specific aspects of authentication,

encompassing blockchain-based identity verification, resource-efficient data sharing, and AI-driven authentication mechanisms.

A. Enhanced Blockchain and RFID Authentication

Leveraging the work of Chen *et al.* [4], our solution focuses on refining the lightweight blockchain-based RFID identity authentication mechanism. This method enhances security between RFID readers and electronic tags while minimizing communication and storage overhead. While their approach adeptly ensures security between RFID readers and electronic tags, certain vulnerabilities require addressing. One such vulnerability pertains to the complexity of blockchain implementation, and the optimization challenges associated with scalability.

To fortify this authentication mechanism, our proposed enhancements pivot on streamlining blockchain implementation and mitigating scalability issues. One key enhancement involves the adoption of a hierarchical blockchain architecture, featuring a multi-tiered structure that segregates transaction processing based on relevance and priority. This architecture optimizes resource allocation, ensuring efficient utilization of computational resources and mitigating scalability concerns.

Furthermore, we introduce an adaptive consensus mechanism that dynamically adjusts to varying IIoT network loads, ensuring optimal performance under fluctuating conditions. Leveraging machine learning algorithms, such as reinforcement learning and neural networks, this mechanism predicts network traffic patterns and adjusts consensus protocols accordingly. For instance, during periods of high network congestion, the consensus mechanism may transition from proof-of-work to proof-of-stake to expedite transaction processing and maintain system integrity.

Additionally, cryptographic primitives are optimized to strike a balance between security and efficiency, enhancing the overall robustness of the authentication mechanism. By leveraging lightweight cryptographic algorithms, such as Elliptic Curve Cryptography (ECC) and Merkle tree-based data structures, cryptographic operations are performed with minimal computational overhead. Moreover, the integration of zero-knowledge proofs and threshold cryptography enhances privacy and resilience against malicious actors.

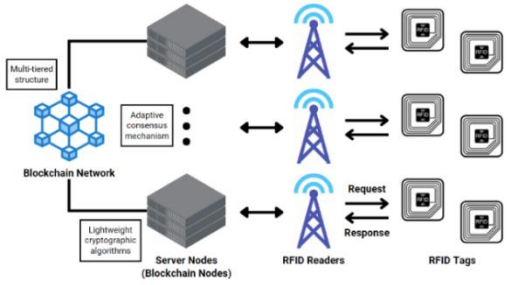

Fig. 1. Enhanced Blockchain-RFID Authentication.

To illustrate, Fig. 3 depicts the refined architecture of the enhanced blockchain-RFID authentication mechanism. Notably, the streamlined blockchain implementation and adaptive consensus mechanism contribute to reduced communication and storage overheads, addressing the weaknesses identified in the previous framework. This fortified authentication mechanism promises heightened security and efficiency, laying a solid foundation for IIoT data security in smart factory environments.

B. Improved Proxy Re-encryption for Data Sharing

Building on the insights from Wang *et al.* [5] in their proposal for a blockchain-enabled data-sharing scheme based on proxy re-encryption, our enhancements aim to address existing limitations while augmenting the scheme's security and efficiency. The original proposal adeptly tackles challenges related to data trustworthiness and storage efficiency; however, certain vulnerabilities warrant refinement.

One notable enhancement involves the integration of homomorphic encryption techniques to bolster data privacy and confidentiality. By leveraging homomorphic encryption, sensitive data can be securely processed while encrypted, mitigating the risk of data exposure during computation. Furthermore, the adoption of secure multi-party computation (MPC) protocols facilitates collaborative data analysis without compromising data privacy, thereby enhancing the scheme's applicability to diverse IIoT use cases.

Moreover, to alleviate computational burdens on resource-constrained IIoT devices, we introduce lightweight cryptographic primitives tailored for IIoT environments. By optimizing cryptographic operations, such as re-encryption and key generation, for efficiency and scalability, we ensure seamless integration with existing IIoT infrastructures. Additionally, the implementation of distributed key management mechanisms further enhances the scheme's resilience against key compromise attacks, safeguarding sensitive data from unauthorized access.

Furthermore, to address concerns regarding the scheme's complexity and scalability, we propose the adoption of a modular architecture that facilitates interoperability with existing IIoT systems. By decoupling data sharing functionalities into modular components, such as data storage, access control, and encryption modules, we enhance system flexibility and scalability. Additionally, the incorporation of standardization protocols, such as the Interoperable Data Sharing Protocol (IDSP), promotes seamless integration with diverse IIoT ecosystems, fostering interoperability and scalability.

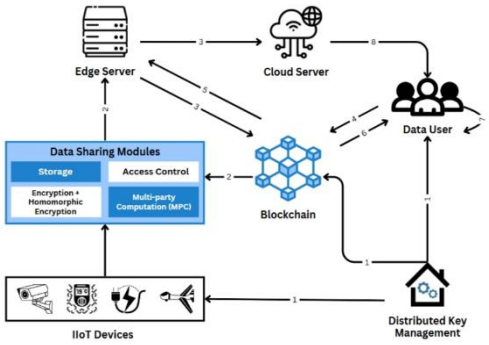

Fig. 2. Enhanced Proxy Re-Encryption-Based Data Sharing Scheme for IIoT.

Fig. 4 illustrates the refined architecture of the enhanced proxy re-encryption-based data sharing scheme. By integrating homomorphic encryption, lightweight cryptographic primitives, and modular architecture, our enhanced scheme offers heightened security, efficiency, and scalability, positioning it as a robust solution for secure data sharing in IIoT environments.

C. Enhanced Transfer Learning and AI-Driven Blockchain Authentication

Incorporating the innovative Authentication mechanism for Transfer Learning (TL) empowered Blockchain (ATLB) proposed by Wang *et al.* [1], our solution introduces several enhancements to address its limitations and further improve its performance in IIoT environments. The original ATLB

mechanism utilizes a G-DDPG-based algorithm for training high-accuracy local authentication models, incorporating both local and cross-region records for improved privacy preservation and authentication accuracy. However, there are areas where further improvements can be made.

First, to tackle the potential computational overhead and improve the scalability of the AI-driven models, we propose the incorporation of federated learning techniques. Federated learning enables decentralized training of AI models across multiple IIoT devices, reducing the need for extensive data transfer and central computation. This approach not only minimizes latency but also preserves data privacy by ensuring that sensitive data remains on local devices.

Second, to enhance the robustness of the authentication mechanism, we propose integrating adversarial training techniques into the model training process. By exposing the AI models to adversarial examples during training, we can improve their resilience against potential attacks, such as evasion and poisoning attacks. This enhancement ensures that the authentication mechanism remains robust even in the face of sophisticated adversarial tactics.

Additionally, to address the challenge of ensuring privacy preservation and preventing collusion and Sybil attacks, we propose the use of secure multi-party computation (MPC) protocols in conjunction with the existing TL and blockchain framework. MPC allows multiple parties to jointly compute authentication results without revealing their individual inputs, thereby enhancing privacy and security. The combination of MPC with TL further strengthens the privacy guarantees of the authentication mechanism.

To further improve the accuracy and efficiency of the authentication process, we propose the use of transfer reinforcement learning (TRL) techniques. TRL leverages the strengths of both transfer learning and reinforcement learning, enabling the AI models to adapt to new environments and user behaviors more quickly and accurately. By continuously learning from new data and adjusting the models in real-time, TRL enhances the adaptability and performance of the authentication mechanism.

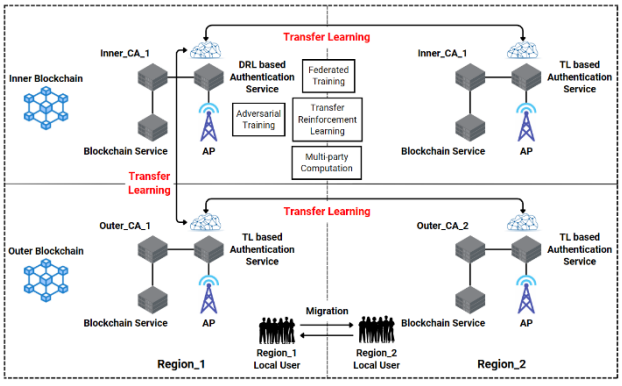

Fig. 3. Enhanced Transfer-Learning and AI-driven Blockchain Authentication.

Fig. 5 illustrates the enhanced Transfer Learning and AI-driven blockchain authentication framework. The integration of federated learning, adversarial training, secure multi-party computation, and transfer reinforcement learning significantly enhances the security, efficiency, and adaptability of the authentication mechanism, making it a robust solution for IIoT environments.

D. Integrated Authentication Framework

This section synthesizes the enhanced methods into a comprehensive and robust authentication framework tailored for Industrial Internet of Things (IIoT) environments. By integrating the blockchain-based RFID authentication mechanism, the proxy re-encryption-based data sharing scheme, and the advanced AI-driven blockchain authentication mechanism, we aim to address the multifaceted challenges of IIoT security, efficiency, and scalability.

The integrated solution framework combines the strengths of each individual method to provide a holistic approach to IIoT authentication. The integration process involves deploying blockchain nodes, RFID readers, proxy re-encryption systems, and AI-driven authentication models across the IIoT environment. Each component interacts seamlessly to deliver a secure, efficient, and adaptable authentication process.

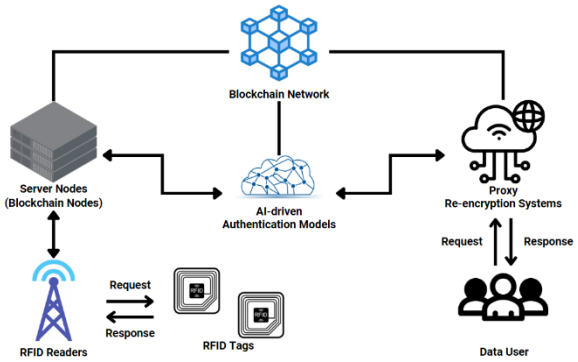

Fig. 4. Integrated Authentication Framework.

Fig. 6 illustrates the integrated solution framework, highlighting the interaction between blockchain nodes, RFID readers, proxy re-encryption systems, and AI-driven authentication models. This comprehensive framework addresses the security, efficiency, scalability, and privacy preservation requirements of IIoT environments.

1) *Enhanced Security:* The integration of blockchain and RFID technologies ensures secure communication between RFID readers and tags, while the proxy re-encryption scheme secures data sharing by enabling fine-grained access control and reducing blockchain storage overhead. The AI-driven authentication mechanism, enhanced with federated learning and adversarial training, adds an additional layer of security by improving the robustness and accuracy of user authentication. Secure multi-party computation further enhances privacy preservation, protecting sensitive data from collusion and Sybil attacks.
2) *Improved Efficiency:* Efficiency is improved using lightweight cryptographic techniques and the decentralized training of AI models via federated learning. This reduces the computational burden on individual devices and minimizes latency in the authentication process. The proxy re-encryption scheme's on-chain and off-chain storage mechanisms alleviate blockchain storage pressure, ensuring efficient data management and access. Transfer reinforcement learning continuously optimizes the AI models, ensuring rapid adaptation to new data and environments.
3) *Ensured Scalability:* The proposed framework is designed to scale effectively with the growing number of users and devices in IIoT networks. The dual-layer blockchain architecture supports both local and cross-region authentication, enabling the system to handle increasing user categories and transaction volumes. The adaptability of the federated learning and TRL techniques ensures that the AI models can manage the scalability challenges posed by extensive IIoT environments.

4) *Privacy Preservation:* Privacy preservation is a key focus of the integrated solution framework. The combination of secure multi-party computation, federated learning, and TL techniques ensures that sensitive data remains protected throughout the authentication process. By integrating local and cross-region records, the framework prevents unauthorized access and enhances privacy against collusion and Sybil attacks.

5 RESULTS AND ANALYSIS

A. Security Analysis

To verify the security of the protocols in proposed solution, an analysis is done to cover various aspects of the proposed solution in security perspective.

1) *Confidentiality*: The bidirectional authentication credentials for RFID are generated from the key information, protecting the pseudonyms and random numbers with the key [4]. Besides, with proxy re-encryption systems, data are encrypted with algorithms before sending out and the respective authorized user can perform the decryption to get the data. This helps to ensure data confidentiality.
2) *Bidirectional Discrimination*: A mutual authentication occurs between a RFID tag and the RFID reader each time authentication happens. The authentication credentials generated by tag will be validated by the reader and vice versa. Success validation from both reader and tag will mark the success of mutual authentication. This mutual authentication ensures that both entities are authentic and helps to prevent unauthorized access.
3) *Anonymity*: The generation of random numbers to each session has prevented each session from linking to a tag. The anonymity of the session ensures that the sessions are impossible to be traced back through the RFID tag [4]. Moreover, in proxy re-encryption systems, the data identity is hidden in the pseudonym. If attackers are to discover the pseudonym, it is required to compute the information in pseudonym from Computational Diffie–Hellman (CDH) Problem which are hard to solve [5]. Therefore, the scheme can ensure the data anonymity.
4) *Integrity*: Both set of credentials generated by RFID reader and tag respectively not only acts the token to be validated during authentication but also used in integrity check. This would help to detect and prevent data tampering from happening. The proxy re-encryption scheme can also ensure integrity of the packaged data because of the collision-resistant hash function.
5) *Privacy*: The zero-knowledge proofs and threshold cryptography integrated have enhanced privacy of the data in the authentication mechanism and resilience against malicious users.

B. Performance Evaluation

The overall evaluation of the proposed system focuses on a few key metrics.

1) *Computational Performance*: The resources required by the proposed system are reduced with the integration of lightweight cryptographic algorithm such as ECC and Merkle tree-based data structures. The cryptographic operations are done with lesser computational overhead produced. The protocol becomes significantly more efficient for longer tag identifiers in RFID due to its reliance on simpler cyclic operations compared to complex hash or encryption operations used by other protocols [4].
2) *System Throughput*: The system throughput has been improved with the use of TRL as the transaction sending rate, number of transactions, and number of block transactions increase.

Throughput reaches a peak and levels off with larger block sizes. This suggests that the transactions can be efficiently processed in various workloads.

3) *Transaction Latency*: Latency increases with higher transaction sending rate, number of block transactions, and block sizes. The proposed solution can maintain latency at the rate of below 15 seconds even under high workloads. This indicates ATLB can handle real-time transactions effectively.
4) *Authentication Accuracy*: With Guided Deep Deterministic Policy Gradient (G-DDPG) algorithm integrated, the accuracy for user authentication has increased. G-DDPG outperforms Deep Deterministic Policy Gradient (DDPG) in terms of False Alarm Rate and Miss Detection Rate for both local and foreign users [1]. Authentication accuracy improves with a larger number of users up to a certain point.
5) *Model Training Time*: Utilizing TRL has significantly reduced the model training time compared to training from scratch. This allows for faster user onboarding and system updates. The reduction is more pronounced with a larger number of regions participating in the network.
6) *Storage Performance*: The proposed protocol requires minimal storage space, comparable to existing protocols. The proxy re-encryption scheme also implements efficient storage mechanisms which reduces the burden on the storage capar=city of blockchain.
7) *Authentication Performance*: The protocol achieves faster authentication compared to existing protocols as it avoids complex operations like PUF (Physical Unclonable Function) or hash functions used by others. This advantage becomes more pronounced with an increasing number of readers.
8) *Blockchain Performance*: The system throughput of the proposed protocol is similar to the most efficient existing protocol across different transaction generation rates. The blockchain operations proposed are lightweight. The interaction number between blockchain and server is reduced by integrated data packaging, making the solution more suitable for IIoT.

The enhanced authentication methods integrating new lightweight identity authentication protocol for RFID tags, proxy re-encryption scheme and AI-driven blockchain authentication mechanism is evaluated. Overall, the proposed solution offers improvements on a few key metrics such as less computational overhead, low transaction latency, high user authentication accuracy, and so on. The proposed protocol experiences a smaller increase in system delay compared to others as the transaction rate increases. This makes it more robust to varying transaction loads. The low overhead of the protocol in terms of transmission and storage lessens the strain on industrial communication networks, which is particularly advantageous in high-density communication contexts such as medical device manufacture. This helps to mitigate the issue of the rapidly expanding number of devices in IIoT networks, ensuring the scalability of the solution. Overall, the proposed protocol offers a secure and lightweight solution for identity authentication in smart factories with high operational loads. It achieves comparable or better performance than existing protocols in terms of storage, computing, authentication, and blockchain performance while requiring less communication and storage resources.

6 Conclusion

In conclusion, the integration of IIoT and blockchain presents a promising avenue for enhancing the security and reliability of industrial operations. Through our exploration of blockchain-enhanced authentication methods in industrial settings, we have uncovered significant potential advantages and practical implications. Leveraging blockchain technology offers secure and tamper-proof solutions for

data authentication and validation, addressing the concerns over data security and privacy vulnerabilities in IIoT systems.

While traditional security solutions often rely on a central authority, which can be a bottleneck and a target for attacks, blockchain offers a compelling alternative for securing the vast and resource-constrained world of IoT. As blockchain is decentralized, the burden of complex security tasks is spread across the entire network. This means that even individual devices with limited processing power can participate in securing the network. Transactions are cryptographically verified and permanently recorded on a shared ledger, creating an immutable and transparent audit trail. This not only makes it extremely difficult to tamper with data but also fosters trust between devices and users within the network. In essence, blockchain leverages the very nature of the IoT – its massive scale and distributed infrastructure – to create a robust and scalable security solution.

Due to the challenges posed by traditional authentication methods and the rapid growth of IIoT devices and users, innovative solutions such as blockchain-based RFID identity authentication, proxy re-encryption, and Transfer Learning empowered blockchain are proposed to overcome these weaknesses. These solutions aim to enhance security, adaptability, and privacy preservation in IIoT environments, thereby safeguarding critical industrial operations from cyber threats and disruptions.

However, the above solutions are not without weaknesses that must be addressed to ensure adaptability to the evolving IIoT environment. Therefore, we propose a novel framework for IIoT authentication leveraging the blockchain-based RFID authentication mechanism, the proxy re-encryption-based data sharing scheme, and the advanced AI-driven blockchain authentication mechanism, to integrate and improve upon the three leading solutions. This comprehensive framework addresses the security, efficiency, scalability, and privacy preservation requirements of IIoT environments Through analysis, it is evident that the proposed authentication framework can offer improvements on a few key metrics which includes a reduction in computational overhead, low transaction latency, high user authentication accuracy, and more, thus making it a viable solution to address the complexity of IIoT authentication.

Looking ahead, continued research and development efforts are essential to further explore the synergies between IIoT and blockchain, as well as to address emerging challenges and opportunities in this domain. By harnessing the potential of blockchain-enabled authentication methods, we can pave the way for secure and efficient industrial operations, ultimately contributing to the advancement of Industry 4.0 and beyond.

7 Acknowledgement

This research work is the outcome of class project of computer security at Faculty of computer science and information technology, Universiti Malaysia Sarawak, Malaysia.

8 Reference

X. Wang, S. Garg, H. Lin, M. J. Piran, J. Hu, and M. S. Hossain, (2021) “Enabling secure authentication in industrial iot with transfer learning empowered blockchain,” IEEE Trans Industr Inform, vol. 17, no. 11.

B. D. Deebak, F. H. Memon, K. Dev, S. A. Khowaja, W. Wang, and N. M. F. Qureshi, (2023) “TAB-SAPP: A trust-aware blockchain-based seamless authentication for massive iot-enabled industrial applications,” IEEE Trans Industr Inform, vol. 19, no. 1,.

P. Zhang, P. Yang, N. Kumar, C. H. Hsu, S. Wu, and F. Zhou, (2024) "RRV-BC: Random reputation voting mechanism and blockchain assisted access authentication for industrial internet of things," *IEEE Trans Industr Inform*, vol. 20, no. 1.

Z. Chen, H. Jiang, J. You, X. Wang, and P. Z. H. Sun, (2024) "RFID lightweight authentication mechanism for smart factories based on blockchain," *IEEE Journal of Radio Frequency Identification*, vol. 8.

F. Wang, J. Cui, Q. Zhang, D. He, C. Gu, and H. Zhong, (2023) "Lightweight and secure data sharing based on proxy re-encryption for blockchain-enabled industrial internet of things," *IEEE Internet Things J*.

J. Lu, J. Shen, P. Vijayakumar, and B. B. Gupta, (2022) "Blockchain-based secure data storage protocol for sensors in the industrial internet of things," *IEEE Trans Industr Inform*, vol. 18, no. 8.

G. Rathee, C. A. Kerrache, and M. Lahby, (2023) "TrustBlkSys: A trusted and blockchained cybersecure system for iiot," *IEEE Trans Industr Inform*, vol. 19, no. 2.

F. Li (2023)., "BLMA: Editable blockchain-based lightweight massive iiot device authentication protocol," *IEEE Internet Things J*, vol. 10, no. 24.

F. Tong, X. Chen, C. Huang, Y. Zhang, and X. Shen, (2023) "Blockchain-assisted secure intra/inter-domain authorization and authentication for internet of things," *IEEE Internet Things J*, vol. 10, no. 9,.

W. Wang, H. Xu, M. Alazab, T. R. Gadekallu, Z. Han, and C. Su, (2022) "Blockchain-based reliable and efficient certificateless signature for iiot devices," *IEEE Trans Industr Inform*, vol. 18, no. 10.

I. A. Abbasi, S. U. Jan, A. S. Alqahtani, A. S. Khan, and F. Algarni, (2024) "A lightweight and robust authentication scheme for the healthcare system using public cloud server," *PLoS One*, vol. 19, no. 1 January,.

N. Nisa, A. S. Khan, Z. Ahmad, and J. Abdullah, (2024) "TPAAD: Two-phase authentication system for denial of service attack detection and mitigation using machine learning in software-defined network," *International Journal of Network Management*, vol. 34, no. 3.

Z. Ahmad, A. S. Khan, K. Zen, and F. Ahmad, (2023) "MS-ADS: Multistage spectrogram image-based anomaly detection dystem for iot security," *Transactions on Emerging Telecommunications Technologies*, vol. 34, no. 8.

I. U. Khan, C. E. Tan, and A. S. Khan, (2014) "The enhanced amplify-and-forward three time slots TDMA-based protocol using inter-relay communication over rician fading channel," *International Review on Computers and Software*, vol. 9, no. 8.

A. S. Khan, H. Lenando, and J. Abdullah, (2014) "Lightweight message authentication protocol for mobile multihop relay networks," *International Review on Computers and Software*, vol. 9, no. 10.

A. M. Iqbal, A. S. Khan, F. Bashir, and A. A. Senin, (2015) "Evaluating national innovation system of malaysia based on university-industry research collaboration: A system thinking approach," *Asian Soc Sci*, vol. 11, no. 13.

A. M. Iqbal, A. S. Khan, S. Parveen, and A. A. Senin, (2015) "An efficient evaluation model for the

assessment of university-industry research collaboration in Malaysia," *Research Journal of Applied Sciences, Engineering and Technology*, vol. 10, no. 3.

A. M. Iqbal, A. S. Khan, S. Parveen, and A. A. Senin, (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*, vol. 4, no. 1, pp. 6–14.

Y. Javed, A. Khan, B. Qureshi, and J. Chaudhry, (2016) "Estimating diabetic cases in KSA through search trends and creating cyber diabetic community"

I. A. Abbasi, A. S. Khan, and S. Ali, (2018) "Dynamic multiple junction selection based routing protocol for VANETs in city environment," *Applied Sciences (Switzerland)*, vol. 8, no. 5.

I. A. Abbasi, A. S. Khan, and S. Ali, (2018) "A reliable path selection and packet forwarding routing protocol for vehicular ad hoc networks", *EURASIP J Wirel Commun Netw*, vol. 2 no. 1

I. A. Abbasi and A. S. Khan, (2018) "A review of vehicle to vehicle communication protocols for VANETs in the urban environment," *Future Internet*, vol. 10, no. 2.