Enhancing Security in Industrial IoT: Authentication Solutions Leveraging Blockchain Technology

by Rebecca Ling Ze Siew

Submission date: 18-Jul-2024 11:34AM (UTC+0700)
Submission ID: 2418550943
File name: oT_Authentication_Solutions_Leveraging_Blockchain_Technology.pdf (498.9K)
Word count: 6991
Character count: 45143

International Journal of Computer Technology and Science
Volume. 1 No. 3 July 2024
e-ISSN :3048-1961, And p-ISSN :3048-1899, Page. 87-105
DOI: https://doi.org/10.62951/ijcts.v1i3.29
Available online at: https://international.arteii.or.id/index.php/IJCTS

Enhancing Security in Industrial IoT: Authentication Solutions Leveraging Blockchain Technology

Rebecca Ling Ze Siew[1], Brendan Chan Kah Le[1], Lee Kai Yue[1], Nuri Nazirah binti Ismail[1], Xavier Liong Zhi Hao[1] & Muhammad Faisal[2]
[1] Faculty of Computer Science and Information Technology, Universiti Malaysia Sarawak,
[2] Director HRIMS, Ministry of Human Rights

Kota Samarahan 94300,Malaysia
85533@siswa.unimas.my 83403@siswa.unimas.my 84299@siswa.unimas.my
85272@siswa.unimas.my 86079@siswa.unimas.my dr.faisalshabbir88@gmail.com

Abstract : *The rapid advancement of Industrial Internet of Things (IIoT) technology necessitates robust authentication solutions to ensure security, scalability, and efficiency. This project, titled "Enhancing Security in Industrial IoT: Authentication Solutions Leveraging Blockchain," examines various blockchain-based authentication methods for IIoT and identifies their strengths and weaknesses. Despite the enhanced security and decentralized nature of blockchain, issues such as scalability, high latency, and computational load persist. To address these challenges, we propose the integration of Multi-Factor Authentication (MFA) as a supplementary solution. MFA can distribute the authentication load, enhance flexibility and security, and reduce latency by utilizing quick-to-verify factors. Moreover, MFA ensures high availability and scalable storage and processing through cloud services, seamlessly integrating with existing systems to provide a superior user experience. This comprehensive approach not only mitigates the inherent limitations of blockchain technology in IIoT but also reinforces the overall security framework, ensuring resilient and efficient authentication mechanisms. The results demonstrate significant improvements in system performance and user satisfaction, establishing MFA as a viable enhancement to blockchain-based IIoT security solutions.*

Keywords: *IIoT; blockchain authentication; MFA; security; scalability*

I. INTRODUCTION

The Industrial Internet of Things (IIoT) plays an important part in Industry 4.0. providing intelligent and effective solutions. However, the interconnectedness of IIoT raises security issues like illegal access and data breaches. These risks prove difficult for traditional techniques to handle, necessitating creativity [1]. Blockchain technology's distributed ledger, immutability, and resistance to tampering make it a promising solution. To safeguard Industry 4.0, this article investigates how blockchain- based authentication might transform IIoT security.

II. RESEARCH BACKGROUND

Blockchain technology serves as a solid foundation for safe authentication by providing a decentralized and tamper-resistant ledger. Its decentralized nature assures that authentication data is managed independently by users, lowering the risk of illegal access or manipulation. The consensus process used in blockchain authentication, which consists of solving computational puzzles and providing evidence of solutions, improves security by prohibiting unauthorized changes to authentication records. Furthermore, the requirement that attackers control the bulk of the network's processing power to compromise authentication data emphasizes the robustness

Received: May 10, 2024; Revised: June 15, 2024; Accepted: July 15, 2024; Published: July 18, 2024;
* Rebecca Ling Ze Siew , 85533@siswa.unimas.my

of blockchain-based authentication systems.Overall, blockchain's decentralized architecture and strong security measures help to develop highly secure authentication techniques [6]. Below figure 1 shows how blockchain is involved in securing communication between devices and the internet through a master-slave chain structure.

The device distributes various data throughout the network, generating a URL link, which is then stored within the blockchain system. Clients request access from the blockchain system, obtainingpermission, and subsequently, the blockchain system distributes the corresponding website to authorized users. These users then retrieve relevant data from the internet via the provided website [1].

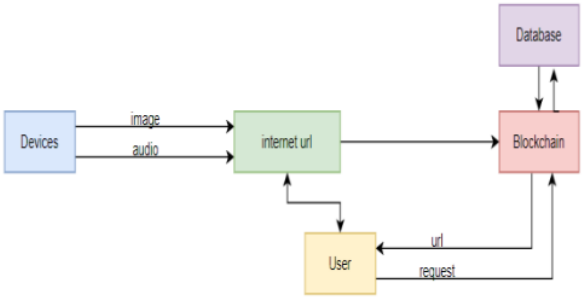

Figure 1: Utilization of blockchain for secure data storage and processing

III. PROBLEM STATEMENTS

The very first problem statement is Authentication and Privacy Challenges in Industrial IoT (IIoT). In this era, assuring a high level of privacy and safety of data is crucial where computers now from different settings, are connecting on the same activity. The solution is to apply Menger identification helps to improve privacy by authenticating them without revealing their identities, enhances security by managing access control using blockchain, and ensures efficient authentication [1].

In addition, the next problem statement is scalability and efficiency issues in blockchain-basedsolutions for IIoT. Blockchain technology promises enhanced IIoT security but faces scalability and efficiency challenges as IIoT ecosystems expand. The first suggested solution is implementing a chained-structured blockchain, similar to Bitcoin, Hyperledger, or Ethereum where new blocks are attached to the long-chain structure. Next is using private blockchain networks with reliable members for IIoT applications, which can reduce computational resources needed for consensus and transactionvalidation by restricting access to a small set of users, resulting in enhanced efficiency and scalability [7].

Lastly, the problem statement is interoperability challenges in blockchain integration

with existing industrial systems. A network structure based on a master-slave chain structure with sub-chainsfor different IoT domains at the bottom layer and a main chain with trusted organization server nodes at the top layer, enabling secure local and cross-chain authentication for IoT devices, is implemented.

Next is providing a framework for assessing the reputation of slave chain nodes and Internet of Things(IoT) devices. This will improve authentication effectiveness and reduce malicious attacks by boosting security by taking transmission delays and consistency into account [9].

IV. RELATED WORK

This article addresses the challenges faced by IoT devices in terms of data security and privacy due to their distributed nature [1]. The problem revolves around ensuring secure authentication for IoT devices,especially at the perception layer, to prevent unauthorized access. The proposed solution involves implementing a blockchain-based authentication system called IoT-chain, leveraging Hyperledger Fabric. Strengths include decentralized security and flexible access control. Weaknesses may include potential scalability issues. Evaluation metrics involve testing the system's throughput and response times under various concurrent access scenarios.

The article discusses the emergence of Industry 5.0 and the Commercial Internet of Things (IIoT) as significant concepts in intelligent systems, particularly in urban traffic management [2]. The problem statement is on handling various traffic issues in urban areas, increasing road network capacity,and improving traffic efficiency and safety through advanced information services and technology. Theproposed solution involves leveraging blockchain technology and a permission-based blockchain approach to enhance security and trust in communication across different domains. Strengths include the use of blockchain for secure communication and identity verification. Weaknesses may include scalability challenges and potential operational mistakes. The proposed solution is through simulations,measuring metrics such as enrollment time, latency, hit frequency, and cache performance to assess system performance and security.

This article addresses blockchain hyperledger technology and the IIoT while addressing the data security concerns associated with the present E-healthcare applications. The problem highlights poor communication channels in E-healthcare, leading to the proposal of BHIIoT, a peer-to-peer consortium network, for secure medical transactions. The BHIIoT solution optimises resource utilisation and efficiency while enhancing E-healthcare data security

through the implementation of a consortium hyperledger network with on/off-chain connection and unique consensus protocols [3]. The strengths of BHIIoT are enhancing security and improving data integrity. The weaknesses of BHIIoT are latency and scalability issues. The authors evaluated their proposed solution using metrics such as resource consumption reduction, productivity improvement, and comparison with state-of-the-artmethods [3].

This article addresses a reliable cybersecurity communication technique that makes decisions throughout communication by utilising each device's trust evaluation system. The problem statement isto enhance secure management and control in industrial sectors amidst increasing cybersecurity risks and IIoT challenges. To improve data security, efficiency, and decision-making, the suggested solution,TrustBlkSys, combines blockchain technology with a trust-enabled IIoT mechanism [4]. The strengthsare enhancing security and enabling a high level of transparency and accountability in communication. The weaknesses could be its vulnerability to attacks targeting the consensus mechanism and potentially hindering adoption and scalability. The authors evaluated metrics such as data security enhancement, efficiency improvement, and comparison against existing approaches [4].

The article addressed is focusing on how the implementation of blockchain based technology can improve the 5G network community. The issue discussed is regarding the need for frequent authentication of the 5G network whenever someone must access it [5]. The existing 4G authenticationprotocols lack effectiveness in handling the authentication demands of 5G network. Hence, the paper proposed one robust solution to the current problem stated which is completely utilizing the usage of blockchain technology in the 5G network which can minimize the authentication process count and enhance the security that can help speed up the 5G's authentication process [5]. The weakness is it requires the implementation and integration of a new consensus algorithm. To achieve this solution proposed, the evaluation metrics such as authentication rate improvement, process authentication countper unit time, processing time and security enhancement in the authentication process are applied.

[6] have summarized an article that highlights the use of biometric authentication systems particularly in this era of escalated security demands in modern technology. However, it still faces somechallenges that trigger the privacy of the information kept. The problem issued is the weak security of the biometric system which is susceptible to information leakage that could lead to unreliability of its modules. The proposed solution suggests that integrating blockchain is implemented to enhance security with the help of special techniques such as information fusion, computational workload, and biometric template protection [6]. The strength of this proposed solution is focusing on providing a distributed, convenient, and

decentralized mechanism for processing authentication via biometrics. However, the economic cost, data privacy, scalability and security, and processing capabilities of this proposed solution are still becoming a big concern within the solution [6]. The author evaluates the proposed solution by how successful the merging of both the biometric system and integration blockchain will provide more security to the biometric authentication system.

The article authored by [7] outlined the challenges of Big Data (BD) dissemination in the IIoTenvironment, where the problem statement is the existing centralized model being prone to single pointsof failure, security, and privacy. The proposed solution to address these issues is a blockchain-based distributed model DMIIoT, focusing more on the security aspects of blockchain technology. It removesthe presence of a third party to fulfill direct data transfer, thus reducing the risks of data loss and man- in-the-middle attacks. However, while the existing encryption mechanism secures data, it may not necessarily secure data transmission, especially in cases of weak key material that can be easily compromised. The evaluation involved a case study on a Smart Grid (SG) system to validate the potential of the proposed model, including aspects such as load balance, energy management cost, andtransmission delay.

The article discusses a development technique for authenticating IoT devices within an industrial network using blockchain technology. It highlights the problem of traditional centralized authentication and security mechanisms, which often rely on third parties and consume significant timeand computing power. The proposed solution suggests implementing the GFE-Chain algorithm [8] to achieve high throughput and low latency while preserving the security and decentralization properties of blockchain technology. This approach promises decentralization, improved performance, and protection against known attacks, but a noticeable gap remains between the theoretical models describedin academic papers and the practical tools required for the full implementation of the algorithm. To evaluate the efficiency of the developed sensor authentication algorithm, the authors employ tools likeAvispa SPAN which is specifically designed to scan security protocols for vulnerabilities automatically.

This article addresses the intelligent terminal of authentication methods in blockchain. The problem statement here is there is limited throughput and increasing time consumption even though a single blockchain can enable trustworthy access and administration of IoT devices in large-scale Internet of Things (IoT) application scenarios. The proposed solution uses a master-slave blockchain structure to enhance the reliability of nodes and IoT devices. The strength of this method is an increasein security measures and the effectiveness of data [9]. The weaknesses are master-slave chain structureincreases complexity when compared to a single-chain architecture and causes performance overhead.The evaluation metrics used by the

author are throughput (TPS), Latency, error node rate and maliciousnode rate to achieve the solution proposed.

This article addresses the implementation through dual chain authentication in edge computingon blockchain. The problem statement is traditional edge computing authentication approaches are insecure for IoT devices due to their widespread distribution and frequent location changes. The proposed solution is by using dual-chain authentication and key agreement protocol that uses blockchain technology. The strength of this solution is enhanced security and an increase in efficiency,such as speed of authentication for frequently used devices. The weaknesses of this solution are increased of storage burden and computational load on edge nodes. Evaluation metrics used by authorsuch as storage consumption [10].

V. PROPOSED SOLUTION

Here, we suggest Multi-Factor Authentication (MFA) serve as an upgraded version of the 10 authentication mechanisms mentioned in related work. The limitation of the 10 authentication mechanisms is scalability issues. Scalability can be defined as an ability of a server to continuously function when the amount of data, and authentication requests of users are increased [11]. The authentication system needs to increase the number of users and devices without sacrificing user experience, security, or performance. Thus, MFA is the best way to overcome this limitation that occurson the authentication mechanisms mentioned. MFA is an electronic authentication method in which a user when accessing some applications and websites, needs to present two or more factors to granted access to the website or application as shown in Figure 2 [12].

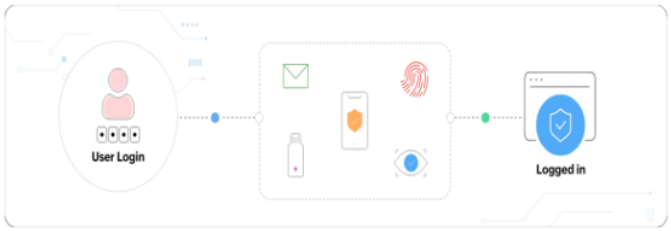

Figure 2: Illustration of how multifactor authentication works

In IIoT environments, high availability and redundancy are essential for continued operation, particularly in the context of urban traffic management systems, where downtime can cause serious disruptions and raise safety issues. The use of a permission-based blockchain to improve identity verification and security in urban traffic communication networks offers several built-in advantages. Itdoes, however, also confront difficulties, namely with scalability

and possible operational errors. These issues can be resolved by including MFA in this architecture, which will increase system reliability overall by guaranteeing high availability and redundancy, enhancing the overall system's reliab ility. The purpose of redundant multi-factor authentication systems is to guarantee that services don't stop working if a server fails. Multiple authentication servers that can process authentication requests concurrently are deployed to do this. The other servers can effortlessly take over the authentication operations in the event of a server loss or outage, preventing any discernible disturbance in service. In urban traffic management, where safe communication and real-time data transmission are crucial for regulating traffic flow, maximizing road usage, and guaranteeing safety, redundancy plays a critical role.Urban traffic management can continue to operate continuously and with high availability even in the event of server failures or maintenance windows by utilizing redundant MFA systems. Furthermore, combining MFA with a permission-based blockchain helps reduce the possibility of operational errors.Although secure, blockchain technologies can be difficult to administer and could pose operational issues if not used properly. By using multi-factor authentication, MFA enhances security and verifies that only authorized users and devices can access the system. This reduces the possibility of operationalmistakes endangering the traffic management system's functionality or security. In addition to improving the overall security posture, the usage of several verification factors makes it more difficultfor attackers to get around authentication systems.

Integrating MFA into existing authentication frameworks not only provides a pragmatic solution to enhance security but also effectively addresses the challenges highlighted in the context of blockchain technology. By leveraging the established authentication mechanisms already in place, MFAintegration sidesteps the need for significant infrastructure changes that would be required to accommodate new consensus algorithms for blockchain. This compatibility and flexibility inherent in MFA integration allow organizations to enhance security measures seamlessly, avoiding the complexities and potential disruptions associated with implementing entirely new consensus mechanisms. Moreover, the streamlined nature of MFA integration ensures that upgrades can be executed without the need for extensive overhauls, a stark contrast to the potential upheaval that mightaccompany the adoption of new consensus algorithms. Also, MFA integration underscores a strategic focus on security enhancement by augmenting existing authentication mechanisms with additional layers of verification. While blockchain technology offers inherent security benefits, the integration of MFA adds an extra layer of protection, enhancing the resilience of authentication processes against evolving threats and vulnerabilities.

An MFA solution is a critical element in addressing the scalability issues inherent in blockchain networks. To provide robust security measures, this suggested MFA solution incorporates a tiered authentication paradigm that seamlessly integrates device credentials, user authentication, and contextual verification. MFA establishes a multidimensional security strategy by demanding the verification of multiple factors before granting access. This layered approach not only strengthens the authentication process but also cleverly distributes the authentication load among multiple systems, reducing stress on the blockchain network and greatly improving scalability, particularly in terms of processing and storage capacity. Furthermore, implementing a hybrid blockchain approach is a criticalstep toward improving data management in IIoT settings. By carefully balancing the benefits of publicand private blockchains, this paradigm enables the effective management of less important data off- chain while prioritizing the storage of crucial authentication data on the blockchain. This division successfully addresses the scalability issues that often plague blockchain implementations, particularly regarding storage capacity, by ensuring that the blockchain network remains streamlined, efficient, andscalable. By using external storage solutions for less important data and blockchain storage for key data,the MFA solution ensures efficient storage resource utilization, allowing for smooth scaling as the IIoT ecosystem expands. Additionally, incorporating edge computing into the MFA system architecture offers a novel way to accelerate authentication procedures while resolving processing scalability issues. Preliminary authentication checks can be effectively handled locally by leveraging edge devices for processing and verifying MFA factors, such as biometric data or contextual information. This significantly reduces the workload on the central blockchain network and speeds up the overall authentication process. In IIoT situations, where real-time decision-making is critical, this distributed processing technique ensures low latency and high responsiveness, thereby improving the scalability of authentication procedures. In summary, scalable storage and processing capacities are efficiently handled by adopting a hybrid blockchain model and incorporating edge computing into the MFA solution. This approach sets the groundwork for a robust, scalable, and future-ready IIoT ecosystem.

A full solution to the scalability problems present in such contexts is provided by integrating MFA into blockchain-based IIoT authentication systems. This effectively distributes authentication demand and improves user experience. Conventional single-factor authentication techniques may causelatency and performance snags when IIoT networks handle an increasing number of users and devices,jeopardizing efficiency and security. In order to prevent server overloads and maintain system performance, MFA distributes the authentication

workload among many methods, hence mitigating these issues. Examples of these factors include passwords, biometrics, one-time passwords (OTPs), and mobile authenticator apps. Because different devices and user roles require varied levels of security, MFA's flexibility and adaptability are essential for blockchain-based IIoT systems.

Adaptive authentication approaches, for example, can be used with MFA to reduce the numberof factors required based on the risk level of each access attempt. This will reduce the load on the blockchain network and eliminate needless authentication procedures. This flexibility reduces user fatigue from frequent authentication requests, which is a significant problem in high-frequency access scenarios, while simultaneously improving security. Furthermore, by enabling users to authenticate only once and access several services without having to repeatedly log in, MFA's interoperability with SingleSign-On (SSO) systems further enhances scalability by drastically lowering the quantity of authentication transactions handled by the blockchain. A more effective and user-friendly experience results from this seamless integration, which is crucial in industrial environments where productivity can be directly impacted by accessibility. Additionally, fast verification is provided via user-friendly authentication factors like biometrics and push alerts, which lower latency in comparison to conventional blockchain consensus techniques. Through distributed topologies and replicated authentication servers, MFA provides a simplified authentication process while retaining high availability, allowing for uninterrupted operation even in the case of server failures. In addition to improving system stability, this approach solves possible operational errors that have been brought to light in certain blockchain applications, like urban traffic control systems. Moreover, MFA can transferprocessing and storage requirements to cloud providers, enabling real-time scaling in response to demand without requiring major infrastructure changes. This feature is crucial for handling dual-chainauthentication's higher processing load and storage needs in edge computing.

MFA promotes more engagement and satisfaction among users by boosting their sense of security and trust, which is essential for the widespread adoption of blockchain-based IIoT systems. MFA systems are continuously improved through user feedback, ensuring that security, performance, and user experience are all balanced while keeping the system easy to use and accommodating new security threats.

By spreading the authentication load across several factors and services and hence reducing therisk of a single point of failure, multi-factor authentication, or MFA, improves system resilience and efficiency. MFA reduces reliance on a single authentication server by utilizing a variety of authentication techniques, including passwords, biometrics, and one-time

passwords. This helps to prevent widespread access concerns if one technique fails. To make sure that no single server is overloaded, load balancing techniques further divide incoming authentication requests among several servers as illustrated in Figure 3. This method improves system resilience and durability while preserving peak performance and responsiveness.

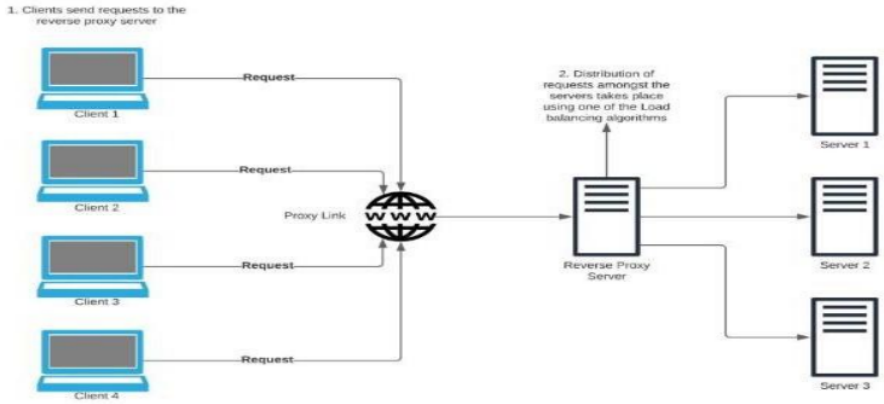

Figure 3: Distribution of load among servers

Another important benefit of MFA is its scalability, which is especially useful when combined with distributed databases and cloud-based authentication systems. Even during periods of high usage, these systems' ability to dynamically distribute resources in response to demand enables them to efficiently handle massive numbers of authentication requests. Additionally, MFA systems have failover and redundancy techniques built in, so if one service goes down, other authentication methods can takeover. By processing requests closer to the user, servers that are geographically distributed reduce latency. Additionally, processing various authentication factors in parallel balances the computational load. Furthermore, dynamic factor selection and monitoring methods are employed by sophisticated MFA systems to adjust to present system loads and anticipate possible bottlenecks. High levels of security, effectiveness, and user happiness are maintained by MFA systems thanks to this all-encompassing, distributed approach.

Using a variety of authentication techniques, MFA significantly enhances security and user experience. MFA provides flexibility and adaptability for authentication. These consist of standard passwords, biometrics such as facial, fingerprint, and voice recognition, and smart cards. USB devices,and OTPs sent by email, text message, or application. Moreover, mobile apps offer authenticator services and push notifications, and behavioural biometrics track mouse and typing patterns. Because of this diversity, MFA may be highly customised to fit the unique requirements of various environments,ranging from consumer apps that need scalable

and user-friendly solutions to enterprise settings with intricate access controls. MFA helps mobile workforces have safe remote access while also supporting regulatory compliance through comprehensive logging and strong authentication methods.

Since MFA is flexible enough to provide multi-layered security with redundant authenticationfactors and adaptive authentication policies that change according to risk levels, it also reduces the danger of single points of failure. Even if one element fails, access is guaranteed via failover mechanisms including backup authentication techniques and ongoing cloud-based service availability.Easy adoption and efficient use are further facilitated by user assistance and education. While easy authentication methods like biometrics and push notifications increase user pleasure, enhanced securitymeasures lower the chance of credential theft and phishing attempts. Organisations can future-proof their authentication systems and retain high security and a great user experience by utilising MFA's adaptability to evolving technologies and customisable implementation options.

By utilizing quick-to-verify authentication factors including OTPs, biometric information, andpush notifications, MFA reduces latency as compared to blockchain-based systems. In contrast to decentralized validation processes and massive computing demands associated with blockchain consensus mechanisms, MFA's localized verification usually necessitates connection with a single server or small cluster, hence decreasing network latency. MFA systems also make use of parallel processing methods and enhanced cryptographic algorithms, which speed verification times and guarantee operational effectiveness. MFA provides quick authentication for financial transactions, business access, e-commerce, and healthcare apps, improving user experience and enabling smooth interactions without sacrificing security.

MFA guarantees that users' regular activities and processes are not disrupted to the greatest extent possible, hence increasing user satisfaction and productivity, by offering speedy and secure authentication options. Furthermore, it is anticipated that advancements in cloud computing, network architecture, and biometric technologies will improve MFA's efficiency by cutting down on latency andstreamlining verification procedures. MFA is still an effective and dependable way to secure access ina variety of settings and apps, even in those where security and user experience are top priorities for businesses.

An MFA solution is a critical element in addressing the scalability issues inherent in blockchain networks. To provide robust security measures, this suggested MFA solution incorporates a tiered authentication paradigm that seamlessly integrates device credentials, user authentication, and contextual verification. MFA establishes a multidimensional security

strategy by demanding the verification of multiple factors before granting access. This layered approach not only strengthens the authentication process but also cleverly distributes the authentication load among multiple systems, reducing stress on the blockchain network and greatly improving scalability, particularly in terms of processing and storage capacity. Furthermore, implementing a hybrid blockchain approach is a criticalstep toward improving data management in IIoT settings. By carefully balancing the benefits of publicand private blockchains, this paradigm enables the effective management of less important data off- chain while prioritizing the storage of crucial authentication data on the blockchain. This division successfully addresses the scalability issues that often plague blockchain implementations, particularly regarding storage capacity, by ensuring that the blockchain network remains streamlined, efficient, andscalable. By using external storage solutions for less important data and blockchain storage for key data,the MFA solution ensures efficient storage resource utilization, allowing for smooth scaling as the IIoT ecosystem expands. Additionally, incorporating edge computing into the MFA system architecture offers a novel way to accelerate authentication procedures while resolving processing scalability issues.Preliminary authentication checks can be effectively handled locally by leveraging edge devices for processing and verifying MFA factors, such as biometric data or contextual information. This significantly reduces the workload on the central blockchain network and speeds up the overall authentication process. In IIoT situations, where real-time decision-making is critical, this distributed processing technique ensures low latency and high responsiveness, thereby improving the scalability ofauthentication procedures. In summary, scalable storage and processing capacities are efficiently handled by adopting a hybrid blockchain model and incorporating edge computing into the MFA solution. This approach sets the groundwork for a robust, scalable, and future-ready IIoT ecosystem.

MFA establishes a robust defence against common cyber-attacks by combining multiple verification elements such as passwords, fingerprints, and facial recognition. This layered approach significantly reduces the vulnerabilities present in single-factor authentication techniques, which are prone to brute force attacks, device loss, and biometric spoofing. By requiring multiple forms of authentication, MFA raises the security bar for potential attackers, enhancing the overall security postureand providing strong protection against unauthorized access.

MFA also fortifies defenses against account takeover (ATO) incidents, brute force attacks, phishing attempts, and man-in-the-middle attacks. For instance, even if users fall for phishing scams, MFA prevents attackers from accessing accounts without the additional

authentication factors. Rate- limiting restrictions and the ability to issue further challenges in response to suspicious activity discourage brute force attacks and bolster defenses against ATO situations. In blockchain systems, MFA ensures only authenticated nodes participate in consensus, reducing the risk of attacks like the 51% attack. Multi-signature wallets, often linked with MFA, require multiple approvals for transactions, enhancing protection against fraud and unauthorized access. Thus, MFA is crucial for both traditional cybersecurity and securing advanced systems like blockchain, safeguarding against evolving threats and vulnerabilities.

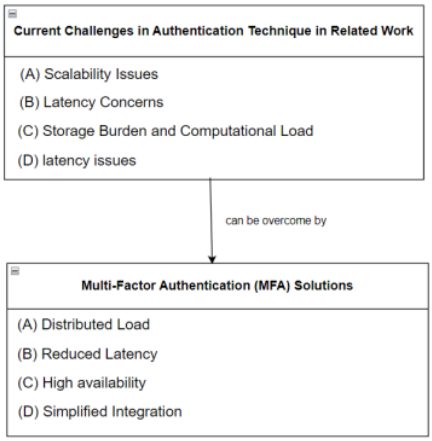

Figure 4: Summary of Related Solution

VI. RESULT AND ANALYSIS

Based on research in [13], the first problem statement is Authentication and Privacy Challenges in Industrial IoT (IIoT), in other words, ensuring a high level of privacy and safety for data within IIoT environment. This is crucial because computers and devices from various settings are interconnected, causing some potential security vulnerabilities. Our proposed solution that can overcome this problemis to apply MFA.

In [14], MFA proposes multiple verification layers to increase their security. For instance, passwords, biometric verification and some security tokens, such as OTPs. All these additional factorscan indirectly increase the difficulty for unauthorized user to gain access to any website, apps and so on. Traditional single-factor authentication such as typing a password only is vulnerable to various attacks, including phishing and brute force. Moreover, MFA provides adaptive authentication, where it can adjust the level of authenticationbased on the condition needed. [15] propose level of authentication can be verify using the IP addresses,login times or user agents. System is able to compute risk level for a given authentication. Let have anexample, if a user attempts to log in from another different location or device, the system

will request extra authentication steps, like needing user to input OTPs sent to their respective mobile device. By lowering needless friction during routine, low-risk access attempts, contextual awareness not only improves user experience but also strengthens security by decreasing risks associated with atypical or potentially malicious activities. With so many interconnected systems and devices in the IIoT, such adaptive authentication offers strong security against illegal access while preserving operationaleffectiveness. Below figure 5 that shows multiple levels of authentication versus the attack success rate.

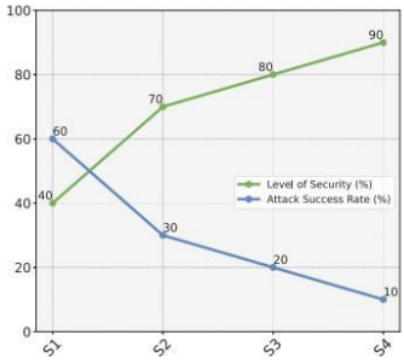

Figure 5: Level of Security and Attack Success Rate settings

Based on figure 5, it proves that continuous increases of the level of security, the rate decreasesat the same time as is getting harder for unauthorized users to access. At figure 5, it shows that at S1, we can see that there are highly vulnerable to attack, which attack success rate is up to 60% while levelof security is only 40%. It shows it is the least secure level of security with the overall alternative. Increasing another level of security to S2, level of security (LS) rise to 30% and attack success rate (ASR) reduce to 30%, showing that improvement of security from S2 to S1. Furthermore, LS increaseto 80%, while ASR reduce to 20%, making it harder for unauthorized user to access it. At the end, S4 uses all authentication setting have, contributing to LS of 90% and ASR of 10%, is the most powerful defence against unauthorized access attempts.

In addition, there is a formula to calculate Attack Success Rate, which is

$$ASR = \frac{S}{S+F} \times 100$$

where ASR represent percentage of attempts that succeed rate, S is the number of successful attack attempts and F is number of failed attack attempt. By using this formula, we able to find out how the level of security affect the attack success rate by unauthorized user.

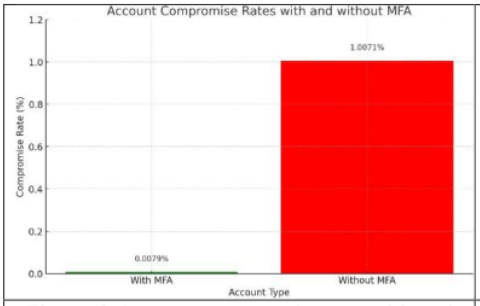

Figure 6: Account compromise rate with and without

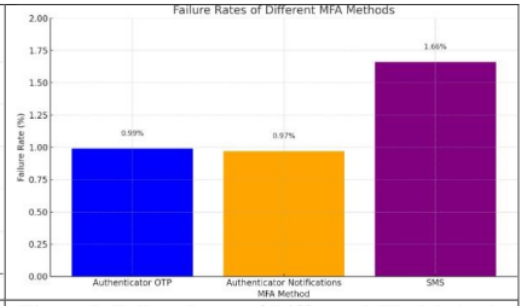

Figure 7: Failure Rates of Different MFA Methods

Next, the implementation of MFA significantly enhances security within the IIoT, particularly when combined with blockchain technology. The figure 6 underscores the effectiveness of MFA, illustrating a substantial reduction in account compromise rates from 1.0071% without MFA to a mere0.0079% with MFA. This stark difference highlights the robustness of MFA in fortifying account security by requiring multiple forms of verification, such as passwords, OTPs, and biometric data. Thecomparison of failure rates among different MFA methods, showing in figure 5—0.99% for Authenticator OTP, 0.97% for Authenticator Notifications, and 1.66% for SMS—further demonstratesthe reliability and flexibility of MFA solutions. These methods can be seamlessly integrated into IIoT systems, ensuring a versatile and robust security framework.

In the context of IIoT, scalability is a critical issue due to the extensive network of interconnected devices and the necessity for secure, efficient communication. Blockchain technology, with its decentralized nature, inherently supports scalability but often struggles with high computationalloads and latency due to consensus mechanisms. Here, MFA's efficiency plays a pivotal role. By distributing the authentication load across multiple factors and services, MFA alleviates the computational burden on blockchain networks, thereby enhancing performance and scalability. The datademonstrates that with MFA, the number of compromises significantly drops, meaning fewer security breaches need to be processed and managed by the blockchain network. This reduction in incidents helps maintain network efficiency even as the system scales.

Moreover, MFA's quick verification processes reduce latency, a significant advantage over traditional consensus-based authentication mechanisms in blockchain. This reduction in latency not only improves user experience but also ensures swift and secure data transmission across the IIoT network. As seen in the graphical representation, methods like OTPs and Authenticator Notifications have low failure rates, suggesting high reliability and fast

processing times which are crucial for maintaining scalability in IIoT systems.

Furthermore, as IIoT networks scale, the risk of cyber-attacks escalates. MFA provides a scalable security solution that grows with the network, maintaining robust protection as the number ofdevices and transactions increases. This scalability, coupled with enhanced security, addresses the dual challenges faced by IIoT systems. Additionally, MFA's seamless integration into existing blockchain frameworks offers an extra security layer without necessitating significant infrastructural changes. This integration is crucial for efficiently scaling IIoT networks while ensuring high security.

In summary, leveraging MFA within blockchain technology offers a comprehensive solution toenhance security in IIoT. It addresses scalability issues by reducing computational load, distributing authentication efforts, lowering latency, and providing robust, scalable security. The graphical data support the effectiveness of MFA in significantly lowering account compromise rates and maintaining high efficiency and reliability, making MFA an essential component in developing secure, efficient, and scalable IIoT systems, fulfilling the overarching goal of enhancing security in IIoT through advanced authentication solutions leveraging blockchain technology.

VII. CONCLUSION

In conclusion, MFA emerges as a cornerstone solution for bolstering security, scalability, and operational reliability within blockchain-based and industrial IoT (IIoT) environments. By mandating multiple authentication factors—such as passwords, biometrics, or tokens—MFA significantly enhances access controls, fortifying defenses against unauthorized access and cyber threats. This comprehensive approach not only mitigates the risks associated with single-factor authentication but also instills confidence in securing sensitive data across diverse industries, including healthcare, finance, and manufacturing. Moreover, MFA's inherent scalability ensures seamless adaptation to increasing user and device volumes, sustaining high availability and operational continuity essential for critical applications like urban infrastructure management. Its integration into existing authentication infrastructures facilitates compliance with stringent regulatory standards, ensuring organizations meet data protection requirements without overhauling established systems. Looking forward, ongoing advancements in MFA technologies should focus on enhancing user experience through intuitive interfaces and streamlined workflows, while also promoting interoperability across different platforms and systems. By continuously evolving to address emerging cybersecurity challenges, MFA stands poised to uphold the integrity and resilience of digital ecosystems,

supporting sustainable growth and innovation in an increasingly interconnected world.

VIII. ACKNOWLEDGMENTS

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

REFERENCE

[1] Almadani, M. S., & Hussain, F. K. (2023). Implementing a Secure Blockchain-Based Wallet System with Multi-Factor Authentication. In *2023 IEEE International Conference on e-Business Engineering (ICEBE)* (pp. 23-30). Sydney, Australia. https://doi.org/10.1109/ICEBE59045.2023.00010

[2] ALSaleem, B. O., & Alshoshan, A. I. (2021). Multi-Factor Authentication to Systems Login. In *2021 National Computing Colleges Conference (NCCC)* (pp. 1-4). Taif, Saudi Arabia. https://doi.org/10.1109/NCCC49330.2021.9428806

[3] Bala, R., & Manoharan, R. (2022). Blockchain based Secure and Effective Authentication Mechanism for 5G Networks. In *2022 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS)* (pp. 1-6). Pune, India. https://doi.org/10.1109/ICBDS53701.2022.9936018

[4] Djonov, M., Galabov, M., & Georgieva-Trifonova, T. (2021). Solving IoT Security and Scalability Challenges with Blockchain. In *2021 5th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT)* (pp. 52-56). Ankara, Turkey. https://doi.org/10.1109/ISMSIT52890.2021.9604700

[5] Fauzi, A. H., & Khan, A. S. (2017). Threats Advancement in Primary User Emulation Attack and Spectrum Sensing Data Falsification (SSDF) Attack in Cognitive Radio Network (CRN) for 5G Wireless Network Environment. *Journal of Telecommunication, Electronic and Computer Engineering (JTEC, 9*(2-10), 179-183.

[6] Fedorov, I. R., Getmaniuk, I. B., & Bezzateev, S. V. (2023). Blockchain-Based Device Authentication Method in Industrial Internet of Things. In *2023 15th International Congress on Ultra-Modern Telecommunications and Control Systems and Workshops (ICUMT)* (pp. 243-249). https://doi.org/10.1109/ICUMT61075.2023.10333273

[7] Gebremichael, T., et al. (2020). Security and Privacy in the Industrial Internet of Things: Current Standards and Future Challenges. *IEEE Access, 8*, 152351-152366. https://doi.org/10.1109/ACCESS.2020.3016937

[8] Gong-Guo, Z., & Wan, Z. (2021, April). Blockchain-based IoT security authentication system. In *2021 International Conference on Computer, Blockchain and Financial Development (CBFD)*. https://doi.org/10.1109/cbfd52659.2021.00090

[9] Huang, Y., Jing, H., Li, C., & Hao, Y. (2021). Research on Intelligent Terminal Authentication Strategy Based on Blockchain. In *2021 2nd International Conference on Intelligent Computing and Human-Computer Interaction (ICHCI)* (pp. 23-26). Shenyang, China. https://doi.org/10.1109/ICHCI54629.2021.00012

[10] Jian, W., Xu, J., Liang, W., & Li, K.-C. (2022). Dual Chain Authentication and Key Agreement Protocol Based on Blockchain Technology in Edge Computing. In *2022 IEEE 24th International Conference on High Performance Computing & Communications; 8th International Conference on Data Science & Systems; 20th International Conference on Smart City; 8th International Conference on Dependability in Sensor, Cloud & Big Data Systems & Application (HPCC/DSS/SmartCity/DependSys)* (pp. 396-401). Hainan, China. https://doi.org/10.1109/HPCC-DSS-SmartCity-DependSys57074.2022.00082

[11] Khan, A. A., Bourouis, S., Kamruzzaman, M. M., Hadjouni, M., Shaikh, Z. A., Laghari, A. A., Elmannai, H., & Dhahbi, S. (2023). Data Security in Healthcare Industrial Internet of Things With Blockchain. *IEEE Sensors Journal, 23*(20), 25144-25151. https://doi.org/10.1109/JSEN.2023.3273851

[12] Khan, A. S., Abdullah, J., Zen, K., & Tarmizi, S. (2017). Secure and Scalable Group Rekeying for Mobile Multihop Relay Network. *Advanced Science Letters, 23*(6), 5242-5245.

[13] Khan, A. S., Halikul, I., & Abdullah, N. F. J. (2015). Secure Authentication and Key Management Protocols for Mobile Multihop WiMAX Networks. *Jurnal Teknologi, 73*(1), 75-81.

[14] Khan, A. S., Javed, Y., Abdullah, J., Nazim, J. M., & Khan, N. (2017). Security Issues in 5G Device to Device Communication. *IJCSNS, 17*(5), 366.

[15] Khan, A. S., Mehdi, M. H., Uddin, R., Abbasi, A. R., & Nisar, K. (2023). Ensemble Based Automotive Paint Surface Defect Detection Augmented by Order Statistics Filtering Using Machine Learning. *Authorea Preprints*.

[16] Khan, A. S., Yahya, M. I. B., Zen, K. B., Abdullah, J. B., Rashid, R. B. A., Javed, Y., Khan, N. A., & Mostafa, A. M. (2023). Blockchain-Based Lightweight Multifactor Authentication for Cell-Free in Ultra-Dense 6G-Based (6-CMAS) Cellular Network. *IEEE Access, 11*, 20524-20541.

[17] Khan, N., Abdullah, J., & Khan, A. S. (2017). Defending Malicious Script Attacks Using Machine Learning Classifiers. *Wireless Communications and Mobile Computing, 2017*.

[18] Khan, S., Abdullah, J., Khan, N., Julahi, A. A., & Tarmizi, S. (2017). Quantum-Elliptic Curve Cryptography for Multihop Communication in 5G Networks. *International Journal of Computer Science and Network Security (IJCSNS, 17*(5), 357-365.

[19] Kumari, A., Tanwar, S., Tyagi, S., & Kumar, N. (2021). Blockchain-Based Massive Data Dissemination Handling in IIoT Environment. *IEEE Network, 35*(1), 318-325. https://doi.org/10.1109/MNET.011.2000355

[20] Morais, D., Zúquete, A., & Mendes, A. (2023). Adaptive, Multi-Factor Authentication as a Service for Web Applications. In *2023 7th Cyber Security in Networking Conference (CSNet)* (pp. 74-80). Montreal, QC, Canada. https://doi.org/10.1109/CSNet59123.2023.10339695

[21] Rathee, G., Kerrache, C. A., & Lahby, M. (2023). TrustBlkSys: A Trusted and Blockchained Cybersecure System for IIoT. *IEEE Transactions on Industrial Informatics, 19*(2), 1592-1599. https://doi.org/10.1109/TII.2022.3182984

[22] Shoaib, M., Ullah, A., Abbasi, I. A., Algarni, F., & Khan, A. S. (2023). Augmenting the Robustness and Efficiency of Violence Detection Systems for Surveillance and Non-Surveillance Scenarios. *IEEE Access, 11*, 123295-123313.

[23] Shukla, H., & Bhushan, B. (2023). Empowering Biometrics Authentication System Using Decentralized Blockchain Based Applications. In *2023 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS)* (pp. 1177-1182). Greater Noida, India. https://doi.org/10.1109/ICCCIS60361.2023.10425327

[24] Vekariya, D., Rastogi, A., Priyadarshini, R., Patil, M., Kumar, M. S., & Pant, B. (2023). Mengers Authentication for efficient security system using Blockchain technology for Industrial IoT (IIOT) systems. In *2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)* (pp. 894-896). Greater Noida, India. https://doi.org/10.1109/ICACITE57410.2023.10182454

[25] Zen, K., Javed, M., Lenando, H. B., Zen, H., & Khan, A. S. (2015). Intelligent Coordinator Selection Mechanism (ICSM) for IEEE 802.15.4 Beacon-Enabled MAC Protocol in Mobile Wireless Sensor Networks. *International Review on Computers and Software, 10*(2), 164.

[26] Zubair, S., Fisal, N., Abazeed, M. B., Salihu, B. A., & Khan, A. S. (2015). Lightweight Distributed Geographical: A Lightweight Distributed Protocol for Virtual Clustering in Geographical Forwarding Cognitive Radio Sensor Networks. *International Journal of Communication Systems, 28*(1), 1-18.

Enhancing Security in Industrial IoT: Authentication Solutions Leveraging Blockchain Technology

ORIGINALITY REPORT

6%	4%	3%	0%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	international.aripi.or.id Internet Source	1%
2	ijaseit.insightsociety.org Internet Source	1%
3	Aparna Kumari, Sudeep Tanwar, Sudhanshu Tyagi, Neeraj Kumar. "Blockchain-Based Massive Data Dissemination Handling in IIoT Environment", IEEE Network, 2020 Publication	<1%
4	Mwaheb S. Almadani, Farookh Khadeer Hussain. "Implementing a Secure Blockchain-Based Wallet System with Multi-Factor Authentication", 2023 IEEE International Conference on e-Business Engineering (ICEBE), 2023 Publication	<1%
5	David Morais, André Zúquete, António Mendes. "Adaptive, Multi-Factor Authentication as a Service for Web	<1%

Applications", 2023 7th Cyber Security in Networking Conference (CSNet), 2023
Publication

6	Ivan R. Fedorov, Ivan B. Getmaniuk, Sergey V. Bezzateev. "Blockchain-Based Device Authentication Method in Industrial Internet of Things", 2023 15th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2023 Publication	<1 %
7	Harsh Shukla, Bharat Bhushan. "Empowering Biometrics Authentication System Using Decentralized Blockchain Based Applications", 2023 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS), 2023 Publication	<1 %
8	Submitted to University of Johannsburg Student Paper	<1 %
9	Kartinah Zen, Muhammad Javed, Halikul Bin Lenando, Hushairi Zen, Adnan Shahid Khan. "Intelligent Coordinator Selection Mechanism (ICSM) for IEEE802.15.4 Beacon-Enabled MAC Protocol in Mobile Wireless Sensor Networks", International Review on Computers and Software (IRECOS), 2015 Publication	<1 %

10	cps-vo.org Internet Source	<1 %
11	www.researchgate.net Internet Source	<1 %
12	www.scilit.net Internet Source	<1 %
13	R Bala, R Manoharan. "Blockchain based Secure and Effective Authentication Mechanism for 5G Networks", 2022 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS), 2022 Publication	<1 %
14	journals.plos.org Internet Source	<1 %
15	libweb.kpfu.ru Internet Source	<1 %
16	norma.ncirl.ie Internet Source	<1 %
17	publisher.unimas.my Internet Source	<1 %
18	semarakilmu.com.my Internet Source	<1 %
19	shura.shu.ac.uk Internet Source	<1 %

20	www.iosrjournals.org Internet Source	<1%

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		

Enhancing Security in Industrial IoT: Authentication Solutions Leveraging Blockchain Technology

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

PAGE 19