International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2024/33 Volume 11, Issue 4, July – August (2024)

RESEARCH ARTICLE

Decentralized Identity Management for Industrial Internet of Things Utilizing Blockchain-Enhanced Multi-Factor Authentication

Mohammed Al Qurashi
Computer Science Department, Faculty of Computing and Information, Al-Baha University, Al-Baha, Saudi Arabia.
✉ malqurashi@bu.edu.sa

Received: 29 May 2024 / Revised: 29 July 2024 / Accepted: 09 August 2024 / Published: 31 August 2024

Abstract – The Industrial Internet of Things (IIoT) is crucial to contemporary industrial ecosystems because it increases efficiency and innovation. However, its swift growth also poses some serious security challenges, especially concerning the management of identities. This research paper introduces a new approach to strengthen IIoT security by using a Decentralised Identity Management System with Blockchain-based MFA. This study suggests an architecture for IIoT digital identity management that involves a private Blockchain network along with smart contracts and different types of MFA to build up one secure, reliable, and tamper-proof system. The approach is evaluated using a wide simulation environment, copying real-world scenarios of IIoT and attack vectors. Key performance metrics used in the analysis of the system include Authentication Success Rate, Incident Detection Rate, System Resilience Score, and Average Response Time under different circumstances, such as normal operations and attempts to break security. Results show great efficacy in authenticating legitimate access, high resistance against common cyber-attacks such as brute force and identity spoofing, and the best combination of security versus performance. This research adds significant value to the IIoT security area because it offers a holistic approach that can help fill in vital gaps concerning risk points within decentralised systems and, hence, lay the groundwork for safer and more productive industrial operations with digitalisation processes.

Index Terms – IIoT, Blockchain, Multi-Factor Authentication, Identity Management, Decentralisation, Smart Contracts.

1. INTRODUCTION

The Industrial Internet of Things (IIoT) is an unprecedented transformation of the industrial operation space, bringing together cutting-edge convergence of intelligent machines and advanced analytics with improved human-machine interface [1]. Secure and reliable identity management is crucial as the IIoT quickly gains adoption in industries [2]. In a way, one could argue that the IIoT would fall within the larger scope of IoT since it is part of the latter's domain. The IoT concentrates mostly on consumer-level devices such as smart homes and wearables, while IIoT is focused on the industrial application areas. This includes machine-to-machine (M2M) communication, where devices can work, communicate, and exchange data with each other without human interference [3]. Embedded Systems, Machine Learning, Big Data, and Cloud Computing have all contributed to this transformation of Smart Grids [4].

The strength of IIoT is derived from enhancing operational efficiency. The adoption of IIoT solutions across different domains has helped industries such as manufacturing, energy, transportation, and agriculture to boost process efficiency, cut costs, and explore new revenue streams and innovative business models [5]. For example, IIoT-driven predictive maintenance enables companies to anticipate machine breakdowns and carry out routine maintenance promptly, thus cutting down downtime and boosting productivity. There is another form that involves watching supply chains as they transpire to promote immediate deliveries and efficient resource allocation. Nonetheless, just like any developing technology, the spread of IIoT poses challenges, mainly in the fields of security and identity management. Since every connected device is important and performs specific tasks, it requires a reliable system for verifying and authenticating identities [6].

This study intends to develop a robust, transparent, and scalable solution for the vulnerable aspect identified by centralised identity management within the IIoT ecosystem. This paper examines the advantages of decentralisation with special emphasis on the eradication of conventional single points of failure by unleashing Blockchain's immutability and transparency in a resilient identity management framework and integration of multi-factor authentications that augment security measures.

The paper is organized as follows: Section 2 covers the related work, Section 3 discusses the limitations of centralized identity management, Section 4 presents blockchain-based multi-factor authentication for IIoT, Section 5 details the proposed system design and implementation, Section 6 focuses on enhancing security, reliability, and transparency, Section 7 outlines the performance metrics and evaluation,

RESEARCH ARTICLE

Section 8 describes the experimental setup, simulation, and results, and Section 9 concludes the work.

2. RELATED WORK

Several notable studies have been conducted, which include a study by [7] that put forward the MIN-IIoT, a universal support system for multiple identifiers, including identity, names of content, services, locations and IP addresses named multi-identifier network architecture. Identity authentication, Proof of Vote (PoV)-based consensus algorithm and trusted computing technology ensure MIN-IIoT's security. A study by [8] presents HIBEChain, a hierarchical blockchain infrastructure that provides scalable and responsible control of IoT devices and data. Blockchain sharding schemes bring HIBEChain to achieve high scalability through parallel processing, and it also puts into use accountability by identity-based keys. Authors [9] concentrate largely on blockchain-based voting systems that enable participation in and management of voting for voters, candidates, and officials. A transaction performed on a blockchain-based system would be secured, verifiable and transparent within seconds. Most common schemes demand further interactions between the vehicles and infrastructure for identification purposes, which may lead to communication overheads. To deal with these issues authors suggest a new blockchain-based scheme for one-time authentication to secure vehicular communication from malicious members. Authors [10] propose a B-RMA for smart devices and cloud networks that also provide security and privacy. The B-RMA proposed can run simultaneously with the IoT-based smart environment to help decentralise the processing of user authentication requests. Authors in [11] tackle both and share the same solution designing a privacy-preserving challenge-response style authentication and authorisation scheme based on decentralised Identities and verifiable credentials. It supports authenticated encryption for data integrity and confidentiality, allowing decentralised permission management of network participants that frequently change. On the other hand, decentralised identity management using Blockchain can guarantee secure and transparent access to patient data with privacy preservation. A study by [12] suggests a decentralised identity management system for healthcare systems called BDIMHS, built on Hyperledger Indy and Hyperledger Aries-based permissioned Blockchain. Most of them are costly from a computational perspective and have limited performance with currently realised schemes that are centralised. These issues can be addressed by a decentralised and lightweight anonymous identity authentication scheme called DAFL proposed by [13]. Existing approaches are impaired by three critical concerns: Illegal authorisation, key disclosure, and privacy leakage. To combat these issues authors, identify a data governance model using blockchain technology and attribute-based encryption that helps to avoid privacy leakage or the misuse of credentials effectively. Authors in [14] find an algorithm for approximate optimal mechanisms, which is a variety of authentication methods ranging from verbal passwords in antiquity to modern multi-factor authentications. Based on the studies conducted it is evident that there is a high need for a secure and efficient authentication approach for IIoT.

3. LIMITATIONS OF CENTRALISED IDENTITY MANAGEMENT

At the time, most industries sought to adopt the so-called 'centralised' identity management systems, as these seemed rather simple in terms of structuring and implementation. Such systems often depend upon a central authority or server that manages and verifies the identity of its users [15]. The model benefits in several ways in theory, yet due to its inherent centralised nature, it is easily victimable in times when insecurity thrives.

3.1. Single Point of Failure

This is because a centralised approach exposes an entire system to risks in case the central server or authorities are breached. This design flaw can be dangerous, and one break may result in devastating outcomes like those experienced in the industrial setup [15].

3.2. Scalability Issues

The expansion of IIoT may result in the overloading of the central server, with many devices being introduced on the network, resulting in latency problems and possible system crashes [16].

3.3. Data Privacy Concerns

When all data is directed towards a single point (hub), the chances of unauthorised access or data breaching increase. Such information clustering renders it a tempting object for malicious entities and attackers.

3.4. Lack of Transparency

Centralised systems are typically opaque. The centralised approach relies entirely on implicit faith in users and devices, having few ways to validate or audit transactions and authentications.

4. BLOCKCHAIN-BASED MULTI-FACTOR AUTHENTICATION FOR IIOT

IIoT concept marks a paradigm change in industrial activities, where interconnected devices make operations smooth but also create intricate security challenges [17]. Traditional MFA methods, though quite efficient in simpler systems, often do not measure up to the distributed and complicated nature of IIoT [18].

This calls for a strong and dynamic solution something Blockchain technology is poised to deliver.

RESEARCH ARTICLE

4.1. Blockchain's Role in Identity Verification

The concept of a decentralised ledger system, on which the technology for Blockchain is based due to its immutability and transparency, provides an innovative way of implementing IIoT identity verification [19]. It aids in constructing an identity management system without central power, where each IIoT device gets its unique and unalterable identification on the Blockchain. This system allows real-time authentication, which greatly reduces risks such as impersonation or fraud. Smart contracts in Blockchain also simplify the identity verification processes and reduce human errors, which ultimately improves productivity levels [19]. Self-executing, they administer themselves without the need for a third party to confirm their success or failure, making it easy, secure, and reliable. Organisations would be able to guarantee an unalterable and trusted system of authentication for the multitude of devices present in IIoT ecosystems by constructing identity data within a Blockchain [20].

4.2. Integrating MFA: Methods and Benefits

When MFA is combined with Blockchain in IIoT, the typical methods of biometric confirmation, such as a one-time code and hardware token, are built into a structure within the Blockchain [20]. This integration also enhances the security of a system and puts multiple verifications in place, making it tremendously challenging for an unauthorised person to circumvent. The complementary nature of MFA and Blockchain stems from the fact that although a cryptographic system designed to protect credentials can be compromised, it would also provide secure management options for various multi-factor systems [21]. This integration has several benefits: higher security, as there are no vulnerable single points that can fail and an enhanced sense of privacy with the ability to control personal information and device data according to multiple standards for regulation [22]. There are, however, challenges related to this integration. This is characterised by very large entry barriers that include scalability, especially concerning the number of IIoT devices and complexity when integrating them with current systems. In addition, Blockchain must be standardised on multiple platforms to spread adoption. Future research could address such challenges, thus creating a safer and more efficient environment within IIoT.

5. PROPOSED SYSTEM DESIGN AND IMPLEMENTATION

Advanced modern industrial processes such as IioT have given rise to the need for strong security architecture, especially in identity management. The proposed approach aims to deal with this by introducing a decentralised identity management system based on Blockchain technology and MFA combined. This system provides better security, reliability and transparency in IIoT environments. Figure 1. depicts the overview of a proposed approach.

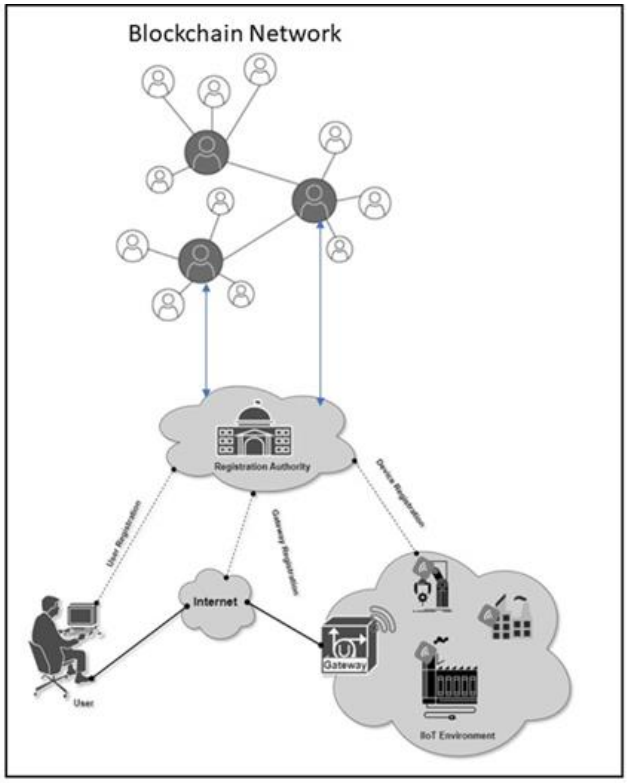


Figure 1 Overview of the Proposed Approach

In the proposed approach, a private permissioned Blockchain network is a key infrastructure that forms an innovative approach to identity management within the IIoT. This IIoT Blockchain network acts as an immutable database that records each digital identity and every transactional activity within the IoT ecosystem.

Each IIoT networked device and user is granted a unique digital identity. This identity, a list of separate verifiable characteristics, is securely stored on the Blockchain. It is also useful for the exact identification of objects and authentication and enables efficient tracking and control over devices and users within a network. Instituting the choice to use a private, permissioned Blockchain is quite tactical because it can guarantee that only known and authorised entities have access or can interact with the network, which gives higher security of control than public ones.

This controlled environment is suitable in the case of industrial applications where a high level of security and integrity are needed. Furthermore, the architecture of this system ensures that all these digital identities are cryptographically protected to remain private and secure from unauthorised access or modification.

RESEARCH ARTICLE

5.1. Blockchain Network

Blockchain technology is a decentralised system that owes its utility to the fact that it eliminates single points of failure. The distributed ledger eliminates most of the risks associated with data breaches or server downtimes that are bound to occur in centralised systems [23]. This decentralisation also makes the system more capable of coping with cyber threats, besides improving its resilience in network management for continued smooth running despite harsh terrains. Furthermore, the Blockchain network has higher consensus mechanisms. These are the mechanisms that prove transactions and changes made to digital identities. There is an important process to ensure that the system remains coherent and credible. Due to the rooted audibility and transparency that is inherent in Blockchain, the system detection for attempted unauthorised access or anomalies comes fast. This database logs every operation and shift so it can be stamped with time for security analysis and compliance issues. Implementing this Blockchain-based system in IIoT will enter into a new, secure era of efficiency [24]. So, Employments IIoT is a solution that offers secure, scalable and resilient identity managements which address some of the most critical problems. This system is not just a preventive measure but an innovative approach for industrial companies to manage their digital landscapes as they become increasingly interconnected [25].

5.2. Identity Registration Module

In the proposed decentralised identity management system for IIoT, a complete process of secure enrollment and digital membership creation was designed utilising all features inherent in Blockchain technology. This is achieved via a rigorous registration protocol for all devices and users in the IIoT network. During the protected enrollment stage, all devices and users undergo a detailed review process. This could mean looking at the devices' make and model or unique identifiers to verify that hardware is traceable items in the network. This step is crucial, especially when building a secure network of devices that assist in minimising risks such as using cheap or counterfeit hardware which may compromise network security. For users, the process involves validating personal and role-relevant credentials as an essential step to ensure that only authenticated individuals can access IIoT network facilitating resources. This verification ensures not only the maintenance of a secure environment but also means allocating proper access levels based on different users' roles and responsibilities, implying the principle of least privilege.

Once the verification process has been made successful, the system is activated. Creating unique digital identities for every device and user is the most important step. Such an identity is a digital image where all necessary identification data has been securely encapsulated. This uniqueness of each identity is essential because it guarantees a special and unquestionable utterness for every participant in the network. Once created, these digital identities are securely stored on the Blockchain. This recording process guarantees that every identity is irrevocable and cannot reset its worth or be altered without the entire network's agreement. With all these digital identities stored in Blockchain, it is adding another level of security by leveraging its built-in properties such as decentralisation transparency and tamper-proof features. Finally, the Blockchain ledger provides a trustworthy and immutable log of all identities, making it an efficient way to handle and safeguard digital personal details in IIoT settings. Such an approach to enrollment and digital ID management not only heightens the security level of IIoT but also streamlines device users. It is critical for an IIoT interconnected world that organisations can retain the levels of integrity and authenticity in their businesses through a proper, stable system.

6. ENHANCING SECURITY, RELIABILITY, AND TRANSPARENCY

In this study for identity management in IIoT, special attention is paid to enhancing security, reliability and transparency. This improvement requires advanced encryption standards for full data protection. This system encrypts all communications via up-to-date cryptographic algorithms and all stored data containing digital identities.

Besides the components mentioned above, our system also conforms to compliance and international security standards. Our system may be developed and conducted according to internationally acceptable security standards and regulations requirements. First of all, this commitment to regulatory compliance not only becomes the most ethical code system but also ensures stakeholders that their data is on the highest levels regarding security and integrity in the IIoT environment.

In addition, this proactive approach of regularly tracking and occasionally auditing our system boosts security. In this study, a good tracking mechanism that monitor the network is employed, which means it can track to ensure there are no irregularities or suspicious activities. As a result of this all-time vigilance, the detection and response periods to potential hazards are greatly reduced, ensuring that one can remain secure from evolving cyber threats.

Additionally, regular security audits have become an integral part of our strategy. It is true that all these sophisticated encryption, rigorous compliance and active monitoring and auditing only increase IIoT system security with enhanced reliability, but the increased exposure above a very respectable level also increases it. Thus, the system should ensure to protection of stakeholders' data and guarantee the integrity of the IIoT environment. It is essential for the proper, secure operation of modern industrial processes.

RESEARCH ARTICLE

7. PERFORMANCE METRICS AND EVALUATION

Table 1 presents the key performance metrics and their respective evaluation methods, which will be utilised to assess the effectiveness of the proposed approach.

Table 1 Performance Metrics

Performance Metric	Description
Authentication Success Rate	Tracks the effectiveness of the MFA system in accurately authenticating legitimate users.
System Resilience Score	Measures the system's ability to withstand and counter security threats and unauthorised access attempts.
Incident Detection Rate	Assesses the efficiency of the system in identifying and responding to security incidents.
Average Response Time	Evaluates the system's operational efficiency, ensuring that security measures do not unduly impact performance.

8. EXPERIMENTAL SETUP, SIMULATION AND RESULTS

This study uses a comprehensive simulation environment that allows validating the efficiency of a Decentralised Identity Management System for IIoT with Blockchain-based Multi-Factor Authentication. The simulation environment involves several pieces of software and hardware, each configured to mimic the complex dynamics encountered in a real-world IIoT ecosystem.

The platforms used include Ethereum with Ganache Hyperledger Fabric for the Blockchain network. Such tools enable us to implement a kind of Blockchain environment in which relevant smart contracts regarding identity management and access control are deployed and thoroughly tested. This is complemented by the virtual modelling of the IIoT network using NS3 Network Simulator 3. This configuration is similar to the intricacies of IIoT infrastructures, which include a network of sensors, actuators and control systems. To properly simulate Multi-Factor Authentication processes, such as OTPs, biometric data and hardware tokens were used along with custom scripts for the simulation of biometrics. This allows for a complete assessment of the MFA system in the proposed framework. Python-based Pandas and Matplotlib libraries are used to analyse the data in our research. These tools provide the support of careful data collection, processing and visualising experimental results in an attempt to obtain insight based on findings.

For this simulation, the hardware setup includes high-performance computers with multi-core processors, 16GB RAM, and 500GD SSD storage. This powerful infrastructure is necessary to effectively serve the simulation software and cope with heavy data processing requirements. Where a hybrid simulation – virtual and physical components – is preferred, networking equipment such as routers and switches that support gigabit Eoethernet with compatibility of IoT devices were implemented.

In this study well-defined parameters were used for simulation which include block time and transaction limits for Blockchain, specific smart contract details, the network configuration, whether public or private, and how many nodes are involved. Settings of IIoT networks take into consideration the number of nodes, variety of devices and communication protocols such as MQTT or CoAP. Network topology, bandwidth and latency are all adjusted to simulate real-world conditions. The configuration parameters of the MFA system include different types of authentication factors, their corresponding authentication protocols, and response time limits. Network latency, throughput and response times are also measured along with key performance metrics such as authentication success rate system resilience score and incident detection rate. Security settings are one of the most critical aspects, including simulation of diverse security attacks like DDoS, and man-in-the-middle, and using security protocols such as TLS / SSL for data encryption. This integrated simulation approach allows for a detailed analysis of the proposed decentralised identity management system to determine its feasibility, security, and efficiency in an IIoT scenario.

Scenarios shown in Table 2, elucidate the crucial insights regarding the performance and capabilities of security in terms of protecting base systems. System activity in normal operation produced a remarkable Authentication Success Rate of 98% a perfect Incident Detection rate and an impressive high score for its Resilience Score at around 99%. The average response time was a quick 150 milliseconds, showing that the system operated well in normal circumstances. Biometric authentication took it slightly down to 96% with a marginally higher response time of about is milliseconds mainly due to the additional processing required for biometric verification but still able to provide high security and detection rates. With a 95% success rate for OTP Authentication and a 98% resilience score, a response time of 180 milliseconds. This minimal reduction in performance compared to biometric methods can be attributed to external dependencies, including mobile network delays. Hardware Token Authentication proved to be much more successful, with a 97% success rate and faster reaction time of a mere 170 milliseconds, confirming the superiority and efficiency of hardware-based utility tokens. In response to a Brute Force attack, the system effectively defended itself evidenced by an

RESEARCH ARTICLE

Authentication Success Rate of 0% for the perpetrators, yet recorded perfect Resilience Scores even with increased responses timed at 30 milliseconds. This increase in response time can reasonably be ascribed to the fact that the system is actively engaged into fighting back this attack. Similarly, the successful resistance against Identity Spoofing Attempts resulted in a 100% Resilience Score; however, the Incident Detection Rate slumped to 95%. As 250 milliseconds marked the response time in this case. A comparison of results obtained in different scenarios is depicted in Figure 2.

Table 2 Test Scenario

Test Scenario	Authentication Success Rate	Incident Detection	Rate System Resilience Score	Average Response Time (ms)
Normal Operation	98%	100%	99%	150
Biometric Authentication	96%	100%	99%	200
OTP Authentication	95%	100%	98%	180
Hardware Token Authentication	97%	100%	99%	170
Brute Force Attack	0%	100%	100%	300

The scalability of the proposed identity management system, for large-scale IIoT deployments is crucial. As the number of IIoT devices increases challenges like network congestion, resource distribution, data size, delays and security become more prominent. To tackle these challenges implementing a network structure to alleviate congestion utilizing resource management methods such as load balancing and dynamic resource allocation and employing data aggregation and compression techniques to handle large amounts of data will be helpful.

The increasing performance overhead, particularly in processing time, latency, and system throughput, is for that purpose that Blockchain and MFA are included in this decentralised identity management system. The experimental results showed an increase in the processing time from 50 to 75 milliseconds, an increase in latency from 100 to 150 milliseconds, and a decrease in throughput from 2000 to 1800 authentication requests per second. These impacts are the results of the inclusion of additional cryptographic procedures and blockchain transaction verification processes. This study proposes an optimised implementation of blockchain that includes sharding and faster consensus techniques, advanced load balancing and dynamic resource allocation, and edge computing to offload authentication operations for mitigating these impacts. Although additional costs will be added by the inclusion of blockchain and MFA, the security benefits are huge, ensuring a fine marriage between tight security measures and efficient system operation.

These experimental outcomes, proving the simulation of various operational and adversarial conditions, demonstrate that the proposed decentralised identity management system is a robust, reliable and adaptable concept for an IIoT environment. All the variations observed using different authentication methods and even under attack conditions show why this system can balance security with performance. This balance is critical for properly handling security in IIoT systems because, quite often, the chances associated with data integrity and system reliability are huge.

RESEARCH ARTICLE

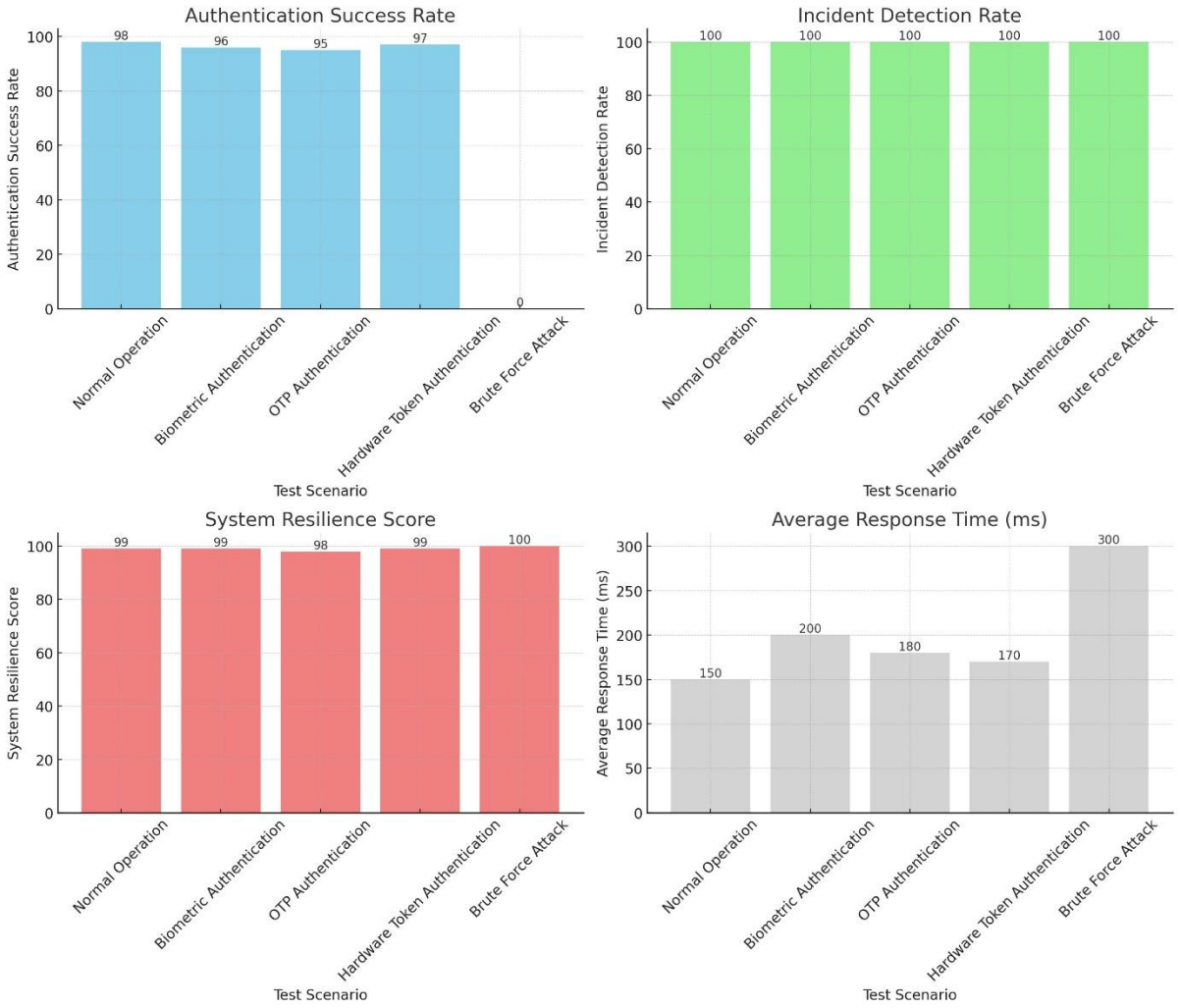


Figure 2 Comparison of Results

9. CONCLUSION

This research paper has provided a comprehensive strategy to improve identity management in IIoT by combining Blockchain technology and Multi-Factor Authentication MFA. As industrial processes become more interconnected and data-driven, the need for strong security mechanisms becomes critical according to what is proposed here incorporation of the immutable and decentralised features typical to Blockchain together with multi-factor authentication guarantees security, durability and transparency levels. The experimental results and performance evaluations have indicated that this approach is feasible in different active situations. The system provided very high authentication success rates and efficient incident detection, including robust integrity against advanced cyber threats. The balance between operational efficiency and strict security measures is determined by the average response time, which means that the system version may perform in highly dynamic industrial fields without diminishing performance levels. Furthermore, international standards, regulatory compliance, continuous monitoring, and regular security reviews strengthen the system's strength. Instead, this approach not only solves the issue of current security issues in IIoT but also sets up a roadmap for future development and improvement in industrial cybersecurity. In light of the results, it can be said that Blockchain and MFA integration into IIoT identity management is a promising direction to protect sensitive industrial infrastructure. Overall, this research is an important contribution to the IIoT security sphere since it provides a flexible and scalable framework that can be further improved with evolving technological trends and emerging threats in this domain.

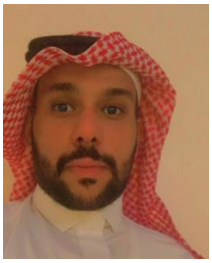
REFERENCES

[1] Castillón, D. C., Martín, J. C., Suarez, D. P. M., Martínez, Á. R., & Álvarez, V. L. (2020). Automation trends in industrial networks and

RESEARCH ARTICLE

IIoT. Industrial IoT: Challenges, Design Principles, Applications, and Security, 161-187.
[2] Javaid, M., Haleem, A., Singh, R. P., Rab, S., & Suman, R. (2021). Upgrading the manufacturing sector via applications of industrial internet of things (IIoT). Sensors International, 2, 100129.
[3] Salama, R., Altrjman, C., & Al-Turjman, F. (2023). An overview of the Internet of Things (IoT) and Machine to Machine (M2M) Communications. NEU Journal for Artificial Intelligence and Internet of Things, 2(3).
[4] Khan, A. S., Yahya, M. I. B., Zen, K. B., Abdullah, J. B., Rashid, R. B. A., Javed, Y., ... & 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.
[5] Leminen, S., Rajahonka, M., Wendelin, R., & Westerlund, M. (2020). Industrial internet of things business models in the machine-to-machine context. Industrial marketing management, 84, 298-311.
[6] Mamdouh, M., Awad, A. I., Khalaf, A. A., & Hamed, H. F. (2021). Authentication and identity management of IoHT devices: achievements, challenges, and future directions. Computers & Security, 111, 102491.
[7] Wang, Y., Li, H., Huang, T., Zhang, X., & Bai, Y. (2021). Scalable identifier system for industrial internet based on multi-identifier network architecture. IEEE Internet of Things Journal.
[8] Wan, Z., Liu, W., & Cui, H. (2022). HIBEChain: A hierarchical identity-based blockchain system for large-scale IoT. IEEE Transactions on Dependable and Secure Computing, 20(2), 1286-1301.
[9] Singh, J., Rastogi, U., Goel, Y., & Gupta, B. (2023). Blockchain-based decentralized voting system security Perspective: Safe and secure for digital voting system. arXiv preprint arXiv:2303.06306.
[10] Noh, J., Kwon, Y., Son, J., & Cho, S. (2022). Blockchain-based one-time authentication for secure v2x communication against insiders and authority compromise attacks. IEEE Internet of Things Journal, 10(7), 6235-6248.
[11] Deebak, B. D., Memon, F. H., Khowaja, S. A., Dev, K., Wang, W., Qureshi, N. M. F., & Su, C. (2022). A Lightweight Blockchain-Based Remote Mutual Authentication for AI-Empowered IoT Sustainable Computing Systems. IEEE Internet of Things Journal, 10(8), 6652-6660.
[12] Philipp, A., & Küpper, A. (2023). DAXiot: A Decentralized Authentication and Authorization Scheme for Dynamic IoT Networks. arXiv preprint arXiv:2307.06919.
[13] Fan, M., Zhang, Z., Li, Z., Sun, G., Yu, H., & Guizani, M. (2023). Blockchain-Based Decentralized and Lightweight Anonymous Authentication for Federated Learning. IEEE Transactions on Vehicular Technology.
[14] Zhang, J., & Datta, A. (2023). Blockchain-enabled Data Governance for Privacy-Preserved Sharing of Confidential Data. arXiv e-prints, arXiv-2309.
[15] Usmonov, M. T. O. G. L. (2021). Autentification, authorization and administration. Science and Education, 2(7), 233-242.
[16] Wu, Y., Dai, H. N., & Wang, H. (2020). Convergence of blockchain and edge computing for secure and scalable IIoT critical infrastructures in industry 4.0. IEEE Internet of Things Journal, 8(4), 2300-2317.
[17] Lin, C. C., Tsai, C. T., Liu, Y. L., Chang, T. T., & Chang, Y. S. (2023). Security and privacy in 5g-iiot smart factories: Novel approaches, trends, and challenges. Mobile Networks and Applications, 1-16.
[18] Khan, N. A. (2022). 5G Network: Techniques to Increase Quality of Service and Quality of Experience. Int. J. Comput. Netw. Appl (IJCNA), 9, 476-496.
[19] Karamitsos, I., Papadaki, M., Al-Hussaeni, K., & Kanavos, A. (2023). Transforming Airport Security: Enhancing Efficiency through Blockchain Smart Contracts. Electronics, 12(21), 4492.
[20] Igboanusi, I. S., Dirgantoro, K. P., Lee, J. M., & Kim, D. S. (2021). Blockchain side implementation of pure wallet (pw): An offline transaction architecture. ICT Express, 7(3), 327-334.
[21] Khan, N. A. (2022). PKI-Based security enhancement for IoT in 5G networks. In Inventive Computation and Information Technologies: Proceedings of ICICIT 2021 (pp. 217-225). Singapore: Springer Nature Singapore.
[22] Khan, N. A., & Al Qurashi, M. (2023). Security Tradeoff in Network Virtualization and Their Countermeasures. In Inventive Computation and Information Technologies: Proceedings of ICICIT 2022 (pp. 741-749). Singapore: Springer Nature Singapore.
[23] Prewett, K. W., Prescott, G. L., & Phillips, K. (2020). Blockchain adoption is inevitable—Barriers and risks remain. Journal of Corporate accounting & finance, 31(2), 21-28.
[24] Khan, A. S., Javed, Y., Saqib, R. M., Ahmad, Z., Abdullah, J., Zen, K., & Khan, N. A. (2022). Lightweight multifactor authentication scheme for nextgen cellular networks. IEEE access, 10, 31273-31288.
[25] Wang, W., Xu, H., Alazab, M., Gadekallu, T. R., Han, Z., & Su, C. (2021). Blockchain-based reliable and efficient certificateless signature for IioT devices. IEEE transactions on industrial informatics, 18(10), 7059-7067.

Author



Dr. Mohammed Al Qurashi is Assistant Professor Cybersecurity at the department of Computer & Technology of the University of Al-Baha. His research is situated in the field of Cybersecurity and Artificial Intelligence, with special focus on Blockchain Technology and future networks. Mohammed has co-authored in renowned international peer-reviewed conference and journal in his area of expertise. Finally, in the context of his expertise, he served with Security Threats Response Management Team at Saudi Aramco.

How to cite this article:

Mohammed Al Qurashi, " Decentralized Identity Management for Industrial Internet of Things Utilizing Blockchain-Enhanced Multi-Factor Authentication ", International Journal of Computer Networks and Applications (IJCNA), 11(4), PP: 519-526, 2024, DOI: 10.22247/ijcna/2024/33.