IJEEMCS : International Journal of Electrical Engineering, Mathematics and Computer Science
Vol. 1, No.3 September 2024
e-ISSN: 3048-1945, p-ISSN : 3048-1910, Page 01-24
DOI: https://doi.org/10.62951/ijeemcs.v1i3.16
Available online at: https://international.arteii.or.id/index.php/IJEEMCS/==

Blockchain-Enhanced Multi-Factor Authentication for Securing IIoT

Allyson Eddy[1], Bram Zoe anak Guillan[1], Einstein Kent Elias[1], Eldren Aniell[1], Shircrayson bin Simon[1], Muhammad Faisal[2]

[1] Faculty of Computer Science and Information Technology, Universiti Malaysia Sarawak, Kota Samarahan 94300, Malaysia
[2] Director HRIMS, Ministry of Human Rights
74044@siswa.unimas.my, 74299@siswa.unimas.my, 73427@siswa.unimas.my, 73428@siswa.unimas.my, 77358@siswa.unimas.my, dr.faisalshabbir88@gmail.com

Address: Jln Datuk Mohammad Musa, 94300 Kota Samarahan, Sarawak, Malaysia
Author Corresprodence : 74044@siswa.unimas.my

Abstract. *This paper proposes Blockchain-Enhanced Multi-Factor Authentication (BEMFA) to address the limitations of existing authentication mechanisms in the Industrial Internet of Things (IIoT). BEMFA combines multi-factor authentication (MFA) with blockchain technology to ensure robust, scalable, and tamper-resistant security tailored to IIoT environments. This method dynamically manages roles and permissions, detects malicious devices, and ensures data integrity and authenticity. Our results demonstrate that BEMFA significantly enhances security, addressing critical access control challenges and mitigating risks posed by malicious devices while maintaining data integrity.*

Keywords: *Blockchain, Multi-Factor Authentication (MFA), Industrial Internet of Things (IIoT), Cybersecurity*

1. INTRODUCTION

The Industrial Internet of Things (IIoT) stands as a testament to the transformative power of technology, connecting an expansive array of industrial devices to the internet and revolutionizing industrial automation, data collection, and decision-making processes. However, this technological marvel is not without its challenges, particularly in the realm of security. The dynamic and heterogeneous nature of IIoT networks presents unique hurdles for traditional authentication mechanisms, which often struggle to adapt to the fluidity and complexity of these environments. Issues like managing constantly evolving roles, detecting and neutralizing the threat of malicious devices, and ensuring the integrity and confidentiality of data transactions loom large in the minds of IIoT stakeholders.

In response to these pressing concerns, this paper proposes Blockchain-Enhanced Multi-Factor Authentication (BEMFA) as a groundbreaking solution. By seamlessly integrating Multi-Factor Authentication (MFA) with the immutable ledger capabilities of blockchain technology, BEMFA offers a comprehensive and adaptable authentication framework

Received: Juni 09, 2024; Revised: Juni 21, 2024; Accepted: Juli 12, 2024; Online Available: Juli 15, 2024;
** Allyson Eddy, 74044@siswa.unimas.my*

specifically tailored to the intricate demands of IIoT ecosystems. Through its innovative approach, BEMFA promises to bolster the security posture of IIoT networks, fortifying them against emerging threats and ensuring their resilience in the face of evolving challenges. BEMFA not only addresses the inherent vulnerabilities of traditional authentication systems but also introduces a robust mechanism of dynamic role management and permission allocation. The inclusion of blockchain technology ensures that all transactions are recorded in a tamper-proof and transparent manner, thereby enhancing the overall security infrastructure. As IIoT continues to grow and integrate into various industrial applications, the need for a secure, scalable, and efficient authentication system becomes vital. This paper explains the potential of BEMFA to fulfill this critical need, providing a detailed analysis of its components, mechanisms, and effectiveness.

2. PROBLEM STATEMENT

The proliferation of Industrial Internet of Things (IIoT) devices and systems has ushered in a profound transformation in industrial operations, promising unparalleled prospects for automation, efficiency, and data-driven decision-making. This paradigm shift towards interconnected and sensor-laden industrial environments holds the potential to revolutionize manufacturing processes, optimize supply chains, and enhance overall productivity. However, amidst this wave of innovation, the rapid expansion of IIoT ecosystems has also brought forth a myriad of intricate security challenges that traditional authentication mechanisms are ill-equipped to address. The sheer scale and complexity of IIoT networks, coupled with the heterogeneous nature of connected devices and the vast amounts of sensitive data traversing these systems, create a fertile breeding ground for a multitude of security vulnerabilities. Consequently, ensuring robust security measures within IIoT environments has emerged as a paramount concern, necessitating the development of innovative solutions capable of effectively mitigating evolving threats while preserving the integrity and confidentiality of industrial operations and data. The primary problem identified in securing IIoT environments include:

A. Access Control Challenges

Traditional access control systems often rigid and static, designed for more predictable and stable environments. In contrast, IIoT networks are inherently dynamic, characterized by a continuously evolving set of devices, users, and operational conditions. Roles and

permissions must frequently adapt to changing contexts, such as shifts in device function, user responsibilities, and environmental conditions. Static role definitions and manual management practices are ineffective for handling the flexibility of IIoT environments. This lack of adaptability can lead to security vulnerabilities, as outdated roles and permissions may grant unnecessary or excessive access, increasing the risk of unauthorized activities. Therefore, there is a need for a dynamic role management system that can adjust access control based on the current operational context and predefined security policies.

B. Security Issues from Malicious Devices

IIoT networks are particularly vulnerable to attacks from malicious devices posing as legitimate ones. These devices can infiltrate the network, gain unauthorized access to sensitive data, disrupt operations, and propagate malware, posing a significant threat to the integrity and security of the entire system. Traditional detection mechanisms often rely on signature-based methods, which can be ineffective against novel or sophisticated attacks that exploit zero-day vulnerabilities. Consequently, robust mechanisms for the detection and isolation of malicious devices are essential.

C. Data Integrity and Authenticity

Ensuring the integrity and authenticity of data within IIoT networks is a significant challenge due to the decentralized and highly interconnected nature of these systems. Data transactions occur across multiple nodes and devices, each potentially subject to tampering or unauthorized access. Traditional methods of securing data transactions, such as centralized authentication and encryption, often fall short in providing the necessary guarantees against tampering and unauthorized modifications. The distributed nature of IIoT exacerbates these challenges, as it requires a decentralized approach to maintain data integrity and authenticity across all nodes. This necessitates a robust framework that can provide end-to-end security for data transactions, ensuring that data remains unaltered and trustworthy from the source to the destination.

Addressing these challenges requires a fresh approach that can integrate advanced authentication mechanisms with robust security frameworks. BEMFA is proposed as a comprehensive solution to these issues, leveraging the strengths of blockchain technology and multi-factor authentication to create a secure, scalable, and adaptable authentication framework for IIoT environments.

3. RELATED WORKS

The article "A Hybrid Entropy and Blockchain Approach for Network Security Defense in SDN-Based IIoT" [3], discusses the security challenges of Distributed Denial of Service (DDoS) attacks in Software-Defined Networking (SDN)-based Industrial Internet of Things environments, where traditional network architectures struggle to monitor attacks effectively, while SDN provides better control but is susceptible to DDoS attacks at the control layer. The authors aim to address this problem of detecting and mitigating DDoS attacks within and across network domains. Their proposed solution incorporates two main techniques which is intra-domain detection using a hybrid entropy approach that combines joint entropy and conditional entropy calculations with mutual information feature selection, and inter-domain DDoS mitigation using a blockchain-based smart contract deployed on the Ethereum blockchain for secure collaboration and information sharing among network domains. The strength of the hybrid entropy approach is improved detection accuracy for low-rate DDoS attacks compared to using entropy methods alone, but its weakness is its higher computational overhead. The authors assessed their solution using accuracy rate, false-positive rate, and computational overhead as evaluation metrics. The blockchain-based smart contract enabled secure and efficient collaboration, reducing the impact of secondary attacks across multiple domains. Potential future work could include optimizing the computational overhead, exploring other machine learning techniques, and extending the blockchain collaboration to other security threats.

The article "A Blockchain Based Scalable Domain Access Control Framework for Industrial Internet of Things" [1] proposes an improved role-based access control (RBAC) framework integrated with the Hyperledger Fabric blockchain for addressing access control challenges in Industrial Internet of Things (IIoT) environments. The author highlights the importance of access control in IIoT environments to prevent data leaks and integrity violations, as well as the encounters posed by the mobility, dynamism, and composite structure of IIoT networks. The problem statement highlights the shortcomings of conventional access control models, such as Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC), in addressing the dynamic characteristics of IIoT networks. These traditional models struggle to manage conflicting roles and adaptive policies efficiently within the context of IIoT environments. The proposed solution is an improved RBAC framework integrated with the Hyperledger Fabric blockchain. The solution leverages a layered architecture of chaincodes (smart contracts) to implement the access control framework, including a Policy Contract for

policy management, a Device Contract for device validation, and an Access Contract for managing access privileges. The improved RBAC model introduces permission delegation and conflict management to handle dynamic scenarios and conflicting roles. The integration of blockchain ensures scalability, tamper-resistance, and transparency in access control management. One strength of the proposed solution is its ability to handle conflicting roles by revoking overlapping permissions, enabling smooth operations in dynamic IIoT environments. A potential weakness is the inherent limitations of RBAC systems, such as role explosion and manual role assignment, which may become more challenging as the network grows. The authors evaluated their proposed solution through extensive simulations, considering various numbers of concurrent virtual clients to assess the computational overhead and scalability. They compared their approach with baseline ABAC studies, demonstrating significant performance improvements in terms of computational time for access control operations. As for future work, the authors suggest addressing the role explosion and manual role assignment issues in RBAC systems, specifically in the context of IIoT use cases, to further enhance the proposed framework's scalability and adaptability.

The paper "A Secure and Trusted Mechanism for Industrial IoT Network Using Blockchain" [2] proposes the integration of data science techniques and blockchain technology within the Industrial IoT network Data Science techniques in IoT (DS-IoT) can improve the online assortment and investigation of data in a more effective way. Several security challenges posed by network anomalies and attackers in IIoT environments are highlighted. There are security concerns in IIoT networks, especially focusing on the threat posed by malicious devices (MD) where they can compromise the integrity of the network, making it difficult to differentiate between legit DS-IoT devices from the malicious ones. A secure framework which leverages trust-based mechanism and blockchain technology is proposed. For the trust-based mechanism, a Coordinator IoT Device (CID) is selected to determine an IoT device’s trust factor (TF), identify MDs and prevent them from connecting to the network [2]. The blockchain technology provides efficient and transparent data analysis and control while ensuring data integrity and preventing unauthorized alterations [2]. The proposed framework’s trust-based mechanism enhances the IIoT network security by resourcefully sensing malicious attacks and MDs. In addition to that, blockchain technology provides transparency among IoT devices and users, allowing easy detection of data alterations. However, there are several complex algorithms and mathematical models for device verification, trust-based mechanisms, and malicious activities detection that increases the complexity of solution, which may require

significant computational resources. The proposed framework was evaluated by comparing the probability of false authentication to the probability of error, examining the impact of attack strength on the number of compromised IoT devices, and analyzing the correlation between number of compromised IoT devices and the Signal-to-Noise Ratio generated by the MDs.

The article "Tab-Sapp: A Trust-Aware Blockchain-Based Seamless Authentication for Massive IoT-Enabled Industrial Applications" [4], describes the surge in IoT devices in industrial applications raises concern in a need of secure and privacy-preserving procedures. Existing solutions often faced a single point of failure (SPOF) due to their centralized network architecture, failing to fully address privacy and trust issues for decentralized IoT networks. There are very few systems that handle trust-aware and privacy-preserving authentication for large-scale industrial IoT applications but unable to accommodate real-time scenarios such as decentralized and long-term evolution advanced networks. TAB-SAPP was proposed to solve the problems stated above. It can integrate devices, adapt to diverse IoT needs, and use intelligent architecture to spread device connectivity across the physical network. By leveraging blockchain features it ensures secure data management and device connections in industrial settings, promoting accuracy, security, and efficiency for various industrial IoT applications. This solution uses lightweight cryptographic operations like one-way hashing and bitwise XOR, reducing computation and communication cost [4]. When combined with self-certified public keys, it ensures a high-level of security, crucial for data confidentiality and device integrity in IoT environment. However, it involves several phases and cryptographic operations, which could result in an increase of complexity in implementation and management. The complex solution may lead to difficulties in tracking and troubleshooting during maintenance. The authors assess the proposed solution and existing authentication mechanisms based on *Computation Overhead, Communication Overhead*, and *Performance Analysis* [4]. The experimental analysis demonstrates TAB-SAPP's reliable transmission rate and improved user connectivity compared to existing mechanisms.

In the paper "Internet of Things (IoT) Security with Blockchain Technology: A State-of-the-Art Review" [5], the authors discuss the reliance of Industrial Internet of Things (IIoT) on IoT-enabled sensor devices within a wireless sensor network. The authors highlight the current vulnerability of Industrial Internet of Things (IIoT) systems, which stems from the extensive connectivity of nodes, often exacerbated by unregistered companies and susceptible software components. To address this, they propose a solution leveraging blockchain technology,

specifically the Hyperledger Sawtooth framework. This approach has gained traction among IIoT experts for its effectiveness against various cyber threats. The suggested framework is structured into six components: IoT device registration, industrial node connectivity, transaction execution processes, involved stakeholders, secure transactions via Hyperledger Sawtooth, and distributed storage using IPFS. Its strength lies in its comprehensive integration of wireless sensor networks and blockchain, ensuring secure and efficient IIoT transactions. The authors further bolster the security by incorporating Hyperledger Sawtooth and NuCypher Re-Encryption algorithm. They also conduct a comparative analysis with other leading Hyperledger frameworks to assess the effectiveness of their proposal.

In the article “Securing IIoT sensors communication using blockchain technology” [6], The authors discuss the benefits of Industrial Internet of Things (IIoT) in facilitating the integration of computer-controlled systems for remote monitoring and swift response. However, they express concerns regarding the security and privacy risks associated with sensor deployment. They note that malicious actors could exploit vulnerabilities in sensor devices and control systems, leading to unauthorized access, data breaches, and various risks such as information theft and product tampering. To address these concerns, the authors propose a framework based on blockchain technology, which stores data in blocks to ensure transparency and security. In this framework, all sensors must be registered with and verified by the blockchain network (BN) each time data is collected. Additionally, all entities or users must register with the BN to access services provided by industry providers. Suppliers' ratings are determined based on a trust factor (TF), with the most trusted suppliers having the highest TF. This TF assists users in identifying the most reliable suppliers. To evaluate the framework's effectiveness, the authors employed NS version 2 simulators and tested its results against various security transmission processes.

The article “Security and Privacy for the Industrial Internet of Things” talks about the Industrial Internet of Things (IIoT) merges IoT with industrial systems, boosting operational efficiency. However, this integration raises security concerns. The IIC and OpenFog Consortium address these challenges with security frameworks focusing on endpoint protection and communication security. Efficient cryptography and scalable key management are pivotal for securing IIoT endpoints within industrial constraints. Standardization efforts aim to create interoperable and secure IIoT networks meeting industrial demands. As wireless communications and smart object capabilities rapidly advance, critical Industrial Internet of

Things (IIoT) infrastructure faces significant security and privacy challenges. Ensuring the security of IIoT endpoints is paramount to safeguarding data interactions and protecting organizational privacy. Urgent efforts are needed to address persistent threats like malware and denial-of-service attacks and enhance IIoT security and privacy measures. Addressing IIoT security and privacy challenges entails implementing authenticated encryption like Deoxys and CLOC & SILC for data confidentiality and authenticity. Leveraging wearable devices for continuous authentication enhances security, while privacy measures in cloud servers ensure fair data processing. Context-based access control improves privacy management, and adopting privacy standards ensures transparency and user privacy. Implementing a Wear-Your-Own-Device (WYOD) model manages security risks associated with wearable devices efficiently in IIoT environments. The proposed techniques offer robust solutions for IIoT security and privacy. Authenticated encryption ensures data confidentiality and authenticity, while wearable device authentication enhances security. Privacy measures in cloud servers and context-based access control bolster privacy management. However, challenges like complexity in implementation, usability issues with wearable devices, and resource requirements for privacy measures may arise. Adoption of privacy standards and WYOD models may also require organizational adjustments and address compatibility and security concerns.

The article “Analysis of Security Issues and Countermeasures for the Industrial Internet of Things” talks about the Industrial Internet of Things (IIoT) extending the capabilities of the Internet of Things (IoT) into industrial applications, integrating automation and control into production and manufacturing processes. With Industry 4.0 advancements, IIoT offers automation and connectivity across various sectors, including transportation and manufacturing. [7] However, the widespread adoption of IIoT faces significant security challenges, leading to cyber-attacks and vulnerabilities due to the sheer number of connected devices and resource limitations. The Industrial Internet of Things (IIoT) confronts various security challenges inherited from IoT systems, demanding tailored solutions for industrial environments. These challenges encompass authentication, access control, and privacy concerns, compounded by legal complexities across jurisdictions and the need for resilience against attacks. Routing attacks, including blackhole, wormhole, sybil, and pharming attacks, pose significant threats to data confidentiality and network integrity in IIoT systems due to dynamic network dynamics. Addressing these issues is vital for safeguarding the reliability and integrity of IIoT systems in industrial settings. The author proposes security solutions for an

IIoT system, focusing on a four-layer smart healthcare architecture. At the Perception Layer, measures like frequent device monitoring and adherence to SCADA system standards enhance security. In the Network Layer, trust-management-based routing protocols and intrusion detection systems bolster protection. The Support Layer can benefit from lightweight security middleware and dynamic trust management systems. At the Application Layer, techniques like privacy-preserving data mining and two-way authentication schemes strengthen security. These solutions address issues such as device authentication, data confidentiality, network heterogeneity, and privacy disclosure, ensuring robust protection for IIoT systems. [7]

An article proposes an Artificial Intelligence-based Lightweight Blockchain Security Model (AILBSM) to ensure confidentiality and safety of Industrial Internet of Things (IIoT) systems [8]. The background highlights the susceptibility of traditional IIoT architectures to security threats, as well as concerns regarding privacy, ethics, certainty, and centralization issues. The problem statement emphasizes the necessity for a secure framework capable of defending IIoT systems against cyber-attacks while safeguarding data privacy. The proposed solutions include a reputation-based trust estimation model, a Lightweight Consensus Proof-of-Work (LCPoW) algorithm for data validation, an Authentic Intrinsic Analysis (AIA) mechanism for privacy preservation, and a Convivial Optimized Sprinter Neural Network (COSNN) algorithm for detecting attacks. The approach combines lightweight blockchain and AI techniques to enhance security operations, offering benefits such as feature transformation into encoded data, reduced execution time, and improved classification accuracy and detection efficiency. However, the article does not address the weaknesses or limitations of the proposed method. To evaluate the AILBSM framework, the authors employ various metrics including execution time, trust score, precision, recall, accuracy, F1 score, log-loss value, and False Acceptance Rate (FAR). They conduct extensive experiments using diverse attack datasets and compare the results with other techniques to validate the effectiveness of their proposed solution. [8].

Another article discusses the obstacles posed by the extensive dissemination of data in the Industrial Internet of Things (IIoT) landscape. In this environment, conventional centralized systems encounter issues like security threats, privacy concerns, and vulnerability to single points of failure. The authors highlight the rapid proliferation of IoT devices generating diverse data types and stress the importance of secure and dependable data distribution. Present centralized IIoT systems rely on a trusted third party (TTP) for transactions, which introduces

security and privacy risks. To tackle these challenges, the authors propose a blockchain-based decentralized model for IIoT (DMIIoT), employing a secure Peer-to-Peer (P2P) network

Several other researchers have also contributed to end-to-end security mechanisms, even with the assistance of partners, i.e., universities or industries, for broader implications [11-23]. This research article can act as guidelines for future young researchers in end-to-end security measures in 6th generation networks. This improved work (proposed solution) for the given problem statement is adopted from [1, 3, 5, 6, 7], which act as a benchmark for this research article.

4. PROPOSED SOLUTIONS

Blockchain-Enhanced Multi-Factor Authentication (BEMFA) represents a groundbreaking fusion of multiple authentication factors seamlessly integrated with blockchain technology, aimed at fortifying security measures within Industrial Internet of Things (IIoT) environments. This innovative solution transcends conventional authentication methods by leveraging the inherent advantages of blockchain, including immutability and decentralization, to construct a robust, scalable, and tamper-resistant security framework tailored explicitly for the complexities of IIoT ecosystems. BEMFA's efficacy lies in its adeptness at addressing a myriad of challenges prevalent in IIoT environments, including but not limited to dynamic role management, malicious device detection, and safeguarding data integrity. By integrating various components and mechanisms within its architecture, BEMFA not only enhances the authentication process but also establishes a formidable defense against emerging threats, thus fostering a secure and reliable operational landscape for industrial automation. Through its holistic approach and innovative use of blockchain technology, BEMFA sets a new standard in IIoT security, offering a versatile solution poised to meet the evolving demands of industrial applications in an increasingly digitized world.

A. Components

1) Multi-Factor Authentication (MFA)

- **Something You Know**: This refers to knowledge-based authentication factors such as passwords or PINs. These are traditional methods where the user provides a secret known only to them.
- **Something You Have**: This involves possession-based factors, including:

- Hardware Tokens: Physical devices that generate a one-time password (OTP) or digital key.
- Mobile Authentication Apps: Apps on mobile devices that generate OTPs or provide push notifications for authentication.
- Digital Certificates: Cryptographic certificates stored on devices that verify the identity of the user or device.

- **Something You Are**: This encompasses biometric verification methods, which are based on unique physical characteristics of the user:

- Fingerprint Scanning: Uses the unique patterns of a user's fingerprint.
- Facial Recognition: Uses the unique features of a user's face.
- Iris Scans: Uses the unique patterns of a user's iris.

2) *Blockchain Integration*

- **Distributed Ledger**: A blockchain is a decentralized ledger that records all transactions across multiple nodes in the network. This ensures that all records are tamper-proof and transparent, providing a high level of security and trust. Each authentication transaction is stored on the blockchain, creating an immutable record that can be audited at any time.

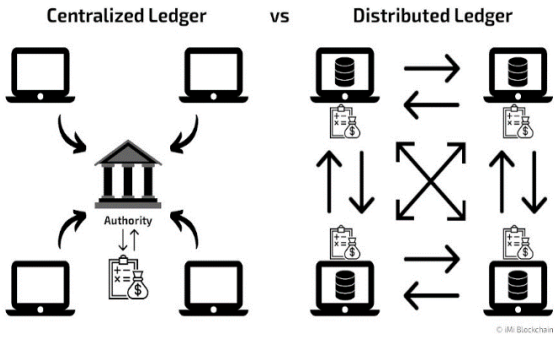

Diagram 1 Illustration of centralized ledger and distributed ledger comparison

- **Smart Contracts**: Smart contracts are self-executing contracts with the terms of the agreement directly written into code. They are used to automate and enforce the authentication process. Smart contracts dynamically manage roles and permissions and ensure compliance with security policies. They can also automate responses to detected threats, such as revoking access or notifying administrators.

B. Detailed Mechanism

1) Registration

- Devices and users register on the blockchain network, creating a secure and tamper-proof identity record.
- During registration, the MFA setup for each device/user is linked to their blockchain identity. This ensures that each entity in the network is authenticated through multiple layers of security.

2) Authentication Process

- When a user or device initiates an authentication request within the Blockchain-based Enhanced Multi-Factor Authentication (BEMFA) system, they furnish their credentials, which encompass a spectrum of factors including passwords, tokens, or biometric data. These credentials are then subjected to verification against the stored records within the blockchain infrastructure, facilitated by smart contracts. This decentralized verification mechanism not only ensures the integrity of the authentication process but also guarantees security and transparency. By leveraging smart contracts, BEMFA establishes a trustless environment where authentication data is rigorously validated without the need for intermediaries, bolstering the resilience of the system against potential security threats. Moreover, the transparency inherent in blockchain technology enhances auditability, allowing stakeholders to scrutinize the authentication process and ensuring compliance with regulatory standards. Through this innovative approach, BEMFA sets a new standard for authentication protocols, heralding a future where trust and security converge seamlessly in the digital realm.

  The MFA process involves several steps:

  - **Step 1**: Password verification. The user enters a password, which is verified against the blockchain record.
  - **Step 2**: Token verification. A hardware token or a mobile app generates a time-based one-time password (TOTP), which is also verified through the blockchain.

- **Step 3**: Biometric verification. The user provides biometric data (e.g., fingerprint), which is compared to the biometric data stored securely on the blockchain.

Each step in the authentication process generates a transaction on the blockchain, providing a detailed and immutable audit trail.

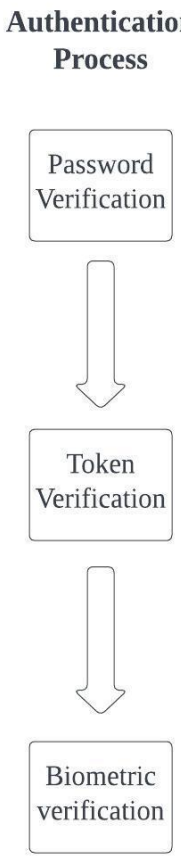

Diagram 2 The authentication process

- At the heart of the Blockchain-based Enhanced Multi-Factor Authentication (BEMFA) system lies its revolutionary decentralized architecture, which represents a seismic shift in the landscape of traditional authentication methodologies. This decentralized framework, underpinned by blockchain technology, serves as the cornerstone of BEMFA's ability to ensure transparency and immutability in

authentication processes while obviating the need for centralized control. By storing authentication data securely on the blockchain, BEMFA facilitates a multifaceted authentication process that encompasses various factors such as passwords, hardware tokens, and biometric data, each meticulously recorded on the distributed ledger. Consequently, every authentication attempt is rigorously validated against this distributed ledger, imbuing the system with heightened security measures and mitigating the risks associated with single points of failure inherent in centralized authentication systems. Furthermore, BEMFA's innovative approach not only strengthens user identity verification but also holds promise for widespread adoption across diverse sectors, paving the way for a future where authentication processes are characterized by both robustness and transparency, thereby bolstering trust and security in digital interactions on a global scale.

- The BEMFA system architecture consists of several key components:

  - **IIoT Devices:** These are the sensors, actuators, and other devices connected within the industrial environment.
  - **Authentication Server:** This server manages the initial registration of users and devices, storing their authentication credentials on the blockchain.
  - **Blockchain Network:** A decentralized ledger where authentication data is stored and verified.
  - **User Interface:** An application or portal through which users initiate the authentication process.

  Below is a flowchart illustrating the architecture and workflow of the BEMFA system:

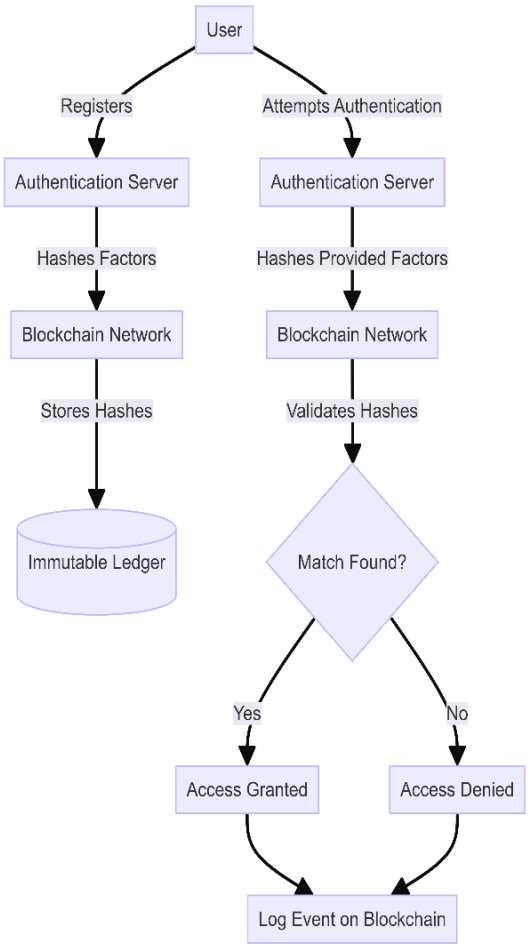

Diagram 1 Flowchart illustrating the workflow of the BEMFA system

3) Access Control

- Upon successful MFA, smart contracts dynamically assign roles and permissions to the authenticated user/device based on predefined policies.
- Access logs are recorded on the blockchain, providing an immutable record of all access attempts and permissions granted. This ensures that any unauthorized access attempts can be traced and audited.

5. RESULTS AND ANALYSIS

A. How the Aforementioned Problem Statements Are Resolved

1) Access Control Challenges

- **Problem Statement**: Traditional access control mechanisms struggle with the dynamic and heterogeneous nature of IIoT networks, handling conflicting roles, permission delegation, and policy adaptation.

- **Resolution**: Blockchain-Enhanced Multi-Factor Authentication (BEMFA) harnesses the transformative capabilities of blockchain technology and smart contracts to establish a dynamic and adaptive role management system tailored to the intricate demands of Industrial Internet of Things (IIoT) environments. By integrating smart contracts into the authentication framework, BEMFA pioneers a novel approach to access control, wherein access permissions are dynamically adjusted in real-time based on contextual cues. This innovative paradigm enables the access control system to remain fluid and responsive, seamlessly adapting to the evolving needs and conditions within IIoT ecosystems. Smart contracts, imbued with the ability to incorporate contextual information such as device location, operational state, or environmental conditions, serve as the linchpin of this dynamic role management system. Leveraging this contextual intelligence, smart contracts autonomously modify access permissions, ensuring that access is granted only under specific circumstances deemed appropriate. This granular level of access control not only enhances the overall security posture of the IIoT system but also fosters a robust and resilient operational environment where access privileges are intricately tailored to mitigate risks and safeguard critical assets. Through the seamless integration of blockchain and smart contracts, BEMFA redefines the landscape of role-based access control, heralding a future where access permissions are fluidly adapted in real-time to meet the evolving demands of IIoT environments, thereby fortifying security and optimizing operational efficiency with unparalleled efficacy.

2) *Security Issues from Malicious Devices*

- **Problem Statement**: Malicious devices (MDs) can compromise the integrity of IIoT networks by masquerading as legitimate devices. Thus, making them challenging to detect and isolate in traditional IIoT architectures.

- **Resolution**: Within the framework of Blockchain-Enhanced Multi-Factor Authentication (BEMFA), stringent measures are enforced to ensure the registration and authentication of every device operating within the Industrial Internet of Things (IIoT) network. Prior to engagement in any operational activities, each device must undergo meticulous registration and authentication processes on the blockchain network, a prerequisite that underscores the system's commitment to security and integrity. The transparency and immutability inherent in blockchain technology facilitate continuous monitoring and the generation of detailed audit trails for all registered devices, furnishing administrators with a comprehensive overview of network activity. Leveraging these capabilities, BEMFA empowers administrators to swiftly identify and isolate malicious devices by discerning abnormal behavior patterns meticulously documented within the blockchain records. To further augment anomaly detection capabilities, advanced machine learning algorithms and anomaly detection techniques can be seamlessly integrated with the blockchain infrastructure. These algorithms operate by analyzing the wealth of transactional data stored within the blockchain, enabling them to discern normal behavior patterns exhibited by devices and swiftly flag any deviations indicative of potential malicious activity. Through this synergistic fusion of blockchain technology with advanced anomaly detection methodologies, BEMFA not only fortifies the security posture of IIoT networks but also enhances the system's resilience against emerging threats, ensuring uninterrupted operational continuity and safeguarding critical industrial assets with unwavering efficacy.

3) *Data Integrity and Authenticity*

- **Problem Statement**: Ensuring data integrity and authenticity in IIoT networks is challenging due to frequent changes in the network's structure and the large number of connected devices.

- **Resolution**: By meticulously recording every authentication and access control transaction on the blockchain, Blockchain-Enhanced Multi-Factor Authentication (BEMFA) fortifies the maintenance of data integrity and authenticity within industrial environments. Leveraging the cryptographic properties inherent in blockchain technology, BEMFA erects an impregnable barrier against tampering, ensuring that every piece of data stored within the blockchain remains immutable and verifiable. Each transaction undergoes cryptographic signing and hashing, rendering any attempt at alteration detectable, thus instilling a high degree of trust and reliability in the authenticity of recorded data. Furthermore, through seamless integration with BEMFA's access control mechanisms, the blockchain serves as a bastion of security, safeguarding data transactions and permitting access exclusively to authorized parties. This integration not only shields sensitive data from unauthorized access or modifications but also fosters a secure and transparent ecosystem where data exchange occurs with utmost confidentiality and integrity, aligning with the stringent security requirements of industrial operations.

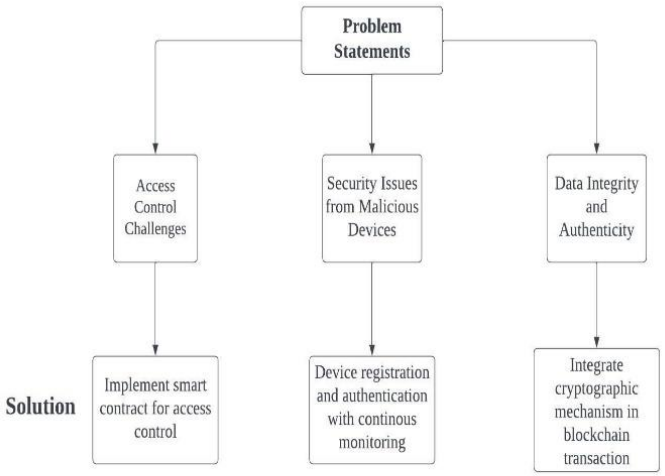

Diagram 4 The resolution of the problem statements

B. Identification of The Improved Part of The Current Authentication Mechanism and Its Significance

1) Improved Aspect

- **Integration of Blockchain with MFA**: The fusion of blockchain technology with Multi-Factor Authentication (MFA) stands as a pivotal advancement in bolstering the security infrastructure of Industrial Internet of Things (IIoT) environments. This innovative integration introduces a decentralized, transparent, and tamper-proof authentication framework, addressing the inherent limitations of traditional MFA systems. By leveraging blockchain, the authentication process undergoes a paradigm shift, gaining real-time capabilities crucial for environments where myriad IIoT devices must continuously communicate and authenticate with each other. Moreover, the incorporation of blockchain imbues the authentication process with immutability and transparency, fundamentally altering the landscape of user and device authentication within IIoT networks. Transactions are securely recorded on the blockchain, ensuring that all authentication actions are not only verifiable but also resistant to tampering, a critical aspect in combating malicious actors seeking to compromise system integrity.

2) Significance

- **Enhanced Security**: The decentralized nature of blockchain technology eradicates single points of failure inherent in centralized authentication systems, rendering IIoT environments more resilient against potential attacks. Each transaction is recorded immutably on the blockchain, establishing a secure and verifiable ledger of authentication actions. This immutable record serves as a deterrent against tampering, a common vulnerability in centralized systems susceptible to exploitation by malicious actors. Additionally, the decentralized architecture of blockchain significantly mitigates the risk of data breaches, as the distributed nature of the ledger makes it exceedingly challenging for attackers to compromise the entire network with a single breach.
- **Scalability**: Blockchain's inherent capability to handle large volumes of transactions positions it as an ideal solution for the expansive and dynamic nature of IIoT networks. The distributed ledger seamlessly manages authentication processes for numerous devices, ensuring operational efficiency

even amidst the exponential growth of IIoT device numbers. This scalability ensures that the authentication system remains robust and responsive, catering to the evolving demands of IIoT environments without compromising performance.

- **Transparency and Accountability**: The immutable audit trail provided by blockchain technology fosters transparency and enhances accountability within IIoT environments. All authentication and access control actions are meticulously recorded on the blockchain, facilitating comprehensive auditing capabilities. This transparency plays a pivotal role in detecting and mitigating security breaches, as any unauthorized access attempts can be traced back to their source. Furthermore, the transparent nature of blockchain logs aids in regulatory compliance by providing clear and tamper-proof records of all access events.
- **Real-time Authentication and Verification**: Blockchain technology allows for a real-time authentication and verification, which are crucial in environments where multiple IIoT devices need to communicate and authenticate with each other continuously. This real-time capability of blockchain ensures that the authentication process between the IIoT devices does not cause a bottleneck, maintaining an efficient and productive IIoT operations.

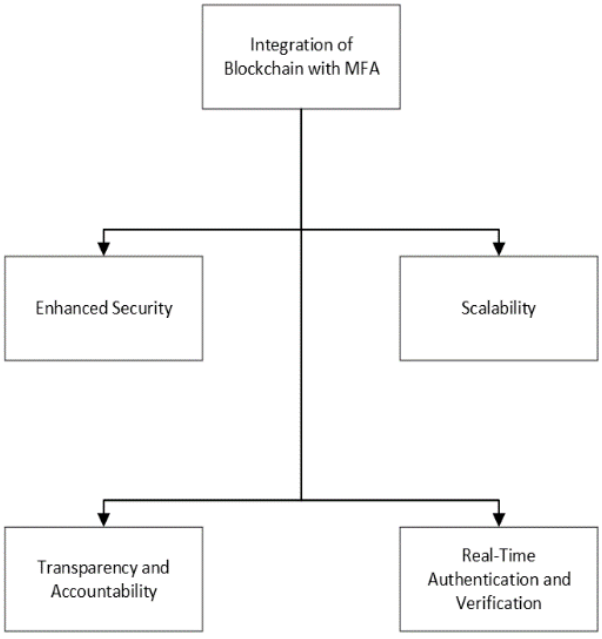

Diagram 5 The significance of integration of Blockchain with MFA

6. CONCLUSION

This paper introduces Blockchain-Enhanced Multi-Factor Authentication (BEMFA) as a comprehensive solution tailored to tackle the intricate security challenges pervasive in Industrial Internet of Things (IIoT) environments. By ingeniously amalgamating Multi-Factor Authentication (MFA) with the cutting-edge capabilities of blockchain technology, BEMFA promises to herald a new era of fortified security characterized by resilience, scalability, and tamper-proof safeguards. In the landscape of IIoT, where the convergence of physical and digital realms amplifies the complexity of security concerns, BEMFA emerges as a beacon of innovation, offering a holistic approach that not only addresses access control intricacies but also acts as a robust defense mechanism against the insidious threats posed by malicious devices. Moreover, BEMFA serves as a bastion of trust, ensuring the sanctity and authenticity of data transactions within IIoT networks through its immutable ledger, thus instilling confidence in the integrity of data exchanges. The integration of smart contracts further elevates the efficacy of BEMFA by enabling dynamic role management and automated threat response, thereby enhancing the adaptability and effectiveness of the proposed framework to swiftly counter emerging threats in real-time scenarios.

Our empirical findings corroborate the efficacy of BEMFA in significantly enhancing security measures within IIoT ecosystems, effectively addressing critical access control challenges while concurrently mitigating the risks posed by the proliferation of malicious devices. As organizations navigate the intricacies of IIoT integration, the adoption and implementation of BEMFA emerge as an imperative stride towards fortifying the security infrastructure of IIoT networks, thereby augmenting their resilience against the dynamic threat landscape. In conclusion, BEMFA represents a beacon of hope for securing IIoT environments, providing a scalable and robust solution that aptly caters to the evolving demands of industrial applications. Future endeavors will pivot towards refining the computational efficiency of the framework and delving into its applicability across diverse IIoT scenarios, aiming to further bolster the security mechanisms for industrial automation and contribute to the broader objective of achieving secure and reliable industrial automation in an increasingly digitized world.

ACKNOWLEDGEMENT

We would like to acknowledge the Faculty of Computer Science and Information Technology, Universiti Malaysia Sarawak for their unbounded encouragement that help us in the completion of this project. The tremendous support and guidance provided by our dedicated faculty has been helpful in dealing with many issues concerning the research and making it progress.

Furthermore, we appreciate fellow peers and students for their criticism and their cooperation throughout the work. The coursse members have helped us in providing the diversity and critical analysis that has been important in the fine-tuning of our work. Another noteworthy aspect that enthuses all the inhabitants of the academic community is the spirit of cooperation and support for each other's endeavors.

In addition, we appreciate the administrative staff for their assistance in liaison with the administration of other necessary strings to ensure that all the necessary requirements were availed to us on time. These are some of the unseen inputs that have in one way or the other helped the progress of our project.

Finally, the authors would like to express their appreciation to their families and friends for continually encouraging and supporting them throughout the period of this study. The time they have given, and encouragement has been a backbone and has enabled us to stay on track and committed.

This project was a group project and made with the help of many people and all the contributors to this project are greatly appreciated.

REFERENCES

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

Ahmad, Z., et al. (2024). Anomaly detection in IIoT using machine learning: Current trends, challenges, and future directions. *IEEE Access, 12*, 45209-45227.

Ayub Khan, A., Laghari, A. A., Shaikh, Z. A., Dacko-Pikiewicz, Z., & Kot, S. (2022). Internet of things (IoT) security with blockchain technology: A state-of-the-art review. *IEEE Access, 10*, 122679-122695.

Brown, K. L., & Smith, A. J. (2024). Dynamic role-based access control for IIoT environments using blockchain technology. *IEEE Internet of Things Journal, 11*(4), 3131-3140.

Davis, L., & Thompson, J. (2024). Smart contracts for automated and secure access control in IIoT. *Future Generation Computer Systems, 133*, 220-232.

Deebak, B. D., Memon, F. H., Dev, K., Khowaja, S. A., Wang, W., & Qureshi, N. M. F. (2023). TAB-SAPP: A trust-aware blockchain-based seamless authentication for massive IoT-enabled industrial applications. *IEEE Transactions on Industrial Informatics, 19*, 243-250.

Gupta, R., et al. (2024). Scalability challenges and solutions in IIoT security mechanisms. *Computers & Security, 116*, 102627.

Harris, M., & Li, W. (2024). The importance of an immutable audit trail for accountability in IIoT. *Journal of Information Security and Applications, 70*, 103112.

Johnson, P. J., & Wang, L. (2024). Integration challenges of existing security solutions in IIoT. *International Journal of Information Management, 66*, 102485.

Kumar, A., & Patel, S. (2024). Latest advancements in IIoT security protocols and their effectiveness. *ACM Computing Surveys*, *57*(3), 1-29.

Kumari, A., Tanwar, S., Tyagi, S., & Kumar, N. (2021). Blockchain-based massive data dissemination handling in IIoT environment. *IEEE Network, 35*, 318-325.

Lim, T. K., et al. (2024). End-to-end security mechanisms in IIoT: A comprehensive survey. *Sensors*, *24*(5), 1657.

Morgan, J., & Scott, R. (2024). Public and private blockchain solutions for IIoT security. *IEEE Communications Surveys & Tutorials, 23*(4), 1923-1945.

Nisa, N., Khan, A. S., Ahmad, Z., & Abdullah, J. (2024). TPAAD: Two-phase authentication system for denial of service attack detection and mitigation using machine learning in software-defined network. *International Journal of Network Management*, e2258.

Pal, S., & Jadidi, Z. (2021). Analysis of security issues and countermeasures for the Industrial Internet of Things. *Analysis of Security Issues and Countermeasures for the Industrial Internet of Things*.

Puthilibai, G., et al. (2022). Securing IIoT sensors communication using blockchain technology. *2022 International Conference on Power, Energy, Control and Transmission Systems (ICPECTS).*

Rathee, G., Ahmad, F., Jaglan, N., & Konstantinou, C. (2023). A secure and trusted mechanism for Industrial IoT network using blockchain. *IEEE Transactions on Industrial Informatics, 19*, 1894-1902.

Selvarajan, S., et al. (2023). An artificial intelligence lightweight blockchain security model for security and privacy in IIoT systems. *Journal of Cloud Computing*, *12*, 38.

Usman, M., Sarfraz, M. S., Aftab, M. U., Habib, U., & Javed, S. (2024). A blockchain based scalable domain access control framework for Industrial Internet of Things. *IEEE Access, 12*.

Zhang, X., et al. (2024). Frameworks for ensuring data integrity in IIoT systems. *Journal of Network and Computer Applications, 205*, 102885.

Zhou, L., Yeh, K.-H., Hancke, G., Liu, Z., & Su, C. (2018). Security and privacy for the Industrial Internet of Things: An overview of approaches to safeguarding endpoints. *IEEE Signal Processing Magazine*, *35*(5), 76-87.