International Journal of Computer Technology and Science
Volume. 1 No. 3 July 2024
e-ISSN :3048-1961, And p-ISSN :3048-1899, Page. 20-40
DOI: https://doi.org/10.62951/ijcts.v1i3.19
Available online at: https://international.arteii.or.id/index.php/IJCTS

Enhancing IIoT Security: AI-Driven Blockchain-Based Authentication Scheme

Azreen Shafieqah Asri[1], Faizatul Fitri Boestamam[1], Harith Zakwan Bin Zakaria[1], Mohammad Amir Alam Rahim Omar[1], Mohammad Hamka Izzuddin Bin Mohamad Yahya[1] & Muhammad Faisal[2]

[1] Faculty of Computer Science and Information Technology,
Universiti Malaysia Sarawak, Kuching, Sarawak, Malaysia
[2] Director HRIMS, Ministry of Human Rights

[1] 74251@siswa.unimas.my [2] 73449@siswa.unimas.my [3] 73484@siswa.unimas.my
[4] 73563@siswa.unimas.my [5] 73571@siswa.unimas.my [6] dr.faisalshabbir88@gmail.com

Abstract: *With the rapid expansion of the Industrial Internet of Things (IIoT), integrating devices, machines, and systems to optimize operations and enable data-driven decision-making, ensuring robust security measures is essential. While blockchain has shown the potential to upgrade traditional authentication methods in IIoT environments, vulnerabilities persist. This paper introduces two innovative methods to enhance blockchain-based authentication in IIoT: first, integrating AI-driven anomaly and threat detection into the blockchain authentication scheme; second, implementing Ethereum smart contracts for enhanced authentication with a two-factor authentication (2FA) system and GFE algorithms. By combining AI for anomaly detection with decentralized smart contracts and blockchain-based 2FA, and leveraging GFE algorithms to enhance blockchain capabilities, the proposed scheme aims to significantly fortify security measures. This integration offers a resilient defense against evolving threats, ensuring transparency, adaptability, and heightened security in IIoT applications.*

Keywords: *Artificial Intelligence, Authentication, Blockchain, Industrial Internet of Things (IIoT), Security*

1. INTRODUCTION

The Industrial Internet of Things (IIoT) is transforming the landscape of industries worldwide, ushering in a new era of interconnectedness, efficiency, and innovation. By harnessing the power of sensors, cloud computing, and advanced analytics, IIoT enables unprecedented levels of automation, optimization, and data-driven decision-making on the factory floor. It also can refer to the interconnected network of industrial devices, machines, and systems to manage all the operational controls, dynamic control of production systems, and collect and analyze data [1]. This technological revolution promises to enhance productivity, reduce operational costs, and improve decision-making processes.

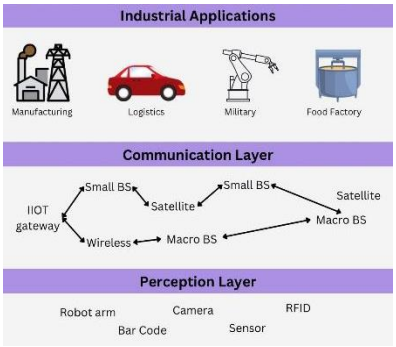

Figure 1. IIoT application.

The IIoT system works like in Fig. 1 where sensors gather data, it's sent over networks

Received: May 10, 2024; Revised: June 15, 2024; Accepted: July 12, 2024; Published: July 16, 2024;
* Azreen Shafieqah Asri , 74251@siswa.unimas.my

accurately, and smart tech analyzes and improves decision-making. However, as the number of connected devices and sensors in IIoT ecosystems expands, so will the attack surface for attackers. Traditional authentication methods, such as passwords and cryptographic keys, are increasingly vulnerable to various cyber threats, including brute force attacks, man-in-the-middle attacks, and insider threats. These vulnerabilities can have severe consequences in IIoT environments, where compromised devices or systems could lead to production halts, equipment failures, and even catastrophic incidents with far-reaching implications.

To address these pressing security challenges, an innovative approach that harnesses the power of artificial intelligence (AI) and the decentralized nature of blockchain technology has emerged as a promising solution for enhancing authentication and access control in IIoT ecosystems. Individually, AI gives systems the ability to analyse large volumes of data, recognise trends, and spot abnormalities in real time. Meanwhile, blockchain, with its decentralized and immutable ledger, provides a tamper-proof framework for recording and verifying transactions. By synergizing these technologies, a formidable defense mechanism against cyber threats emerges, capable of ensuring the authenticity and integrity of data within IIoT networks.

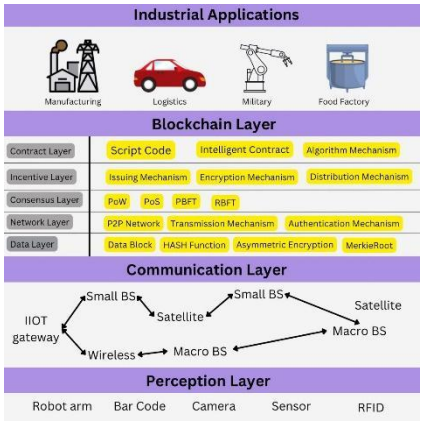

Figure 2. Blockchain application.

By adding blockchain in Fig. 2, data is securely verified and stored, providing reliable services for industrial applications [27].

At the core of this AI-driven, blockchain-based authentication scheme lies the integration of advanced machine learning algorithms and decentralized ledger technology. The AI component continuously monitors and analyzes patterns in device behavior, network traffic, and user interactions, establishing a baseline of normal operations. By leveraging techniques such as anomaly detection, predictive modeling, and behavioral analysis, the system can identify deviations or anomalies that may indicate potential threats or unauthorized access attempts. Simultaneously, the blockchain component serves as a tamper-proof and

decentralized ledger for securely storing and verifying authentication credentials, device identities, and access logs. This distributed and transparent nature of blockchain ensures data integrity, non-repudiation, and accountability, making it virtually impossible for malicious actors to manipulate or forge authentication records without detection.

The synergy between AI and blockchain in this authentication scheme provides a multi-layered defense against evolving cyber threats. While the AI component continuously adapts and learns from new data patterns, the blockchain component ensures the immutability and transparency of authentication records, creating a robust and resilient security framework.

There are two problem statements issued in this article. First, in the IIoT environments, there are prevalent vulnerabilities in security mechanisms and authentication issues attributed to centralized systems, reliant on trusted third parties, and large associated costs [25]. Next, the rapid growth of the IoT sparked an interest in its industrial application due to dispersed evolving technology and topology, creating a novel model and significant deficiencies concerning data storage, transactions, security, and privacy within IIoT [1]. To address the problem statement regarding vulnerabilities in security mechanisms and authentication issues in IIoT environments, which are attributed to centralized systems reliant on trusted third parties and associated with large costs, the integration of blockchain with enhanced security mechanisms and AI technologies integration presents a viable solution.

2. RELATED WORKS

The field of industrial internet security has advanced significantly, driven by the growing demand for robust, fast, and scalable authentication and key negotiation systems. Traditional authentication methods, which rely primarily on certificate management and key escrow, have encountered various obstacles, including high computational costs, security vulnerabilities, and complex management requirements. Recent research has moved its focus to new innovations that overcome these difficulties. Blockchain technology has emerged as a top solution, offering decentralised and immutable frameworks that improve security and trust. Several blockchain-based authentication solutions have been developed, each of which uses distinct consensus mechanisms and cryptographic algorithms to increase performance and security. This section provides an overview of the key developments in industrial internet security, highlighting the various approaches and innovations that have been proposed. Examining these related studies provides a better knowledge of the existing landscape and ongoing attempts to improve the security and efficiency of industrial internet systems.

A study has been conducted in 2023 about The Role of AI and Blockchain in Supply

Chain Traceability [16]. The article revealed that AI in addition to Blockchain can improve supply chain efficiency, accuracy, visibility, and transparency.Artificial intelligence technology, such as machine learning as well as computer vision, can analyse enormous volumes in supply chain data to find trends, patterns, abnormalities, potential threats, and inefficiencies. This can help to make better decisions and improve supply chain performance [16]. In the article, the authors mentioned that AI and blockchain may reduce the possibility of food fraud while also increasing transparency by tracking the source as well as quality of food supplies. Moreover, it also mentioned that Machine learning algorithms were utilised as well to forecast demand and optimise supply networks, reducing waste and increasing efficiency.

Table 1: Comparison between AI and Blockchain with Traditional Methods.

Metric	AI and Blockchain	Traditional Methods
Time to Trace Product	1 hour	1 day
Traceability Accuracy	98%	80%
Cost of Traceability	$10,000	$25,000
Number of Steps in Traceability Process	5	10

The table above, from K. Sherin et al. [16], compares Blockchain and AI to traditional supply chain tracing approaches. The overall result shows that Blockchain technology and AI reduce the time it takes to trace a product from two days to one hour. Next, the traceability accuracy increases from 80% to 98%. The cost of traceability is decreased to $10,000 rather than $25,000, and the total amount of steps in the traceability process is reduced from ten to five in earlier techniques. However, applying blockchain and AI for supply chain traceability brings a number of obstacles and limitations. Data privacy, scalability, connection, platform stability, and investment requirements are among the challenges associated with blockchain technology.

Next, Z. Rahman et al mentioned that the industry 4.0, marked by interconnected systems utilizing IoT and AI technologies, enhances productivity and operational efficiency but simultaneously exposes industrial systems to advanced persistent threats (APTs) [29]. These threats are sophisticated and stealthy, aiming to gain long-term control over systems via vulnerable IoT edge devices and servers. The integration of blockchain technology with AI provides a promising solution to these security challenges. The proposed system leverages consortium blockchain (CBC) to ensure secure data transfer and storage in a decentralized manner, eliminating the need for traditional public-key infrastructure and reducing costs. AI-

driven detection on edge devices filters and detects malicious data at the source, enhancing overall security. The novel certificateless data transfer approach, utilizing partial secret sharing for device authentication, further improves security and reduces operational costs. Additionally, deep transfer learning (DTL) enhances threat detection by reusing knowledge from previous tasks, while a distributed hash table (DHT) offers efficient, robust, and scalable data storage. Experimental results demonstrate that this blockchain-based AI-enabled system outperforms traditional methods in efficiency and effectiveness in detecting APTs, with faster transaction processing rates, higher data integrity, and reduced dependency on centralized systems. Integrating blockchain with AI thus provides a robust framework for securing Industry 4.0 systems, offering significant improvements in security, efficiency and trustworthiness for industrial IoT ecosystems. However, there are some disadvantages to this method. The complexity and computational demands of implementing blockchain and AI technologies can be significant, particularly for small to medium-sized enterprises (SMEs) with limited resources. Edge devices, despite improvements, may still struggle with the computational load required for real-time AI processing. Moreover, while blockchain provides enhanced security, it also introduces latency in data processing due to its consensus mechanisms, which could affect the real-time responsiveness required in industrial applications.

Selvarajan et al. offer the next study, AI-based Lightweight Blockchain Security Model (AILBSM), which integrates trust management, privacy preservation, and threat detection. The proposed AILBSM framework consists of three layers of security operations: trust assessment, which confirms the IIoT sensor device's reliability; data authentication and attack the avoidance using a lightweight blockchain technology algorithm; and attack categorization via an artificial intelligence system [23]. Figure 3 depicts the technique in three parts, the first of which is detecting Advanced Persistent Threats (APT) in the data. Next, the APT identification state and data transactions will be updated, and the data will be saved in a distributed hash table (DHT). Trust verification checks data from IIoT sensor devices to prevent tampering and misdirection. Trust verification examines data from IIoT sensor devices to detect tampering and misdirection. The lighter consensus Proof-of-Work (LCPoW) algorithm ensures the anonymity of systems used in the IIoT. Data authentication protects the IIoT system from any assaults and invasions. An Authentic Intrinsic Analysis (also known as the approach) converts features into encoded data, which reduces the intensity of attacks. The Convivial Optimised Sprinter Neural Network (COSNN) algorithm uses privacy protection module input to accurately classify normal and invader data [23]. The findings indicate that the Artificial Intelligence Lightweight Blockchain Security Model (AILBSM) considerably improves

security and privacy in Industrial Internet of Things (IIoT) systems. By integrating a blockchain-based privacy preservation technique using the Lightweight Consensus Proof of Work (LCPoW) mechanism, the model minimizes execution time while ensuring high security during data transmission to the InterPlanetary File System (IPFS). The AI component, a Clustered One-Shot Neural Network (COSNN), effectively detects and classifies cyber threats, outperforming traditional methods in terms of accuracy, detection rate, False Alarm Rate (FAR), and F1 score. Evaluated through various performance metrics, the model demonstrates reduced time consumption and high computational efficiency, making it suitable for real-time IIoT applications. While the Lightweight Consensus Proof of Work (LCPoW) is less computationally demanding than older approaches, it still requires significant resources to generate proofs and maintain hash chain integrity. The requirement for unique addresses for each sensor device in the blockchain network can also pose scalability issues, particularly in large-scale IIoT environments.

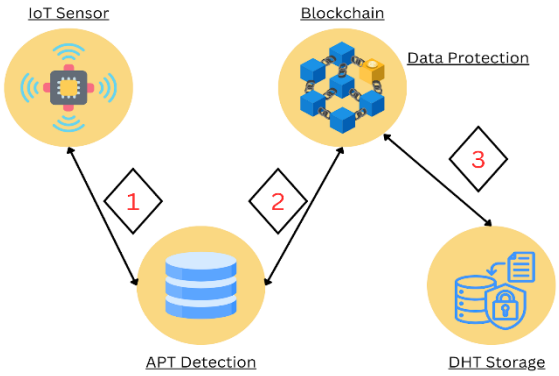

Figure 3. High-level view of the proposed blockchain AI-enabled data protection technique

In [25], the authors mentioned how distributed ledger technology like Blockchain, has an impact on domains like IoT, healthcare, and transportation, emphasizing its role in ensuring privacy and security within Cyber-Physical Systems (CPSs). It highlighted the pressing need for robust security and privacy measures in IoT-based structures, identifying authentication challenges in decentralized settings, and 3 proposed using blockchain-based authentication mechanisms to address security challenges. It emphasizes the importance of lightweight solutions for authentication data management, potentially leveraging cloud computing and lightweight cryptosystems. The strengths of the proposed approach lie in blockchain's robustness to provide privacy and security solutions, particularly in decentralized architectures. The strategy faces deficiencies like computational costs, communication overheads, and the need for lightweight solutions, compounded by IoT-enabled smart device authentication

concerns. Despite blockchain's potential, cloud computing integration is required for complete support, as well as lightweight authentication data management in resource-limited IoT applications. The evaluation metrics were used to assess the security and authentication mechanisms in IoT devices within smart city environments, helping to assess the adoption of distributed solutions, evaluate the blockchain effectiveness in enhancing privacy and security, identify authentication challenges, assess the importance of lightweight solutions, and outline future research directions.

Several other researchers have also contributed in end-to-end security mechanisms even with the assistance of the counter partners i.e. universities or industries for broadening implications [3], [5-9], [17], [19], [20], [22], [22]. This research article can act as the guidelines for future young researchers in end-to-end security measures in 6th generation networks. This improved work of AI-Driven Blockchain-Based Authentication Scheme and for the given problem statement is adopted from [23], which acts as a benchmark for this research article.

3. PROPOSED SOLUTIONS

The combination of Blockchain, IIoT, and AI forms a powerful system that enhances the capabilities of each technology. Blockchain provides a secure platform for IoT devices, ensuring an unchangeable record of device data and enabling AI to perform complex analyses with guaranteed data integrity.

Table 2: Integration benefits from blockchain and AI

Blockchain	AI	Integration Benefits
Decentralized	Centralized	Enhanced Data Security
Deterministic	Changing	Improved Trust on Robotic Decisions
Immutable	Probabilistic	Collective Decision Making
Data Integrity	Volatile	Decentralized Intelligence
Attacks Resilient	Data, Knowledge and Decision-centric	High Efficiency

Table 2 shows the integration benefits from blockchain and AI. AI further enhances this system by offering advanced data analysis, and pattern recognition, which can foresee problems, optimize operations, and make real-time decisions. The combination of AI and blockchain offers many advantages beyond traditional business uses. Merging AI's strong analytical abilities with blockchain's secure, decentralized structure allows these technologies to be applied in education, healthcare, energy, social impact, agriculture, urban planning, and more as shown in Fig. 4.

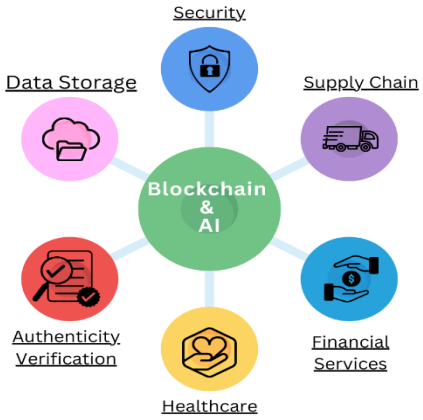

Figure 4. Application of AI and blockchain in sectors

This allows for decisions based on data and more effective resource management in various domains. Decentralizing data storage and management through blockchain reduces the risk of single points of failure, making IoT systems more resilient to attacks. The immutability of blockchain ensures that IIoT data remains unaltered, providing a solid foundation for AI to perform reliable analyses.

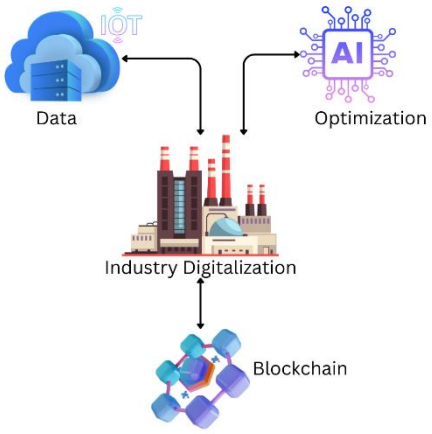

Figure 5. Interaction between Blockchain, IoT, and AI

4.1. Motivation of Combining AI and Blockchain

Over the next 5-10 years, the software development services are expected to increasingly adopt blockchain and AI technologies [13]. Forward-thinking, tech-savvy industry leaders recognize the significant potential of integrating these two technologies. Although advanced, AI will never fully replace human judgment and therefore may not achieve widespread public adoption. One major obstacle to AI's widespread use is the lack of accountability for its actions.

Public trust in AI could grow if its decision-making processes were transparent and recorded.

Combining blockchain with AI can help uncover these hidden processes. Blockchain technology ensures that all AI decisions are recorded on a distributed ledger, making it ideal for auditing and security-sensitive applications. Blockchain's inherent encryption also ensures the data's security. This makes it ideal for storing private and sensitive information, such as medical records or personal recommendations. AI requires continuous, large-scale data, and current research and development efforts are focused on enabling AI algorithms to securely process encrypted data. However, it is important to note that while blockchain itself is highly secure, additional layers or applications built on top of it are not impervious to breaches [13].

4.2. Real Life Application of Blockchain, AI, and IIoT

3.2.1. Supply Chain

The integration of Blockchain, AI, and IIoT revolutionizes supply chain management by improving product authenticity, optimizing logistics, and increasing transparency:

- Product Authenticity: Blockchain creates an unchangeable ledger, securely recording each product’s journey from production to consumer, reducing counterfeit risks.
- Optimized Logistics: AI analyzes data from IIoT devices to streamline logistics processes like routing and inventory management, ensuring timely delivery and lowering costs.
- Enhanced Transparency: IIoT devices track goods at every stage, and blockchain securely records this data, making the supply chain more transparent and building trust among consumers and stakeholders.

3.2.2. Smart Manufacturing

In manufacturing, the collaboration between IIoT, AI, and Blockchain leads to significant improvements in predictive maintenance and quality control:

- Predictive Maintenance: IIoT devices monitor equipment performance, and AI analyzes this data to predict maintenance needs, reducing downtime and extending equipment life.
- Quality Control: AI identifies defects and ensures product quality during manufacturing. Blockchain provides a secure, tamper-proof record of all quality checks and maintenance actions, essential for compliance and audits.

4.3. Enhanced Blockchain-Based Authentication Scheme

Blockchain technology offers a decentralized, secure, and tamper-proof mechanism for authentication in IIoT environments. The enhanced blockchain-based authentication process

can be done by integrating:

- **GFE algorithm utilizes Transport Layer Security (TLS) Hand Shake Mechanism Implementation [14]:** A GFE-chain algorithm is developed specifically for authenticating IoT devices in industrial networks using blockchain technology. It enhances blockchain authentication by utilizing a TLS handshake mechanism based on standards 1.2 and higher, ensuring mutual authentication through pre-generated certificates to prevent unauthorized access. This algorithm effectively eliminates Man-in-the-Middle (MITM) attacks and safeguards against TLS version downgrading by verifying the certificate chain, thereby enhancing network security and reliability. By uniquely identifying specific sensors, the GFE-chain algorithm provides robust protection against unauthorized access and forgery of identification data, ensuring a secure and reliable blockchain-based authentication process [14].
- **Ethereum-based smart contract [18]:** Implementing Ethereum-based smart contracts can design a smart contract that manages the authentication process securely and autonomously. The smart contract can include functions for generating and verifying OTPs (One-Time Passwords) using Ethereum's inherent randomness sources like block timestamps and difficulties. It would interact with users' Ethereum addresses, requiring them to sign authentication challenges with their private keys via a mobile wallet. This approach ensures that authentication is decentralized and 5 tamper-proof, mitigating vulnerabilities associated with traditional centralized systems. By leveraging blockchain technology, the smart contract enhances security, scalability, and user control in IIoT authentication, thereby offering a robust solution for securing industrial IoT applications [18].
- **Blockchain-Based 2FA System [18]:** The proposed solution harnesses the power of blockchain technology and smart contracts to create a decentralized, highly secure method for two-factor authentication (2FA). By integrating blockchain technology and smart contracts, this 2FA system offers a comprehensive and modern solution to authentication challenges, ensuring both security and user trust. This method mitigates the risks associated with insecure passwords, addresses major privacy concerns, removes the necessity for a third-party trust provider, and provides a resilient framework for IIoT applications. Traditional systems often depend on central authorities that are vulnerable to breaches, whereas this solution utilizes the Ethereum blockchain framework and the smart contract to enhance security and trust. The proposed system will generate access tokens through smart contracts, which manage all authentication-related tasks, including

decision handling of on-chain access control. When a user attempts to access a resource, the smart contract on the blockchain generates a one-time password (OTP) that is sent to the user's mobile device. The user then signs this OTP to authenticate their identity and access the system. This dual-channel authentication ensures that even if one channel is compromised, the other remains secure due to the tamper-proof nature of the blockchain. By eliminating the need for a centralized authority, this system allows users to store their identity data directly on their mobile devices, which then interact with the blockchain for validation. This decentralization enhances security by removing single points of failure and improves privacy by avoiding the central storage of sensitive information. The solution adheres to the National Institute of Standards and Technology (NIST) guidelines for 2FA, emphasizing the use of two independent channels for transmitting second factors (disposable secrets) [18]. This can prevent issues with the storing, protection, and exchange of secrets by verifiers and users. The Ethereum blockchain serves as an independent channel, fulfilling this requirement and making the 2FA process robust and secure, especially for IIoT applications [18].

4.4. AI-Driven Anomaly and Threat Detection

Artificial Intelligence can be integrated to enhance the blockchain authentication scheme by providing real-time detection of blockchain abnormal behavior and threat attack.

- **Anomaly Detection [10]:** Five types of anomalous attacks in blockchain can be identified: account-based, smart contract, consensus, transaction-based, and system-based [21]. Focusing on abnormal behavior in transactions within the blockchain network can reveal malicious activities. These anomalous transactions need to be identified before they are recorded in the blockchain ledger. AI technology uses machine learning and is capable of learning the patterns of abnormal behavior in blockchain transactions [10]. By monitoring block sizes, the number of transactions, and the intervals of their creation, machine learning can analyze transactions for deviations from the norm. Anomaly detection involves identifying transactions that differ significantly from the average pattern within a given timeframe. Integration can be achieved through unsupervised learning models that analyze transaction data recorded in blocks. The Half-Space Tree learning model, for example, is used for continuous partial learning in a streaming data environment, enabling effective anomaly detection. Visualization techniques, such as Principal Component Analysis, help in presenting the results of anomaly detection effectively [10].
- **Threat Detection [28]:** A sophisticated AI-based method for detecting cyber threats,

which can be effectively integrated with blockchain authentication to enhance security in Industrial IoT (IIoT) environments. The proposed method employs an attention mechanism-based model to analyze heterogeneous data sources, such as network flows and system logs, assessing their status and identifying anomalies. A Random Forest (RF)-based classifier is used to detect these anomalies with high precision, accuracy, recall, and F1-score, significantly outperforming traditional models. To ensure transparency and interpretability, the model utilizes SHAP (SHapley Additive exPlanations) values, which elucidate the importance of various features in the anomaly detection process. By integrating this AI threat detection method with a blockchain-based authentication system, the framework can provide a decentralized and secure method for verifying device and user identities, eliminating reliance on centralized authorities and enhancing trust. Blockchain's immutable ledger ensures that all transactions and data exchanges are secure and tamper-proof, while the AI model continuously monitors and identifies potential security breaches in real-time. This integration not only fortifies the IIoT environment against advanced persistent threats but also ensures robust, transparent, and reliable security measures. [28] The combination of AI, blockchain, and IIoT creates a robust framework that significantly enhances industrial operations. For instance, AI-integrated smart contracts automate decision-making processes, ensuring accurate and efficient contract execution without the need for intermediaries. AI further enhances smart 6 contracts by enabling them to adapt to real-time data and changing conditions, maintaining their relevance and effectiveness over time. Blockchain’s decentralized nature secures IIoT data, while AI provides advanced threat detection, identifying and mitigating security risks in real-time. Additionally, AI-driven analytics optimize IIoT operations, leading to better resource management, reduced downtime, and higher overall operational efficiency.In summary, integrating AI with blockchain in IIoT systems brings about significant improvements in security, efficiency, and operational effectiveness. This integration drives innovation and ensures robust, secure, and efficient industrial operations, highlighting the indispensable role of AI in harnessing the full potential of IIoT.

4. RESULTS AND ANALYSIS

This section presents an analysis of how the proposed AI-enhanced blockchain-based authentication mechanism addresses the identified problem statements in Industrial Internet of Things (IIoT) environments. The main focus includes resolving key vulnerabilities associated

with centralized systems, such as security breaches and high costs, through decentralization and advanced AI-driven security measures. Specific improvements to existing authentication mechanisms are highlighted, emphasizing the significance of these enhancements in terms of security, efficiency, and operational resilience. By integrating AI for real-time monitoring, adaptive risk assessment, and biometric authentication, and employing blockchain technology for decentralized trust and secure data storage, the solution offers a robust and comprehensive approach to meeting the unique security requirements of IIoT networks. This section aims to provide a thorough evaluation of the proposed solution, demonstrating its effectiveness in overcoming current challenges and improving overall system performance.

The proposed AI-enhanced blockchain-based authentication mechanism aims to address the critical security challenges identified in the IIoT environments. The solution focuses on eliminating the vulnerabilities inherent in centralized systems, improving the efficiency and security of device-to-device communication, and leveraging advanced technologies to create a robust, scalable framework for IIoT. An analysis of how the proposed solution resolves each of the identified problem statements are as follows:

4.1. Problem Statement #1: Centralized Vulnerabilities and High Costs in IIoT Environments

In the IIoT environments, there are prevalent vulnerabilities in security mechanisms and authentication issues attributed to centralized systems, reliant on trusted third parties, and large associated costs [25]. The proposed AI-driven and enhanced blockchain-based authentication mechanism addresses the issues related to centralized vulnerabilities and high costs in IIoT environments through:

- **Full Decentralization**: The blockchain-based approach eliminates the reliance on centralized systems and third-party intermediaries. By utilizing a decentralized ledger, the solution ensures that all authentication transactions are distributed across multiple nodes. This decentralization mitigates single points of failure and reduces the dependency on costly centralized infrastructures. The elimination of third-party intermediaries also reduces operational costs associated with maintaining and securing a centralized authentication system [25].
- **GFE Algorithm and TLS Implementation:** The incorporation of the GFE algorithm and Transport Layer Security (TLS) enhances the security of network channels. The GFE algorithm ensures that data is encrypted and secure during transmission, while TLS provides a robust protocol for securing communications over the network. This combination mitigates various attacks, such as man-in-the-middle attacks, ensuring that data remains confidential and integral during transmission [14].

- **Ethereum-Based Smart Contracts:** Utilizing Ethereum smart contracts automates the authentication process, ensuring that only authenticated devices and users can access the IIoT network. These smart contracts are self-executing, with the terms of the agreement directly written into code, eliminating the need for a centralized authority to manage and verify authentication [18].
- **Blockchain-Based 2FA System:** The proposed solution includes a blockchain-based two-factor authentication (2FA) system, which adds an additional layer of security. This system uses smart contracts to generate one-time passwords (OTPs) or tokens that must be signed by users to gain access. By decentralizing the 2FA system and integrating it with blockchain technology, the solution reduces the risk of unauthorized access and enhances user security [18].
- **AI-Driven Enhancements:** AI enhances the blockchain authentication scheme by providing real-time analysis of blockchain behavior and network traffic. An attention mechanism-based model analyzes heterogeneous data sources, such as network flows and system logs, assessing their status and identifying anomalies. A Random Forest (RF)-based classifier detects these anomalies with high precision, accuracy, recall, and F1-score, significantly outperforming traditional models [28]. By continuously monitoring and analyzing these patterns, AI can 7 detect and prevent malicious activities before they are recorded on the blockchain. This proactive approach to threat detection reduces the risk of unauthorized access and enhances the overall security of the IIoT network. Explainable AI (XAI) also provides clear insights into detected threats, enabling security personnel to respond effectively and take appropriate actions.

4.2. Problem Statement #2: Inefficiencies and Security Concerns in IIoT Convergence with Blockchain

The rapid growth of the IoT sparked an interest in its industrial application due to dispersed evolving technology and topology, creating a novel model and significant deficiencies concerning data storage, transactions, security, and privacy within IIoT [1]. The convergence between IIoT and blockchain presents new issues such as inefficient IIoT nodes, and resources-heavy ledgers. Traditional security algorithms need improvement. The adoption of blockchain hyperledger technologies has been restricted by the lack of a unified protocol for secure IoT design and the reliance on centralized networks in IIoT architecture, resulting in security, and privacy concerns. A framework that leverages the blockchain Hyperledger Sawtooth is proposed to establish a secure and trusted execution environment for industrial

activities [1]. This framework incorporated distinct communication channels, pseudo-chain codes, and consensus policies, to ensure resource efficiency, smooth industrial node transactions, and content broadcast, that will address the IIoT security and privacy challenges. The challenges arising from the convergence of IIoT and blockchain, including inefficient IIoT nodes, resource-heavy ledgers, and traditional security algorithms that need improvement. The proposed solution addresses the inefficiencies and security concerns in IIoT convergence with blockchain through several key enhancements:

- **GFE Algorithm and TLS Handshake Mechanism:** The GFE-chain algorithm, combined with TLS handshake mechanisms, ensures mutual authentication and prevents unauthorized access. By verifying the certificate chain, this approach eliminates Man-in-the-Middle (MITM) attacks and safeguards against TLS version downgrading, enhancing network security and reliability. This solution uniquely identifies specific sensors, providing robust protection against unauthorized access and forgery of identification data.
- **Ethereum-Based Smart Contracts:** The implementation of Ethereum-based smart contracts establishes a secure, decentralized authentication and access control mechanism. This 2FA system leverages blockchain technology to eliminate the need for third-party trust and mitigate the risks associated with weak passwords. The smart contracts handle on-chain access control decisions and authentication processes, generating tokens as one-time passwords (OTPs) for users to verify their identity. This method ensures secure and reliable authentication without relying on centralized authorities.
- **AI-Driven Anomaly and Threat Detection:** AI enhances the blockchain authentication scheme by providing real-time analysis of blockchain behavior and network traffic. An attention mechanism-based model analyzes heterogeneous data sources, such as network flows and system logs, assessing their status and identifying anomalies. A Random Forest (RF)-based classifier detects these anomalies with high precision, accuracy, recall, and F1-score, significantly outperforming traditional models [28]. By continuously monitoring and analyzing these patterns, AI can detect and prevent malicious activities before they are recorded in the blockchain ledger. This integration of AI ensures continuous monitoring of IIoT networks, detecting and mitigating security risks in real-time. The integration of AI-driven with blockchain-based authentication represents a significant improvement to the current authentication system in IIoT environments. The proposed solutions improve critical aspects of the current authentication mechanism,

addressing specific vulnerabilities and inefficiencies, and enhancing security, efficiency, and operational resilience. The key improvements and their significance are as follows:

- **Decentralized Authentication Transactions:** Leveraging a blockchain-based ledger for authenticating transactions enhances decentralization, eliminates single points of error, and minimizes dependency on costly centralized infrastructure. It assures that authentication transactions are distributed over various nodes, which improves security and reduces the possibility of across-the-system intrusions [25].
- **Integration of the GFE Algorithm with TLS for Secure Communication:** Using the GFE method for data encryption with Transport Layer Security (TLS) for secure connections improves network channel security. It guarantees that data is safe and intact during transmission, reducing dangers like man-in-the-middle attacks. This is crucial for maintaining the security and privacy of sensitive data in IIoT situations [25].
- **Automated Authentication using Ethereum-based Smart Contracts:** Automating authentication with Ethereum smart contracts decreases the danger of human mistakes and security breaches that come with manual processes. Smart contracts guarantee that only authenticated devices and users may access the 8 network, improving overall system security and performance [18]. ● An authentication solution for two factors (2FA) based on blockchain: Implementing a blockchain-based two-factor authentication (2FA) system that generates one-time passwords (OTPs) or tokens using smart contracts offers a second layer of authentication, making unauthorized access more difficult, and as a result, the risk of unauthorized access drops significantly, and user security improves [18].
- **AI-driven anomaly detection and threat identification:** In Industrial IIoT contexts, advanced AI-based techniques are used for proactive threat detection and real-time network traffic and device behaviour monitoring. These techniques evaluate the state and spot abnormalities in a variety of data sources, such as network flows and system logs, by using a model based on an attention mechanism. Classifiers based on RF outperform classical models in terms of precision, accuracy, recall, and F1-score. SHAP values guarantee transparency and interpretability by elucidating the importance of different characteristics in anomaly identification. By enabling decentralized identity verification of devices and users, decreasing dependency on centralized authority, and increasing trust, the integration of AI threat detection with blockchain-based authentication improves security. Blockchain technology ensures the security of all transactions and data transfers through its immutable ledger, and its AI model continually monitors and

instantly detects possible security breaches. By ensuring strong, transparent, and dependable security measures, this integration strengthens the IIoT environment against sophisticated persistent attacks [10, 28].

- **Resource Management and Optimization:** Algorithms driven by AI can uncover inefficiencies and optimize resource utilization, improving IIoT network performance and scalability. By optimizing resource utilization, the system can handle more transactions while maintaining performance and security [1].
- **Improved Privacy and Data Integrity:** AI-driven anomaly detection enhances privacy and data integrity by detecting odd activity and unauthorized access attempts. Data integrity and privacy are critical for preserving user trust and overall security in IIoT systems. Early detection of irregularities enables prompt mitigation of potential threats, maintaining the integrity of sensitive data.
- **Dynamic Responses to Emerging Threats:** AI's capacity to learn from new data and adapt to changing risks enables dynamic responses to emerging dangers. This continual modification improves the system's ability to guard against developing security threats, resulting in a more robust and future-proof security mechanism. The proposed blockchain-based authentication method with AI enhancements greatly improves the current methods of authentication in IIoT environments. Some of the major improvements include decentralized authentication transactions, safe communication via TLS and GFE, automatic authentication using smart contracts based on Ethereum, and AI-based anomaly and threat detection. Collectively, these improvements minimize the risks connected to conventional authentication techniques, offering a foundation for safe and dependable authentication that is specifically designed to meet the demands of IIoT contexts.

5. CONCLUSION

The combination of Blockchain and Artificial Intelligence (AI) offers a viable approach for addressing crucial security concerns in Industrial Internet of Things (IIoT) contexts. This research paper has proposed an AI-driven blockchain-based authentication scheme that combines the strengths of these two powerful technologies to enhance authentication, anomaly detection, and threat mitigation in IIoT networks. The proposed solution addresses the vulnerabilities associated with centralized systems, such as security breaches and high costs, by leveraging the decentralized nature of blockchain technology. The incorporation of AI-driven anomaly and threat detection mechanisms further enhances the security posture,

enabling real-time monitoring of device behaviour and network traffic, identifying potential threats, and preventing unauthorized access attempts. Through the implementation of secure authentication protocols, including the GFE algorithm, TLS handshake mechanisms, Ethereum-based smart contracts, and a blockchain-based 2FA system, the proposed solution establishes a robust and reliable authentication framework. This comprehensive approach not only eliminates the reliance on centralized authorities but also automates the authentication process, reducing the risk of human errors and ensuring that only authenticated devices and users can access the IIoT network. Furthermore, the combination of blockchain technologies and AI addresses the inefficiencies and security concerns arising from the convergence of IIoT and blockchain. By employing techniques such as the Half-Space Tree learning model and Principal Component Analysis, AI-driven anomaly detection can proactively identify and mitigate security threats, ensuring the integrity and confidentiality of data within the IIoT network. While the proposed solution represents a significant advancement in IIoT security, it is essential to acknowledge that the implementation of AI and blockchain technologies is not without challenges. Issues such as data privacy, scalability, and computational demands must be addressed to ensure the effective and efficient deployment of this solution in real-world scenarios.

Overall, the AI-driven blockchain-based authentication scheme proposed in this research paper offers a comprehensive and robust approach to enhancing the security and reliability of IIoT environments. By combining the power of AI and blockchain technologies, this solution not only addresses current vulnerabilities but also provides a foundation for future-proof security mechanisms capable of adapting to emerging threats and evolving technological landscapes.

6. ACKNOWLEDGEMENT

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

REFERENCES

[1] Abubakar, M., Jaroucheh, Z., Al Dubai, A., & Liu, X. (2022). A lightweight and user-centric two-factor authentication mechanism for IoT based on blockchain and smart contract. In *2022 2nd International Conference of Smart Systems and Emerging Technologies (SMARTTECH)* (pp. 91-96). https://doi.org/10.1109/SMARTTECH54121.2022.00032

[2] 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. https://doi.org/10.1109/ACCESS.2022.3223370

[3] Babu, E. S., Devi, A. A., Kavati, I., & Srinivasarao, B. K. N. (2023). Blockchain-based authentication mechanism for edge devices in fog-enabled IoT networks. In *TENCON 2023 - 2023 IEEE Region 10 Conference (TENCON)* (pp. 558-563). https://doi.org/10.1109/TENCON58879.2023.10322432

[4] Deep, A., Perrusquía, A., Aljaburi, L., Al-Rubaye, S., & Guo, W. (2024). A novel distributed authentication of blockchain technology integration in IoT services. *IEEE Access, 12*, 9550-9562. https://doi.org/10.1109/ACCESS.2024.3349955

[5] Dong, J., et al. (2024). Blockchain-based certificate-free cross-domain authentication mechanism for Industrial Internet. *IEEE Internet of Things Journal, 11*(2), 3316-3330. https://doi.org/10.1109/JIOT.2023.3296506

[6] 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.

[7] 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

[8] Hassan, M. U., Rehmani, M. H., & Chen, J. (2023). Anomaly detection in blockchain networks: A comprehensive survey. *IEEE Communications Surveys & Tutorials, 25*(1), 289-318. https://doi.org/10.1109/COMST.2022.3205643

[9] Khalil, U., Mueen-Uddin, Malik, O. A., & Hussain, S. (2022). A blockchain footprint for authentication of IoT-enabled smart devices in smart cities: State-of-the-art advancements, challenges and future research directions. *IEEE Access, 10*, 76805-76823. https://doi.org/10.1109/ACCESS.2022.3189998

[10] 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.

[11] Khan, A. S., et al. (2023). Blockchain-based lightweight multifactor authentication for cell-free in ultra-dense 6G-based (6-CMAS) cellular network. *IEEE Access, 11*, 20524-20541. https://doi.org/10.1109/ACCESS.2023.3526940

[12] Khan, A. S., et al. (2023). Ensemble based automotive paint surface defect detection augmented by order statistics filtering using machine learning. *Authorea Preprints*.

[13] Khan, A. S., Halikul, I., & Johari Abdullah, N. F. (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. *International Journal of Computer Science and Network Security (IJCSNS), 17*(5), 366-371.

[15] Khan, N., Abdullah, J., & Khan, A. S. (2017). Defending malicious script attacks using machine learning classifiers. *Wireless Communications and Mobile Computing, 2017*.

[16] 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.

[17] 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

[18] Liu, Y., & Li, S. (2023). Hybrid cyber threats detection using explainable AI in Industrial IoT. In *2023 International Conference on Human-Centered Cognitive Systems (HCCS)* (pp. 1-6). https://doi.org/10.1109/HCCS59561.2023.10452621

[19] Rahman, Z., Yi, X., & Khalil, I. (2023). Blockchain-based AI-enabled Industry 4.0 CPS protection against advanced persistent threat. *IEEE Internet of Things Journal, 10*(8), 6769-6778. https://doi.org/10.1109/JIOT.2022.3147186

[20] Saravanabhavan, C., et al. (2022). Blockchain-based secure Menger's authentication for Industrial IoT. In *2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)* (pp. 1302-1308). https://doi.org/10.1109/ICACITE53722.2022.9823904

[21] Selvarajan, S., et al. (2023). An artificial intelligence lightweight blockchain security model for security and privacy in IIoT systems. *Journal of Cloud Computing: Advances, Systems and Applications*. https://doi.org/10.1186/s13677-023-00412-y

[22] Seo, B.-S., Baek, J.-M., & Ko, K.-M. (2024). AI-enabled abnormal behaviour detection and visualization technology on blockchain network. In *2024 International Conference on Electronics, Information, and Communication (ICEIC)* (pp. 1-4).

[23] Sherin, K., Kaur, N., Joshi, A., Nayak, R. B. P., & Srinivas, K. (2023). The role of AI and blockchain in supply chain traceability. In *2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)* (pp. 918-922). https://doi.org/10.1109/ICACITE57410.2023.10183214

[24] Shoaib, M., et al. (2023). Augmenting the robustness and efficiency of violence detection systems for surveillance and non-surveillance scenarios. *IEEE Access, 11*, 123295-123313.

[25] Taherdoost, H. (2022). Blockchain technology and artificial intelligence together: A critical review on applications. *Applied Sciences*, *12*(24), 12948. https://doi.org/10.3390/app122412948

[26] Wang, X., Garg, S., Lin, H., Piran, M. J., Hu, J., & Hossain, M. S. (2021). Enabling secure authentication in Industrial IoT with transfer learning empowered blockchain. *IEEE Transactions on Industrial Informatics*, *17*(11), 7725-7733. https://doi.org/10.1109/TII.2021.3049405

[27] Zen, K., et al. (2015). Intelligent coordinator selection mechanism (ICSM) for IEEE802. 15.4 beacon-enabled MAC protocol in mobile wireless sensor networks. *International Review on Computers and Software*, *10*(2), 164-171.

[28] Zhou, W., Liu, M., Chen, C., & Luo, Z. (2021). A research on the development and application of blockchain technology in Industrial Internet of Things. In *2021 Computing, Communications and IoT Applications (ComComAp)* (pp. 83-88). https://doi.org/10.1109/ComComAp53641.2021.9653137

[29] 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.