International Journal of Computer Technology and Science
Volume. 1 No. 3 July 2024
e-ISSN :3048-1961, And p-ISSN :3048-1899, Page. 01-19
DOI: https://doi.org/10.62951/ijcts.v1i3.18
Available online at: https://international.arteii.or.id/index.php/IJCTS

Securing Industrial IoT: Blockchain-Integrated Solutions for Enhanced Privacy, Authentication, and Efficiency

Derrick Lim Kin Yeap [1], Jason Jong Sheng Tat [2], Jason Ng Yong Xing [3], Joan Sia Yuk Ting [4], Mildred Lim Pei Chin [5],& Muhammad Faisa [7]
[1,2,3,4,5] Faculty of Computer Science and Information Technology, Universiti Malaysia Sarawak, KotaSamarahan 94300, Malaysia
[6] Director HRIMS, Ministry of Human Rights,

[1] 74597@siswa.unimas.my [2] 75127@siswa.unimas.my [3] 75125@siswa.unimas.my
[4] 75182@siswa.unimas.my [5] 75638@siswa.unimas.my [6] dr.faisalshabbir88@gmail.com

Abstract: *The Industrial Internet of Things (IIoT) enhances the connectivity and efficiency of living lifestyles. However, it also comes with significant security vulnerabilities. Traditional authentication methods are often inadequate, leading to IIoT devices opened to security threats. This paper proposes a comprehensive security framework integrating blockchain, cryptographic techniques, smart contracts, and deep learning-based Intrusion Detection Systems (IDS) to tackle the mentioned issue. Blockchain ensures data integrity and prevents tampering through a decentralized ledger. A decentralized device identity management system enhances user verification, while secure communication protocols using Hash-based Message Authentication Codes (HMAC) safeguard data integrity. Smart contracts automate transactions, providing transparent, secure record-keeping without a central authority. The deep learning-based IDS, utilizing Contractive Sparse Autoencoder (CSAE) and Attention-Based Bidirectional Long Short-Term Memory (ABiLSTM) networks, effectively detects cyber threats. Evaluation metrics, including precision, recall, F1-score, and False Acceptance Rate (FAR), demonstrate high accuracy and low false alarm rates across datasets. This framework addresses the need for secure, efficient, and scalable authentication in IIoT, combining blockchain's security features with advanced cryptographic and anomaly detection techniques, offering robust defence against cyber threats.*

Keywords: *Blockchain; IIoT; Authentication*

1 INTRODUCTION

The Industrial Internet of Things (IIoT) has brought an exciting new era of connection and efficiency to a variety of industrial industries. However, the rapid growth of smart devices connected to the internet has created substantial security threats for IIoT networks. The interchange of data between IoT devices has rendered systems vulnerable to cyberattacks, endangering security and privacy. Challenges faced in IIoT devices also includes diverse device performance, wide distribution, and vulnerable to spoofing and third-party attacks [9]. Furthermore, the authentication procedure in IIoT systems confronts issues in accurately assessing node stability and avoiding malicious activity, especially as the number of connected devices grows. According to Rathee et. al. [3], a trust management and blockchain technology was proposed to enhance the security of IIoT networks. Blockchain integration with IIoT infrastructure provides a strong solution to these problems. The decentralized and immutable ledger design of blockchain reduces the possibility of unauthorized tampering or data breaches by guaranteeing data integrity and tamper-proof transactions. Industrial firms can simplify operational procedures, protect sensitive data, and establish strong authentication mechanisms

Received: May 10, 2024; Revised: June 15, 2024; Accepted: July 12, 2024; Published: July 16, 2024;
* Derrick Lim Kin Yeap , 74597@siswa.unimas.my

by utilizing the built-in security features of blockchain technology. The potential of blockchain-integrated solutions for industrial IoT security is examined in this article, which highlights the need of improved efficiency, privacy, and authentication for streamlining industrial processes and building confidence in digital ecosystems.

2 PROBLEM STATEMENT

With the emergence of Industry Internet of Things (IIoT), usage of smart devices that connects to the internet increases. This poses a security risk to the IIoT networks [3], [4]. For instance, with the rapid increase in data exchange between IoT devices, security and data privacy has become vulnerable towards cyber-attacks. On the other hand, as more and more devices are accessing the internet, the process for authenticating a user has become a challenge in IIoT systems where current traditional techniques may fall short in providing weak level of security [7]. Figure 1 depicts the traditional approach of IIoT.

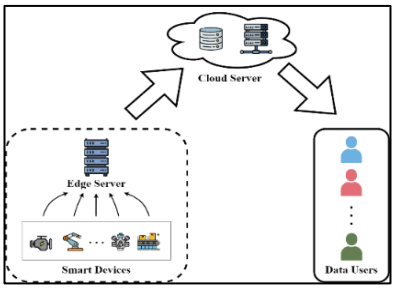

Figure 1. Traditional Approach of IIoT

3 RELATED WORKS

3.1. Article 1

Various work has been carried out to secure the IIoT. For instance, Aljuhani et al. [1] study highlights the vulnerability of industrial internet of things (IIOT) networks to security threats due to the diverse nature of devices and communication channels [1]. Data transmitted over insecure medium can be interpreted by malicious entities, emphasized the lack of security measures in IIOT networks and to highly subjected to cyberattacks. Traditional approaches may not be sufficient to protect against evolving threats in IIOT environments. Thus, this technique was proposed to ease short-handed. The proposed solution applies a novel deep learning-based intrusion detection system (IDS) and session-based two-way authentication and key management system for safe interaction over the blockchain network, utilizing the Proof-of-Authority (PoA) agreement system for transaction validation and block creation based on miner vote over the cloud server [1]. As compared to traditional approaches, this study leverages the strengths of deep learning for efficient cyberattack detection and

blockchain in securing communication and providing a comprehensive security solution for IIOT networks. However, there is insufficient evaluation and comparison that exists and provide a clearer justification that this approach is effective and efficient.

Accordingly, the evaluation metrics that are used to evaluate the model include accuracy, precision, recall value, F1-measures. As such, this model was tested and being evaluated with two different types of datasets. Thus, a Receiver Operating Characteristics (ROC) curve graph was being plotted to contrast the True Positive Rate (TPR) against False Positive Rate (FPR).

3.2. Article 2

Following, there has been a significant improvement in the efficiency and quality of services in various industrial applications. However, a major challenge faced in the IIoT ecosystem is the conflict between the need for data sharing and the necessity to preserve privacy and a balance or trade-offs of these two conflicting requirements. As such, Yang et al. [2] proposed a scheme named Multiparty Computation (MPC) scheme that is privacy-aware and publicly auditable in leveraging blockchain technology and provide a transparent platform for tracing any malicious activities in the environment.

This proposed scheme seems to ensure the privacy by allowing the participants to share input keys for computation without revealing raw data, thus protecting data ownership and utilizing block chain technology for data commitments and computation evidence but still, this architecture might impact the scalability and performance of the model, leading to another trade-offs issue, efficiency vs effectiveness. In short, computation latency, communication overhead, key size influence and performance analysis are the evaluation metrics that is being used by Yang et al. [2] to review the outcomes of the proposed framework.

3.3. Article 3

Next, the background of the following article highlights the increasing connectivity of devices in Industry of Internet of Things (IIoT), generating large amounts of data causing it to be vulnerable to security risks such as unauthorized access to sensitive data. The problem statement underscores the vulnerability of IIoT networks to cyber-attacks and difficulties in establishing a secure and reliable environment for data exchange and communication among IoT devices. According to Rathee et. al. [3], a trust management and blockchain technology was recommended to enhance the security of IIoT networks. The proposed solution includes a Coordinator IoT Device (CID) to calculate the trust factor of devices within the network. Blockchain technology was utilized to implement a secure data model to prevent unauthorized alterations towards stored information, ensuring the transparency in sharing data and immediate identification of malicious data records or alterations.

The proposed solution provides enhanced security and data integrity by utilizing blockchain to store data where the simulation of the framework yields a 91% rate of success against networks without blockchain. It also enhances the network's ability to identify and authenticate devices via Trust Factor Computation. However, the framework might face challenges in real-time scenario due to potential delay in block verification process and increasing number of devices which impose security risks. The evaluation matrix used by the authors to assess the framework is the ability to detect and withstand attacks, effectiveness in preventing unauthorized alteration of data, and the probability of false authentication [3].

3.4. Article 4

Furthermore, with the rapid increase in data exchange between IoT devices, security and privacy has become a concern in the industry Internet of Things (IIoT). The vulnerability of existing Certificateless Signature (CLS) schemes towards attacks such as man-in-the-middle attacks, key generation center compromised attacks etc. are being highlighted. Therefore, a pairing-free certificateless scheme that utilizes blockchain technology and smart contracts is proposed to improve safety and efficacy of IIoT protocols [4]. The proposed system includes a Smart Contract Key Generation Center (SC-KGC) responsible for generating and distributing keys to users with the utilization of blockchain and smart contract which provides a decentralized and automatic approach to key management.

The proposed system is proved to be more effective and secure at the same time being decentralized. However, there would be some complexity during the implementation and maintenance. This proposed system also faces scalability challenges where more evaluation needs to be carried out to ensure its efficiency. The evaluation matrix used by the author to assess the proposed system included security analysis, performance evaluation which includes computation and communication cost, comparative analysis with other papers, and simulation of Type-I and Type-II adversaries.

3.5. Article 5

According to Kan et al. [5], the authors emphasized data security in Healthcare Industrial Internet of Things (IIoT) applications using blockchain technology. Transforming the lifecycle of wireless medical sensor networks is discussed to optimize data management and increase trust in blockchain-enabled environment. The problem addressed in the article revolves around the inefficiencies and vulnerabilities in centralized E-healthcare applications. These problems include the registration of users authentication, authorization, information sharing, collaboration, usage of resources, and privacy protection. The authentication mechanism proposed using Blockchain Hyperledger-enabled IIot (BHIIoT) utilizes

blockchain technology to enhance data security, privacy preservation, and resource management. It includes a consortium Hyperledger network with on-chain and off-chain communication channels for secure data sharing and interconnectivity. The architecture automates E-healthcare transactions, implements lightweight authentication mechanisms, and ensures privacy preservation through health ledger management.

The proposed solution improved efficiency by automating E-healthcare transactions, which reduces resource consumption in terms of computational energy, network bandwidth, and data preservation costs. However, the potential weakness of complexity exists as implementing and managing a blockchain-enabled architecture require specialized knowledge and resources, potentially increasing the complexity of the healthcare system.

3.6. Article 6

Further, according to Wang et al. [6] study, a lightweight and secure data-sharing scheme based on proxy re-encryption for Industrial Internet of Things (IIoT) enabled by blockchain technology, security and efficiency challenges are addressed in data sharing within the IIoT ecosystem. The study focuses on the limitations of existing data-sharing schemes in terms of security, computational overhead, and data supervision. Presenting a blockchain-enabled data sharing approach based on proxy re-encryption could solve the mentioned issue. The proposed solution includes key components namely storage and access authentication, on-chain and off-chain collaborative storage mechanisms, data packaging support, and lightweight blockchain operations.

The scheme enables effective data supervision, preventing misuse and enhancing security in IIoT systems. On the other hand, the adoption challenge in introducing a new data-sharing scheme as thorough integration and compatibility testing is required.

3.7. Article 7

On the other hand, the following article examines how IIoT, AI, and cloud computing are integrated into Industry 4.0, emphasizing how these technologies connect real-world objects to the virtual world to increase efficiency. According to Zhang et al. [7], resource limitations, safe data transfer, and user privacy protection are issues that IIoT systems face, particularly in the 5G age. The main issue is the need for enhanced security and dependability in the IIoT, especially in authentication, where current techniques have difficulty evaluating node stability and thwarting malicious activity.

The paper suggests the RRV-BC system, which combines blockchain-assisted access authentication and a random reputation voting mechanism. This technique uses verifiable random functions to lower consensus communication costs while strengthening access

authentication using blockchain and reputation voting. Although it has advantages like improved fault tolerance and data security, it has drawbacks like complexity and scalability.

3.8. Article 8

Moreover, a novel approach for Trust-Aware Blockchain-Based Seamless Authentication for Massive IoT-Enabled Industrial Applications, known as TAB-SAPP, is covered in the study performed by Deebak et al [8]. It emphasizes privacy protection and device integration in a variety of remote scenarios, addressing the urgent demand for strong authentication in IoT-enabled industrial settings [8]. The primary issue addressed is the creation of safe and easy authentication in large-scale Internet of Things systems, considering several variables such device connectivity, data generation, storage, and operation through smart contracts.

TAB-SAPP is a revolutionary concept that uses decentralized infrastructure, encrypted chain-like blocks for data storage, distributed Internet of Things (IoT) devices for data creation, and smart contracts for system management. By utilizing blockchain technology, it manages industrial data and device IDs, improves device authentication, and uses less computing power. A trust-aware security paradigm, easy IoT device integration, and secure blockchain-based authentication are some of its main advantages. The possible drawbacks include single points of failure and scalability problems. TAB-SAPP could be improved by addressing issues with scalability, removing single point of failure vulnerabilities, maximizing resource efficiency, and improving computation and communication in networking systems for industrial applications.

3.9. Article 9

In addition, Li et al. [9] addresses the challenges faced in IIoT devices which has diverse device performance, wide distribution, and vulnerable to spoofing and third-party attacks [9]. The problem statement is to establish a secure and efficient device authentication in IIoT environments as existing authentication technologies lack scalability, efficiency, and dynamic security, hindering the authentication process for IIoT devices. The proposed solutions are lightweight distributed consensus algorithm, leveraging validate-practical Byzantine fault tolerance (vPBFT), lightweight identity authentication protocol (BLMA) to address authentication difficulties among industrial devices, signature algorithm to reduce communication cost and resource usage between devices, and chameleon hash function for blockchain maintenance.

The strength of the proposed technique includes enhanced security, efficiency improvements, reduce resource consumption and communication cost, dynamic security

features, and scalability for large-scale IIoT environments. The weaknesses of the proposed technique are complex implementation, significant resource requirements, and challenges related to compatibility, interoperability, and industry acceptance. The evaluation metrics used in the article include security analysis, energy consumption comparison between other schemes, computational cost analysis, and communication overhead assessment of the PBFT consensus algorithm regarding processing time and traffic generated.

3.10. Article 10

Last but not least, the IIoT revolutionized industrial applications by integrating IoT technology with industrial equipment, which led to significant advancements in Industry 4.0. It combines IoT, mobile communications, AI, cloud computing, and big data analysis in industrial processes. The problem statement is that current authentication method in IIoT only have single-factor authentication and lack flexibility to the increasing number of users and diverse user categories. The solution proposed by Wang et al. was Transfer Learning empowered Blockchain (ATLB), which leverages blockchain technology and transfer learning to enhance privacy preservation for industrial applications [10]. It trains a user authentication model with a leading deep determined policy gradient algorithm and transfers the model locally or cross-regionally to lower model training time.

The strength of the proposed technique is that ATLB provides accurate authentications for IIoT applications and can achieve high throughput and low latency in authentication process. However, it may require significant computational resources for training and deployment, and effectiveness may vary based on complexity and scale of the industrial IoT environment. The evaluation metrics used are authentication accuracy, throughput, latency, privacy preservation and task completion and data reliability.

3.11. Summary

Several other researchers have also contributed in end-to-end security mechanism even with the assistance of the counter partners i.e. universities or industries for broaden implications [11-22]. This research article can act as the guidelines for future young researchers in end-to-end security measures in 6^{th} generation networks. This improved work Securing Industrial IoT: Blockchain Integrated Solution for Enhanced Privacy, Authentication, and Efficiency for the given problem statement is adopted from [6], which act as a benchmark for this research article.

4 PROPOSED SOLUTION

To address the challenges of secure and flexible authentication for IIoT devices, blockchain-enabled authentication frameworks that integrate decentralized identity management, cryptographic techniques, smart contract-based access control, and deep learning-based intrusion detection systems (IDS) is proposed. Figure 2 shows the proposed model.

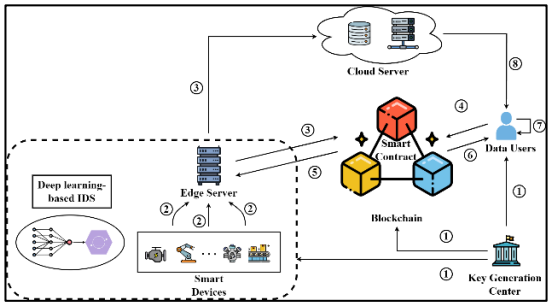

Figure 2. Proposed Model

4.1. Decentralised Device Identity Management

According to Wang et al. [6], blockchain technology is considered a potential option due to its decentralized, tamper-proof, and traceable characteristics, which ensure the safety and efficiency of data access and authentication. This scheme is proposed in multiple works, however, deficiencies in terms of efficiency and security still need further improvement [6]. Weak security and unchecked identification system could lead to leaking of private and important data. The attackers could also take advantage of it and launching both active and passive attacks [6].

In most existing schemes, entities in the IIoT authentication system subscribe to services based on production tasks. Therefore, only these subscribed devices can access the stored data [6]. However, in some cases, the blockchain only verifies the data uploader's identity without determining if the uploader is subscribed to the corresponding service. As a result, it may store illegitimate data. In a worst-case scenario, the blockchain might not even verify if the data uploader or data user is subscribed to the device, let alone the service

With this proposed solution, we aim to build a user verification algorithm for device identity management before entering the smart contract section. This user verification algorithm will function as an additional security layer that ensures only authorized and subscribed devices can interact with the IIoT network and access stored data. The algorithm will rigorously check the identity of devices attempting to access the network. This involves verifying not only the identity of the data uploader but also ensuring that the uploader is subscribed to the appropriate service related to the production tasks. By incorporating this step

before data reaches the blockchain, we prevent unauthorized devices from entering the system and interacting with the smart contract.

The algorithm will also verify that devices are subscribed to the corresponding services they intend to access. This is crucial in ensuring that only legitimate devices involved in the production tasks have the right to upload or retrieve data. This step ensures that any data stored on the blockchain comes from a verified and subscribed source, reducing the risk of illegitimate or malicious data being recorded. Once a device passes the user verification algorithm, it proceeds to interact with the smart contract. The smart contract will then execute predefined actions based on the verified and authenticated data. This integration ensures that all operations carried out by the smart contract are based on trustworthy data, enhancing the reliability and security of the entire IIoT ecosystem.

By verifying both the identity and subscription status of devices, the proposed solution significantly reduces the risk of data misuse. Unauthorized devices and users will be barred from accessing sensitive information or uploading fraudulent data. This robust verification process ensures that data shared within the IIoT network is accurate, legitimate, and securely managed. The enhanced verification process guarantees that only data from trusted and authorized sources is stored and shared within the network. This builds a higher level of trust among IIoT devices and users, promoting a secure and reliable data-sharing environment. Ensuring data trustworthiness not only protects the integrity of the IIoT network but also enhances the overall efficiency and productivity of industrial operations.

While adding an additional verification step may introduce some overhead, the design of the user verification algorithm is optimized for scalability and efficiency. It ensures minimal impact on the performance of the IIoT network while providing maximum security. This solution is scalable and can be adapted to various industrial environments, accommodating the growing number of devices and services in the IIoT ecosystem. In summary, the proposed solution of integrating a user verification algorithm for device identity management before the smart contract section enhances the security and trustworthiness of data in IIoT networks. It ensures that only authorized and subscribed devices can access and share data, thereby preventing data misuse and maintaining the integrity of the IIoT environment.

4.2. Secure Communication Protocols

Cryptographic techniques are essential in securing communications between IIoT devices and backend systems, ensuring both the confidentiality and integrity of data. One of the key methods employed is the Hash-based Message Authentication Code (HMAC), which

combines a secret key with a hash function to secure message transmissions. HMAC operates by utilizing a secret key along with a cryptographic hash function to produce a unique hash value for each message. This process ensures that the message remains confidential during transmission, as only parties possessing the secret key can generate or verify the correct hash value.

To facilitate secure communication, a secret key is generated during both the encryption and decryption processes [8]. This secret key is then used in conjunction with the hash function to encode the data being transmitted. The hash function itself is a mathematical process that converts the input data into a fixed-length string of characters, known as hash values. These hash values are unique to the input data, meaning even a small change in the input will result in a significantly different hash value. This property of hash functions is crucial for ensuring data integrity, as it allows the system to detect any alterations to the data during transmission.

By combining the cryptographic capabilities of HMAC with the robust properties of hash functions, the message can be kept confidential and its integrity ensured. The HMAC algorithm ensures that any tampering with the message can be easily detected, as the hash value generated from the altered message will not match the original hash value produced with the secret key. This dual approach of using a secret key for encryption and hash functions for integrity checking creates a secure communication channel that protects against unauthorized access and data corruption.

In the context of IIoT, where secure and reliable communication is paramount, these cryptographic techniques provide a robust framework for protecting sensitive data. The use of HMAC and hash functions ensures that data exchanged between devices and backend systems remains confidential and unaltered, even in the presence of potential cyber threats. This level of security is essential for maintaining the trust and efficiency of IIoT networks, where the integrity and confidentiality of data are critical for operational success.

In summary, the implementation of cryptographic techniques, specifically HMAC and hash functions, in IIoT communications ensures that data remains confidential and its integrity is maintained throughout transmission. The use of a secret key during encryption and decryption processes, combined with the fixed-length output generated by hash functions, creates a secure communication channel that can effectively safeguard against unauthorized access and data tampering.

4.3. Smart Contracts for Access Control

Furthermore, these secret keys could serve as reference keys when passing through the smart contract to keep track and confirm the successive flow of transactions. By incorporating secret keys, the smart contract can ensure the authenticity and integrity of each transaction, providing an additional layer of security. This mechanism allows the smart contract to verify that each transaction originates from a legitimate and authorized source, thereby preventing unauthorized access and fraudulent activities.

Smart contracts can automate the transaction process while providing transparency and secure records to all parties involved. The automation aspect of smart contracts significantly reduces the need for manual intervention, thus minimizing human error and increasing efficiency. Every transaction recorded on the blockchain is transparent and immutable, meaning that once a transaction is recorded, it cannot be altered or deleted. This feature ensures that all parties involved in the transaction have access to the same immutable record, fostering trust and accountability.

Moreover, each party involved in the transaction would own a copy of the transaction record. This decentralized approach ensures that no single entity has control over the transaction history, enhancing the system's resilience against tampering and corruption. Each party can independently verify the transaction records and detect any anomalies that may occur during the mining process. If any discrepancies are found, they can be addressed promptly, ensuring the integrity of the entire transaction flow.

The use of smart contracts in this context aligns with the principles outlined in various studies [3], [6], [8], which highlight the benefits of using blockchain technology for secure and transparent data management in Industrial Internet of Things (IIoT) environments. Smart contracts not only streamline the transaction process but also provide a robust framework for verifying and validating transactions in real-time. This capability is crucial in environments where trust and data integrity are paramount, such as IIoT networks.

In summary, by leveraging secret keys and smart contracts, the proposed solution ensures that transactions within the IIoT network are secure, transparent, and verifiable. Each party involved in the transaction process can independently confirm the authenticity of the transactions and monitor for any anomalies, thereby maintaining the integrity and trustworthiness of the entire system.

4.4. Deep Learning Intrusion Detection System (IDS) for Anomaly Detection

In [1], the integration of an Intrusion Detection System (IDS) with Artificial Intelligence (AI) has shown to be highly effective in detecting network anomalies and cyberattacks,

offering superior performance compared to traditional methods. The primary advantage of employing AI in IDS is its capability to reduce human errors by automating the detection process, thus providing a more reliable and accurate security solution. This deep-learning-based IDS leverages advanced AI components to analyse vast amounts of data and identify any deviations from normal network behaviour, which could indicate potential intrusions or cyber threats from hijackers.

The system utilizes a Contractive Sparse Autoencoder (CSAE) for feature extraction. CSAE is a type of neural network that learns efficient representations of input data by minimizing reconstruction error and incorporating a regularization term to ensure robustness and sparsity in the features. This process effectively condenses the data into a more manageable form, highlighting the most critical features necessary for accurate anomaly detection. By focusing on these key features, the IDS can more effectively distinguish between normal and abnormal network behaviour.

Following the feature extraction phase, the Attention-Based Bidirectional Long Short-Term Memory (ABiLSTM) networks are employed to process the extracted features. ABiLSTM networks are an advanced type of recurrent neural network (RNN) designed to handle sequential data and capture long-term dependencies. The bidirectional nature allows the network to consider both past and future contexts in the data sequence, while the attention mechanism helps the model to focus on the most relevant parts of the sequence when making decisions. This dual capability enhances the IDS's ability to detect subtle anomalies that may signify cyberattacks.

Finally, a Softmax Classifier is used to identify and categorize the detected anomalies. The Softmax Classifier is a standard component in neural network architectures for multi-class classification problems. It converts the output of the neural network into a probability distribution over the possible classes, allowing the IDS to classify the type of cyberattack with a high degree of confidence. This classification step is crucial for determining the appropriate response to different types of detected intrusions.

In summary, the integration of CSAE for feature extraction, ABiLSTM networks for anomaly detection, and the Softmax Classifier for classification forms a robust and efficient deep-learning-based IDS. This system not only improves the accuracy of intrusion detection but also automates the process, significantly reducing the likelihood of human errors and enhancing the overall security of the network.

5 RESULT AND ANALYSIS

5.1. Secure Communication Protocols

Secure Communication Protocols utilises HMAC to enable a more secure and confidential communication between IIOT devices and backend system. It is a cryptographic technique that uses the combination of hash function and secret key, providing confidentiality of a message or transmission. The message is encrypted and hashed multiple times during transmission to ensure the messages are safe from third party. The integration of HMAC in secure communication protocols highlights their critical role in safeguarding data integrity and confidentiality in network communications.

HMAC consists of two parts which are shared set of cryptographic keys for sender and recipient for generating and verifying HMAC, and a generic cryptographic hash function such as SHA-256. The HMAC computation is as follows:

$$HMAC(K, m) = H((K' \oplus opad)||\, H((K' \oplus ipad)||M))$$

- *H*: Cryptographic hash function.
- *K*: Secret Key.
- *K'*: Block sized key derived from K, either by padding to right with zeros up to block size or hashing to less than or equal to block size then padding to right with zeros.
- *M*: Message.
- *opad, ipad*: padding values used in HMAC computation.
- $\oplus$*:* XOR (exclusive OR) operator.
- ||: concatenation.

The key and message are hashed in separated steps in HMAC. Firstly, the sender hashes the data with a secret key and send it to the server as a request. Then the server generates its own HMAC to prevent extension attacks which could potentially expose parts of the key as additional MACs are generated. After the process is completed, the message will be irreversible and hack-proof. This can ensure the confidentiality of the messages transferred between devices.

5.2. Smart Contracts for Access Control and Improved Decentralised Device Identification Management

Smart contract is implemented to improve access control by indirectly enhance security, transparency, and immutability. Cryptographic secret keys are central to this mechanism, serving as reference keys to track and confirm transactions. These keys help verify and validate transactions, ensuring their integrity and authenticity. Moreover, these keys are important in driving an automation to reduce human error and tampering, meanwhile

blockchain allows all parties to have a transparent transaction record, aiding in anomaly detection. Therefore, manual inspection will only be used in tracking the transaction record. As such, an AI should be implemented to aid this manual inspection as well.

Access control is managed through decentralized, tamper-resistant smart contracts that verify identities and enforce policies automatically, eliminating the need for a central authority. All access requests and transactions are logged on the blockchain, providing a transparent audit as mentioned previously. Therefore, the following techniques and algorithms will be implemented in smart contract to enhance the performance, improve the efficiency and security.

Primitively, smart contracts' key formulae and methods include encryption and decryption, where the plaintext *MM*M is encrypted using the secret key *KK*K to produce the ciphertext *CC*C (*C=EK(M)C = E_K(M)*C=EK (M)), and the ciphertext *CC*C is decrypted using the same secret key *KK*K to retrieve the original plaintext *MM*M (*M=DK(C)M = D_K(C)*M=DK (C)). Hashing is also employed, where each transaction *TT*T is hashed to ensure its integrity (*H(T)=hash(T)H(T) = \text{hash}(T)*H(T)=hash(T)). The hash function produces a fixed-size output *H(T)H(T)*H(T) from the input transaction data *TT*T, and stored hashes *H(Tstored)H(T_{\text{stored}})*H(Tstored) are compared with new hashes *H(T)H(T)*H(T) to validate transactions.

Furthermore, decentralised device identification management uses another technique to improve the security factor by verifying the user from getting access with the data content with using implementing the verification algorithm in Edge Server (ES) as shown in figure 1.2 above. Assume there are ɳ final messages corresponding to α, which are *(σn, cn, Un, PIDn, PKn, APK, tsn).*

- *σn*: A signature.
- *cn*: A challenge or cryptographic value.
- *Un:* Some unique identifier or data related to the message.
- *PIDn*: A device or process ID.
- *PKn*: A public key.
- *APK*: Another public key or cryptographic key.
- *Tsn:* A timestamp.

ES would first check on the timestamp of the message sent from the user to prevent any potential replay attacks where the message would be discarded if it is not fresh. However, this is not enough. ES will then classify if the keys of the message if the message is approved for the services' accessibility. After the early assessment, the further verification algorithm as

known as small exponential test technique is being applied. Thus, the algorithm will then choose a vector $v = \{v1, v2, \ldots, vn\}$ and then verify the message by batch with the algorithm. The equation of the algorithm is listed as followed:

$$\left(\sum_{i=1}^{n}(vi \cdot \sigma i)\right) \cdot P = \sum_{i=1}^{n}(vi \cdot PKi) + \left(\sum_{i=1}^{n}(vi \cdot si)\right) \cdot P\text{pub} + \sum_{i=1}^{n}(vi * Ui * si)$$

As such, the equation has to be balanced where left hand side is equals to the right-hand side to approve the message to be access with the service is being classified and assigning to.

5.3. Deep Learning Intrusion Detection System (IDS) for Anomaly Detection

As mentioned in the previous sections, this solution can effectively detect and mitigate cyber threats. Deep Learning IDS helps in analysing the network traffic with the aid of deep learning using Contractive Sparse Autoencoder (CSAE) and Attention-Based Bidirectional Long Short-Term Memory (ABiLSTM) Networks to identify anomalies and potential security breaches [1].

With this solution, the session based mutual authentication and key agreement mechanism for the current authentication mechanism is improved by establishing a secure data sharing channel [1].

The evaluation metrics used for this solution are precision, recall, F1 score, and false acceptance rate (FAR) as follows where TP is True Positive, FP is False Positive, TN is True Negative, FN is False Negative [1]:

$$Precision = \frac{TP}{TP + FP}$$

$$Recall = \frac{TP}{TP + FN}$$

$$F1 - Measure = \frac{2 \times recall \times precision}{recall + precision}$$

$$FAR = \frac{FP}{FP + TN}$$

Figure 5.1 and 5.2 below shows the result of the evaluation metrics on 2 different dataset which are ToN-IoT and the EDGE-IIoTSet respectively [1]. In figure 3 and 4 below, the average precision among detecting all types of attacks for both dataset is above 90% which

shows a high confidence of the IDS. Next, the average FAR of among detecting all types of attacks in both datasets are low which indicates low false alarm rate.

Parameters	Backdoor	DDoS	DoS	Injection	MITM	Normal	Password	Ransomware	Scanning	XSS
Precision	99.950	96.561	98.910	92.980	92.203	99.996	98.142	99.304	98.736	99.068
Recall	99.834	92.613	98.877	96.769	86.759	100.00	99.533	99.237	99.591	97.581
F1-score	99.892	94.546	98.894	94.837	92.565	99.998	98.832	99.271	99.162	98.319
FAR	0.00002	0.0014	0.00049	0.0032	0.00001	0.00006	0.00085	0.00030	0.00059	0.00041

Figure 3: Prediction result based on the Deep-Learning based IDS using NoT-IoT dataset [1].

Parameters	Normal	DDoS_UDP	DDoS_ICMP	SQL_injection	DDoS_TCP	Vulnerability_scanner	Password	DDoS_HTTP	Uploading	Backdoor	Port_Scanning	XSS	Ransomware	Fingerprinting	MITM
Precision	100.00	99.90	100.00	61.47	72.76	94.72	43.18	93.11	63.05	99.06	87.38	47.11	99.35	100.00	100.00
Recall	100.00	100.00	99.98	12.89	99.76	84.35	88.50	76.23	44.36	97.78	32.02	77.23	95.23	97.40	100.00
F1-score	100.00	99.953	99.99	21.31	84.15	89.23	58.05	83.83	52.06	98.42	36.44	58.52	97.25	72.94	100.00
FAR	0	0.00006	0	0.0021	0.0100	0.0012	0.031	0.0014	0.0050	0.0001	0.0003	0.0067	0.00003	0	0

Figure 4: Prediction result based on the Deep-Learning based IDS using EDGE-IIoTSet dataset [1].

6 CONCLUSION

The study emphasizes the vulnerability of IIoT networks to security threats due to the diverse nature of devices and communication channels. To enhance the safety and security of IIoT protocols, a comprehensive solution is proposed that includes decentralized device identity management, secure communication protocols, smart contracts for access control, and a deep learning-based intrusion detection system (IDS) for anomaly detection.

Decentralized device identity management is achieved through the implementation of a Smart Contract Key Generation Center (SC-KGC), which is responsible for generating and distributing cryptographic keys to devices. This decentralized approach enhances data security by eliminating the single point of failure inherent in centralized key management systems, thereby improving privacy preservation and reducing the risk of key compromise.

Secure communication protocols are essential for maintaining the confidentiality and integrity of data transmitted between IIoT devices and backend systems. These protocols leverage cryptographic techniques, such as encryption and hash-based message authentication codes (HMAC), to ensure that only authorized devices can access and transmit data. The use of secure communication protocols prevents unauthorized access and data tampering, thereby safeguarding sensitive information.

Smart contracts are employed for access control, automating the process of verifying and granting access to data and services within the IIoT network. By embedding access control rules within smart contracts, the system ensures that only authenticated and authorized devices

can interact with the network. This automation reduces the likelihood of human error and enhances the efficiency of access management.

The integration of a deep learning-based IDS further strengthens the security of the IIoT network by continuously monitoring for anomalies and potential intrusions. The IDS utilizes advanced AI techniques, such as Contractive Sparse Autoencoder (CSAE) for feature extraction and Attention-Based Bidirectional Long Short-Term Memory (ABiLSTM) networks for anomaly detection, to identify and respond to cyber threats in real-time. This proactive approach enables the system to detect and mitigate security breaches before they can cause significant harm.

The results and analysis of the proposed system indicate that leveraging blockchain technology and smart contracts significantly improves the security and efficiency of IIoT applications. The decentralized approach to key management through SC-KGC enhances data security and privacy preservation, while the use of secure communication protocols ensures the confidentiality and integrity of data. Additionally, the integration of a deep learning-based IDS provides robust anomaly detection capabilities, further safeguarding the network from potential cyber threats.

Overall, integrating blockchain technology and smart contracts with secure communication protocols and deep learning-based IDS can significantly improve the security of IIoT networks. This comprehensive solution addresses the diverse security challenges posed by the heterogeneous nature of IIoT devices and communication channels, ensuring a more resilient and trustworthy IIoT environment.

7 ACKNOWLEDGEMENT

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

REFERENCES

[1] 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.

[2] Abdullah Ayub Khan *et al.*, “Data Security in Healthcare Industrial Internet of Things with Blockchain,” *IEEE Sensors Journal*, vol. 23, no. 20, pp. 25144–25151, Oct. 2023, doi: https://doi.org/10.1109/jsen.2023.3273851 .

[3] Ahamed Aljuhani *et al.*, “A Deep Learning Integrated Blockchain Framework for Securing Industrial IoT,” *IEEE Internet of Things Journal*, vol. 11, no. 5, pp. 1–1, Jan. 2023, doi: https://doi.org/10.1109/jiot.2023.3316669 .

[4] Ahmad, Z., et al., *MS-ADS: Multistage Spectrogram image-based Anomaly Detection System for IoT security.* Transactions on Emerging Telecommunications Technologies, 2023. **34**(8): p. e4810.
[5] B. D. Deebak, F. H. Memon, K. Dev, S. A. Khowaja, W. Wang, and N. M. F. Qureshi, "TAB-SAPP: A Trust-Aware Blockchain-Based Seamless Authentication for Massive IoT-Enabled Industrial Applications," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 1, pp. 1–1, 2022, doi: https://doi.org/10.1109/tii.2022.3159164 .
[6] Chan, K. Y., Abdullah, J., & Khan, A. S. (2019). A framework for traceable and transparent supply chain management for agri-food sector in malaysia using blockchain technology. *International Journal of Advanced Computer Science and Applications*, *10*(11).
[7] F. Li *et al.*, "BLMA: Editable Blockchain-Based Lightweight Massive IIoT Device Authentication Protocol," *IEEE internet of things journal*, vol. 10, no. 24, pp. 21633–21646, Dec. 2023, doi: https://doi.org/10.1109/jiot.2023.3308725 .
[8] F. Wang, J. Cui, Q. Zhang, D. He, C. Gu, and H. Zhong, "Lightweight and Secure Data Sharing Based on Proxy Re-Encryption for Blockchain-Enabled Industrial Internet of Things," *IEEE internet of things journal*, vol. 11, no. 8, pp. 14115–14126, Apr. 2024, doi: https://doi.org/10.1109/jiot.2023.3340567 .
[9] G. Rathee, F. Ahmad, N. Jaglan, and C. Konstantinou, "A Secure and Trusted Mechanism for Industrial IoT Network Using Blockchain," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 2, pp. 1–10, 2022, doi: https://doi.org/10.1109/tii.2022.3182121 .
[10] Iqbal, A. M., Khan, A. S., Iqbal, S., & Senin, A. A. (2011). Designing of success criteria-based evaluation model for assessing the research collaboration between university and industry. *International Journal of Business Research and Management*, *2*(2), 59-73.
[11] Khan, A. S., Balan, K., Javed, Y., Tarmizi, S., & Abdullah, J. (2019). Secure trust-based blockchain architecture to prevent attacks in VANET. *Sensors*, *19*(22), 4954.
[12] Khan, A. S., Fisal, N., Kamilah, S., & Abbas, M. (2010). Efficient distributed authentication key scheme for multi-hop relay in IEEE 802.16 j network. *International Journal of Engineering Science and Technology (IJEST)*, *2*(6), 2192-2199.
[13] Khan, A. S., Mehdi, M. H., Uddin, R., Abbasi, A. R., & Nisar, K. (2023). Ensemble Based Automotive Paint Surface Defect Detection Augmented By Order Statistics Filtering Using Machine Learning. *Authorea Preprints*.
[14] Khan, A. S., Yahya, M. I. B., Zen, K. B., Abdullah, J. B., Rashid, R. B. A., Javed, Y., Khan, N. A., & Mostafa, A. M. (2023). Blockchain-based lightweight multifactor authentication for cell-free in ultra-dense 6G-based (6-CMAS) cellular network. *IEEE Access*, *11*, 20524-20541.
[15] Kilat, V. S., Khan, A. S., James, E., & Khan, N. A. (2023). Recapitulation of Survey on Taxonomy: Security Unmanned Aerial Vehicles Networks. *Journal of Computing and Social Informatics*, *2*(1), 21-31.
[16] 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.
[17] P. Zhang, P. Yang, N. Kumar, C.-H. Hsu, S. Wu, and F. Zhou, "RRV-BC: Random Reputation Voting Mechanism and Blockchain Assisted Access Authentication for Industrial Internet of Things," *IEEE transactions on industrial informatics*, vol. 20, no. 1, pp. 713–722, Jan. 2024, doi: https://doi.org/10.1109/tii.2023.3271127 .

[18] Razali, M. Q. B., Khan, A. S., Khan, S. B. S., & Manggau, A. A. (2023). Awareness of National Cyber Security Weaknesses Due to Cyber-Attacks Through the Use of UAV. *Journal of Computing and Social Informatics*, *2*(1), 13-20.

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

[20] W. Wang, H. Xu, M. Alazab, T. R. Gadekallu, Z. Han, and C. Su, "Blockchain-Based Reliable and Efficient Certificateless Signature for IIoT Devices," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 10, pp. 1–1, 2021, doi: https://doi.org/10.1109/tii.2021.3084753 .

[21] W. Xiaoding, S. Garg, H. Lin, Md. Jalilpiran, J. Hu, and M. S. Hossain, "Enabling Secure Authentication in Industrial IoT with Transfer Learning empowered Blockchain," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 11, pp. 1–1, 2021, doi: https://doi.org/10.1109/tii.2021.304940

[22] Y. Yang, J. Wu, C. Long, W. Liang, and Y.-B. Lin, "Blockchain-Enabled Multiparty Computation for Privacy Preserving and Public Audit in Industrial IoT," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 12, pp. 9259–9267, Dec. 2022, doi: https://doi.org/10.1109/tii.2022.3177630 .