SMDI
Digital Management Sciences Journal *Vol.1/ Issue2*

Received: 24-6-2024 Accepted:28-6-2024 Published: 30-6-2024

Research Article

The impact of Block chain-Based System on Goods Tracking and management in Industrial Environment

1. Sherene Saw Tyng Xin
Faculty of Computer Science and Information Technology, Universiti Malaysia Sarawak
Kota Samarahan, Malaysia
Email: 76757@siswa.unimas.my
2. Gigi Yong
Faculty of Computer Science and Information Technology, Universiti Malaysia Sarawak Kota Samarahan, Malaysia
Email: 74905@siswa.unimas.my
3. Tang Jhen Nee
Faculty of Computer Science and Information Technology, Universiti Malaysia Sarawak Kota Samarahan, Malaysia
Email: 77363@siswa.unimas.my
4. Teng Li Ying
Faculty of Computer Science and Information Technology, Universiti Malaysia Sarawak Kota Samarahan, Malaysia
Email: 76977@siswa.unimas.my
5. Wallance Tang Zong Chao
Faculty of Computer Science and Information Technology, Universiti Malaysia Sarawak Kota Samarahan, Malaysia
Email: 77122@siswa.unimas.my
6. Shakeel Ahmed
Department of eLearning (ELC), Jazan University
Email: shakeel@jazanu.edu.sa

Citation
Xin, S., S., T., Yong, G., Nee, T., J., Ying, T., L., Chao, W., T., Z., and Ahmad, S., (2024) The impact of Blockchain-Based System on Goods Tracking and management in Industrial Environment, *Digital Management Sciences Journal* , *1*(2), pp 91-105

ABSTRACT

In the domain of Industrial Internet of Things (IIoT), the demand for robust and secure methods for goods tracking and management has become growingly critical. Conventional methods face significant challenges, including authentication, computational overhead, cyber security, and data integrity. To address these issues, this paper proposes a block-chain based system for goods management and tracking with enhanced authentication mechanism by leveraging the decentralized nature of block-chain technology and integrating Elliptic Curve Digital Signature Algorithm (ECDSA) with Elliptic Curve Cryptography-Zero Knowledge Proof (ECC-ZKP). The proposed solution aims to ensure the authenticity and the integrity for all the transaction while providing high level privacy-preserving verification without revealing information. The research in this paper demonstrates that the proposed block-chain-based system significantly enhances security performance, key management and operational efficiency, addressing the existing challenges in IIoT goods tracking and management, providing a resilient framework for more secure industrial operations in managing goods.

Keywords: Digital Management, Industrial Internet of Things (IIoT), blockchain, authentication, ECDSA, ECC-ZKP

1. Introduction

With the emergence of the Internet of Things (IoT), devices can communicate autonomously with each other, generating data without human intervention. The IoT is essential across various critical sectors like energy, agriculture, and communications, evolving into the Industrial Internet of Things (IIoT) 0. However, this advancement brings various issues and challenges, especially in the realm of goods tracking and management. The rapid expansion of IIoT poses unpredicted challenges, especially in transparency, cybersecurity, and data integrity. Conventional methods for tracking and managing goods in industries face inefficiencies and vulnerabilities to breaches. To address these challenges, a block chain-based system emerges as a promising solution to act as an authentication platform due to its multiparty consensus and immutability 0. Using block chain technology in goods tracking and management offers key advantages like ensuring data integrity and security through cryptographic measures. It also enables real-time visibility for stakeholders to monitor the status and the location of goods, resulting in transparency across supply chains. Each transaction or interactions, from production to delivery process, can be securely stored or recorded on the block chain. In this context, this paper aims to explore the potential of block chain in developing a robust and transparent system for tracking and managing goods in industry.

Fig 1 illustrates an ecosystem of the supply chain generated by block chain technology, with interconnected nodes symbolizing various stages of the supply chain, including consumers, retailers, distributors, suppliers, and manufacturers as data users. As a central node, smart contracts enable secure transactions between parties. This decentralized and unchangeable system guarantees the integrity and security of supply chain, enhancing trust and operational efficiency in goods tracking and management.

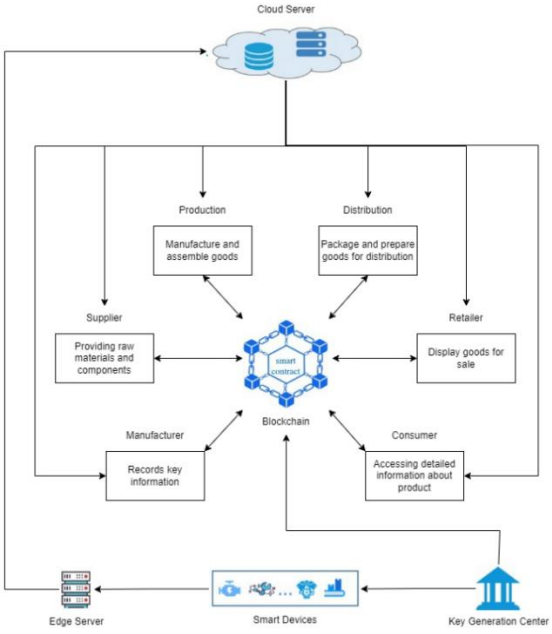


Fig. 1: Block chain-based data-sharing framework for goods tracking and management 0

2. Problem statements

In recent years, various mechanisms have been designed and proposed to address the challenges. However, the current solutions often fall short in resolving the issues specific to IIoT. There are still

many emerging problems that need to be addressed.

1) **Centralized authentication:** Conventional IoT device authentication schemes overly depend on trusted centralized third-party platforms 0. This centralized authentication approach can lead to security vulnerabilities. Despite most existing authentication schemes being block chain-based, numerous drawbacks remain in the current solutions.
2) **Resources consumption and computational overhead:** Industrial-scale IoT devices with constrained computational capabilities face challenges in traditional authentication methods, sacrificing resources and time, resulting in re-authenticating certificates during device communication 0. While symmetric encryption is used for authentication, key distribution remains challenging, especially for large-scale IoT.
3) **Vulnerability to cyber security:** Existing industrial systems, especially with the rise of IIoT, are vulnerable to cyber security threats and challenges. Intruders can easily attack and tamper with stored and manufacturing data, resulting in incorrect decisions made and controls that caused a substantial danger to interconnected systems 0. The diverse characteristics of industrial organizations leads to vulnerability to a variety of cybersecurity threats, requiring secure control and persistent management procedures.

To address these challenges, we can introduce a block chain-based system with enhanced authentication mechanism to enhance data integrity and security in industrial environments. By utilizing the immutability and decentralized nature of block chain technology, data tempering can be mitigated and the integrity of stored data can be guaranteed. Additionally, smart contracts can play a vital role in automating and securing transactions, which reduces the possibility of data manipulation and unauthorized access.

3. Related works

Rathee et al. 0 had proposed a security protocol employing trust assessment system in the device for decision-making to address various cyber security threat and challenges. The paper had identified various challenges and threats in the fast-rising manufacturing paradigm where the current industrial mechanism is vulnerable to attacks and tampering results in incorrect decision, inefficient data tracing hindering the monitoring and control process, security issues in transmission and communication due to their nature and physical configuration, high confidentiality, authentication and integrity required in persistent management of smart devices and the existing cyber security challenges in centralized data transmission. Hence, to address to the issues stated, a reliability-enhanced IIoT system integrating transparent and autonomous monitoring with trusted control, Trust-BlkSys is proposed with the aim to achieve enhancement on information protection, productivity, and precise decision-making during transmission of message as well as providing continuous surveillance and protection to the environment from a distance. The strengths of this proposed techniques lie in the enhanced security through integration of trust evaluation and transparent communication environment and improved data delivery as the proposed mechanism could ensure high data delivery through accurately identifying the malicious nodes. However, this proposed solution has higher complexity, requires intensive resources as well as scalability issues which can be a concern when dealing with large number of devices. This proposed solution is evaluated with several metric, convergence time where it measures the time taken for the system to reach a stable state, sensitivity, to identify its behaviour, data delivery ratio, to calculate the percentage of successful

data transmission and false authentication rate to measure the percentage on accuracy of malicious node identified.

The paper by Zhang et al. 0 presents a block chain based novel verification system for data security in IIoT where it aims to uphold a decentralized, verified, and synchronized transaction record without centralized control. This paper is presented to address the existing issues of difficulty in authentication and authorization identification due to reliance across diverse sophisticated software and hardware platforms, complex key management problem as the conventional key structure system is prone to single and failures and the existing node's reliability concerns as the conventional IoT device overdependence on centralized third-party platforms for trust. The solution is proposed to prevent attackers from counterfeiting legitimate users' access while reducing the burden on the block chain. The proposed architecture consists of 3 layers, layers of IoT entities, virtual nodes, and block chain infrastructure. A fast consensus verification algorithm is also applied to enhance the fault tolerance capability. The strength of the proposed solution is its ability to improvise the transaction per second by 29% and the fault tolerance rate sees an average improvement of 5% as well. However, the proposed solution requires high storage cost associated with the ECDSA and faces scalability issues for the consensus algorithm. Transaction per second, fault tolerance and security performance are utilized to assess the performance of the proposed solution.

The study by Dong et al. 0 is to set up a dependable trust management across various industrial enterprises. The solution is proposed to address the issues of complex certificate management and key escrow issues. This study proposed an inter-domain reciprocal authentication mechanism for the Decisional Diffie-Helman problem and symmetric encryption algorithm to achieve secure authentication and bring a solution to the key retention issue. An Ethereum consortium block chain based on Proof-on-Authority is built to prove real-life applications while key mechanism is constructed to elevate the security properties as well as reducing the overall computing resources. Strength of this study include its ability to resist attacks, identification of impersonation attacks and distributed denial-of-service. However, the proposed solution faced challenges in certain security properties where it lacks support for anonymity and inability to achieve public key revocability. Computational cost analysis, communication cost analysis and security properties are used as evaluation metrics to determine performance.

The paper presented by Li et al. 0 mainly discussed on the cooperative identity verification protocol known as Block chain-Based Lightweight Massive Authentication (BLMA) for large-scale IIoT devices and validate-practical Byzantine algorithms for fault tolerance. This paper is proposed to address the existing problem of security and issues on identity authentication for resource constrained IIoT devices. Hence, a simplified vPBFT consensus algorithm is developed to establish agreement on authentication results, online and offline signature mechanism is introduced for computational resource reduction purposes, verification protocol called BLMA is proposed to address the problem of terminal identity while ensuring high security needs. The strength of the proposed system is scalability, reduced overhead cost, energy consumption and enhanced security. However, delay is expected to be longer than desired in the consensus process and the storage overhead may be an issue when situated in environments with limited resources. This proposed solution used transmission overhead, operational latency, confidentiality assurance, risk evaluation, communication overhead analysis, energy consumption performance, computational overhead comparison and observational outcomes of certificate invalidation procedure analysis as metrics to measure the performance.

The paper discussed by Li et al. 0 enhance protection on data privacy of the IIoT and guarantee the security and reliability of cross-domain devices. This paper revolves around the security and trust issues of inter-domain devices as diverse domain utilize different authentication systems resulting them to be incompatible and unable to authenticated. Privacy of the device faces high risk in information leaking when identity is required or when multidomain network is under attack. Hence, a double layer consortium block chain security framework incorporating cross-domain interaction through virtual sub-chains and device trust level is proposed to store the private and large data on block chain device and minimize the sharing of domain data between different entities. A layered trust system based on federated block chain monitoring is also proposed to improve the trust and break down barriers between domains. The proposed solution managed to improve the overall detection accuracy, reduce device authentication overhead and improvise its overall trust evaluation. However, this proposed solution is extremely complex for implementation and extensive robust network resources are required. The solutions are evaluated with abnormal behavior recognition, resource utilization, system stability and experimental platform in completing device authentication.

The paper discussed by Qian et al. 0 focuses on Hybrid Physical Unclonable Function (hybrid-PUF) integrated consortium block chain for IIoT verification which assign various devices generating distinct types of PUFs and utilizing them for diverse functions within Hybrid Physical Unclonable Function-based Consortium Block chain (HPCchain). Several problems are addressed in the paper, the fast-increasing network complexity are causing issues on privacy and trust, accommodation of multiple communication methods can cause fragile network connection leading to eavesdropping and stacks, uniformed authentication scheme can leads the system to be vulnerable to fake identities, traditional storing methods can poses risk in data leakage and unauthorized modification and the existing authentication scheme lacks of consideration for architectural differences that hinders the realization of uniform IIoT authentication. Hence, HPCchain, a hybrid-PUF-based consortium block chain composed of multiple layers, asset layer, block chain layer, data layer and application layer and organization with interconnected channels for IIoT authentication. HPCchain topology consist of two parts as well, organization and channel as well as Certificate Authority (CA) and Peer. Supported by hybrid-PUF, consistent registration and verification for HPCchain is presented. This strength of this proposed solution is enhanced security with hybrid-PUF based authentication offering inherent resistance to cloning and tampering, reducing redundant execution where it manages to achieve higher transaction throughput improving the overall performance and efficiency. However, the proposed solution could pose challenges in environment variability as consistent and reliability across the entire network is compulsory and the complexity of system architecture may bring deployment challenges as well. The proposed solution is evaluated with performance comparison, storage overhead, inspection on PUF-Based consensus mechanism and inspection on authentication.

The paper by Aljuhani et al. 0 proposed a solution to safeguard communication and guarantee data confidentiality. This proposed solution is to address to the security and privacy challenges where the sensitive nature of IIoT makes them vulnerable to cyber issues and the limitation in existing solution where low performance, computation overhead and scalability issues are detected. Thus, a new deep learning-driven Intrusion Detection System (IDS) integrating contractive sparse auto encoder (CSAE), attention-based bidirectional long short-term memory and softmax classifier is proposed for enhanced detection. Session-oriented reciprocal authentication and key agreement is suggested as well for secure communication. The strength of proposed solutions lies in its robustness with its low False Acceptance Rate and the model also managed to achieve high accuracy on ToN-IoT and Edge-IIoTset datasets.

However, potential computational overhead and scalability issues may exist since IIoT is fast growing and employ integration of multiple devices. The solution is evaluated with precision, F1-Score, recall and False acceptance Rate to access its accuracy in detecting cyber attacks.

The paper by Rathee et al. 0 address the need of secure communication, bringing enhancement in security and trust. The proposed solution aims to address the vulnerabilities of IIoT towards attackers which lead to high security risk. Hence, a centralized IoT device is selected to handle the responsibilities of IoT devices and exclude the MD from network participation as well as establish a secure and trusted environment. Block chain based data model is also integrated to achieve transparency in data. This block chain based solution managed to enhance the overall security level through the provision of a transparent and tamper-proof system while maintaining the integrity of stored information. However, the solution experienced potential delay in block verification process which may be a concern in real time application. The proposed solution is evaluated with success rate, network performance and trust computation accuracy.

The study by Wang et al. 0 is focusing on ensuring secure and efficient data sharing since IIoT has been integrating various smart device and emerging technology in production process. However, the existing conventional block chain based schemes faces challenges in security and efficiency such as data tampering, privacy breaches and intensive computational overhead. Hence, a block chain-powered data-sharing protocol utilizing proxy re-encryption is proposed where the framework would utilize both on-chain and off-chain collaborative storage methods to conserve storage capacity as well as enhancing the data packing to improvise the existing data storage efficiency. The strength of this solution is guaranteed confidentiality, integrity and anonymity of data as well as reducing the overall computation overhead. However, this proposed solution heavily rely on the infrastructure of block chain which may be a concern when applied in decentralized or resource-constrained environments. This study uses evaluation metrics of security analysis, performance evaluation, scalability, and comparisons with related scheme analysis to measure the performance.

The paper proposed by Khan et al. 0 focuses on challenges related to data security in electronic healthcare environment through the integration of Hyper ledger block chain technology and the IIoT. This study is proposed to address data security issues as well as the increasing issues of node connectivity rate, parallel data sharing failure, and delivery which leads to challenges within centralized healthcare system application such as user registration, authentication, access control, data sharing, resource utilization, and privacy concerns. Hence, an IIoT-based modular system enabled by Hyper ledger block chain BHIIoT utilizing a tailored efficient block chain multi-prood-of-work (POW) is proposed with a consortium employing dual communication pathways, on-chain and off-chain, for peer-to-peer linkage and information exchange while incorporating the NuCypher threshold re-encryption mechanism, chain codes and trace transactions. The proposed solution managed to reduce the overall computational resources, network bandwidth, and improvise its productivity but this solution also highlights the potential security issues in future with reliance on centralized network pathways for internet-based information sharing. This proposed solution is evaluated several metrics such as transaction procurement and delivery, resource utilization, confidentiality maintenance, interconnectivity, cryptographic method, linkage of server less nodes, scale, and effectiveness.

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 [1-12]. This

research article can act as the guidelines for future young researchers in end-to-end security measures in 6 the generation networks. This improved work of a block chain-based system for goods tracking and management in industrial environment for the given problem statement is adopted from Wang et al. 0 and Zhang et al. 0 which act as a benchmark for this research article.

4. PROPOSED SOLUTIONS

Just as mentioned, various solutions have been proposed and implemented to address the existing issues especially transparency, cyber security and data integrity. However, it is undeniable that the issues still exist in the authentication mechanism which can cause loss. Hence, a block-chain based system for goods management and tracking with enhanced authentication mechanism is proposed with reference on 0 to achieve robust security and efficiency. The paper by Zhang et al. 0 involves the integration of block chain and Elliptic Curve Digital Signature Algorithm (ECDSA) in their authentication mechanism for secure access authentication in IIoT. The respective paper uses ECDSA to generate public and private key pairs and apply digital signature to authenticate the identity of device and operators within the block chain network. Thus, A new solution involving integration of ECDSA with Elliptic Curve Cryptography-Zero Knowledge Proof (ECC-ZKP) is proposed to bring enhancement into the authentication mechanism of our block chain-based system.

Utilizing block chain-based system that embodies decentralized nature, it distributes control, authority and ownership among a network of participants or nodes eliminating the traditional centralized authentication which rely on central authority for identities management and verification. With block chain-based system, the data will be stored in multiple nodes in decentralized network where each node will maintain a copy of nodes which greatly improve its fault tolerance as failure of a small number of nodes would not affect the network and data integrity. Besides, block chain practices immutable ledger for guaranteed integrity in data where they are tamper-resistant and transparent which are important for the goods tracking and management system where the data such as transaction, shipment, payment records and authentication data can be securely recorded on the block chain. The block chain based system also does include smart contract as an automated self-executing agreement that automates enforcement of policies that govern the goods management process. For instance, the smart contract can define rules for automated invoicing and payment settlement issues as well ensuring trust and reducing the risk of dispute in transactions. Focusing on authentication, the decentralized nature of block chain would allow the users to authenticate themselves and interact with the system securely through unique digital identity represented by a public-private key pair and with smart contract all the attempts to access to the networks will be recorded by a smart contract to create a tamper-proof record on the block chain. Modification and alteration are impossible to ensure transparency traceability in the authentication events.

Although block chain-based system with decentralized nature had provide a very secure environment but further enhancement is still required. Hence, an integration of ECDSA, ECC and ZKP into the block chain based goods tracking and management system is proposed to enhance the authentication mechanism. ECDSA will be used to create digital signatures to verify the authenticity and integrity of messages and transactions where in this management system, it will ensure all the transactions are securely signed by the participants' private key and authenticated using participants, public key. As for ECC, the foundation to ECDSA, it will be used to generate key pairs and perform encryption and decryption on sensitive information as well as signature verification operations using ECC-based key pairs to ensure confidentiality. ZKP is then integrated for privacy enhancement security purposes to avoid

revealing the actual information where it will be used to verify attributes such as authenticity and compliance. Fig 2 below shows the flow of the enhanced authentication mechanism with the integration of ECDSA, ECC and ZKP.

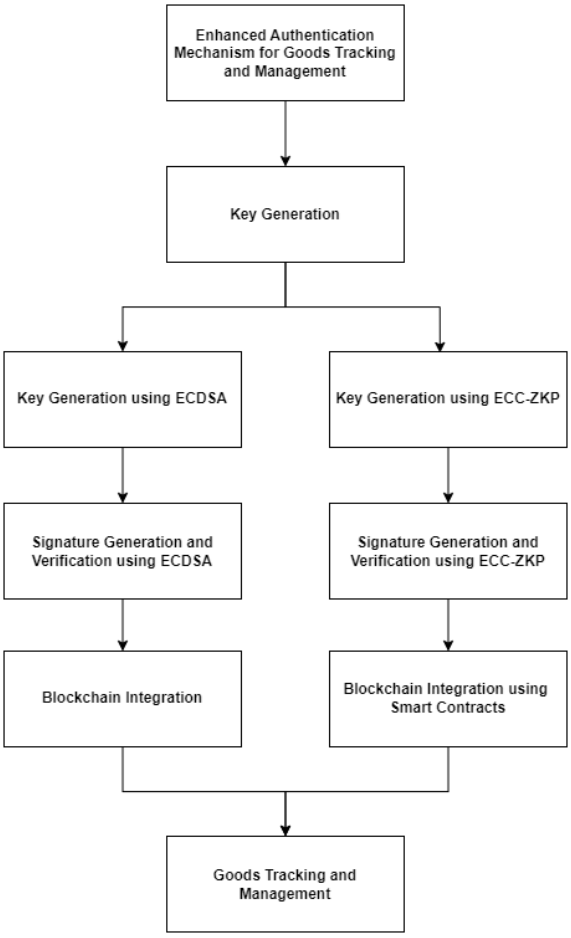


Fig. 2: The Flow of Authentication and Data Management in Goods Tracking and Management System

Key Generation

The overall authentication mechanism begins with the initialization of the elliptive curve parameter. The mechanism then begins with key pair's generation for authentication purpose. The key pairs will be generated with ECDSA where a private key will be randomly selected from a range and computed. Then, the mechanism proceeds to key pairs of generation with ECC-ZKP. Hence, when a user joins the networks that integrate ECDSA and ECC-ZKP, key pairs will be generated from each algorithm. The key pairs generated by ECDSA will be used for digital signature and authentication purposes in transactions while the key pairs generated by ECC-ZKP will be used create and verify proofs.

Signature Generation and Verification

The key generated in the previous step will be used in this step for signature generation and verification. Signature generation and verification are required to ensure that data is tamper-resistant, verify the authenticity of messages and transactions, serve as evidence to prevent denial from the parties involved as well as provide a way for user to prove claims without disclosure of sensitive information. With ECDSA, the private key and a cryptographic hash function will be used to generate a unique signature

for the message. The elliptic curve parameters, private key and the hash message are then combined for signature creation. As for the verification with ECDSA, public key, hashed message and signature received would use to validate the signature validity and authenticity of the transaction. The ZKP is then used for proof generation and verification for ZKP, the generation process is done by the prover while the verification is completed by verifier. The prover will firstly select a claim to prove without disclosing their sensitive information then perform cryptographic operation to generate a commitment to the claim. The prover then receive challenge from verifier where it generates a response using their private key. In verification process, the verifier will receive response from the prover and verifies the response from the prover to ensure it is valid. The verifier then uses the commitment, response and public key to perform cryptographic operations. Throughout this process, the verifier could confirm the validity of prover's claim without learning any sensitive information.

Block chain Integration

The signature from the ECDSA and proof generated from the ECC-ZKP will be integrated into the block chain. This process is required to ensure the integrity of transactions through tamper-resistant record, authenticate the transactions and allow user to prove claims without disclosure of sensitive information. Block chain integration with ECDSA Signature uses the signature generated and broadcast to the block chain network. Each node on the network work independently to verify the signature with sender's public key to confirm on the authenticity. As for ECC-ZKP proof integration, the generated proof is also broadcast to the block chain network and the nodes will verify on the proof to ensure the validity of the claims made. However, ECC-ZKP will be involving smart contract as it consists nature which involves complex cryptographic protocols. The deployment of smart contracts would allow the block chain to autonomously verify and validate the proof. But smart contracts were not included in ECDSA as ECDSA focus on traditional generation and verification. The signature will be stored directly on the block chain without other additional computational logic.

The block chain will then serve as distributed ledger for the recording purposes. The transactions will be securely authenticated now with the integration of ECDSA, ECC and ZKP. With this proposed solution, ECDSA signatures will be used to ensure the authenticity and the integrity for all the transaction while ECC-ZKP will provide high level privacy-preserving verification which allow user to prove its claim without revealing any sensitive information. Transparency is also proved with tamper-resistant and traceable trail.

5. Results and analysis

The proposed solution for enhanced authentication mechanism above aim to address to the problem statement. The result of the proposed solution is as below:

With block chain technology, its decentralized authentication helps to reduce the centralized attacks through the elimination of traditional centralized authentication. Operating in a trustless environment, transaction and authentication are validated through cryptographic instead of central authority had help to enhance the overall security as well. Besides, the immutable nature of block chain that disallow any alteration or modification had provided further guarantee on the authentication of the critical data which proven a robust layer of security. The transparency and traceability nature are further proved when every authentication event is time-stamped and permanently recorded. The overall decentralized authentication with block chain had improve the system to a much more resilient system towards attack that targets on centralized system such as Distributed Denial of Service (DDoS) where it normally launch it attacks

toward the central server, crippling the entire system. But, with decentralized authentication, attacking one node would not bring much affect as it requires the attackers to breach majority nodes simultaneously to cripple the overall system. The use of smart contract to automate various process such as key management, authentication, real-time management and goods tracking which execute predefined actions automatically when specific conditions are met had reduced the overall human errors while speeding up the operational workflow and reducing the resources required. The automated process allows the system to allocate more processing power and resources to more critical tasks as well as reducing the need for operational cost that can be significant in long run.

Simulations are carried out with python using Jupyter Notebook to test on the solution proposed, ECDSA integrated with ECC-ZKP. The simulation is carried out to analyse the performance of the proposed solution in the aspect of computation resources and security in comparison to the sole ECDSA solution. Apart from simulation, the proposed solution is analyzed through several equations as well.

The proposed solution ECDSA with ECC-ZKP is analyzed with the three equations below to measure on the performance improvement, resource consumption and computational overhead. The details of the analysis are as follows.

$$\text{Improvement} = \frac{\text{Time}_{\text{ECDSA}} - \text{Time}_{\text{ECDSA-ECC-ZKP}}}{\text{Time}_{\text{ECDSA}}} \times 100\%$$

The equation above is used to measure the improvement in performance for the proposed solution where the positive percentage calculated would indicate the improvement brought. With the equation, the positive percentage recorded would indicates the improvement brought by the proposed solution. Hence, high percentage achieved would suggest significant performance improvements.

$$\text{Resource Consumption Ratio} = \frac{\text{Time}_{\text{ECDSA-ECC-ZKP}}}{\text{Time}_{\text{ECDSA}}}$$

The equation above is used to measure the rate of resource consumed by the proposed solution. Comparisons is made to analyze the resource consumption for different solution. If the calculation of the equation managed to achieve a ratio less than 1, then the result indicated that resource consumption is reduced. However, a ratio with value of 1 would define same amount of resources consumption and ratio greater than 1 would suggest higher resource consumption which may result from longer key or complex mathematical calculations.

$$\text{Computational Overhead} = \text{Time}_{\text{ECDSA-ECC-ZKP}} - \text{Time}_{\text{ECDSA}}$$

The equation above is used to analyze the proposed solution on the computation overhead. If the result is a negative overhead, then the proposed solution is highly efficient and suitable which leads to better performance. But, if zero overhead is achieved, then it indicates similar performance while positive in overhead would suggest that the respective proposed solution is lower in efficiency which leads to take more time and lower in performance. All the results from both simulation and equation on various aspects are depicted clearly with analysis in the table below.

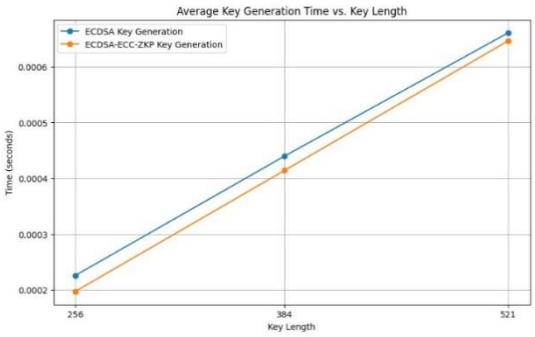
The proposed integration of ECDSA, ECC and ZKP into the block chain based technology managed to

enhance performance, reduce consumption and computational overhead through the optimization of authentication process. Table 1 below shows the average key generation time recorded form the simulation of comparison between sole ECDSA and the proposed ECDSA-ECC-ZKP. The experimented is simulated across three different key length, 256, 384 and 521 to test on its performance on computational resources when much more complex operations are involved for longer keys. The integration of ECC-ZKP into ECDSA may introduce additional complexity, but the overall key generation time is lower compared to sole ECDSA which suggest that the algorithm maybe more efficient in resource utilization and reduced computational overhead. Besides, with lower generation time proven by ECDSA with ECC-ZKP, it does suggest the high efficiency in handling long key length which leads to better performance in all three key lengths. Fig 3 below illustrated that the average key generation time increases as the key get longer and complex operation are required for both method in overall, but the ECDSA integrated with ECC-ZKP still managed to achieve lower average time than sole ECDSA.

Table 1: Average Key Generation Time for Different Key Length

Key Length	Average Key Generation Time (seconds)		Improvement (%)	Resource Consumption Ratio	Computational Overhead
	ECDSA	ECDSA with ECC-ZKP			
256	0.00022590	0.00019731	12.66	0.873439575	-0.00002859
384	0.00043973	0.00041402	5.85	0.941532304	-0.00002571
521	0.00066085	0.00064645	2.18	0.978209881	-0.00001440

Fig. 3: Average Key Generation vs Key Length



The reduction in computational overhead and computational resources is also proven with the simulation through three key length 256, 384 and 521 for signature generation and signature verification. Just as mentioned, the integration of ECC-ZKP into ECDSA generally would require more computational resources due to the increased in complexity since it combine two cryptographic techniques. But lower average signature generation and verification time is observed for ECDSA with ECC-ZKP across all the three key lengths just as shown in Table 2 and Table 3 below. From the result, it is possible to indicate the improved efficiency and reduced computational overhead. Fig 4 and Fig 5 below is a graph depicted according to the data collected from simulation, where increased of time are observed for both signature generation and signature verification as the key length increase. Still, ECDSA with ECC-ZKP managed to achieve slightly lower average signature generation and signature verification time

Table 2: Average Signature Generation Time for Different Key Length

Key Length	Average Signature Generation Time (seconds)		Improvement (%)	Resource Consumption Ratio	Computational Overhead
	ECDSA	ECDSA with ECC-ZKP			
256	0.00049558	0.00047101	4.96	0.950421728	-0.00002457
384	0.00119600	0.00098037	18.03	0.819707358	-0.00021563
521	0.00138570	0.00128186	7.49	0.925063145	-0.00010384

Fig. 4: Average Signature Generation Time vs Key Length

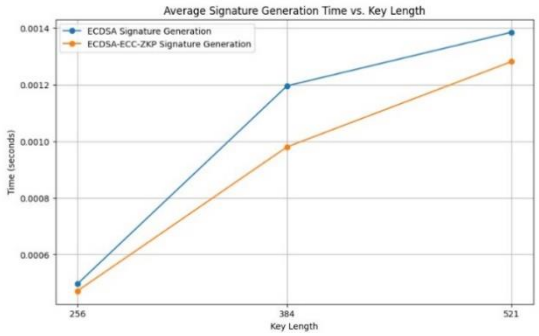
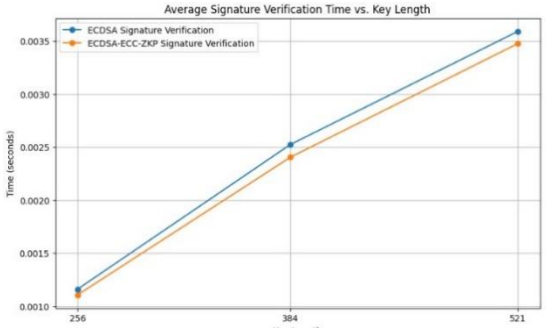


Table 3: Average Signature Verification Time for Different Key Length

Key Length	Average Signature Verification Time (seconds)		Improvement (%)	Resource Consumption Ratio	Computational Overhead
	ECDSA	ECDSA with ECC-ZKP			
256	0.00115974	0.00110604	4.63	0.953696518	-0.00000537
384	0.00252350	0.00240340	4.76	0.952407371	-0.00012010
521	0.00359139	0.00347633	3.20	0.967962265	-0.00011506

Fig. 5: Average Signature Verification vs Key Length



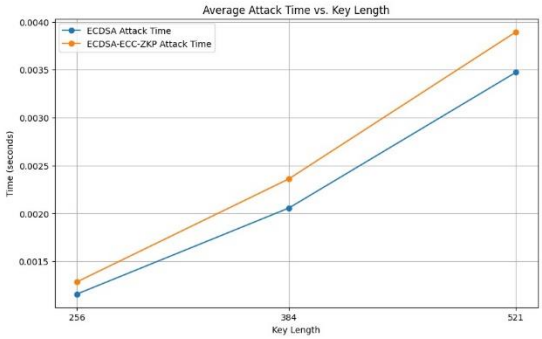
The proposed solution managed to be enhancement in the security aspect as well. Similarly, the proposed solution is simulated across three key lengths of 256, 384 and 521 to test on the average time taken for an attack on ECDSA integrated with ECC-ZKP and sole ECDSA. The integration of ECDSA with ECC-ZKP add an additional security layer compared to the sole ECDSA which can help to enhance the security against certain attacks. Table 4 below shows the average time taken for an attacker to break into the system. The data recorded from the simulation are depicted in graph shown in Fig 6. The results had shown that ECDSA integrated with ECC-ZKP took a slightly higher average attack time compared to

sole ECDSA solution which indicates that the proposed solution demonstrated enhanced security and resilience against certain attacks that target on the cryptographic system. The time taken by two solution increases as the key length increases but the ECDSA integrated with ECC-ZKP still require longer average attack time compared to sole ECDSA solution for attackers to compromise the security of the system.

Table 4: Average Attack Time for Different Key Length

Key Length	Average Attack Time (seconds)	
	ECDSA	ECDSA with ECC-ZKP
256	0.00115767	0.00128466
384	0.00205656	0.00236084
521	0.00347293	0.00389461

Fig. 6: Average Attack Time vs Key Length



6. **Conclusion**

To address the existing challenges, a solution integrating the Elliptic Curve Signature Algorithm (ECDSA) with Elliptic Curve Cryptography-Zero Knowledge Proof (ECC-ZKP) into a block chain-based system for goods tracking and management has been proposed. The proposed system demonstrates significant enhancements in efficiency, security, resource consumption, and computational overhead. Moreover, the solution addresses challenges in IIoT, such as vulnerabilities to centralized authentication and cyber security threats. The results in this paper indicate that the proposed ECDSA-ECC-ZKP integrated with a block chain-based system provides better performance in key generation, resistance to attacks, signature generation, and verification times across various key lengths. The enhanced authentication mechanism ensures the authenticity of transaction and data integrity by utilizing ZKP to protect privacy without revealing any sensitive information. The smart contracts and the immutable ledger nature of block chain further enhance security by automating and safeguarding the transactions. Future work should aim to further optimize the integration process and explore additional techniques to strengthen the system's robustness.

7. **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

Abbasi, I., A., (2024). "A lightweight and robust authentication scheme for the healthcare system using public cloud server." plos one 19(1): e0294429.

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.

Ahmad, Z., (2023) ms-ads: multistage spectrogram image-based anomaly detection system for iot security. Transactions on emerging telecommunications technologies, 34(8): p. E4810.

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.

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

Aqeel, S., Shahid Khan, A., Ahmad, Z., & Abdullah, J., (2022). A comprehensive study on dna based security scheme using deep learning in healthcare. Edpacs, 66(3), 1-17.

Asim, J., khan, A. S., Saqib, R. M., Abdullah, J., Ahmad, Z., Honey, S., Afzal, S., Alqahtani, M. S., & Abbas, M., (2022) Block chain-based multifactor authentication for future 6g cellular networks: a systematic review. Applied sciences, 12(7), 3551

Iqbal, A. M., Khan, A. S., Abdullah, J., Kulathuramaiyer, N., & Senin, A. A. (2022). Blended system thinking approach to strengthen the education and training in university-industry research collaboration. Technology analysis & strategic management, 34(4), 447-460.

Iqbal, A. M., Kulathuramaiyer, N., Khan, A. S., Abdullah, J., & Khan, M. A. (2022). Intellectual capital: a system thinking analysis in revamping the exchanging information in university-industry research collaboration. Sustainability, 14(11), 6404.

Jan, S. U., abbasi, I. A., algarni, F., & Khan, A. S. (2022). A verifiably secure ecc based authentication scheme for securing iod using fanet. Ieee access, 10, 95321-95343.

Jambli, M. N., Khan, A. S., & Shoon, S. C. (2016). A survey of vasnet framework to provide infrastructure-less green iots communications for data dissemination in search and rescue operations. Journal of electronic science and technology, 14(3), 220-228.

Khan, A. S., abdullah, J., lenando, H., & Nazim, J. M. (2016). Green resource allocation for multiple ofdma based networks: a survey. Journal of electronic science and technology, 14(2), 170-182.

Aljuhani, A. (2024) "a deep-learning-integrated block chain framework for securing industrial iot," in ieee internet of things journal, vol. 11, no. 5, pp. 7817-7827, 1 march1, , doi: 10.1109/jiot.2023.3316669.

Dong,, J. g. Xu, c. Ma, j. Liu and u. G. O. Cliff, "block chain-based certificate-free cross-domain authentication mechanism for industrial internet," in ieee internet of things journal, vol. 11, no. 2, pp. 3316-3330, doi: 10.1109/jiot.2023.3296506.

Wang, F., J. Cui, Q. Zhang, D. He, C. Gu and H. Zhong, (2024) "lightweight and secure data sharing based on proxy re-encryption for block chain-enabled industrial internet of things," in ieee internet of things journal, vol. 11, no. 8, pp. 14115-14126, doi: 10.1109/jiot.2023.3340567.

Zhang, P. P. Yang, N. Kumar, C. -H. Hsu, S. Wu and F., Zhou, (2024) "rrv-bc: random reputation voting mechanism and block chain assisted access authentication for industrial internet of things," in ieee transactions on industrial informatics, vol. 20, no. 1, pp. 713-722, jan., doi: 10.1109/tii.2023.3271127.

Li, F. (2023) "Blma: editable block chain-based lightweight massive iiot device authentication protocol,"

in ieee internet of things journal, vol. 10, no. 24, pp. 21633-21646, doi: 10.1109/jiot.2023.3308725.

Rathee, G., C. A. Kerrache and M. Lahby, (2023) "trustblksys: a trusted and block chained cyber secure system for iiot," in ieee transactions on industrial informatics, vol. 19, no. 2, pp. 1592-1599, doi: 10.1109/tii.2022.3182984.

Li , C. (2023) "federated hierarchical trust-based interaction scheme for cross-domain industrial iot," in ieee internet of things journal, vol. 10, no. 1, pp. 447-457, doi: 10.1109/jiot.2022.3200854.

Qian, K. Y. Liu, X. He, M. Du, S. Zhang and K Wang, (2023) "hpcchain: a consortium block chain system based on cpu-fpga hybrid-puf for industrial internet of things," in ieee transactions on industrial informatics, vol. 19, no. 11, pp. 11205-11215, nov. 2023, doi: 10.1109/tii..3244339.

Rathee ,G., F. Ahmad, N. Jaglan and C. Konstantinou, (2022) “secure and trusted mechanism for industrial iot network using block chain," in ieee transactions on industrial informatics, vol. 19, no. 2, pp. 1894-1902, feb. 2023, doi: 10.1109/tii.2022.3182121.

Khan, A., A., (2023) "data security in healthcare industrial internet of things with block chain," in ieee sensors journal, vol. 23, no. 20, pp. 25144-25151, doi: 10.1109/jsen.2023.3273851