International Journal of Computer Technology and Science
Volume. 1 No. 3 July 2024
e-ISSN :3048-1961, And p-ISSN :3048-1899, Page. 41-55
DOI: https://doi.org/10.62951/ijcts.v1i3.24
Available online at: https://international.arteii.or.id/index.php/IJCTS

# Multi-Factor Authentication Using Blockchain: Enhancing Privacy, Security and Usability

**Irenna Wanisha[1], Jaymaxcklien Bravyain[1], Jeremy Silas [1], Luqmanul Hakim Bin Mohammad Bakery[1], Melvianna Samuel[1] &Muhammad Faisal[2]**

[1] Faculty of Computer Science and Information Technology, Universiti Malaysia Sarawak, Kuching, Sarawak, Malaysia

[2] Director HRIMS, Ministry of Human Rights

[1] 75057@siswa.unimas.my 75132@siswa.unimas.my 75164@siswa.unimas.my 73533@siswa.unimas.my 70362@siswa.unimas.my [2] dr.faisalshabbir88@gmail.com

***Abstract:*** *In the ever-changing digital world, strong security protocols are essential. As a vital line of defence against unwanted access, blockchain uses several verification techniques to boost security. This article investigates the use of blockchain technology to tackle privacy, security, and usability issues. By reducing the dangers associated with conventional centralised systems, blockchain's decentralised and immutable structure offers a secure platform for storing and verifying authentication credentials. This method increases user trust by using smart contracts to guarantee transparent and unchangeable authentication procedures. The suggested blockchain-based method strengthens security and enhances privacy by removing sources of failure and decreasing dependence on outside verification. Furthermore, user-centric design and expedited procedures improve the system's usability by making secure authentication more approachable and less obtrusive. This paper offers a thorough examination of the suggested system, stressing its benefits, possible drawbacks, and directions for future investigation. The results indicate that blockchain technology presents a viable solution to ensure that digital authentication frameworks combine privacy, security, and usability.*

***Keywords:*** *Authentication, Blockchain, Privacy, Security, IIoT*

## I. INTRODUCTION

Blockchain technology also known as the backbone of famous trends nowadays; Cryptocurrency such as bitcoin. It has gained a highly immense popularity due to it centralized and secured system. A blockchain consist of a distributed ledger that records transactions across network in between computer and yet not limited to cryptocurrency user. Blocks also exist in the chain which linked together hence the name blockchain [1].

Blockchain authentication is a way to secure verification that involves the blockchain network that also improve the security and transparency of a transaction [2]. By relying on cryptographic techniques and consensus techniques and validated transactions while securing the network, no server or third party are needed to have the central authority and act as authenticator. Figure 1 shows the blockchains basics techniques and transaction that have been collected through all 10 articles.

*Received: May 10, 2024; Revised: June 15, 2024; Accepted: July 15, 2024; Published: July 18, 2024;*
* Irenna Wanisha , 75057@siswa.unimas.my

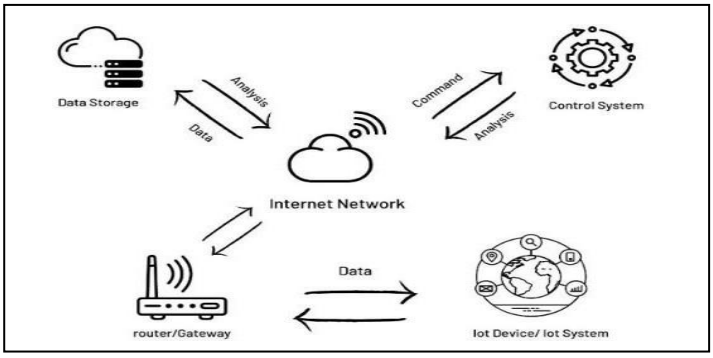


**Figure 1.** Basics techniques and transactions of IoT blockchain.

The security and integrity of blockchain mechanisms rely on public key cryptography, digital signatures, and consensus algorithms. Public key cryptography secures communication through encryption, while digital signatures confirm the genuineness of transactions. Consensus algorithms, including Proof of Work (PoW) and Proof of Stake (PoS), enable decentralized consensus on transaction validity, preserving the integrity of the blockchain without a central authority.

The importance of these technologies is steadily being acknowledged, leading to the increasing integration of IoT and blockchain in various fields to improve authentication and security. IoT devices, which often lack robust security measures, experience substantial advantages from blockchain's strong security features. By utilizing blockchain's decentralized and unchangeable nature, the integration strengthens the overall security framework, safeguarding the integrity and confidentiality of data in IoT ecosystems.

The objective of this paper is to examine and deliberate on the current body of literature regarding the resemblances and variances in blockchain authentication techniques, specifically within the realm of IoT incorporation. An in-depth evaluation of numerous suggested solutions aiming to combat the current shortcomings in blockchain authentication mechanisms will be undertaken. Through the comparison of diverse methods, this paper endeavors to emphasize inventive tactics and optimal approaches for enhancing authentication protocols, with the ultimate goal of bolstering the security and dependability of both blockchain and IoT environments.

## II. PROBLEM STATEMENT

1. Security Concerns with Internet of Things (IoT)

While IoT networks have a lot of potential, their wide and varied terrain also makes it easy for security flaws to increase rapidly [1]. This vulnerability results from features that many IoT devices have by default. Strong security measures like encryption are frequently limited

by low processing and memory capacities. Furthermore, pre-configured weak credentials, such default passwords, give attackers easy access to them. Moreover, these gadgets usually do not receive regular software upgrades that could close security gaps, unlike traditional computers. Finally, attempts to properly secure the entire network are hampered by the enormous diversity of devices made by various manufacturers, which results in a patchwork of security methods. Attackers can take advantage of these circumstances to execute a variety of assaults, such as replaying data, spoofing servers, and impersonating authentic users, and breaching systems as a result of inconsistent identification rules and a lack of reciprocal authentication [3].

2. Lack Reliable Authentication Policies

The issues highlighted up in the analysis indicate that the systems established lack reliable authentication policies, particularly when it comes to authorizing access to systems [4]. The lack of this element makes systems susceptible to security breaches, which can compromise the confidentiality and integrity of data when accessing devices and sharing data. The research underscores the pressing requirement to enhance authentication measures in order to effectively address these security vulnerabilities. Without strong authentication processes, IIoT systems are exposed to the dangers of unauthorized access, data tampering, and disruptions in operations. It is crucial to fortify these protocols to protect sensitive data, uphold operational integrity, and ensure secure and reliable interactions within the IIoT environment, ultimately promoting wider acceptance and confidence in IIoT technologies.

3. Limitation Of Range Of 5G Cells

The problem statement in the referenced articles emphasizes a key issue in 5G networks: the constraint on the range of 5G cells, which affects the user authentication process during cell transitions [4]. 5G networks feature numerous, smaller cells compared to previous generations, with the goal of delivering fast, low-latency connectivity. However, when users move between these compact cells, their devices must undergo authentication with each new cell they enter. This frequent handover and authentication procedure can result in connectivity interruptions and delays as the device shifts between cells. The continual authentication processes needed to uphold a dependable 5G connection present technical hurdle, including the need to ensure smooth transitions without compromising security or causing significant service disruptions. It is essential to tackle these problems in order to guarantee seamless, high-quality user experiences in 5G networks. This highlights the importance of effective and strong authentication methods that can smoothly manage rapid cell transitions.

## III. RELATED WORKS

1. Blockchain-Based Device Authentication Method in Industrial Internet of Things

The implemented strengthened blockchain-based authentication solution for IoT devices in the industrial network provides a significantly secured and strengthened system access point against unauthorized access and data forgery. But on the other side, the authentication protocols implemented in the research are very susceptible to attacking. It means inputting the infrastructure under significant risk and security breaches. Although on the bright side, the security weaknesses and vulnerabilities found in the research could help enhance and secure the studied solutions to be generally applied in the entirety of the industrial IoT architecture without specific reinforcement [5].

2. Towards A Lightweight Identity Management and Secure Authentication for IoT Using Blockchain

Based on the article of where the lightweight identity management involving blockchain they provide a decentralized and secure solution for IoT networks by building trusting and proper communication across the nodes. Using machine learning to properly identify denial-of-service threats improves the system's security. However, incorporating blockchain into IoT networks can place a strain on communication, power, and memory resources, especially for devices with limited capabilities. Blockchain security must be carefully balanced with design concerns like as power and latency in IoT devices [6].

3. A Deep Learning Integrated Blockchain Framework for Securing Industrial IoT

Consequently, new technology has entered the manufacturing and industrial sectors, leading to the Industrial Internet of Things (IIoT). In spite of that, the IIoT ecosystem are open to various security and privacy risks as it consists of both homogeneous and heterogeneous networks and devices that are connected via unsecured communication. Hence, an innovative deep-learning-based intrusion detection system (IDS) and a private blockchain are implemented in a deep-learning-integrated blockchain architecture. The strength of both IDS and blockchain is that they act as a defence mechanism against cybercrime in such a network of connections, while the weakness is they experience lack of adaptability, high complexity of computation, and confirmation delay. Lastly, the evaluation metrics used by the authors to assess their proposed solution are using open-source datasets, ToN-IoT and Edge-IIoTset [1].

4. TrustBlkSys: A Trusted and Blockchained Cybersecure System for IIoT

Devices in the IIoT are able to communicate with one another through the industrial Internet to some extent. Despite the fact that intelligence greatly advances, current industrial systems suffer from a number of security flaws that allow hackers to easily manipulate and

target data storage or production systems. Thus, TrustBlkSys, a system combining trust evaluation and blockchain technology, is used. Trust evaluation assesses each device's trustworthiness during communication, while blockchain monitors and validates the trustworthiness. The strength of the system is to improve the efficiency, accuracy, and security of data while sending messages inside the system, while the weakness is there is scalability issue within the system. Lastly, the evaluation metric used by the authors assessed in relation to a number of security metrics, including the possibility harmful devices in terms of computation of trust value, fake authentication, and data delivery rate, as well as device sensitivity during communication and convergence time for information transmission [7].

5. A Blockchain-Based Cross-Domain Authentication Management System for IoT Devices

IoT devices, including self-driving cars and smartwatches, must have a secure authentication system in place to guarantee the safety and confidentiality of the data they store. It is usually compromised in cross-domain settings where it may connect to services hosted by different domains than the device itself. A secure device management system can be developed to counteract unauthorised access and security breaches by addressing difficulties with control of access, authentication, and privacy protection. A Blockchain-based Cross-Domain Authentication management System for IoT Devices is suggested as a solution to this problem. It stores confidential information in a Merkle tree structure, with only the root being uploaded to the smart contract. This technique's cheap on-chain storage, quick off- chain authentication, and centralization are among its best points. However, it requires further optimization to address transaction throughput issues such as the increase in the number of nodes. To measure the effectiveness of the proposed solution, metrics such as time consumption for device data updates, merkle tree leaf numbers and concurrent device authentication request number are used to assess [2].

6. Survey On Blockchain Enabled Authentication for Industrial Internet of Things

In Industrial Internet of Things (IIoT), security has become a vulnerability that could lead to a security breach of the entire system. Such vulnerabilities stem from data confidentiality, data integrity, authentication, device management and data encryption which shows that there is a need for a secure and reliable authentication mechanism to ensure the safety of the IIoT operations. The proposed technique includes the blockchain-enabled cross- domain device authentication, Blockchain Trust based Authentication, Blockchain based edge computing authentication, Blockchain based adaptive authentication and authorization, and a biometric based authentication using blockchain. The strengths of these techniques are collaborative authentication which results in a strong fault tolerance and a high- level security. The

weaknesses are the time complexity, limitations and scalability of these blockchain based authentication mechanisms. Time complexity, fault tolerance, security, privacy preservation and efficiency in authentication protocols were used as evaluation metrics in evaluating these techniques [8].

7. A Blockchain-Based Authentication Scheme and Secure Architecture for IoT-Enabled Maritime Transportation Systems

Recent technological breakthroughs have resulted in dramatic shifts across the transportation sector, with Intelligent Transportation Systems (ITS) spreading into new realms such as space and undersea applications. This study aims to provide an integrated IoT-based system specifically designed for efficient and safe marine transportation management, reflecting the industry's increased emphasis on technological innovation. Authentication protocols based on privacy policies are the primary way for ensuring communication integrity and dependability, as well as identifying privacy security. However, A new system that can meet user requests and manage the growing volume of data required is desperately needed to continue employing this method. Every node duplicate and maintains a copy of the database thanks to the blockchain network design. The whole data collection won't be affected if one of the nodes fails. The difficult problems in the current field of information security, like identity theft, data manipulation, and Distributed Denial of Service (DDoS), are solved by this feature. Consequently, upcoming blockchain technology advancements and uses may raise the network security index for the marine sector. Blockchain technology has the potential to improve the maritime industry's network security [4].

8. Security For Internet-Of-Things Enabled E-Health Using Blockchain and Artificial Intelligence: A Novel Integration Framework

Health technologies, ranging from telemedicine platforms to wearable devices and advanced diagnostic tools, serve as lifelines during crises like the COVID-19 pandemic. They enable remote consultations, monitoring, and early detection of symptoms, ensuring timely interventions and reducing the burden on healthcare systems. Moreover, these technologies bridge gaps in healthcare access, reaching underserved communities and vulnerable populations, thus promoting fairness and equity in healthcare delivery. Their role extends beyond crisis management, contributing to long-term improvements in healthcare infrastructure and patient outcomes. These technologies have various benefits, including ease, cost savings, simple access, and rapid retrieval of health information. They include a diverse set of instruments such as electronic health records, mobile health (m-Health), robotic surgery, and telemedicine/telehealth. However, the sensitive nature of the data they create raises

concerns about cyber- attacks and illegal access, jeopardizing the security, integrity, and availability of e-health data across AI, IoT, and blockchain ecosystems [9]. Efforts are underway to discover economical solutions to implement the suggested framework. Additionally, there is an emphasis on developing strategies to preserve energy while incorporating Blockchain at the IoT node. Furthermore, effort is being done to develop a new algorithm specifically for the integrated architecture.

9. Blockchain Based Secure and Effective Authentication Mechanism For 5G Networks

The article seeks to increase the security and efficiency of mobile networks by employing Blockchain technology to improve 5G authentication. The authentication procedure for 5G networks includes frequent handovers between access points, which result in greater authentication and could threaten security and performance. The technique suggested is to employ the capabilities of Hyperledger Fabric to apply the UEAPBFT consensus algorithm, which has been developed for 5G network authentication. The strength that can be found is suggested UEAPBFT technique improves 5G authentication security while drastically cutting processing times however, there could be scalability issues and implementation complexity with the suggested technique. The authors measured the suggested technique using metrics like processing timePT and average throughputAR in order to measure the performance increase generated by 5G authentication [10].

10. Blockchain Enabled Architecture for Secure Authentication in The Metaverse Environment

The study is the Eduverse, which focuses on learning by students in the Metaverse. Authentication and identity management play an essential role in this setting because of security concerns including impersonation, server spoofing, replay attacks, and the requirement for identity interoperability. The articles focus on the problem of authentication in education and emphasize that there are no all-encompassing fixes for security issues. Based on Blockchain technology, the proposed approach delivers an extensible and centralized authentication mechanism for the Eduverse. This architecture effectively addresses identified safety concerns by utilizing the tamper-proof and fundamental security of Blockchain technology. The strengths in this article include safe transactions, immutability, and centralized identity management. However, there may be shortcomings due to challenges with efficiency and scalability that call for additional work. Evaluation metrics will be used to assess the scope, efficacy, and capacity to handle authentication issues in the Eduverse test bed [3].

11. Other Related Research Articles

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 [11-23]. This research article can act as the guidelines for future young researchers in end-to-end security measures in 6th generation networks. This improved work (proposed solution) for the given problem statement is adopted from [11], which act as a benchmark for this research article.

## IV. PROPOSED SOLUTIONS

Numerous researches have been made to use blockchain to protect IIoT networks. However, there has some limitation and challenge found in the blockchain technology. The first limitations and challenges found is related to the privacy concern. With this, blockchain's data privacy flaws can be exploited by hackers. Then, research about a blockchain-based access control system for IoT device management was suggested but, the networks stop functioning in the event of an attack on the central management hub. It is proved that blockchain technology has limitations and challenges with scalability, high computational complexity, and consensus lag [1].

Hence, an optimised blockchain architecture called OptChain was created especially for Industrial Internet of Things (IIoT) contexts, with the goal of providing efficient and safe device authentication and data integrity. A Software as a Service (SaaS) product called OptChain gathers, links, and evaluates data from the supply chain to improve transparency, resilience, and visibility performance. It provides traceability solutions for a range of applications and industries, such as manufacturing, distribution, raw materials, recycling, and warehousing. To assist in creating a sustainable, compliant, and efficient supply chain, it offers features like digital identity, evidence of compliance, mapping, onboarding, traceability, and digital twins.

Blockchain sharding protocols have been the focus of study and development on OptChain in order to provide quick and safe cross-shard transactions. High performance and scalability in blockchain transactions are achieved by utilising a unique proof-of-stake system and a lightweight cross-shard communication protocol.

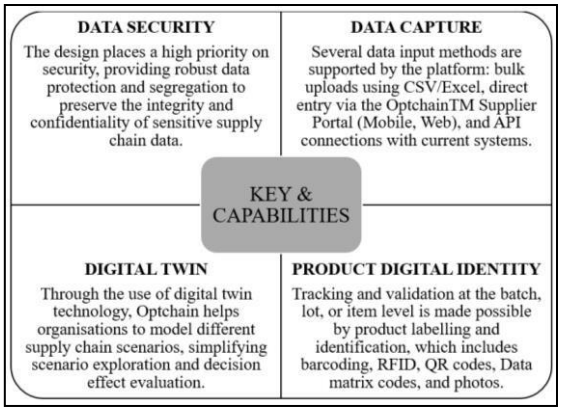


**Figure 2**. Key and Capabilities of OptChain.

While incorporating several enhancements, it expands upon the private blockchain idea from [11]. The following are the enhancements of OptChain.

1. Merkle Tree-based Data Storage

OptChain addresses the difficulty of utilising blockchain technology to integrate massive amounts of IoT data. It accomplishes this by using a Merkle tree structure, a cryptographic technique that essentially turns all authentication records and device data into a fingerprint. The advantage is in having the blockchain store only the fixed-sized hash known as the Merkle root. All of the detailed data is essentially summarised in this root and is then efficiently stored off-chain. There are several benefits to this strategy. First of all, by recalculating the hash and comparing it to the Merkle root on the blockchain, anyone may confirm the accuracy of the off-chain data. Second, compared to storing everything directly on the blockchain, transaction speeds and fees go down when only the root is kept on-chain. Lastly, by keeping the majority of data off-chain, OptChain greatly lessens the burden on blockchain storage, making it a scalable solution for handling enormous volumes of IoT data. OptChain, to put it briefly, combines the efficiency and economy of off-chain storage with the security and transparency of blockchain technology.

2. Consortium Consensus Mechanism

Consortium blockchains make use of a special consensus algorithm intended for networks with pre- selected participants that are permissioned. In contrast to conventional public blockchains that depend on free competition (such as Proof of Work), consortium blockchains employ a permission-based, lightweight methodology in which trusted nodes cooperate to verify transactions. These nodes might be security firms, important industrial partners, or even government agencies. Within the network, this carefully chosen group guarantees a high degree of confidence. Effective consensus algorithms such as Proof of Authority (PoA) and Practical Byzantine Fault Tolerance (PBFT) are also embraced by the

consortium method. In comparison to public blockchains, these algorithms are especially chosen for their speed and scalability, which allows for speedier transaction confirmation times. Furthermore, the consortium approach reduces energy consumption greatly by doing away with the requirement for large amounts of processing power. This mechanism's capacity to strike a balance between efficiency, security, and speed is what gives it its real power. Consortium blockchains provide a high level of security while facilitating faster transaction processing by depending on pre-screened, reliable validators. They are therefore perfect for applications that require quick validation and energy efficiency without sacrificing data accuracy.

3. Smart Contract-based Authentication and Access Control

OptChain uses smart contract-based authentication and access control, a sophisticated method of network communication security. Custom OptChain smart contracts are utilised by this system for every kind of device, such as actuators, sensors, and gateways. These smart contracts serve as gatekeepers, outlining the precise authentication standards that every device must satisfy in order to gain entry. With this degree of specificity, only approved devices are able to communicate with the network. These smart contracts also do more than just provide access control. They have the ability to authenticate cryptographically verifiable proofs of a device's identity, known as device signatures. Through the verification process, security is reinforced by making sure that only authorised devices are interacting. Furthermore, the technology enables dynamic modifications according on trust scores. Devices that behave securely all the time may be given more access privileges; devices that behave suspiciously may be subject to limitations. This approach has several advantages. First of all, it permits fine-grained access control, which makes network security more sophisticated. Second, a permanent and auditable trail of activity is created by recording every attempt at access on the blockchain. This openness encourages responsibility and makes security audits easier. OptChain's automated smart contract access control policies also remove the need for human involvement, making the security posture stronger and more impregnable. Essentially, a complete solution for network communication security is provided by OptChain's Smart Contract- based Authentication and Access Control.

4. Lightweight Client for IIoT Devices

OptChain's capacity to easily interface with Industrial IoT (IIoT) devices that are resource- constrained is one of its main advantages. Because IIoT devices have limited processing power and memory, traditional blockchain solutions sometimes perform poorly in these contexts. By releasing a thin OptChain client made especially for IIoT, OptChain addresses this issue. By using this client, IIoT devices can operate a full blockchain node

instead of requiring them to execute such a resource-intensive procedure that would quickly deplete it. Instead, for authentication, devices just need to get in touch with the nearest OptChain node. As a result, the IIoT device's computational load is greatly decreased. Furthermore, to reduce the resource requirements for device-side activities, OptChain makes use of effective cryptography libraries as TweetNaCl or NaCl. The reason these libraries were picked in particular is that they work well on low-end devices. Due to the combination of an MCU (microcontroller unit)-controlled device's lightweight client and effective cryptography, even the most basic devices can be part of the OptChain network. MCUs, which are utilised in wearables, industrial controllers, sensors, actuators, and other components, are the workhorses of the IIoT world. OptChain provides access to a greater variety of scalable and secure IIoT applications by enabling these devices to use it.

5. Cross-Domain Authentication

OptChain's innovative Cross-Domain Authentication functionality dissolves barriers between industrial sectors. Secure authentication between systems and devices located in completely different industrial sectors is made possible by this functionality. Consider a situation where a gateway run by Company B wants to verify the identity of a sensor made by Company A. In this case, traditional methods may be unable to succeed since there is no common trust domain. But OptChain uses the consortium idea to address this elegantly. Through the inclusion of people from many fields in the consensus method, OptChain promotes confidence between various domains. These individuals serve as validators, guaranteeing the authenticity of devices and transactions, irrespective of their place of origin. This cross-domain flexibility has many advantages. It creates the foundation for easy and safe data sharing between organisations. Organisations may work together and exchange insightful data without sacrificing security. This encourages creativity and simplifies procedures throughout whole supply chains. OptChain's Cross-Domain Authentication underpins the Industrial Internet of Things (IIoT), providing a secure framework for constructing reliable IIoT ecosystems. OptChain makes it possible to securely communicate across devices made by various companies and industries, which facilitates the development of IIoT applications that are genuinely connected and cooperative.

## V. RESULTS AND ANALYSIS

Through the use of the OptChain architecture, multiple problems faced by traditional blockchain systems can be overcome such as the privacy and data exposure concerns in traditional blockchain systems. Using the Merkle Tree-based Data Storage which stores only

the Merkle root on the blockchain, this significantly reduces risk of data exposure. The device authentication data which consist of the device ID, timestamp, authentication data will also be stored off- chain in secured and distributed storage system thus reducing the overall on-chain storage. The downside regarding the Merkle Tree-based Data storage is that it introduces the need for a secure and reliable off-chain storage solutions which in other words require additional costs and infrastructure to fully implement.

By applying the Consortium Consensus Mechanism, the OptChain architecture reduces the scalability issues the traditional consensus mechanism as it uses a lightweight, permission-based consensus among trusted nodes thus increasing scalability performance and the security of the blockchain. However, this approach introduces a degree of centralization as consortium members have control of consensus process thus increases concerns regarding decentralization.

The blockchain network will host the Merkle root with hashes that respond to the device authentication details and information. The Merkle Root will be recorded in the fabric on the Optchain channel, which is also a component of the Optchain where the fabric network consists of the users and devices on the blockchain.

By applying the lightweight client for this authentication mechanism, it enables the use of low- resource devices such as microcontroller units to participate in the OptChain network thus allowing resource-constrained IIoT devices into blockchain based systems.

By introducing smart contract-based authentication, it provides a decentralized and auditable system for managing permissions and security policies. The smart contract-based authentication also allows a fine-grained access control and real-time permission modifications based on trust scores which offers flexibility and adaptability in dynamic IIot environments. The complexity of smart contract development and potential vulnerabilities need to be considered and mitigated to ensure a safe authentication mechanism.

The cross-domain authentication is applied to facilitate authentication and data sharing across different industrial domains. This enables a more comprehensive and efficient IIoT supply chains. However, managing and maintaining trust relationships across diverse organizations may introduce complexities and operational challenges.

The OptChain architecture aims to address several limitations of traditional blockchain systems in the specific field of IIoT. The enhanced features include the Merkle Tree-based data storage, the consortium consensus, smart contract-based access control and cross-domain authentication offers improvements in blockchain especially in scalability, performance and security. It is expected that the effectiveness of OptChain depends on real-world implementation as a factor especially when it is done to be adopted by industry partners. Extra

considerations should be given to potential weaknesses in the system especially the centralization concerns in the consortium consensus model and the complexities of smart contract development and off- chain storage management.

## VI. CONCLUSION

The project proposed a comprehensive framework intended to enhance authentication and security in the industrial Internet of things (IIoT) sector. It significantly improves data integrity, transaction speed, and on-chain storage effectiveness by utilizing cutting-edge technologies including smart contract- driven authentication, an effective IIoT consumer, and cross-domain authentication techniques.

OptChain smart contract mechanisms are used to maintain auditable access logs, provide exact access control, and impose stringent security measures. By taking a comprehensive approach, IIoT networks may be made safe and sensitive data and systems can only be accessed by authorized parties. Smart contracts make auditable records possible, which is necessary for security audits and regulatory compliance since they offer a clear and verifiable path of access.

Minimizing the computational demand on IIoT devices—which usually have limited processing power—is the goal of the streamlined consumer. This promotes the solution's scalability and wider acceptability in diverse IIoT scenarios in addition to improving the devices' performance and efficiency. The research makes it possible to apply cutting-edge security measures without sacrificing device performance by optimizing the client.

Cross-domain authentication, which facilitates safe and easy communication across various systems and domains and so enhances the integration and cooperation of diverse IIoT components, is another essential component of the architecture. The reliable functioning of interconnected IIoT networks depends on the establishment of a coherent and uniform security posture, which can only be achieved through interoperability.

Blockchain technology underpins the whole system by ensuring data integrity through transparent and unchangeable records. Transactions become faster and more reliable when this technology is used to streamline transaction operations. Reducing costs and improving access speeds, together with keeping just relevant data on the blockchain, all contribute to the efficacy of on-chain storage options.

The project encompassing approach addresses critical verification issues and offers a flexible, reliable, and efficient framework that encourages the creation of blockchain-based IIoT solutions. The initiative not only fosters greater confidence in linked systems but also lays the foundation for future advancements in IIoT security by strengthening data security and

reliability. Through a uniform and consistent security stance across diverse domains, this underlying premise considerably improves the dependability and robustness of IIoT systems, paving the way for more robust and resilient industrial networks.

## VII. ACKNOWLEDGEMENT

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

## REFERENCES

[1] Aljuhani, A., et al. (2023). A deep learning integrated blockchain framework for securing industrial IoT. *IEEE Internet of Things Journal*, 1. https://doi.org/10.1109/jiot.2023.3316669

[2] Aqeel, S., Khan, A. S., Ahmad, Z., & Abdullah, J. (2022). A comprehensive study on DNA based Security scheme Using Deep Learning in Healthcare. *EDPACS, 66*(3), 1-17.

[3] Asim, J., Khan, A. S., Saqib, R. M., Abdullah, J., Ahmad, Z., Honey, S., Afzal, S., Alqahtani, M. S., & Abbas, M. (2022). Blockchain-based multifactor authentication for future 6G cellular networks: A systematic review. *Applied Sciences, 12*(7), 3551.

[4] Bala, R., & Manoharan, R. (2022). Blockchain based secure and effective authentication mechanism for 5G networks. *IEEE International Conference on Metaverse Computing, Networking and Applications (MetaCom)*. https://doi.org/10.1109/icbds53701.2022.9936018

[5] Balan, K., Abdulrazak, L. F., Khan, A. S., Julaihi, A. A., Tarmizi, S., Pillay, K. S., & Sallehudin, H. (2018). RSSI and public key infrastructure based secure communication in autonomous vehicular networks. *International Journal of Advanced Computer Science and Applications, 9*(12).

[6] Fedorov, I. R., Getmaniuk, I. B., & Bezzateev, S. (2023). Blockchain-Based device authentication method in industrial internet of things. *IEEE Xplore*. https://doi.org/10.1109/icumt61075.2023.10333273

[7] Ikharo, B. A., Obiagwu, A., Obasi, C., Hussein, S. U., & Akah, P. (2021). Security for Internet-of-Things enabled E-Health using blockchain and artificial intelligence: a novel integration framework. *IEEE Xplore*. https://doi.org/10.1109/icmeas52683.2021.9692368

[8] 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.

[9] 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.

[10] Ismail, S., Dawoud, D. W., & Reza, H. (2022). Towards a lightweight identity management and secure authentication for IoT using blockchain. *2022 IEEE World AI IoT Congress (AIIoT)*. https://doi.org/10.1109/aiiot54504.2022.9817349

[11] Jambli, M. N., Khan, A. S., Lenando, H., Abdullah, J., & Suhaili, S. M. (2017). A Dynamic Energy Savvy Routing Algorithm for Mobile Ad-Hoc and Sensor Networks. *Advanced Science Letters, 23*(6), 5542-5546.

[12] 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.
[13] Khan, A. S. (2014). Secure and efficient distributed relay-based rekeying algorithm for group communication in mobile multihop relay network. *International Journal of Communication Networks and Information Security, 6*(3), 189.
[14] Khan, A. S., & Iqbal, A. M. (2018). Mobile Multihop Relay Wimax Networks: Security Perspectives. *Universiti Malaysia Sarawak*.
[15] Khan, A. S., Fisal, N., Esa, M., Kamilah, S., Zubair, S., Maqbool, W., & Bakar, Z. A. (2014). Privacy Key Management Protocols and Their Analysis in Mobile Multihop Relay WiMAX Networks. *Security for Multihop Wireless Networks*, 43.
[16] Khan, N., Abdullah, J., & Khan, A. S. (2015). Towards vulnerability prevention model for web browser using interceptor approach.
[17] Lenando, H., Gharin, A. H., Jambli, M. N., Abdullah, J., & Khan, A. S. (2015). Neighbor selection protocol for heterogeneous information dissemination in Opportunistic Networks.
[18] Lenando, H., Sian, G. S., Khan, A. S., & Fauzi, A. H. (2014). Identify the best location to place data based on social interaction in opportunistic network.
[19] Liu, Y., et al. (2024). A Blockchain-Based Cross-Domain authentication management system for IoT devices. *IEEE Transactions on Network Science and Engineering, 11*(1), 115–127. https://doi.org/10.1109/tnse.2023.3292624
[20] Patwe, S., & Mane, S. B. (2023). Blockchain enabled architecture for secure authentication in the metaverse environment. *IEEE International Conference on Metaverse Computing, Networking and Applications (MetaCom)*. https://doi.org/10.1109/i2ct57861.2023.10126452
[21] Rathee, G., Kerrache, C. A., & Limam, M. (2023). TrustBlkSyS: a trusted and blockchained cybersecure system for IIoT. *IEEE Transactions on Industrial Informatics, 19*(2), 1592–1599. https://doi.org/10.1109/tii.2022.3182984
[22] Sukumaran, R. P., & Benedict, S. (2021). Survey on blockchain enabled authentication for Industrial Internet of Things. *2021 Fifth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*. https://doi.org/10.1109/i-smac52330.2021.9640973
[23] Zhang, P., Wang, Y., Aujla, G. S., Jindal, A., & Al-Otaibi, Y. D. (2022). A Blockchain-Based authentication scheme and secure architecture for IoT-Enabled maritime transportation systems. *IEEE Transactions on Intelligent Transportation Systems*, 1–10. https://doi.org/10.1109/tits.2022.3159485