
Journal of Informatics and Web Engineering

Vol. 4 No. 1 (February 2025)

eISSN: 2821-370X

Hyperledger Fabric Blockchain for Securing the Edge Internet of Things: A Review

Muhammad Haziq Zulhazmi Hairul Nizam¹, Muhammad Afiq Ahmad Nizam², Muhammad Hadi Husaini Jummadi³, Nik Nor Muhammad Saifudin Nik Mohd Kamal⁴, Ahmad Anwar Zainuddin^{5*}

^{1,2,3,4,5}Kulliyah of Information and Communication Technology, International Islamic University Malaysia, Jln Gombak, 53100 Kuala Lumpur, Malaysia.

*corresponding author: (anwarzain@iium.edu.my; ORCID: 0000-0001-6822-0075)

Abstract - Life has become more convenient, efficient, and productive in aspects like homes, healthcare, and other businesses' due to applied IoT. Nonetheless, the proliferation of IoT has led to enormous data production, which has presented daunting tasks of providing sound protective security solutions. It is crucial to address the above challenges in order to protect the data assets in IoT systems. This work deals with the concern on how to extend Hyperledger Fabric to IoT, this being a very crucial aspect in allowing for secure techniques in the collection, storage and sharing of data. Hyperledger Fabric offers advanced capabilities of smart contract and offers authorized and conditional access control, and this feature alone is enough to fulfil the IoT security needs. Therefore, this paper introduces a new solution related to the existing security problems in permissioned blockchain architecture, which is based on a four-tier architecture integrated into the Hyperledger Fabric platform. As for architecture, our proposal divides it into four layers: the application layer, the blockchain platform layer, the cloud storage layer and the IoT device layer, to tackle the problems of security and efficiency of the whole process. To establish the proposed solution, a data literature review has been carried out to collate the analysis and apply the data from the different studies. This paper shows that the deployment of blockchain technology in IoT environments also optimises IoT systems in terms of security, efficiency, and capacity in terms of IoT applications. As more and more IoT solutions appear and evolve, the usage of block chain technology as a whole and the specific Hyperledger Fabric platform in particular opens the way to overcoming the rather fluid issues of this constantly developing sphere.

Keywords— *Hyperledger Fabric, Blockchain Technology, Internet of Things, Four-Layer Architecture, Security*

Received: 13 July 2024; Accepted: 18 September 2024; Published: 16 February 2025

This is an open access article under the [CC BY-NC-ND 4.0](https://creativecommons.org/licenses/by-nc-nd/4.0/) license.



1. INTRODUCTION

Hyperledger Fabric's advantages are to mitigate the security weakness of other current permissioned blockchain systems. Through incorporating blockchain technology to the IT structure of Internet of Things (IoT) solutions with the aim of increasing security and privacy data. Thus, IoT system performance and reliability are improved as well as

security challenges are solved by this integration. For providing better security features and proper data handling, it provides a non-rigid and adaptive mechanism which can easily shift according to IoT environment.

However, because IoT has massive data and computing capability and a series of applications, its security is a crucial issue, blockchain with decentralized and unalter ability characteristics becomes a potential solution to the security issues of IoT applications. When comparing different types of blockchain, Hyperledger Fabric is an ideal choice, as it allows the user to set the access and meets strict security requirements. Nonetheless, Hyperledger Fabric is a permissioned blockchain solution while in public blockchains, anyone can participate within a network. This feature is crucial especially in the case of IoT where security is vital since unauthorized access may result in the loss of lives and property among other losses.

IoT is one of the most revolutionary technologies of the current epoch which has helped organizations and companies in enhancing the efficiency in several fields such as e-commerce, smart home, and several other related sectors in the medical field. IoT links a very large range of devices together, making it very easy to transfer information and talk to one another, and this leads to a world full of opportunities. But as the number of IoT devices running within networks increases there are concerns with security and privacy of user's data. Effective security measures are mandatory to protect the data that became the potential target of threat and vulnerability that endanger IoT systems.

This research aims at improving the security of the IoT systems by incorporating Hyperledger Fabric in four-layer architecture. These four layers include application layer, blockchain platform layer, cloud storage layer and IoT device layer. All the layers have their unique importance to contribute in the safety of the system and making it work at maximum capability. On one hand, the application layer is designed for performing user interactions and application related processes; On the other hand, the blockchain platform layer aims at maintaining safe and efficient data transactions. The cloud storage layer is responsible for having level access storage solutions while the IoT device layer handles the relation between the IoT devices and the network.

This is because in IoT applications there are many devices that communicate sensitive data with one another. Heterogeneous and large-scale IoT assume standard security mechanisms are ineffective because of their inability to tackle contemporary IoT complications adequately. The inclusion of Hyperledger Fabric into IoT architecture offers vigorous security systems since Fabric relies on cryptography and consensus algorithms. This minimizes chances of unauthorized access to the data and affords the data the necessary protection from manipulation. Moreover, the feature of Hyperledger Fabric to generate dense audit trails improves the levels of openness and proofs, which can also be viewed as improving the levels of security of IoT systems.

The 2017 release of Hyperledger Fabric, a blockchain technology from the Linux Foundation, provides a secure, extensible, and modular foundation for business applications [1]. It is used extensively worldwide in sectors such as finance and healthcare. Developed with Bitcoin in 2008, blockchain technology provides a decentralized, immutable digital ledger to securely record transactions and is used across a range of industries worldwide [2]. Having gained popularity in the 2010s, the IoT is a network of interconnected devices with embedded sensors and software that enables improved data collection and automation [3]. It is widely used in smart homes, healthcare and industrial automation. Healthcare is the systematic provision of medical care across a global network of facilities with the aim of improving health and quality of life. Since the invention of computers and the Internet, privacy and integrity have been a constant concern. Security, which is critical to IT and IoT, includes protecting against unauthorized access and attacks on systems and data.

This paper is arranged as follows: Section 1 gives a brief introduction to Hyperledger Fabric Blockchain for Securing the Edge IoT. Section 2 focuses on the existing literature of integration of Hyperledger Fabric in healthcare, e-commerce, banking transactions, smart homes and the security levels. Section 3 describes the methodology that is used for this research. Section 4 showcased evaluation and discussions of the proposed strategies to strengthen Hyperledger Fabric in securing IoT. Finally, Section 5 concludes the content of this research.

2. LITERATURE REVIEW

The papers by Wazzan [4] and Ataei [5], review current literature that summarizes studies done to integrate blockchain technology into securing IoT networks, emphasizing authentication as well as protection of data. Wazzan et al. go on to review the different approaches that IoT takes toward the detection of Botnet malware, underlining the IoT-based security approach, whereas gaps in the current method are addressed by recommending research in such methodologies. Ataei et al. deal with the application of Hyperledger Fabric in IoT systems for real-time data processing. Their work investigates the contribution of scalable authentication and protection of sensitive data, such as medical information in IoT edge networks, using Hyperledger Fabric combined with smart contracts and Physical Unclonable Functions (PUFs). Both papers emphasize that blockchain-based security solutions are fundamental for robust authentication and integrity in IoT applications, although they also recognize that some of the advantages of Hyperledger Fabric are not depending on the application context.

Although the paper by Yorozu[6] is mainly concerned with electron spectroscopy studies for magneto-optical media, the underlying insights may be instructive in applying blockchain technology in energy-distribution networks. In today's smart grid context, blockchain will be one of the most important game-changing tools, especially Hyperledger Fabric, in pursuit of network security and efficiency. The paper postulates that energy distribution networks would be more resilient and transparent by leveraging the decentralized ledger of Hyperledger Fabric. For this purpose, such a blockchain framework is necessary to protect against cyber threats, breach of a single point of failure, and tamper-proofing the transactions. This study outlines that the integration of blockchain technology made it possible to perform effective and safe energy transactions, enhancing the overall reliability and functionality of smart grids.

Table 1 provides a comprehensive overview of Hyperledger Fabric Blockchain for Securing the Edge IoT based on existing literature from 2020 onwards.

Table 1. Literature Review

Article	Key Finding / Argument	Supporting Evidence / Sample / Characteristics/ Methods	Strength / Limitations	Significance/ Implications
Research Question: Hyperledger Fabric-based Blockchain architecture and IoT				
[7]	Due to its ability to offer more scalable solutions than IPv6, blockchain can be utilized in the IoT.	Address conflicts are greatly decreased by the 160-bit addressing of the blockchain, which can produce $1.46 * 10^{48}$ unique addresses. $4.3 * 10^9$ more addresses are generated than with IPv6. removes the requirement for IP address assignment by an IANA-affiliated central body.	Several distinct addresses and high scalability. address management that is decentralized and independent of IANA.	Lessens the dependency on centralized authorities, increasing the efficiency and independence of IoT networks. enables the identification and addressing of IoT devices in a more secure and scalable manner.

[8]	The paper suggests utilizing Hyperledger Fabric to create a smart home security control system.	To improve security, the system makes use of Fabric's multi-party consensus and tamper-proof mechanisms. Every smart home gateway is a peer with its local ledger, and all of the devices are certificate-registered.	Utilizes the strong security features of Fabric, including: B. Tamper-resistance; additional testing might be required for the experiment before it can be developed on a larger scale.	It demonstrates how blockchain technology, and more specifically Hyperledger Fabric, can be used to secure smart home systems. Implications for enhancing IoT security are extensive.
[9]	"RPM in IoT: Centralization drawbacks, such as single-point failures and data manipulation, can be addressed to strengthen RPM using IoT and blockchain integration."	RPM systems gather health data from IoT devices, which blockchain is then used to securely manage and track.	Improves the dependability and security of data in RPM systems. Limitations: Difficulties with technology adoption and possible privacy issues.	Enhances the management and observation of patients, which may cut down on hospital stays and medical expenses.
[10][11]	The study aims to shed light on some of the security and privacy challenges that IoT systems face. The authors suggest an enhanced access control mechanism that guarantees the safe and effective administration of IoT devices, taking into account the decentralized and distributed nature of blockchain technology.	The study emphasizes the potential advantages of blockchain technology as well as the current difficulties with IoT access control. A decentralized access control system is created by combining Hyperledger Fabric with IoT devices in the suggested architecture.	Because blockchain is decentralized, there is less chance of unauthorized access and single points of failure, which improves the security of IoT access control systems. Limitations: Adoption may be hampered by the specialized knowledge and experience needed to implement and maintain a blockchain-based access control system.	The suggested system strengthens IoT access control security and fortifies it against intrusions and unauthorized access by utilizing blockchain technology.
[12][13]	The paper describes the permissioned network on which Hyperledger Fabric runs. This implies that everyone who joins is known to the other participants and	The document clarifies that access to the network is restricted to approved users only. Membership providers enforce access control and identity management. This limits access to sensitive patient data, protecting privacy and security.	In the healthcare industry, protecting patient data's integrity and confidentiality is crucial. Because of the design of Hyperledger Fabric, these worries are successfully handled. Limitation: Despite	Hyperledger Fabric greatly lowers the risk of data breaches and unauthorized access by guaranteeing that only authorized participants can access vital data, addressing a key issue in the healthcare industry.

	needs to authenticate.		the fact that Hyperledger Fabric is meant to be scalable, practical applications need to tackle the scalability issues brought about by the massive volume of medical data.	
[14]	In order to scale Hyperledger Fabric, an approach that accomplishes 20,000 transactions per second—nearly seven times faster than the initial system—is presented in this article. The study shows how the scalability of Hyperledger Fabric can be enhanced by adding more effective algorithms and parallel execution.	While mechanism is a less important consideration for permissioned blockchains, the authors concentrated on performance above mechanism. To increase performance, they made a number of architectural modifications, such as separating resource roles, using memory hierarchy, and implementing parallel execution.	Multi-core processors are effectively utilized in parallel execution. Limitations: Considerable alterations to the current infrastructure might be needed.	Hyperledger Fabric's increased scalability offers businesses wishing to expand their blockchain solutions a clear route forward.
[15][16]	A blockchain-enabled drug traceability system called Hyperledger Fabric can track pharmaceuticals at every stage of the supply chain, guaranteeing their safety and authenticity.	The paper addresses the issues with fake medications in the pharmaceutical sector and suggests Hyperledger Fabric as a fix. Blockchain technology is used by Hyperledger Fabric to generate a transparent and safe transaction ledger that can be used to detect fake medications.	The paper offers a novel solution that makes use of blockchain technology to deal with a pressing issue facing the pharmaceutical sector. Limitation: Scalability, governance, and identity registration are among the difficulties that are acknowledged in the article.	False medications are a serious risk to public health. The pharmaceutical supply chain's drug safety may be enhanced by Hyperledger Fabric.
[17][18]	The study evaluates the needs of	A thorough examination of the body of research on Hyperledger Fabric case	strong emphasis on performance metrics and real-world	Identifies potential research topics, such as optimizing operability

	<p>blockchain applications and how well they are met by Hyperledger Fabric. It identifies critical requirements such as scalability, confidentiality, interoperability and governance as essential for enterprise blockchain applications.</p>	<p>studies is included in the analysis. Case studies from companies like Change Healthcare, Honeywell Aerospace, and Walmart show how Hyperledger Fabric is being used in the real world and its advantages.</p>	<p>applications to present a fair picture of the technology's potential. Limitations: A number of performance assessments rely on simulated environments, which might not accurately represent actual circumstances.</p>	<p>and scalability to increase Hyperledger Fabric's usefulness in a variety of use cases.</p>
[19]	<p>Proposes an implementation of an ILMS on Hyperledger Fabric to overcome security issues such as DoS attacks, viruses, tempering, hacking, required in conventional ILMS while sustaining centrality, confidentiality, and immutability by recording transactions in a blockchain platform.</p>	<p>The proposed model has three modules: User Authentication, Catalog Management, and Transaction Management can be developed using Hyperledger Fabric because of its application of permissioned blockchain in an enclosed library setting. The model includes SHA-256 as the hashing algorithm for data integrity and timestamps for ordering of transaction and includes pseudocode and process flows for add a book, issue book, and return book.</p>	<p>Veil improves security and promotes transparency due to decentralized and distributed systems, hash functions and time stamps included in the system, and role based access for librarians and students. This is a blockchain-based ILMS which is ILMS-T, the limitations that may affect this system include the following; no real-world implementation or evaluation within a library setting and environment, the system may be slow and it is not clear how this system will interact with current ILMS or how data migration might be done.</p>	<p>In this system, blockchain applies the features of decentralization, immutability, and security to fix the major security issues raised in conventional ILMS and enhances the transparency of library operations.</p>
[20]	<p>This paper recommends the combination of Hyperledger Fabric as a</p>	<p>The paper introduces the prototype network that consists of Org1, Org2, IoT, and Orderer and illustrates the considered</p>	<p>One strength is being able to offer a feasible framework for implementing IoT and blockchain,</p>	<p>The proposed approach offers a decentralized access control system for IoT devices, improving data</p>

	<p>blockchain with IoT devices. It describes the most common IoT architecture and related security and privacy issues. The recommended system for the proposed environment takes on the blockchain-based access control system to ensure that the users are separated from the devices.</p>	<p>work flow (device registration, access control, and chaincode installation). It also has performance benchmarks on Raspberry Pi 4B IoT terminal yielding about 192 transactions per second.</p>	<p>using the characteristics of blockchain for storing key information and implementing access control. A limitation is that the implications of the score metrics are rudimentary and the scalability of the suggested method and other related issues are not highlighted.</p>	<p>governance and enabling secure machine-to-machine transactions. The work highlights the potential of using single-board computers as IoT platforms integrated with blockchain networks.</p>
[21]	<p>The article suggests a decentralized strategy by integrating IoT applications onto the Hyperledger Fabric blockchain platform. The main discovery is that Hyperledger Fabric distinguishes between the execution and consensus phases, enforces policy-based endorsements, and delivers improved performance suitable for IoT situations.</p>	<p>Smart contracts are used to establish rules and validate transactions from IoT devices within the smart home environment. Simulations are conducted to assess the impact on performance in terms of throughput, latency, and transaction payload size.</p>	<p>It utilizes Hyperledger Fabric's capability to differentiate execution from consensus to enhance performance in IoT situations. The article notes that conducting a detailed analysis of overheads is not feasible at this early stage of research. Future work requires integration with additional IoT domains and more in-depth performance analysis.</p>	<p>The article addresses security, privacy, and performance issues in IoT through the use of blockchain technology. The investigation sets the groundwork for upcoming projects involving the combination of blockchain with various IoT applications and domains.</p>
[22]	<p>The paper assesses how smart contracts function across various blockchain platforms in terms of scalability, system intricacy, and consensus mechanisms, shedding light on the advantages and</p>	<p>A comparison table is offered for various blockchain smart contract platforms such as Bitcoin, Ethereum, Hyperledger Fabric, NEM, Stellar, Waves, Lisk, NXT, Monax, and Qtum. Included are details about their smart contract languages, consensus protocols,</p>	<p>The paper delivers a detailed examination of smart contracts, their merging with IoT, and the related potential and difficulties. Limitation: The paper is mainly theoretical and does not include practical implementation</p>	<p>The article emphasizes how smart contracts have the capability to facilitate the merging of blockchain and IoT, which may result in the creation of fresh decentralized applications and business models. The paper proposes potential areas for future</p>

	obstacles of linking smart contracts between blockchain and IoT.	cryptocurrencies, system complexity, and scalability.	specifics or case studies.	research.
[23]	The article suggests a grammar and compiler to help create smart contracts for securing IoT firmware updates with Hyperledger Fabric, a blockchain platform.	The ANTLR tool is utilized for implementing the grammar and creating lexical and syntax analyzers. A compiler's purpose is to interpret the rules of grammar and create a chaincode file that works with Hyperledger Fabric. An experimental system involving a Vue.js front-end interface, a Golang back-end server, and a compiler service is created and tested across various scenarios.	Simplifies the process of developing smart contracts for securing IoT firmware updates. Also creates chaincode files for Hyperledger Fabric that are ready for deployment without requiring extra input from end users. Restricted to creating chaincode files exclusively for Hyperledger Fabric. In the future, it might be necessary to enhance the grammar to encompass additional use cases.	The suggested method could help in making it easier to use blockchain technology for securing IoT firmware updates. Automating the process of generating smart contracts decreases the workload and potential discrepancies among various manufacturers.

3. RESEARCH METHODOLOGY

This research paper is based solely on qualitative research and analysis of the application of Hyperledger Fabric Blockchain in enhancing Edge IoT device security, thorough literature analysis, which is followed by the suggestion and verification of a novel technique for blockchain-based IoT device security.

3.1 Literature Review and Data Collection

The Literature Review enables this study to identify and explore the application of Hyperledger Fabric Blockchain in the protection of edge IoT devices from other related works including scholarly journals, conference proceedings and research papers. International scientific articles were initially searched using the following key terms: "Blockchain," "Hyperledger Fabric," "Edge IoT," "Security," "Privacy," and "IoT".

The research papers and studies selected for this study that were found from search engines such as IEEE Xplore, Google Scholar and ACM Digital Library were rigorously examined in the process of data extraction, finding out relevant data, conclusions, and insights related to the suggested tactics and enhancements in edge IoT device security employing Hyperledger Fabric Blockchain.

3.2 Proposed Technique: Application of Hyperledger Fabric Blockchain

To achieve the proposed objectives, an analysis of the collected data was performed by defining the main themes, tendencies and the lack of publications in the subject area. The insight elaborated on the theoretic and implementational assessments of the Hyperledger Fabric Blockchain for adopting edge IoT devices.

3.2.1 Detailed Approach

- **Assessment Criteria:** Throughput, transaction delay, computational requirements, network scalability and per-communication cost are the commonly used measures to assess this technique. These criteria were chosen to provide a profound evaluation of Hyperledger Fabric Blockchain effectiveness in a real IoT environment.
- **Implementation Strategy:** This technique is achieved by incorporating Hyperledger Fabric Blockchain into the Edge IoT infrastructure. The aim of this integration is to provide a more efficient and safe mechanism for data protection, IoT devices and security violation issues.
- **Experimental Methods:** The proposed method was validated by simulating and carrying out experimental work on this software. These experiments were designed put into practice with respect to the evaluation metrics discussed above to quantify impact of adopting blockchain in the system. The results of these tests provide empirical evidence for practical effectiveness of the proposed method.

4. RESULTS AND DISCUSSIONS

To innovate Hyperledger Fabric Blockchain for securing the Edge IoT, there are several key strategies and enhancements that can be considered based on the insights from the provided sources.

4.1. Adaptability for ARM Architecture

To support ARM architectures, especially the 64-bit ARMv8 processors that are common in edge IoT devices, the focus has been on modifying Hyperledger Fabric (HLF) since 2020. Although there are no official Docker images available for this architecture, project managers have found ways to get around this by making changes to the existing images that make them compatible with ARM-based IoT devices. This adaptability is essential because ARM processors, which are perfect for edge computing environments because of their low power consumption and efficiency, dominate the IoT ecosystem. The version of official Hyperledger Fabric Docker images source must be ported for specific change in adaptability of the ARM architecture of edge IoT devices as shown in Figure 1 [24],[25]. As there are no official or public images available against Hyperledger Fabric (HLF) supporting 64-bit ARMv8 architecture, Project Managers could tweak these images that ultimately improve the compatibility entrance for edge-IoT devices that exclusively relies on ARM processors [26],[27].

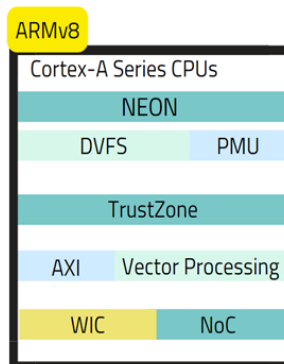


Figure 1. Advanced RISC Machine (ARMv8) Processor

Table 1 key findings emphasize the importance of energy efficiency, scalability, and enhanced cryptographic processing capabilities in Hyperledger Fabric's major efforts to secure edge IoT by adapting to the ARM architecture. By emphasizing the value of customized Docker images, energy efficiency, and security features like TrustZone, these 2020 developments seek to improve Hyperledger Fabric's compatibility with resource-constrained IoT environments.

4.1.1 Explanation of Components

- **Cortex-A Series CPUs:** The main component of the system responsible for processing data. It retrieves, interprets,

and carries out commands and is suitable for running complex workloads like those in Hyperledger Fabric Blockchain.

- **WIC:** This section serves as the Wait-for-Interrupt Controller. It oversees interruptions, signals that prompt the processor to pause its current task and address a more pressing matter.
- **Floating Point Unit (FPU):** This component is required in computing the advanced calculations required in performing complex operations especially those that require cryptographic computations, which are common in most of the blockchain projects.
- **NEON SIMD:** One of the elements of the ARM architecture, called NEON or Single Instruction, Multiple Data, is used to enhance media processing speeds. Which when applied to some of the blockchain operations that can occur in parallel will increase the computational throughput.
- **Vector Processing:** They allow for several data to be processed at the same time, vector processing units that are present in some of the ARM cores are required for applications that require a great deal of computation.
- **Dynamic Voltage and Frequency Scaling (DVFS):** Using this feature, ARMv8-A processors can manage their power usage according to demand, creating a great foundation for the IoT to run under Hyperledger Fabric.
- **Power Management Interface (PMU):** One of the essential factors influencing the edge IoT devices is power management, and ARM's Power Management Unit (PMU) might control and perform the power usage.
- **TrustZone for Scalability in Security:** The separation of the trusted and non-trusted hardware environment is achieved through ARM architecture feature called TrustZone. These are security solutions that can grow as the number of connected devices increases, can be implemented on other IoT devices and perform efficiently.
- **AXI Interconnect:** The Advanced eXtensible Interface (AXI), a component of the ARM AMBA (Advanced Microcontroller Bus Architecture), allows for high-speed communication between the CPU, memory, and other peripherals, enhancing network scalability and performance.

4.2. Lightweight Mutual Authentication and Authorization Model

Figure 2 indicates the lightweight mutual authentication and authorization model is proposed to secure edge IoT including privacy-preserving for edge computing [30],[31].

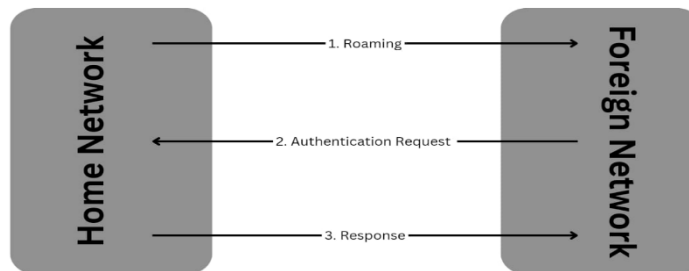


Figure 2. The mutual authentication procedure for the global roaming in mobility environments

- **Roaming:** The device from the Home Network initiates a connection while in the Foreign Network, sending a roaming request to the Foreign Network.
- **Authentication Request:** The Foreign Network then forwards an authentication request back to the Home Network, asking it to verify the identity of the roaming device.
- **Response:** After the Home Network verifies the device, it sends a response back to the Foreign Network, allowing the device to access the network.

This should ensure that the data of the sensor nodes is private through a permissioned fabric platform to allow the IoT sensors, edge nodes, and base stations to be trusted through private blockchain [32],[33]. Store IoT data in edge nodes in a Blockchain manner that makes it hard to change or delete it, while providing for metadata accountability [34],[35].

4.3. ChainCodes for Tamper-Proof Storage

ChainCodes are suggested to maintain form immutable blockchain databases and that allow for data to be accessed easily as depicted in Figure 3 [36]. These ChainCodes are the essential components, which help establish the safe storage of IoT data, improving its security and integrity, thus – the overall framework of the IoT ecosystem [37].

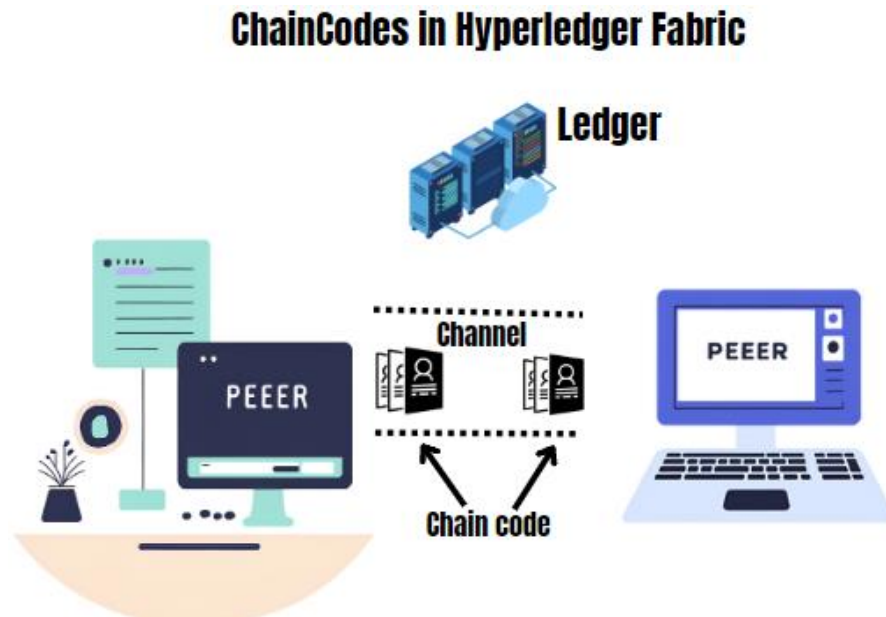


Figure 3. The Process of ChainCodes in Hyperledger Fabric

In Figure 3, every peer symbolizes a group or individual who is providing data. Chaincodes, the invisible components, establish the guidelines for handling this information. They serve as guardians, determining the formatting, validation, and storage of sensor data on the shared ledger.

The system's security is centered around this shared ledger. It is a blockchain, an unalterable sequence of digital blocks. Every block is cryptographically linked to the previous one, forming a record that cannot be altered. Once sensor data in a transaction is verified and included in the ledger, it is permanently recorded [38]. The unchangeable nature, a fundamental aspect of blockchain technology, stops unauthorized changes or removals. All participants must agree in order for any one entity to manipulate the data, promoting trust and transparency in the network.

Chaincodes also allow for a thorough audit trail. Each time a chaincode processes a transaction, it creates a digital record on the ledger. This detailed documentation enables approved users to review the data's history like a symphony, ensuring every note played can be verified for a thorough understanding[39].

While channels may not be clearly shown in the diagram, they are essential for access control [40]. Channels serve as virtual pathways in the network, separating transactions among certain participants. Chaincodes can be structured to function within these channels, providing permission exclusively to authorized entities. This division stops unapproved individuals from altering or accessing sensitive data, safeguarding the privacy and security of all participants' information [41].

4.4. Blockchain-Based Data Traceability for 5G-Enabled Edge Computing

Legal academics should detail concrete tracing methodologies of data leveraging the blockchain technology for 5G-enabled edge computing [42],[43]. This entails creating a client library for NodeJS which will serve to enhance the audit capability of the IoT metadata such that all transactions as well as movements in the IoT system can be effectively audited. This is important in ensuring that IoT infrastructure is well protected, and an accountable environment

maintained [44].

4.5. Performance Evaluation

Figure 4 indicates the implementation of Hyperledger Fabric in IoT computing environments. The proposed architecture of the blockchain should be examined whether it outperforms or underperforms in the given domain through the use of experimental techniques and measures such as throughput, transaction latency, amount of computation required, network utilization, and other communication expenses for a number of networks. This evaluation is rather important for recognizing a prospective of the blockchain solution in many different and various contexts [45].

By implementing these innovations, Hyperledger Fabric can be effectively leveraged to enhance the security and privacy of edge IoT computing environments [46]. These strategies address key challenges such as device compatibility, data protection, and system performance, thereby paving the way for more secure and efficient IoT deployments [47].

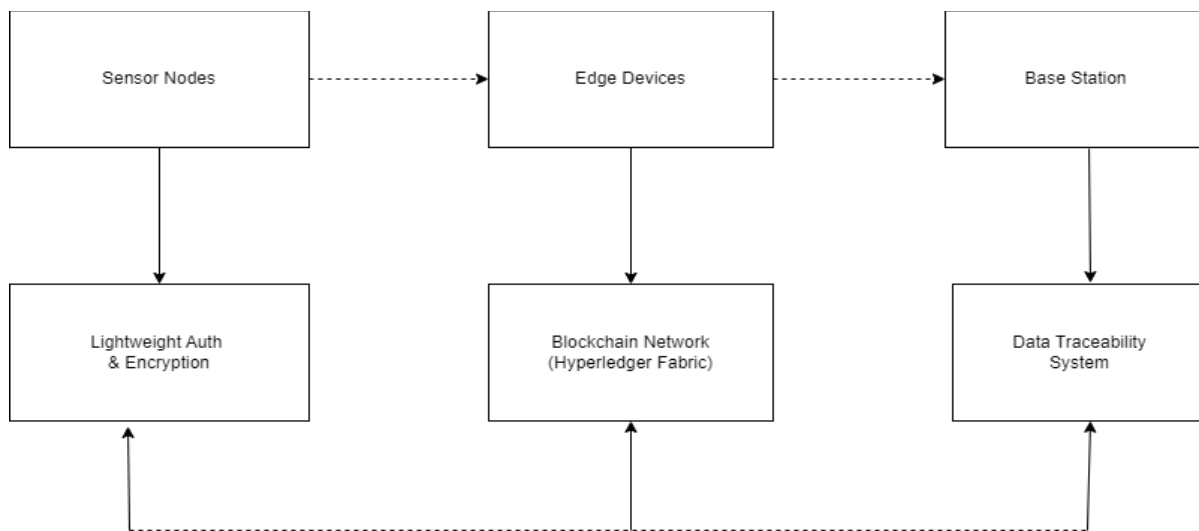


Figure 4. The Implementation of Hyperledger Fabric in IoT Computing Environments

4.5.1 Explanation of Components

Sensor Nodes: The outermost periphery of the IoT network that is directly attached to the physical sensors and gathers data. These nodes require sharing information with the other part of the network while maintaining the highest level of security[48].

Edge Devices:Analyze the information and store it within the local environment. These gateway nodes operate in intermediate levels, between the sensor nodes and the base station, where they filter data.

Base Station:The middle node that may transmit/send data to edge devices and possibly Cloud services. It collects data from edge devices, processes and encrypts it and forwards it to the blockchain network for further continuation of the process.

Lightweight Auth & Encryption:This layer offers a secure manner for sending and receiving data between different nodes and the base station. It entails policies and procedures that help to reduce the amount of resource consumed in these edge devices while at the same time enabling data privacy and accuracy.[49]

Blockchain Network (Hyperledger Fabric):It is the most important part of the entire security framework[50]. Through the smart contracts often referred to as the ChainCodes, it is able to check compliance to rules and policies

and record all the transactions in a permanent manner [51]. This work makes it possible for participants in the network to authenticate and authorize each other.

4.6. Data Traceability System

This system uses the power of the blockchain to ensure that any data that is collected in, and sent throughout the IoT system is between accountable and reproducible. This system has the ability to hold a record of all the transactions that take place so that there can be trust and efficacy in the system [52].

This illustrates a high-level view of how Hyperledger Fabric can be integrated into an edge IoT security framework, focusing on secure data collection, processing, and transmission [53]. Each individual component plays a vital assigned role in facilitating and maintaining the integrity, confidentiality, and traceability associated with IoT data for the purpose of a trustworthy edge IoT ecosystem [54].

5. CONCLUSION

Therefore, incorporating blockchain technology like Hyperledger Fabric in edge IoT environments is a great leap towards addressing the severe security challenges that such systems have. Using Hyperledger Fabric's intrinsic components such as the immutability and encryption of ledger records as well as the right permission mechanisms, IoT applications can establish added security, reliability, and effectiveness. It is a winning solution that ensures the protection of the information that is very important for the enterprise and minimizes the threats connected with information leakage and cyber-attacks. As the IoT develops and evolves consequently ambitions strong blockchain solutions like Hyperledger Fabric will be required to ensure user data and privacy. The results of this research highlight the potential for Hyperledger Fabric to serve as a cornerstone technology in ongoing efforts to secure IoT ecosystems and pave the way for more secure and resilient digital infrastructures.

ACKNOWLEDGEMENT

This work is supported by the Department of Computer Sciences, KICT, IIUM, Centre of Excellence Cybersecurity, KICT, IoTeams, KICT and Silverseeds Lab Network.

FUNDING STATEMENT

The authors received no funding from any party for the research and publication of this article.

AUTHOR CONTRIBUTIONS

Muhammad Haziq Zulhazmi Hairul Nizam: Project Administration, Abstract, Results and Discussions
Muhammad Afiq Ahmad Nizam: Literature review, Conclusion, Research Methodology
Muhammad Hadi Husaini Jummadi: Writing – Review & Editing.
Nik Nor Muhammad Saifudin Nik Mohd Kamal: Validation, Writing – Original Draft Preparation
Ahmad Anwar Zainuddin: Project Supervisor

CONFLICT OF INTERESTS

No conflict of interests were disclosed.

ETHICS STATEMENTS

The paper follows The Committee of Publication Ethics (COPE) guideline.

REFERENCES



- [1] H. Liu, D. Han, and D. Li, "Fabric-iot: A Blockchain-Based Access Control System in IoT," *IEEE Access*, vol. 8, pp. 18207–18218, 2020, doi: 10.1109/ACCESS.2020.2968492.
- [2] H. Honar Pajooh, M. Rashid, F. Alam, and S. Demidenko, "Multi-Layer Blockchain-Based Security Architecture for Internet of Things," *Sensors*, vol. 21, no. 3, p. 772, Jan. 2021, doi: 10.3390/s21030772.
- [3] X. Liu, M. Zhao, S. Li, F. Zhang, and W. Trappe, "A Security Framework for the Internet of Things in the Future Internet Architecture," *Future Internet*, vol. 9, no. 3, p. 27, Jun. 2017, doi: 10.3390/fi9030027.
- [4] M. Wazzan, D. Algazzawi, O. Bamasaq, A. Albeshri, and L. Cheng, "Internet of Things Botnet Detection Approaches: Analysis and Recommendations for Future Research," *Applied Sciences*, vol. 11, no. 12, p. 5713, Jun. 2021, doi: 10.3390/app11125713.
- [5] M. Ataei, A. Eghmazi, A. Shakerian, R. Landry, and G. Chevrette, "Publish/Subscribe Method for Real-Time Data Processing in Massive IoT Leveraging Blockchain for Secured Storage," *Sensors*, vol. 23, no. 24, p. 9692, Dec. 2023, doi: 10.3390/s23249692.s.
- [6] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," *IEEE Transl. J. Magn. Japan*, vol. 2, pp. 740–741, August 1987 [Digests 9th].
- [7] F. P. Oikonomou, J. Ribeiro, G. Mantas, J. M. C. S. Bastos, and J. Rodriguez, "A Hyperledger Fabric-based Blockchain Architecture to Secure IoT-based Health Monitoring Systems," in 2021 IEEE International Mediterranean Conference on Communications and Networking (MeditCom), Athens, Greece: IEEE, Sep. 2021, pp. 186–190. doi: 10.1109/MeditCom49071.2021.9647521.
- [8] F. Pelekoudas-Oikonomou, J. Ribeiro, G. Mantas, F. Bashashi, G. Sakellari, and J. Gonzalez, "A Tutorial on the Implementation of a Hyperledger Fabric-based Security Architecture for IoMT," in 2023 IFIP Networking Conference (IFIP Networking), Barcelona, Spain: IEEE, Jun. 2023, pp. 1–6. doi: 10.23919/IFIPNetworking57963.2023.10186443.
- [9] S. Pancari, A. Rashid, J. Zheng, S. Patel, Y. Wang, and J. Fu, "A Systematic Comparison between the Ethereum and Hyperledger Fabric Blockchain Platforms for Attribute-Based Access Control in Smart Home IoT Environments," *Sensors*, vol. 23, no. 16, p. 7046, Aug. 2023, doi: 10.3390/s23167046.
- [10] H. Honar Pajooh, M. Rashid, F. Alam, and S. Demidenko, "Hyperledger Fabric Blockchain for Securing the Edge Internet of Things," *Sensors*, vol. 21, no. 2, p. 359, Jan. 2021, doi: 10.3390/s21020359.
- [11] D. Gordijn, R. Kromes, Thanassis Giannetsos, and Kaitai Liang, "Combining ID's, Attributes, and Policies in Hyperledger Fabric," Jul. 2023, doi: 10.5281/ZENODO.8112950
- [12] S. B. Toumia, C. Berger, and H. P. Reiser, "Evaluating Blockchain Application Requirements and their Satisfaction in Hyperledger Fabric." arXiv, 2021. doi: 10.48550/ARXIV.2111.15399.
- [13] C. Gorenflo, S. Lee, L. Golab, and S. Keshav, "FastFabric: Scaling hyperledger fabric to 20 000 transactions per second," *Int. J. Netw. Manag.*, vol. 30, no. 5, p. e2099, Sep. 2020, doi: 10.1002/nem.2099.
- [14] A. Iftekhhar, X. Cui, Q. Tao, and C. Zheng, "Hyperledger Fabric Access Control System for Internet of Things Layer in Blockchain-Based Applications," *Entropy*, vol. 23, no. 8, p. 1054, Aug. 2021, doi: 10.3390/e23081054
- [15] A. Nedaković, A. Hasselgren, K. Krlevska, and D. Gligoroski, "Hyperledger fabric platform for healthcare trust relations—Proof-of-Concept," *Blockchain Res. Appl.*, vol. 4, no. 4, p. 100156, Dec. 2023, doi: 10.1016/j.bcra.2023.100156.
- [16] L. Hang and D.-H. Kim, "Optimal blockchain network construction methodology based on analysis of configurable components for enhancing Hyperledger Fabric performance," *Blockchain Res. Appl.*, vol. 2, no. 1, p. 100009, Mar. 2021, doi: 10.1016/j.bcra.2021.100009.




- [17] G. Al-Sumaidae, R. Alkhudary, Z. Zilic, and A. Swidan, "Performance analysis of a private blockchain network built on Hyperledger Fabric for healthcare," *Inf. Process. Manag.*, vol. 60, no. 2, p. 103160, Mar. 2023, doi: 10.1016/j.ipm.2022.103160.
- [18] H. Lee, "The acceleration of blockchain technology adoption in Taiwan," *Heliyon*, vol. 9, no. 11, p. e21887, Nov. 2023, doi: 10.1016/j.heliyon.2023.e21887.
- [19] A. Pericherla, P. Paul, S. Sural, J. Vaidya, and V. Atluri, "Towards Supporting Attribute-Based Access Control in Hyperledger Fabric Blockchain," in *ICT Systems Security and Privacy Protection*, vol. 648, W. Meng, S. Fischer-Hübner, and C. D. Jensen, Eds., in IFIP Advances in Information and Communication Technology, vol. 648., Cham: Springer International Publishing, 2022, pp. 360–376. doi: 10.1007/978-3-031-06975-8_21.
- [20] C. M. Naga Sudha and J. V. N. J., "TrackChain: Hyperledger based pharmaceutical supply chain – Resource utilization perspective," *Heliyon*, vol. 10, no. 1, p. e23250, Jan. 2024, doi: 10.1016/j.heliyon.2023.e23250.
- [21] M. Q. Nguyen, D. Loghin, and T. T. A. Dinh, "Understanding the Scalability of Hyperledger Fabric." arXiv, 2021. doi: 10.48550/ARXIV.2107.09886.
- [22] E. A. Shammar, A. T. Zahary, and A. A. Al-Shargabi, "An Attribute-Based Access Control Model for Internet of Things Using Hyperledger Fabric Blockchain," *Wirel. Commun. Mob. Comput.*, vol. 2022, pp. 1–25, Jul. 2022, doi: 10.1155/2022/6926408.
- [23] U. Satapathy, B. Ku. Mohanta, S. S. Panda, S. Sobhanayak, and D. Jena, "A Secure Framework for Communication in Internet of Things Application using Hyperledger based Blockchain," in *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, Kanpur, India: IEEE, Jul. 2019, pp. 1–7. doi: 10.1109/ICCCNT45670.2019.8944811.
- [24] A. Singh, A. Payal, and S. Bharti, "A walkthrough of the emerging IoT paradigm: Visualizing inside functionalities, key features, and open issues," *J. Netw. Comput. Appl.*, vol. 143, pp. 111–151, Oct. 2019, doi: 10.1016/j.jnca.2019.06.013.
- [25] L. D. Xu, Y. Lu, and L. Li, "Embedding Blockchain Technology Into IoT for Security: A Survey," *IEEE Internet Things J.*, vol. 8, no. 13, pp. 10452–10473, Jul. 2021, doi: 10.1109/JIOT.2021.3060508.
- [26] F. Pelekoudas-Oikonomou *et al.*, "Blockchain-Based Security Mechanisms for IoMT Edge Networks in IoMT-Based Healthcare Monitoring Systems," *Sensors*, vol. 22, no. 7, p. 2449, Mar. 2022, doi: 10.3390/s22072449.
- [27] "Towards A Blockchain Enabled Integrated Library Management System Using Hyperledger Fabric: Using Hyperledger Fabric", *IJCIS*, vol. 1, no. 3, pp. 17–24, Sep. 2022, Accessed: Jun. 07, 2024. [Online].
- [28] J. Ali, T. Ali, S. Musa, and A. Zahrani, "Towards Secure IoT Communication with Smart Contracts in a Blockchain Infrastructure," *Int. J. Adv. Comput. Sci. Appl.*, vol. 9, no. 10, 2018, doi: 10.14569/IJACSA.2018.091070.
- [29] A. Rashid and M. J. Siddique, "Smart Contracts Integration between Blockchain and Internet of Things: Opportunities and Challenges," in *2019 2nd International Conference on Advancements in Computational Sciences (ICACS)*, Lahore, Pakistan: IEEE, Feb. 2019, pp. 1–9. doi: 10.23919/ICACS.2019.8689132.
- [30] X. He, R. Gamble, and M. Papa, "A Smart Contract Grammar to Protect IoT Firmware Updates using Hyperledger Fabric," in *2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, Vancouver, BC, Canada: IEEE, Oct. 2019, pp. 0034–0042. doi: 10.1109/IEMCON.2019.8936223.
- [31] M. Gebhard, M. Schluse, M. Hoppen, and J. Roßmann, "A multi-domain networking infrastructure enabling the situation-specific choreography of decentralized things," in *Annals of Scientific Society for Assembly, Handling and Industrial Robotics*, T. Schüppstuhl, K. Tracht, and D. Henrich, Eds., Berlin, Heidelberg: Springer Berlin Heidelberg, 2020, pp. 127–137. doi: 10.1007/978-3-662-61755-7_12.

- [32] M. N. M. Bhutta *et al.*, “A Survey on Blockchain Technology: Evolution, Architecture and Security,” *IEEE Access*, vol. 9, pp. 61048–61073, 2021, doi: 10.1109/ACCESS.2021.3072849.
- [33] E. Mahe, R. Abdallah, S. Tucci-Piergiovanni, and P.-Y. Piriou, “Adversary-Augmented Simulation to evaluate fairness on Hyperledger Fabric.” arXiv, 2024. doi: 10.48550/ARXIV.2403.14342.
- [34] T. Guggenberger, J. Sedlmeir, G. Fridgen, and A. Luckow, “An in-depth investigation of the performance characteristics of Hyperledger Fabric,” *Comput. Ind. Eng.*, vol. 173, p. 108716, Nov. 2022, doi: 10.1016/j.cie.2022.108716.
- [35] O. Wu, S. Li, H. Zhang, L. Liu, Y. Wang, and H. Li, “An Optimized Scheduling Algorithm for the Multi-channel Hyperledger Fabric,” in *2022 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking (ISPA/BDCloud/SocialCom/SustainCom)*, Melbourne, Australia: IEEE, Dec. 2022, pp. 636–643. doi: 10.1109/ISPA-BDCloud-SocialCom-SustainCom57177.2022.00087.
- [36] T. R. Gadekallu *et al.*, “Blockchain for Edge of Things: Applications, Opportunities, and Challenges,” *IEEE Internet Things J.*, vol. 9, no. 2, pp. 964–988, Jan. 2022, doi: 10.1109/JIOT.2021.3119639.
- [37] Y. Du, Z. Wang, and V. C. M. Leung, “Blockchain-Enabled Edge Intelligence for IoT: Background, Emerging Trends and Open Issues,” *Future Internet*, vol. 13, no. 2, p. 48, Feb. 2021, doi: 10.3390/fi13020048.
- [38] M. Shen *et al.*, “Blockchains for Artificial Intelligence of Things: A Comprehensive Survey,” *IEEE Internet Things J.*, vol. 10, no. 16, pp. 14483–14506, Aug. 2023, doi: 10.1109/JIOT.2023.3268705.
- [39] Md. S. I. Bhuiyan, A. Razzak, M. S. Ferdous, M. J. M. Chowdhury, M. A. Hoque, and S. Tarkoma, “BONIK: A Blockchain Empowered Chatbot for Financial Transactions,” in *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, Guangzhou, China: IEEE, Dec. 2020, pp. 1079–1088. doi: 10.1109/TrustCom50675.2020.00143.
- [40] Q. Xu, Y. Lin, Q. Jiang, and M. Zhang, “Cache-based Optimization for Block Commit of Hyperledger Fabric,” in *2020 International Conference on Data Mining Workshops (ICDMW)*, Sorrento, Italy: IEEE, Nov. 2020, pp. 902–906. doi: 10.1109/ICDMW51313.2020.00129.
- [41] J. Li, D. Niyato, C. S. Hong, K.-J. Park, L. Wang, and Z. Han, “Cyber Insurance Design for Validator Rotation in Sharded Blockchain Networks: A Hierarchical Game-Based Approach,” *IEEE Trans. Netw. Serv. Manag.*, vol. 18, no. 3, pp. 3092–3106, Sep. 2021, doi: 10.1109/TNSM.2021.3078142.
- [42] I. A. Ridhawi, S. Otoum, and M. Aloqaily, “Decentralized Zero-Trust Framework for Digital Twin-based 6G.” arXiv, 2023. doi: 10.48550/ARXIV.2302.03107.
- [43] S. Hamdan, M. Ayyash, and S. Almajali, “Edge-Computing Architectures for Internet of Things Applications: A Survey,” *Sensors*, vol. 20, no. 22, p. 6441, Nov. 2020, doi: 10.3390/s20226441.
- [44] D. Khan, L. T. Jung, M. A. Hashmani, and M. K. Cheong, “Empirical Performance Analysis of Hyperledger LTS for Small and Medium Enterprises,” *Sensors*, vol. 22, no. 3, p. 915, Jan. 2022, doi: 10.3390/s22030915.
- [45] S. Sutradhar, S. Karforma, R. Bose, S. Roy, S. Djebali, and D. Bhattacharyya, “Enhancing identity and access management using Hyperledger Fabric and OAuth 2.0: A block-chain-based approach for security and scalability for healthcare industry,” *Internet Things Cyber-Phys. Syst.*, vol. 4, pp. 49–67, 2024, doi: 10.1016/j.ioteps.2023.07.004.
- [46] A. Banushri and R. A. Karthika, “Hyperledger Blockchain and Lightweight Bcrypt Symmetric Key Encryption to Boost Cloud Computing Security Effectiveness,” in *2023 International Conference on Circuit Power and Computing Technologies (ICCPCT)*, Kollam, India: IEEE, Aug. 2023, pp. 1525–1530. doi: 10.1109/ICCPCT58313.2023.10245926.

- [47] J. Chen, M. Hoppen, D. Boken, J. Reitz, M. Schluse, and J. Rosmann, "Identity, Authentication and Authorization in Forestry 4.0 Using OAuth 2.0," in *2022 3rd International Informatics and Software Engineering Conference (IISEC)*, Ankara, Turkey: IEEE, Dec. 2022, pp. 1–6. doi: 10.1109/IISEC56263.2022.9998287.
- [48] S. S. Saha, C. Gorog, A. Moser, A. Scaglione, and N. G. Johnson, "Integrating Hardware Security into a Blockchain-Based Transactive Energy Platform," in *2020 52nd North American Power Symposium (NAPS)*, Tempe, AZ, USA: IEEE, Apr. 2021, pp. 1–6. doi: 10.1109/NAPS50074.2021.9449802.
- [49] J. Chen and J. Roßmann, "Integration of an IoT Communication Infrastructure in Distributed Production Systems in Industry 4.0," in *Annals of Scientific Society for Assembly, Handling and Industrial Robotics 2022*, T. Schüppstuhl, K. Tracht, and J. Fleischer, Eds., Cham: Springer International Publishing, 2023, pp. 367–377. doi: 10.1007/978-3-031-10071-0_30.
- [50] H. Xue, D. Chen, N. Zhang, H.-N. Dai, and K. Yu, "Integration of Blockchain and Edge Computing in Internet of Things: A Survey." arXiv, 2022. doi: 10.48550/ARXIV.2205.13160.
- [51] K. Zhang, X. Gui, D. Ren, T. Du, and X. He, "Optimal pricing-based computation offloading and resource allocation for blockchain-enabled beyond 5G networks," *Comput. Netw.*, vol. 203, p. 108674, Feb. 2022, doi: 10.1016/j.comnet.2021.108674.
- [52] O. Wu, Z. Wang, and Z. Li, "Performance Modeling of Hyperledger Fabric 2.0: A Queuing Theory-Based Approach," *Wireless Communications and Mobile Computing*, vol. 2023, pp. 1–20, Dec. 2023, doi: 10.1155/2023/9957995.
- [53] Y. Kim, K.-H. Kim, and J.-H. Kim, "Power Trading Blockchain using Hyperledger Fabric," in *2020 International Conference on Information Networking (ICOIN)*, Barcelona, Spain: IEEE, Jan. 2020, pp. 821–824. doi: 10.1109/ICOIN48656.2020.9016428
- [54] S. De Angelis, F. Lombardi, G. Zanfino, L. Aniello, and V. Sassone, "Security and dependability analysis of blockchain systems in partially synchronous networks with Byzantine faults," *International Journal of Parallel, Emergent and Distributed Systems*, pp. 1–21, Oct. 2023, doi: 10.1080/17445760.2023.2272777.

BIOGRAPHIES OF AUTHORS

	<p>Muhammad Afiq Ahmad Nizam is a student in Kulliyah of Information and Communication Technology, International Islamic University Malaysia. His interest includes study in Information Technology and Cybersecurity He can be contacted at email: muhdafiqnizam@gmail.com.</p>
	<p>Muhammad Haziq Zulhazmi Hairul Nizam is a student in Kulliyah of Information and Communication Technology, International Islamic University Malaysia. His research focuses on general view, methodology and recommendation of Hyperledger Fabric and blockchain technology He can be contacted at email: mhaziq.zulhazmi@gmail.com.</p>

	<p>Muhammad Hadi Husaini Jummadi is a student in Kulliyah of Information and Communication Technology, International Islamic University Malaysia. His research focuses on general view, methodology and recommendation of Hyperledger Fabric and blockchain technology He can be contacted at email: hadi.iium.oct2023@gmail.com.</p>
	<p>Nik Nor Muhammad Saifudin Nik Mohd Kamal is a computer science graduate from Kulliyah of Information and Communication Technology, International Islamic University Malaysia (KICT, IIUM), majoring in network security. He has a solid background in the concept of computer science and practical experience in the field of Internet of Things (IoT). He, being a person who can labor adeptly with the Arduino IDE, would like to apply the skills learned and knowledge in creative projects within the sectors of computer science and network security. He has a burning desire to contribute toward advanced technological development in these fields. He can be reached at saifudinkamal11@gmail.com.</p>
	<p>Ahmad Anwar Zainuddin is an Assistant Professor at the International Islamic University Malaysia (IIUM). He holds a Ph.D. and is recognized for his expertise in Computer Engineering. His research interests include Internet-of-Things (IoT), Artificial Intelligence (AI), Blockchain, and acoustic wave electrochemistry biosensors, indicating a focus on interdisciplinary applications of technology. He emphasizes the importance of AI concepts, problem-solving skills, and adaptability in a fast-paced tech landscape. His contributions to research and academia align with the ICT body of knowledge, particularly in areas such as biosensors and AI integration. He can be contacted via email: anwarzain@iium.edu.my.</p>