APTISI Transactions on Technopreneurship (ATT)
Vol. 8, No. 1, March 2026, pp. 138−151
E-ISSN: 2656-8888 | P-ISSN: 2655-8807, DOI:10.34306

Consortium Blockchain Framework for Secure Digital Medical Record Innovation

Irwan Sembiring[1], Bintang Kristianto Aji[2], Teguh Indra Bayu[3*]
[1, 2, 3]Faculty of Information Technology, Satya Wacana Christian University, Indonesia
[1]irwan@uksw.edu, [2]2672021014@student.uksw.edu, [3]teguh.bayu@uksw.edu
***Corresponding Author**

Article Info

Article history:

Submission June 26, 2025
Revised August 8, 2025
Accepted December 15, 2025
Published January 19, 2026

Keywords:

Blockchain
Electronic Medical Records
Consortium
NFC
Smart Contract

ABSTRACT

Healthcare systems face growing challenges in protecting patient information, with more than 276 million healthcare records breached in 2024 alone. **This study presents** a proof-of-concept consortium blockchain framework that integrates Near Field Communication (NFC) based authentication with smart contract driven consensus to securely verify and synchronize Electronic Medical Records (EMRs) across multiple healthcare facilities. **The system was tested** in a simulated network of three Virtual Private Servers, achieving an average NFC verification time of 2.9 seconds and a consensus propagation time of 0.4 seconds, demonstrating stable performance suitable for near-real-time operations.Although these **results** are promising, the evaluation was limited to synthetic datasets, small-scale network conditions,and basic database security configurations. **Future work** will focus on scaling the system to larger and more diverse networks, strengthening cybersecurity measures, and ensuring full compliance with HIPAA and GDPR standards. By supporting the United Nations'3rd Sustainable Development Goal on Health and the 9th Sustainable Development Goal on Infrastructure and Innovation, **this research contributes** to the development of secure, interoperable, and sustainable healthcare information systems.

DOI: https://doi.org/10.34306/att.v8i1.777

1. INTRODUCTION

According to [1], over 276 million healthcare records were breached in 2024, marking a major surge in data security incidents. This highlights the urgent need for tamper proof verification mechanisms such as blockchain. Blockchain, a breakthrough in network and information technology, functions as a cryptographically secured chain of interlinked data blocks resistant to unauthorized changes [2]. Each block contains the previous block hash, transactional data, and a timestamp, ensuring that any alteration modifies the hash value, thus maintaining an immutable audit trail [3].

The implementation of blockchain technology involves four main network types, Public, Private, Hybrid, and Federated/Consortium Blockchains [4]. Public blockchains allow open participation and unrestricted access, while private blockchains limit access to authorized entities only. Hybrid blockchains combine both approaches by making certain parts public and keeping sensitive data private. Federated or consortium blockchains resemble private ones but require approval from a governing authority for participant registration [4–6].

Smart contracts operationalize the verification protocols within blockchain architectures, functioning as "automatable and enforceable agreements" that activate once predefined conditions are met [7]. Their implementation varies across platforms such as Bitcoin, Ethereum, Private Ethereum, Corda, and Hyperledger, each exhibiting unique architectural and operational characteristics [8]. Validating smart contract algorithms before deployment is crucial to prevent vulnerabilities that could lead to failures or security breaches [9].

In recent years, blockchain adoption in healthcare has accelerated significantly [10], aligning with the evolution of electronic health (e-health) networks [11]. When designing secure blockchain-based healthcare systems, minimizing unauthorized patient data exposure becomes a primary concern [12–14]. Integrating blockchain with Radio Frequency ID/NFC sensors enables the creation of a secure and reliable document lifecycle system covering creation, digitalization, certification, verification, and monitoring [15].

These advancing technologies blockchain's immutability, smart contract automation, healthcare digitization, and NFC-based authentication together offer a strong foundation for improving EMRs verification [16]. In this study, the research propose a framework that uses blockchain to enable secure and tamper-resistant data exchanges, tailored specifically for healthcare systems. This investigation presents a comprehensive performance evaluation of the deployed framework, analyzing its efficacy, security parameters, and operational efficiency in real-world healthcare contexts. By addressing the critical intersection of data integrity, privacy preservation, and authentication security, this research contributes to the evolving discourse on blockchain-enabled healthcare information systems. This research could be in line with the United Nations 3rd SDGs (Health agenda) [17], and United Nations 9th SDGs (Infrastructure agenda) [18].

2. THE HEALTHCARE SYSTEM MODEL

The proposed framework introduces a secure and efficient system for managing EMRs using NFC integrated with blockchain verification. It features a multi-layered architecture combining hardware, networking, and security protocols, as shown in Figure 1. The system employs personal tokens stored on Mifare Classic 1K NFC cards, which act as portable and secure keys for accessing patient information. These cards interact with a robust hardware–software ecosystem to maintain data integrity, confidentiality, and availability across healthcare facilities. A consortium blockchain network enables multiple healthcare institutions to securely access and verify patient data while preserving privacy and accessibility [19, 20].

The hardware architecture includes key components selected for reliability, security, and interoperability. The Mifare Classic 1K NFC cards store patient data tokens, chosen for their suitable memory capacity and proven security standards. The PN532 module operates as the main interface for reading and writing NFC data, ensuring secure communication between the physical card and the system's processing units. Together, these elements support a cohesive framework that enhances trust, transparency, and efficiency in EMRs management.

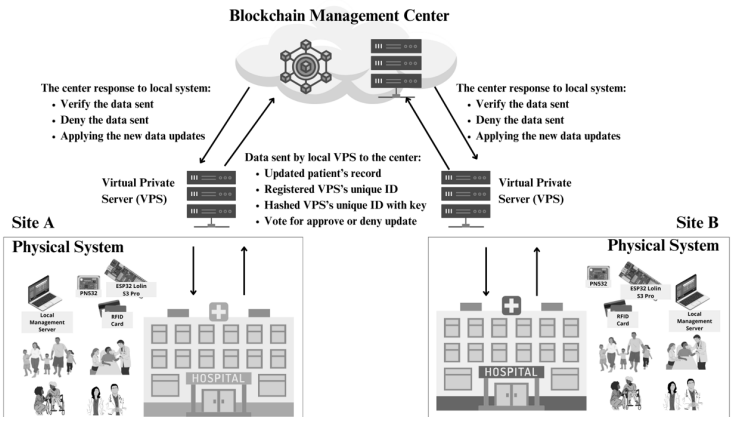

Figure 1. The Healthcare System Model

The ESP32 Lolin Pro S3 microcontroller acts as the local processing unit at each access point, performing essential functions such as powering the NFC system, receiving data from the PN532 module, generating cryptographic hashes, transmitting verified information to VPSs or backup systems, and receiving re-

sponses. It was chosen for its strong processing capabilities, built-in wireless connectivity, affordability, and energy efficiency, making it ideal for healthcare environments. The framework's networking architecture operates across multiple layers to ensure reliable data transmission and resilience, utilizing Local Area Networks (LAN) for internal communication, internet connections for inter-facility data exchange, and VPSs for centralized data management. This multi-tiered setup enhances redundancy and maintains secure communication channels, ensuring continuous system operation.

Blockchain technology serves as the core of the system's security infrastructure, addressing confidentiality, integrity, and availability [21, 22]. Its distributed ledger ensures that patient data remains tamper-resistant and verifiable across consortium nodes, with each transaction generating a unique cryptographic signature to create an immutable audit trail. Smart contracts automatically verify data integrity by comparing cryptographic hashes from the access point with those on the blockchain, reducing human error and processing time. These contracts also support the network's consensus mechanism, ensuring consistent records across all nodes. For structured data management, the system integrates MySQL databases that work alongside the blockchain layer, where blockchain functions primarily as a verification and integrity assurance mechanism rather than the main storage medium. The overall operational workflow proceeds systematically from patient identification to data verification and network-wide synchronization [23].

The system begins by reading a patient's NFC medical card using the PN532 module connected to the ESP32 microcontroller. The microcontroller extracts patient data and generates a cryptographic hash, serving as a unique digital fingerprint to ensure data integrity [24]. This data and its hash are verified against local records to confirm authenticity. Once validated locally, the verified data is transmitted to the blockchain management center, where smart contracts automatically compare the transmitted hash with blockchain-stored values [25]. If verification is successful, updates are executed through the consensus mechanism and propagated to all VPSs within the consortium network to maintain synchronized and accurate records [26].

As shown in Figure 1, Site A and Site B represent separate healthcare facilities within the consortium, each equipped with a local PC management server and hardware components (PN532 module and ESP32 microcontroller) for NFC data processing. These systems handle two main data types: patient information and its cryptographic hash. The VPSs perform verification of data hashes sent by local systems, ensuring cross-site integrity. In case of primary VPS unavailability, operations automatically shift to backup VPS or localhost servers. These contingency systems replicate the main VPS's verification functions, allowing continuous operation and data integrity even during network interruptions [27].

2.1. The NFC Verification System

The NFC verification system employs a secure, multi-layered authentication protocol for patient identification in healthcare environments. As depicted in Figure 2, the operational workflow begins with an initialization phase, during which all hardware components are powered on and communication protocols are established. This stage ensures that each system module is properly configured, synchronized, and ready for secure data processing. The preparation phase forms the foundation for subsequent authentication operations by guaranteeing stable connectivity and reliable system readiness.

In the next phase, two key hardware components are simultaneously activated: the ESP32S3 microcontroller and the PN532 NFC reader module. The ESP32S3 serves as the main computational unit, initializing its communication interfaces to process authentication data. At the same time, the PN532 module activates its Radio Frequency (RF) field and enters standby mode to detect NFC cards. This synchronized activation enables the system to read and process encrypted patient information efficiently. The dual-component coordination ensures minimal latency and high reliability during data exchange, laying the groundwork for secure patient verification [28, 29].

Once fully operational, the system proceeds to the data acquisition phase. Patients present their NFC cards containing cryptographically hashed identification tokens to the PN532 reader. Upon detection, the PN532 captures the hashed data and transfers it to the ESP32S3 for cryptographic processing. The microcontroller then applies a salt value to the received hash, producing a salted hash while preserving the original. This dual-hash mechanism enhances verification security by reducing susceptibility to dictionary and brute-force attacks, thereby reinforcing the confidentiality and integrity of patient authentication data.

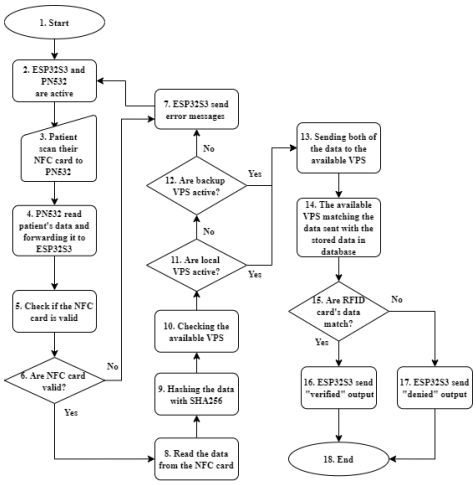

Figure 2. The NFC Data Verification System Workflow

As illustrated in Figure 2, the verification process advances as the ESP32S3 transmits both the original and salted hash values to a local VPSs, which functions as the primary authentication authority. The VPS securely stores registered patient identifiers and performs a two-step verification process:

- Matching the original hash with stored records.
- Validating the salted hash through recalculation and comparison.

This dual verification approach minimizes unauthorized access risks. If the primary VPS is inaccessible due to network or system issues, the ESP32S3 automatically switches to a backup VPS with synchronized authentication databases, ensuring continuous operation without manual intervention [30, 31].

When both the primary and backup VPS are unavailable, the ESP32S3 triggers an error-handling protocol, generating a specific alert that notifies administrative personnel for troubleshooting. Upon successful verification when both hash values are confirmed by either VPS the server transmits a digitally signed "verified" response to the ESP32S3. This confirmation finalizes the authentication process and grants the patient access to relevant healthcare information or services, maintaining both system security and operational reliability.

2.2. The Blockchain VPSs Verification and Smart Contract System

The operational framework of this VPS blockchain smart contract system implements a robust verification mechanism through a distributed consensus protocol to maintain database integrity across the consortium network. The process works as follows:

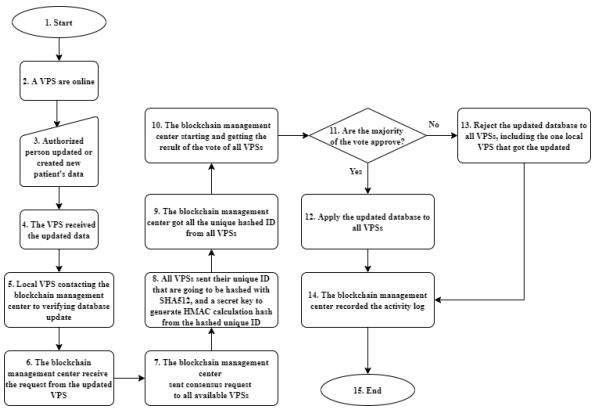

Figure 3. The Verification System Workflow

As illustrated in Figure 3, when an authorized entity performs a modification to the local VPS database, the system automatically initiates a verification sequence [32, 33]. The local VPS communicates with the

blockchain management center to authenticate and validate the proposed database changes. This verification request includes the cryptographic signatures of the modification and the requester's credentials [34]. Upon receiving the request, the blockchain management center launches a consensus protocol by broadcasting participation invitations to all VPS nodes registered within the consortium network. This decentralized process ensures that every database modification is reviewed collectively rather than controlled by a single authority. Each participating VPS transmits its unique identifier, which undergoes cryptographic hashing with a salt value to conceal identity while maintaining verifiability [35]. This cryptographic mechanism prevents identity spoofing and ensures that only legitimate consortium members participate in the verification process [36].

The approval mechanism for database updates operates under a dual-layered verification protocol. First, the system verifies that the hashed and salted VPS identifier corresponds to a valid consortium member [37]. Second, the proposed modification must secure majority approval from participating VPSs in the consensus process. If the majority rejects the update, the system denies it and all VPSs including the initiator retain the original database content [38, 39]. Conversely, if approved, the updated data is propagated synchronously to all connected VPSs, ensuring consistency and integrity across the distributed network. This blockchain-based verification framework, as demonstrated in Figure 3, offers robust protection against unauthorized modifications while reinforcing transparency, reliability, and tamper-resistant data management [40, 41].

2.3. Integrated System Architecture and Data Interaction Flow

To address both architectural clarity and component interactions, Figure 4 provides an integrated schematic. Unlike earlier figures that separated hardware verification and blockchain consensus, this updated diagram consolidates the system architecture with labeled data flows, showing the complete cycle from NFC card authentication to blockchain consensus and verification.

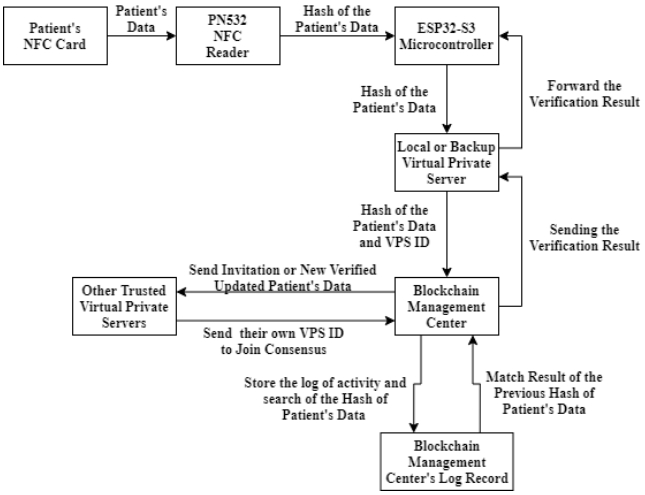

Figure 4. The Integrated System Architecture and Data Interaction Flow

2.4. Literature Review

This section reviews relevant research across three main areas: blockchain applications in healthcare, security concerns in Internet of Things (IoT) implementations, and the role of smart contracts in compliance enforcement. Together, these studies provide the foundation for identifying current limitations and motivating our proposed contribution [42].

2.5. Blockchain Applications in Healthcare

Blockchain has been extensively studied as a means to enhance security, privacy, and interoperability within healthcare systems, particularly in addressing IoT-related security challenges. For instance, [43] reviewed major IoT security issues, emphasizing authentication methods and demonstrating how blockchain can mitigate risks arising from device heterogeneity and resource limitations. Likewise, [12] proposed a blockchain-based framework integrated with the InterPlanetary File System (IPFS) to ensure secure health record sharing through decentralized storage and fine-grained access control [44]. Beyond storage management, [45] introduced the Decentralized Attribute-Based Access Control (DAAC) framework to standardize

access policies across e-health platforms. However, this framework lacks integration with real-time authentication technologies such as NFC, which are vital for lightweight and cost-efficient implementations in healthcare environments [46].

Complementary research by [11] proposed a health data propagation model combining steganography and encryption to enhance confidentiality during transmission. Although this approach strengthens data security, it fails to address traceability and auditability across healthcare institutions, limiting its usefulness in multi-provider ecosystems. Collectively, these studies highlight the potential of blockchain in healthcare while revealing a persistent gap most existing solutions focus primarily on secure storage or encryption, neglecting the integration of consortium blockchain, smart contracts, and NFC-based authentication. Such integration is crucial for achieving comprehensive verification, access control, and traceability across institutions in a scalable and practical healthcare infrastructure.

2.6. Security Concerns of IoT Implementation

The integration of IoT devices into healthcare has enabled real-time monitoring, data collection, and automated decision-making, but it also introduces significant security challenges. Research efforts have attempted to address these issues through blockchain-enabled frameworks. For instance, [43] emphasized the role of blockchain in mitigating device heterogeneity and resource limitations, while [12] investigated decentralized record management through blockchain–IPFS integration. Building on this, [45] proposed distributed ledger frameworks designed to improve data integrity and trust across multiple stakeholders.

Despite these advances, most IoT–blockchain solutions remain focused on generalized notions of security rather than practical, low-cost authentication mechanisms. Few studies have considered the use of lightweight hardware, such as ESP32-S3 microcontrollers or PN532 NFC modules, which could support real-time patient authentication while remaining feasible for healthcare institutions with limited resources. This lack of hardware–blockchain integration highlights another critical gap in the literature [47, 48].

2.7. Smart Contracts and Compliance Enforcement

Smart contracts have also gained traction as a mechanism for strengthening governance in healthcare data management. They allow policies to be enforced automatically, ensuring compliance with access rules and regulatory requirements [7]. While their potential is well recognized, most prior implementations rely on Ethereum-based contracts, which may not be suitable for private or consortium networks that must adhere to strict regulations such as HIPAA. In contrast, our study adopts a consortium blockchain model and designs smart contracts to coordinate multi-node, voting-based consensus for synchronizing medical databases. This approach provides a balance between privacy, control, and scalability, while ensuring compliance with regulatory standards [49–51].

2.8. Identified Gaps and Our Contribution

From the literature, several shortcomings can be observed. Many solutions still rely on centralized trust models, which contradict the decentralized philosophy of blockchain. Interoperability across healthcare providers remains limited due to the absence of multi-institutional consensus mechanisms [52]. Moreover, few systems integrate cost-effective hardware-based authentication, and real-world performance evaluation particularly regarding latency and resilience under failure conditions has been largely overlooked.

To address these limitations, this work introduces a proof-of-concept framework that leverages ESP32-S3 microcontrollers, PN532 NFC modules, and MIFARE Classic cards to demonstrate practical, low-cost authentication. The framework employs smart contract driven consensus across distributed VPSs nodes to achieve multi-node database verification. Furthermore, it provides comprehensive performance evaluation, including latency benchmarks and failover recovery tests, while maintaining alignment with GDPR and HIPAA standards to ensure regulatory compliance and real-world applicability [53].

3. RESULTS AND DISCUSSION

This section presents a comprehensive evaluation of the proposed consortium blockchain prototype for secure EMRs verification in healthcare environments. The discussion begins with the latency performance of NFC-based authentication, followed by reflections on its practical implications within clinical workflows.

3.1. Latency Performance of NFC-Based Patient Verification

A critical aspect of the prototype is the latency of patient verification using NFC cards in combination with local NFC readers. As illustrated in Figure 5, the scatter plot captures the temporal performance across approximately 120 sequential verification attempts. The x-axis represents the number of trials, while the y-axis indicates processing time in milliseconds. The observed verification times ranged between 2,217 and 4,696 milliseconds, with the majority clustering consistently within the 2,500-3,500 millisecond interval. This concentration suggests a stable operational baseline for the NFC devices employed. Across more than 100 trials, the average latency was measured at 2,879 milliseconds, with a standard deviation of 441 milliseconds, indicating relatively low variability in performance.

From an operational standpoint, these results are significant. A verification latency of approximately 2.8 seconds may not achieve real-time immediacy but remains well within acceptable thresholds for most clinical applications, particularly in outpatient and administrative contexts. Importantly, the consistency of the results demonstrates that the NFC-based mechanism is both reliable and predictable, reducing the likelihood of authentication bottlenecks in practice. The absence of extreme outliers further underscores the robustness of the system, strengthening its potential for integration in multi-institutional healthcare environments where both reliability and predictability are essential.

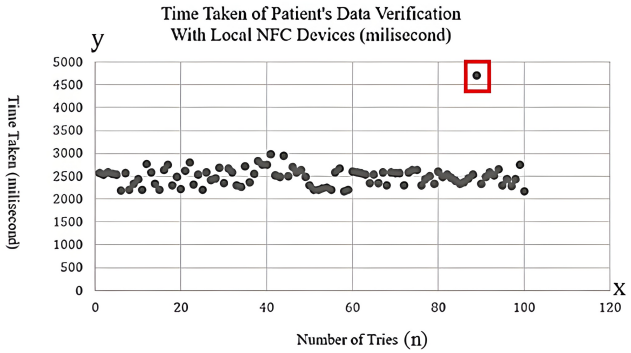

Figure 5. The Latency Result of Patient's Data Verification from NFC Card With Local NFC Device

The scatter plot in Figure 5 illustrates the temporal performance characteristics of NFC technology when applied to patient data verification in healthcare settings. Across approximately 120 sequential attempts, verification times consistently ranged between 2,217 ms and 4,696 ms, with the majority clustering between 2,500–3,500 ms. This distribution indicates a stable operational baseline for the NFC devices under evaluation. Over 100 trials, the mean latency was recorded at 2,879 ms with a standard deviation of 441 ms, reflecting dependable system performance. A single notable outlier occurred at the 89th attempt, where the processing time reached 4,696 ms almost twice the average duration. This anomaly is likely attributable to transient interference, temporary queue congestion, or momentary hardware fluctuations. Despite this deviation, the overall latency profile demonstrates consistent and reliable performance, underscoring the suitability of NFC-based verification for clinical integration where predictable response times are essential.

3.2. The Latency Result of VPSs Smart Contract

The scatter plot in Figure 6 illustrates the performance of smart contract execution and consensus establishment across multiple VPSs. The x-axis represents the sequential implementation attempts, while the y-axis records the corresponding execution times in milliseconds. As observed, the majority of consensus executions were completed within a window of 200–500 ms, indicating predictable performance. The system achieved an average propagation delay of 388 ms with a standard deviation of 104 ms, reflecting a stable operational profile. The fastest consensus round was recorded at 201 ms, while the slowest extended to 1,443 ms. Although sporadic spikes such as the maximum latency were detected, these remained relatively rare and did not significantly disrupt overall performance.

The consistency across trials confirms that the smart contract driven consensus mechanism can deliver efficient and dependable synchronization of medical records across distributed VPS nodes. From a practical perspective, maintaining consensus finalization in sub-second intervals positions the system as viable for near

real-time healthcare operations. Compared to public blockchains where confirmation times can span several seconds to minutes this consortium-based approach offers a significant improvement in both responsiveness and suitability for clinical environments, where data timeliness and security must be tightly coupled.

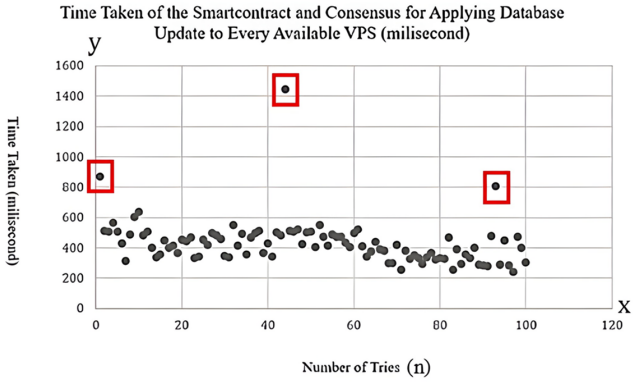

Figure 6. The Latency Result of the Smart Contract and Consensus Model

As shown in Figure 6, the majority of consensus executions completed within 200–500 ms, with an average propagation time of 388 ms and a standard deviation of 104 ms. The minimum observed execution time was 201 ms, while the maximum reached 1,443 ms. A few isolated outliers most notably at attempts 1, 44, and 93 extended beyond the typical range, likely caused by transient congestion, resource contention, or additional validation rounds. Despite these rare spikes, the overall distribution demonstrates that the smart contract consensus mechanism operates with consistent efficiency, maintaining predictable variation and ensuring stability under normal operating conditions.

3.3. Prototype Implementation and Proof-of-Concept

This section illustrates the practical deployment of our consortium blockchain framework by recreating a realistic hospital scenario through a proof-of-concept prototype. Instead of remaining at the level of theoretical design, the system was physically built and tested using low-cost yet reliable hardware to reflect conditions that could feasibly occur in healthcare environments. At each site, patient authentication was carried out using an ESP32-S3 microcontroller paired with a PN532 NFC reader and MIFARE Classic 1K card. Once a patient's NFC card was scanned, the device immediately computed a cryptographic hash of the data and securely transmitted it to a designated VPSs for verification. To mimic the complexity of real-world collaboration between hospitals, two independent facilities were simulated Site A and Site B each equipped with the same hardware configuration. These setups enabled data to be read, encrypted, and transmitted securely in a manner that closely resembles routine patient verification workflows as illustrated in Figure 7.

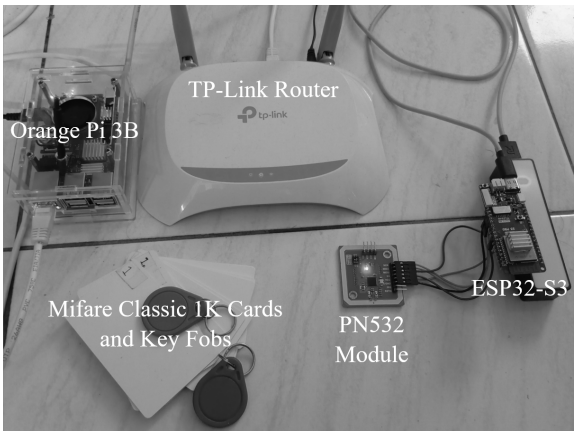

Figure 7. A Orange Pi 3B, a TP-Link router and ESP32S3, PN532, and Some Mifare Classic 1K

Local blockchain nodes were established using Orange Pi 3B boards connected through TP-Link routers, allowing each site to operate as a lightweight server while participating in the distributed ledger. At the same time, a centralized blockchain management center coordinated multi-node consensus, ensuring that data integrity and synchronization were consistently maintained across the simulated healthcare network.

Through this practical configuration, the prototype demonstrates how blockchain can be seamlessly integrated with NFC-based patient verification in settings that mirror real-world clinical workflows, balancing technical robustness with operational feasibility.

3.4. Software That Prototype Use

This section describes the software stack employed in the prototype, beginning with the operating systems, Ubuntu OS on the Orange Pi 3B and Windows 10 OS on the Blockchain Management Center. These platforms provided the foundational environment for running the blockchain and smart contract system. On the hardware side, the ESP32S3 microcontroller was programmed using the Arduino IDE, a widely adopted development environment that enables developers to write and upload code to microcontrollers. In this implementation, the Arduino IDE allowed the ESP32S3 to read and write data from NFC cards and transmit it securely to the local VPSs.

To manage the blockchain services, the servers were configured with Docker containers connected through a Macvlan network. This container-based approach provided a lightweight yet robust alternative to traditional virtual machines, enabling each service to run in an isolated environment while maintaining efficient resource usage. Such modularity proved particularly advantageous for replicating healthcare scenarios that demand scalability and reliability.

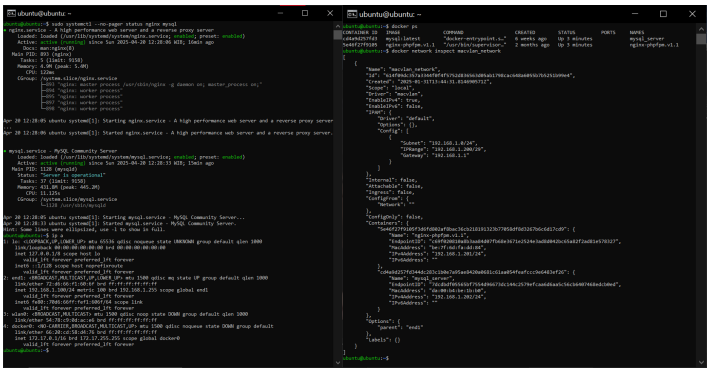

Figure 8. Orange Pi 3B Server Services and Docker Containers Running

As shown in Figure 8, the Orange Pi 3B servers hosted multiple Docker containers, each responsible for distinct blockchain-related services such as node synchronization, smart contract execution, and consensus management. The containers operated within a Macvlan network configuration, enabling them to communicate directly with other devices on the same physical network while preserving isolation between services. This configuration ensured low latency and high throughput two essential factors for real-time healthcare data verification. Additionally, by using Docker's lightweight virtualization approach, system updates and service scaling could be performed seamlessly without disrupting ongoing blockchain operations.

Furthermore, this setup demonstrated the feasibility of deploying a decentralized healthcare infrastructure using affordable, readily available hardware components. The modular design allowed individual services such as blockchain nodes, database servers, and verification modules to be scaled independently based on workload demand. This flexibility provides a strong foundation for future integration of additional healthcare facilities into the consortium network while maintaining system security, efficiency, and interoperability across distributed environments.

3.5. Hardware Selection Justification

The hardware selection for the prototype was driven by considerations of cost-effectiveness, availability, compatibility with blockchain and cryptographic operations, and real-world deployability in healthcare environments. The Orange Pi 3B was employed as the VPSs due to its affordability, market availability, and seamless compatibility with Ubuntu OS. Its ARM architecture provides an efficient platform for lightweight

blockchain protocols without excessive power consumption, making it well-suited for scalable deployments. A TP-Link router was used to ensure stable local networking between blockchain nodes and access points, leveraging its reliability and widespread availability.

The ESP32S3 microcontroller was selected for its processing capability to compute cryptographic hashes and its integrated wireless connectivity, which enables efficient NFC authentication without additional infrastructure. The PN532 NFC reader was chosen for its compatibility with existing hospital systems and its ability to support both reading and writing of NFC tokens, such as the Mifare Classic 1K cards. These cards, while less advanced than modern cryptographic smart cards, provide a practical balance between usability, cost, and standardized communication protocols (ISO/IEC 14443 Type A). Collectively, these components form a hardware stack that is affordable, scalable, and practical, positioning the system as a viable solution for blockchain-based EMRs verification in healthcare settings.

3.6. Prototype Result

Figures 1, Figures 2, Figures 3, and Figures 4 illustrate the system architecture and workflow, while the scatter plots validate the prototype's performance in terms of verification time and smart contract execution speed. The prototype achieved the following outcomes:

1. Verified NFC hashed data in approximately 2.5 seconds.
2. Executed blockchain consensus in roughly 400 milliseconds.
3. Handled failover scenarios, such as unresponsive or unavailable VPSs, without data loss.

3.7. Statistical Analysis of Results

To evaluate the stability and reliability of the verification system, the research conducted 100 sequential tests for NFC-based patient data verification and an additional 100 tests for smart contract–based consensus across distributed VPSs. For NFC verification latency, as shown in Figure 5, the system achieved a mean latency of 2,879 ms with a standard deviation of 441 ms, ranging from a minimum of 2,217 ms to a maximum of 4,696 ms. A single outlier occurred at the 89th attempt, producing a temporary spike to 4,696 ms, which was likely attributable to transient interference or buffering delays. When this outlier was excluded, the adjusted mean latency decreased to 2,796 ms with a reduced standard deviation of 314 ms.

For smart contract execution and consensus latency, as indicated in Figure 6, the results indicated a mean execution time of 388 ms with a standard deviation of 104 ms, bounded between a minimum of 201 ms and a maximum of 1,443 ms. Three notable outliers were observed at the 1st (869 ms), 44th (1,443 ms), and 93rd (808 ms) attempts, which suggest occasional performance fluctuations under specific conditions.

To provide a concise comparative view, Table 1 summarizes the key performance metrics obtained from both NFC verification and smart contract consensus experiments. These findings confirm the framework's feasibility for real-world healthcare applications. It ensures secure and tamper-proof exchange of EMRs across facilities.

Table 1. Performance metrics of NFC verification and smart contract consensus tests

Scenario	Mean (ms)	SD (ms)	Min (ms)	Max (ms)	Notable Outliers
NFC Verification	2,879	441	2,217	4,696	1 (at 89th attempt: 4,696 ms)
Smart Contract Consensus	388	104	201	1,443	3 (at 1st, 44th, 93rd attempts)

The comparative analysis in Table 1 highlights that NFC verification exhibited higher latency and variability compared to smart contract consensus, with a mean latency of 2,879 ms versus 388 ms, respectively. This difference is primarily due to communication overhead, as NFC involves physical device interaction and potential signal interference, whereas smart contract processes operate in a digital environment optimized for computational efficiency. The lower standard deviation of smart contract latency (104 ms) indicates greater consistency and stability across distributed VPSs. Overall, these results confirm that while NFC-based verification ensures reliable on-site authentication, smart contract consensus provides faster and more scalable validation, and their integration enhances the overall reliability, security, and performance of the blockchain-enabled EMRs system.

3.8. Regulatory Compliance and Privacy Enforcement

Ensuring regulatory compliance is a core objective of the proposed framework. Given the strict privacy requirements of the Health Insurance Portability and Accountability (HIPAA) or the General Data Protection Regulation (GDPR), the framework integrates specific technical mechanisms to uphold patient confidentiality, access control, and auditability. The system enforces granular access control by linking each patient record to hashed unique identifiers stored on the blockchain. Access to patient data is only permitted when a valid NFC token is presented and verified by smart contracts. These smart contracts enforce predefined verification policies, ensuring that only authorized medical personnel, devices, or systems can retrieve or modify sensitive data. This aligns with HIPAA's minimum necessary standard and GDPR's principle of data minimization. Each data access or update event is cryptographically logged into an immutable blockchain ledger. This creates a complete, tamper-proof audit trail, that might satisfy GDPR's accountability requirements and HIPAA's audit control safeguards.

The system incorporates patient consent by design through NFC tokens. Each patient is given control over their data by presenting a physical NFC card, which acts as a gatekeeper for authentication. This model supports GDPR's requirement for explicit consent and aligns with the notion of patient-controlled data. While this framework currently operates within a simulated environment, future work will expand its compliance scope by integrating multi-factor authentication, real-time monitoring for policy violations, and policy-based access revocation, enabling full alignment with both HIPAA and GDPR in real-world healthcare deployments.

4. MANAGERIAL IMPLICATIONS

While this prototype might tackle healthcare cyber attacks such as cryptic attacks with partially decentralized databases and unauthorized EMRs changes by healthcare personnel, its deployment in real-world healthcare faces many challenges. These start with how the prototype needs to be adjusted to the existing healthcare database structure, which may differ across healthcare systems. Additionally, convincing healthcare staff to adopt this prototype and training them to use and maintain the system are crucial. For hospital administrators and IT managers, these change management considerations highlight the importance of staff readiness, compatibility with existing systems, and phased adoption strategies to ensure a smooth transition to blockchain-based EMR verification.

Although the prototype demonstrates low-latency performance and robustness in a controlled setting, some limitations remain. The experiments were conducted using synthetic healthcare datasets rather than real-world EMRs, and the system was evaluated on a small-scale consortium network with only three VPS nodes. Latency results might differ in larger healthcare networks with more nodes, higher transaction volumes, or under real-world network conditions. Future work will explore scalability testing, extended fault-tolerance under node failures, and security testing against advanced cyberattack vectors. Also, the prototype needs to meet compliance with nationwide regulations such as Health Insurance Portability and Accountability or General Data Protection Regulation to ensure compliance with patient privacy secrecy standards and patient data exchange regulations, such as access control, to ensure this prototype is appropriate for deployment in healthcare settings.

5. CONCLUSION

This study shows that the proposed consortium blockchain framework, which combines NFC based authentication with smart contract driven consensus, can provide secure and reliable verification of EMRs across multiple healthcare facilities. In testing with a simulated network of three VPSs, the system processed NFC verification in about 2.9 seconds and synchronized updates in roughly 0.4 seconds, demonstrating stable performance that could work well in real-time healthcare operations.

However, these results were based on synthetic data, a small-scale network, and basic database security, so performance may vary in larger and more complex healthcare environments with real patient records. Future work will focus on expanding the system to larger networks, improving fault tolerance, strengthening cybersecurity protections, and ensuring full compliance with HIPAA and GDPR standards.

By supporting the United Nations 3rd Sustainable Development Goal on health and the 9th goal on resilient infrastructure and innovation, this framework offers a practical and forward-looking approach to building secure and connected healthcare systems.

6. DECLARATIONS

6.1. About Authors

Irwan Sembiring (IS) https://orcid.org/0000-0002-6625-7533

Bintang Kristianto Aji (BK) -

Teguh Indra Bayu (TI) https://orcid.org/0009-0003-9754-2809

6.2. Author Contributions

Conceptualization: IS and TI; Methodology: IS; Software: BK; Validation: TI; Formal Analysis: IS; Investigation: BK; Resources: BK; Data Curation: IS; Writing Original Draft: IS; Writing Review and Editing: TI and BK; Visualization: BK; All authors, TI, BK and IS, have read and agreed to the published version of the manuscript.

6.3. Data Availability Statement

The data presented in this study are not publicly available.

6.4. Funding

The authors received support from Satya Wacana Christian University, Indonesia.

6.5. Declaration of Conflicting Interest

The authors declare that they have no conflicts of interest, known competing financial interests, or personal relationships that could have influenced the work reported in this paper.

REFERENCES

[1] A. Steve, "Healthcare data breach statistics," *The HIPAA Journal*, 2024, accessed: Apr. 26, 2025. [Online]. Available: https://www.hipaajournal.com/healthcare-data-breach-statistics/

[2] J. Leng, M. Zhou, J. L. Zhao, Y. Huang, and Y. Bian, "Blockchain security: A survey of techniques and research directions," *IEEE Transactions on Services Computing*, vol. 15, no. 4, pp. 2490–2510, 2022.

[3] G. J. Mendis, Y. Wu, J. Wei, M. Sabounchi, and R. Roche, "A blockchain-powered decentralized and secure computing paradigm," *IEEE Transactions on Emerging Topics in Computing*, vol. 9, no. 4, pp. 2201–2222, 2021.

[4] F. E. Alzhrani, K. A. Saeedi, and L. Zhao, "A taxonomy for characterizing blockchain systems," *IEEE Access*, vol. 10, pp. 110 568–110 589, 2022.

[5] G. Subramanian and A. S. Thampy, "Implementation of blockchain consortium to prioritize diabetes patients' healthcare in pandemic situations," *IEEE Access*, vol. 9, pp. 162 459–162 475, 2021.

[6] M. Murod, S. Anhar, D. Andayani, A. Fitriani, and G. Khanna, "Blockchain based intellectual property management enhancing security and transparency in digital entrepreneurship," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 7, no. 1, pp. 240–251, 2025.

[7] W. Zou *et al.*, "Smart contract development: Challenges and opportunities," *IEEE Transactions on Software Engineering*, vol. 47, no. 10, pp. 2084–2106, 2021.

[8] C. Yang, J. Chen, B. Zeng, and L. Liao, "Overview of blockchain privacy protection," in *Proceedings of the 2022 IEEE 8th International Conference on Big Data Security on Cloud, High Performance and Smart Computing, and Intelligent Data Security (BigDataSecurity/HPSC/IDS)*, 2022, pp. 212–217.

[9] J. Chen, X. Xia, D. Lo, J. Grundy, X. Luo, and T. Chen, "Defining smart contract defects on ethereum," *IEEE Transactions on Software Engineering*, vol. 48, no. 1, pp. 327–345, 2022.

[10] H. Saeed *et al.*, "Blockchain technology in healthcare: A systematic review," *PLoS One*, vol. 17, 2022.

[11] L. Zhang, W. Han, S. Chen, and K. K. R. Choo, "An efficient and secure health data propagation scheme using steganography-based approach for electronic health networks," *IEEE/ACM Transactions on Networking*, vol. 32, no. 2, pp. 1261–1272, 2024.

[12] L. Da Costa, B. Pinheiro, W. Cordeiro, R. Araujo, and A. Abelem, "Sec-health: A blockchain-based protocol for securing health records," *IEEE Access*, vol. 11, pp. 16 605–16 620, 2023.

[13] F. Zidan, D. Nugroho, and B. A. Putra, "Securing enterprises: harnessing blockchain technology against cybercrime threats," *International Journal of Cyber and IT Service Management*, vol. 3, no. 2, pp. 168–173, 2023.

[14] I. Handayani, D. Apriani, M. Mulyati, A. R. A. Zahra, and N. A. Yusuf, "Enhancing security and privacy of patient data in healthcare: A smartpls analysis of blockchain technology implementation," *IAIC Transactions on Sustainable Digital Innovation (ITSDI)*, vol. 5, no. 1, pp. 8–17, 2023.

[15] T. C. Y. Ng, D. Y. W. Liu, and A. C. Y. Leung, "Leveraging blockchain and rfid/nfc technology for secure and traceable logistics for documents with digital twin," in *Proceedings of the 2024 IEEE International Conference on Blockchain (Blockchain 2024)*, 2024, pp. 428–433.

[16] Q. Aini, H. D. Purnomo, I. Setyawan, D. Manongga, U. Rahardja, I. Sembiring, S. Maulana *et al.*, "The effect of perceived costs on blockchain adoption intention: an empirical study," in *2023 11th International Conference on Cyber and IT Service Management (CITSM)*. IEEE, 2023, pp. 1–6.

[17] U. Nations, "Ensure healthy lives and promote well-being for all at all ages," https://sdgs.un.org/goals/goal3#targets_and_indicators, 2025, accessed: Aug. 13, 2025.

[18] ——, "Build resilient infrastructure, promote inclusive and sustainable industrialization and foster innovation," https://sdgs.un.org/goals/goal9#targets_and_indicators, 2025, accessed: Aug. 13, 2025.

[19] A. Sutarman, J. Williams, D. Wilson, and F. B. Ismail, "A model-driven approach to developing scalable educational software for adaptive learning environments," *International Transactions on Education Technology (ITEE)*, vol. 3, no. 1, pp. 9–16, 2024.

[20] O. Bianchi and H. P. Putro, "Artificial intelligence in environmental monitoring: Predicting and managing climate change impacts," *International Transactions on Artificial Intelligence*, vol. 3, no. 1, pp. 85–96, 2024.

[21] Y. Qiao, Y. Xue, Y. Zhai, D. Zhang, B. Chen, A. V. Vasilakos, M. S. Hossain, and S. Mumtaz, "A secure and efficient sharing scheme for medical iot data based on consortium blockchain," *IEEE Internet of Things Journal*, 2025.

[22] A. K. Gupta, D. Raj, Y. K. Sharma, A. Sharma, M. K. Singh, and A. K. Agrawal, "Electronic healthcare data sharing application based on hyperledger consortium blockchain network," in *2025 International Conference on Networks and Cryptology (NETCRYPT)*. IEEE, 2025, pp. 1405–1410.

[23] F. E. Putra, M. Khasanah, and M. R. Anwar, "Optimizing stock accuracy with ai and blockchain for better inventory management," *ADI Journal on Recent Innovation*, vol. 6, no. 2, pp. 190–200, 2025.

[24] L. Meria, S. Fabian, T. Mariyanti *et al.*, "Digital transformation and blockchain technology: A viewpoint from emerging markets," *Blockchain Frontier Technology*, vol. 4, no. 1, pp. 50–57, 2024.

[25] R. A. Alzahrani and J. M. Easton, "A secure and scalable blockchain framework for data sharing and cost distribution in railway condition monitoring," *IEEE Access*, 2025.

[26] D. Apriani, V. T. Devana, A. P. Sagala, P. A. Sunarya, U. Rahardja, and E. P. Harahap, "Security using blockchain-based otp with the concept of iot publish/subscribe," in *AIP Conference Proceedings*, vol. 2808, no. 1. AIP Publishing, 2023.

[27] T. Karvinen, "Configuration management of distributed systems over unreliable and hostile networks," Ph.D. dissertation, University of Westminster, 2023.

[28] R. Widayanti, A. B. Mutiara, and A. Tarigan, "Data governance in blockchain-based systems for internship grade conversion," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 6, no. 3, pp. 509–521, 2024.

[29] Y. Kushwaha, N. Lal, and M. Manjul, "Securing electronic health records: A blockchain-enhanced attribute-based encryption approach," in *2024 International Conference on Communication, Control, and Intelligent Systems (CCIS)*. IEEE, 2024, pp. 1–6.

[30] P. Singh, S. Sagar, S. Singh, H. M. Alshahrani, M. Getahun, and B. O. Soufiene, "Blockchain-enabled verification of medical records using soul-bound tokens and cloud computing," *Scientific Reports*, vol. 14, no. 1, p. 24830, 2024.

[31] D. Cahyadi, A. Faturahman, H. Haryani, E. Dolan *et al.*, "Bcs: Blockchain smart curriculum system for verification student accreditation," *International Journal of Cyber and IT Service Management*, vol. 1, no. 1, pp. 65–83, 2021.

[32] S. A. Faaroek, A. S. Panjaitan, Z. Fauziah, and N. Septiani, "Design and build academic website with digital certificate storage using blockchain technology," *IAIC Transactions on Sustainable Digital Innovation (ITSDI)*, vol. 3, no. 2, pp. 175–184, 2022.

[33] M. Rakhmansyah, M. S. Hadi, S. R. P. Junaedi, F. A. Ramahdan, and S. N. W. Putra, "Integrating blockchain and ai in business operations to enhance transparency and efficiency within decentralized ecosystems," *ADI Journal on Recent Innovation*, vol. 6, no. 2, pp. 157–167, 2025.

[34] A. Alnuaimi, D. Hawashin, R. Jayaraman, K. Salah, and M. Omar, "Trustworthy healthcare professional credential verification using blockchain technology," *IEEE Access*, vol. 11, pp. 109 669–109 688, 2023.
[35] T. Hariguna, Y. Durachman, M. Yusup, and S. Millah, "Blockchain technology transformation in advancing future change," *Blockchain Frontier Technology*, vol. 1, no. 01, pp. 13–20, 2021.
[36] T. Hariguna, B. B. Madon, and U. Rahardja, "User'intention to adopt blockchain certificate authentication technology towards education," in *AIP Conference Proceedings*, vol. 2808, no. 1. AIP Publishing, 2023.
[37] G. Silva, G. Godwin, and O. Jayanagara, "The impact of ai on personalized learning and educational analytics," *International Transactions on Education Technology (ITEE)*, vol. 3, no. 1, pp. 36–46, 2024.
[38] D. Martinez, L. Magdalena, and A. N. Savitri, "Ai and blockchain integration: Enhancing security and transparency in financial transactions," *International Transactions on Artificial Intelligence*, vol. 3, no. 1, pp. 11–20, 2024.
[39] M. P. Thanigesan and P. Vinothiyalakshmi, "Advanced blockchain-enabled electronic document management system with integrated verification module: A review," *International Journal of Environmental Sciences*, pp. 735–752, 2025.
[40] A. S. M. Ali, S. Ali, K. Ziaullah, M.-I. Joo, and H.-C. Kim, "Iomt and blockchain synergy: A novel approach to health data validation and storage," *IEEE Access*, 2025.
[41] S. Rana, R. M. Nor, M. E. Hossain, and M. Amiruzzaman, "Enhancing entrepreneurial security in cryptocurrency wallets using cloud technology," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 7, no. 2, pp. 481–491, 2025.
[42] T. Nurhaeni, L. Nirmalasari, A. Faturahman, and S. Avionita, "Transformation framework design on digital copyright entities using blockchain technology," *Blockchain Frontier Technology*, vol. 1, no. 01, pp. 35–43, 2021.
[43] S. Biswas, K. Sharif, F. Li, I. Alam, and S. P. Mohanty, "Daac: Digital asset access control in a unified blockchain based e-health system," *IEEE Transactions on Big Data*, vol. 8, no. 5, pp. 1273–1287, 2022.
[44] P. A. Suraya, T. Ramadhan, N. Lutfiani, A. Khoirunisa, and U. Rahardja, "Blockchain, information and speculation calculations in indonesia: Recent work," in *2022 10th International Conference on Cyber and IT Service Management (CITSM)*. IEEE, 2022, pp. 1–8.
[45] S. Almarri and M. Frikha, "Authentication and access control mechanisms to secure iot environments: A comprehensive slr," 2024.
[46] S. Khan, M. Khan, M. A. Khan, M. A. Khan, L. Wang, and K. Wu, "A blockchain-enabled ai-driven secure searchable encryption framework for medical iot systems," *IEEE Journal of Biomedical and Health Informatics*, 2025.
[47] S. Kosasi, U. Rahardja, N. Lutfiani, E. P. Harahap, and S. N. Sari, "Blockchain technology-emerging research themes opportunities in higher education," in *2022 International Conference on Science and Technology (ICOSTECH)*. IEEE, 2022, pp. 1–8.
[48] N. Yaqub, J. Zhang, M. I. Khalid, W. Wang, M. Helfert, M. Ahmed, and J. Kim, "Blockchain enabled policy-based access control mechanism to restrict unauthorized access to electronic health records," *PeerJ Computer Science*, vol. 11, p. e2647, 2025.
[49] F. Ullah, J. He, N. Zhu, A. Wajahat, A. Nazir, S. Qureshi, M. S. Pathan, and S. Dev, "Blockchain-enabled ehr access auditing: Enhancing healthcare data security," *Heliyon*, vol. 10, no. 16, 2024.
[50] J. Siswanto, V. A. Goeltom, I. N. Hikam, E. A. Lisangan, and A. Fitriani, "Market trend analysis and data-based decision making in increasing business competitiveness," *Sundara Advanced Research on Artificial Intelligence*, vol. 1, no. 1, pp. 1–8, 2025.
[51] N. Dey and S. Ghosh, "Blockchain-enabled healthcare data security and management: Innovations and challenges in the indian context," in *International Conference on Information Systems Security*. Springer, 2024, pp. 413–421.
[52] F. H. Bappy, E. Cheon, and T. Islam, "Centralized trust in decentralized systems: Unveiling hidden contradictions in blockchain and cryptocurrency," in *Proceedings of the 2025 ACM Conference on Fairness, Accountability, and Transparency*, 2025, pp. 1960–1971.
[53] R. Vayyala, "Ensuring data quality and integrity in modern enterprises," in *Data Governance, DevSecOps, and Advancements in Modern Software*. IGI Global Scientific Publishing, 2025, pp. 17–46.