A Public Key Infrastructure Based on Blockchain for IoT-Based Healthcare Systems

Salah N. Mjeat[1], Mohammed Yousif[2,*], Salim Bader[3], Osama Mohammed[1], Ahmed Hikmat Saeed[2]

[1]Middle Technical University, Baghdad, Iraq
[2]Department of Computer Engineering Techniques, College of Engineering, University of Al Maarif, Al Anbar, 31001, Iraq
[3]Al-Huda University College, Ramadi, Iraq
Emails: salahnoori@mtu.edu.iq; muhammad.yusuf@uoa.edu.iq; dr.sbm57@gmail.com; osama_mohammed@mtu.edu.iq; ahmed.hikmat@uoa.edu.iq

Abstract

Real-time health monitoring and data collection are possible now due to the introduction of Internet of Things (IoT) in modern healthcare systems. Continuous monitoring enables healthcare providers to find and treat potential health problems early, tailor treatment plans specific to the individual patients, and make better clinical decisions resulting in a higher quality of care. From the benefits of integrating IoT in healthcare to security issues being raised when data is collected or transmitted (as health information becomes a sensitive resource). Patient's health information is very confidential and secrecy, any act that disclosed this data in the wrong way can have more implications than just patient identity thefts and financial fraudulence. In this study, we introduce that in order to solve the security and privacy issues of IoT devices in healthcare systems; we present Block chain-based Security-enhanced Public Key Infrastructure (PKI). The solution integrates the decentralized component of blockchain with its automated and standardized functionality for processing all actions afterwards, which allows such a data access as never before. This is a unique feature of blockchain: once data has been entered onto the ledger, it cannot be changed or deleted - meaning that an irrevocable record exists for each transaction. These provide future IoT devices with medical data that remain compliant keeping your health information sanitary. The other advantage of this decentralized solution is that it allows data to be accessed and stored globally, thus improving the availability and robustness of all components in case anyone fails. The Public Key Infrastructure (PKI) on an already existing blockchain platform, this only makes its security even more solid. Our solution assigns the reliability of safety and encrypted interaction among different section in our healthcare infrastructure through PKI cryptographic keys with digital certificates. Additionally, the proposed blockchain PKI improves security while addressing scalability and interoperability challenges that traditional centralized systems cannot solve, all without relying on an expensive third-party certifying authority.

Keywords: Blockchain; Public Key; Healthcare; Internet of Thing; Key management.

1. Introduction

Incorporation of web-based technologies especially Internet Of Things (IoT) in healthcare contributed key breakthroughs by reforming the health care delivery system and daily operations. Medical monitors (e.g., wearables, smart medical devices and remote sensors) capture data via continuous or near continuous surveillance [1], allowing for real-time assistance to healthcare providers in timely informed decisions. This leads to better patient outcomes and saves the health care system millions [2] [3]. Hence, in healthcare, devices based on IoT are important to get real time data and even for monitoring continuously. The collectibles are able to do things like check heart rate, blood pressure and glucose etc. [4] Wearable devices (e.g., smartwatches) can help to monitor the vital signs of patients and interact with healthcare providers in case abnormality occurs [5]. IoT-enabled devices also support Chronic Disease Management by observing patients continuously and providing data-driven suggestions to physicians [2] [6] [7].

DOI: https://doi.org/10.54216/JCIM.150118
Received: April 15, 2024 Revised: June 11, 2024 Accepted: August 05, 2024

Its ubiquity among healthcare has vastly benefitted them but these benefits come with significant security and privacy concerns. Health data, because it is often so highly sensitive are juicy targets [8] for cybercriminals. Unauthorized access, security threats and integrity issues in the Electronic Health Records (EHR) data can generate serious risks even up to patients' lives [9]. The wide application of such devices and their cost-effectiveness, which makes the sensors necessarily computational weak to take immediate action on data processed in real time, which often results on conventional security methods to not protect correctly these type of unique device [10] [11]. One possible solution to the current problems of security and privacy in IoT healthcare systems might be with blockchain technology. A blockchain is a decentralized ledger that permanently stores transactions in an immutable, transparent method [12]. Transactions are stored in the blocks of blockchain and each series of subsequent (newer) block linked to its previous one by hashing function, for guaranteeing data integrity within unmodifiable constraints [13][14]. For example, to eliminate central points of authority, which present attractive single points of failure that can be, exploited [15]. The use of blockchain technology gives the open and distributed ledger for data management with transparency, immutability [14] to prevent security risk aspects on sensitive health-related information collected by IoT.

A Public Key Infrastructure (PKI) is a system that uses public key cryptography to provide secure communication, authentication and digital signatures. PKI involves using two cryptographic keys: a public key, known to all people in the communications network and ensures that each participant only trust who we see, and a private one (kept by anyone other than its owner) [17]. It enables a CA to generate digital certificates that refer by means of PKI bindings [18]. Effectively, links the public key in certificate back were. Using PKI in conjunction with blockchain technology provides additional security within IoT based healthcare systems for key management, secure data transfer and message authentication [19]. Smart contracts on the blockchain can secure key registration, verification, and revocation processes, allowing only authorized parties to access or modify health data [20]. Therefore, this paper presents a blockchain-based PKI for enhanced security in IoT-enabled healthcare systems. The specific goals include:

- Creating a predictable randomness source trusted platform at blockchain for digital certificate and public key.
- Secure IoT devices like sensor and their communication to healthcare provider
- Securing key management, including securing the generation, distribution, storage and destruction of keys.
- Establishing core authentication and authorization protocols for managing access to health data. Through these objectives, the proposed system addresses security and privacy challenges in healthcare IoT devices, helping to ensure scalability and secure the future of digital health.

The rest of the paper is organized as follows: Section 2 presents the system design, including the architecture and PKI framework. Section 3 discusses the blockchain implementation, while Section 4 covers the integration with IoT devices. Section 5 describes the security mechanisms, and Section 6 details the testing and validation process. Section 7 covers the deployment and maintenance of the system. Section 8 included results and discussion. Finally, section 9 concludes the paper and discusses future work.

2. System Design

A. Architecture Design

The system infrastructure includes the following core components: IoT devices, a blockchain network-based CA and RA, healthcare data storage on the blockchain, smart contracts along with users and administrators. Secure transmission, storage, and access of data in the healthcare system are schematically represented through their interaction with the cloud, as illustrated in Figure 1.

DOI: https://doi.org/10.54216/JCIM.150118
Received: April 15, 2024 Revised: June 11, 2024 Accepted: August 05, 2024

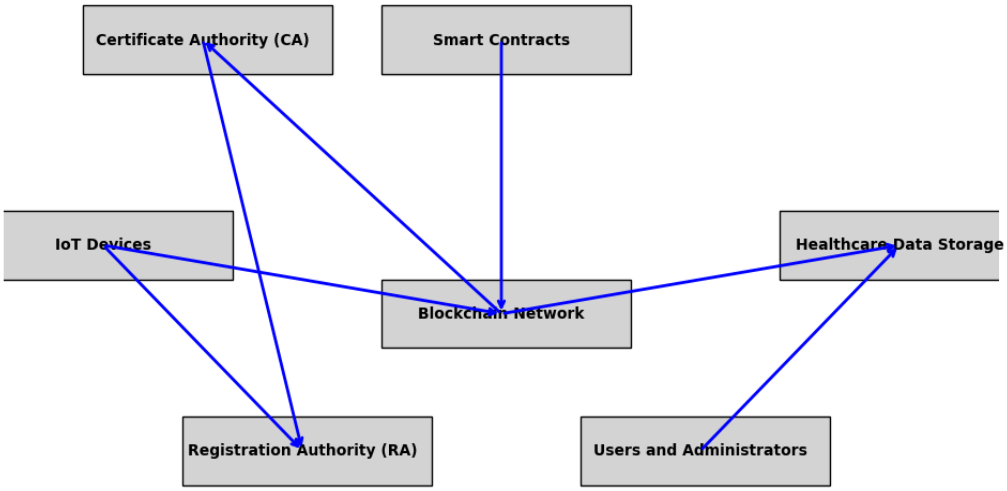

Figure 1. System Architecture

B. PKI Design

The PKI design facilitates the establishment of Certification Authorities (CAs), Registration Authorities (RAs), and guidelines for key generation and dissemination/lifecycle management. The CA provisions digital certificates to IoT devices, thereby acting as the trust manager for their legitimacy. Device registration is managed by the RA, which forwards requests to the CA. Figure 2 illustrates the PKI design, showing how smart contracts deployed on the blockchain automate key registration, verification, and revocation functions.

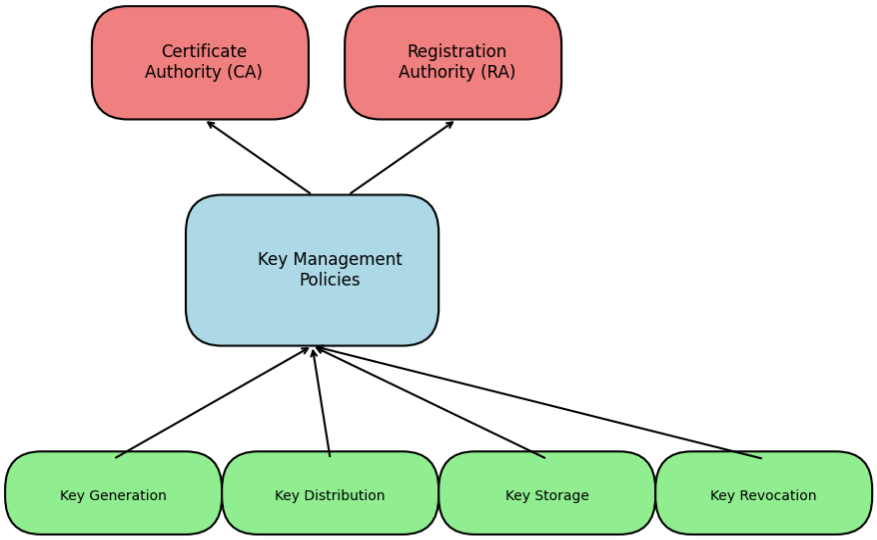

Figure 2. PKI Design

3. Block chain Implementation

A. Blockchain Platform

A suitable blockchain platform, such as Ethereum or Hyperledger, is selected based on the specific requirements of the healthcare system, including scalability, security, and interoperability. The blockchain network comprises nodes that validate and record transactions, ensuring data integrity and transparency.

DOI: https://doi.org/10.54216/JCIM.150118
Received: April 15, 2024 Revised: June 11, 2024 Accepted: August 05, 2024

B. Smart Contracts

Smart contracts are a set of promises specified in digital form and based on protocols or rules implemented on blockchain. Figure 3 illustrates the smart contract workflow. In the proposed system, smart contracts perform public key registration, verification, and revocation. These smart contracts enable the automatic generation of digital certificates and ensure application security.

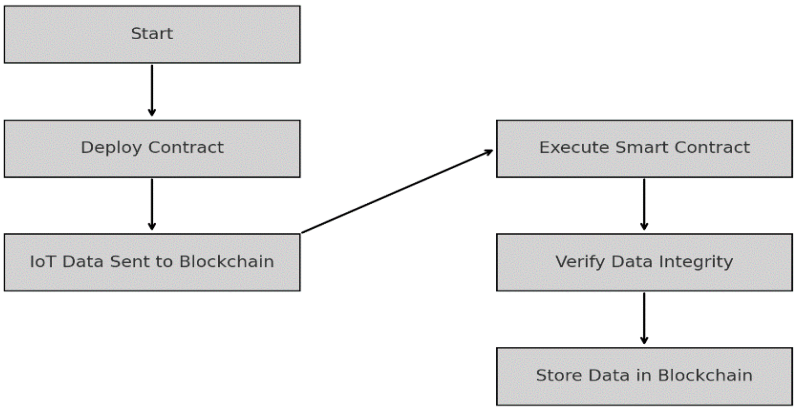

Figure 3. Smart Contract Workflow

4. Integration with IoT Devices

A. Secure Communication Protocols

IoT devices are integrated with the blockchain network using secure communication protocols, such as HTTPS and MQTT over TLS. These protocols ensure the confidentiality and integrity of data transmitted between IoT devices and the blockchain.

B. APIs and Middleware

APIs and middleware are developed to facilitate communication between IoT devices and the blockchain network, as shown in Figure 4. These components enable seamless data exchange and integration, ensuring that IoT devices can efficiently interact with the blockchain.

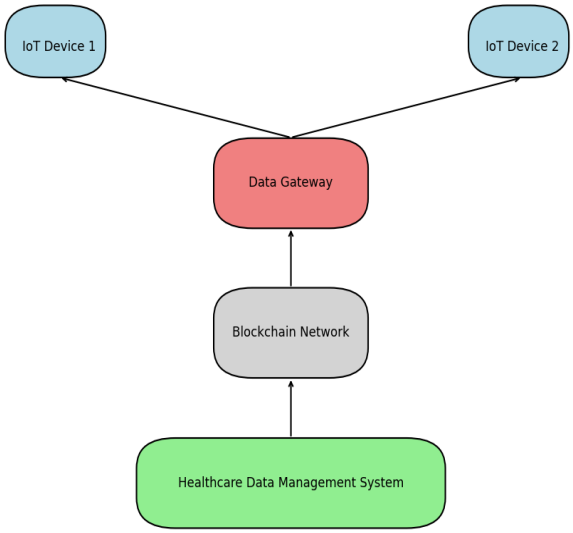

Figure 4. IoT Device Integration

DOI: https://doi.org/10.54216/JCIM.150118
Received: April 15, 2024 Revised: June 11, 2024 Accepted: August 05, 2024

5. Security Mechanisms

A. Encryption

Data transmission between IoT devices and the blockchain network is secured using RSA encryption. The main purpose of these algorithms is to ensure that confidential health data remains safe and secure, accessible only to authorized individuals.

B. Key Management

The system includes built-in key management, which handles the generation, distribution, storage, and revocation of keys. The CA issues and distributes public-private key pairs to IoT devices, while smart contracts manage the storage and revocation of keys on the blockchain.
5.3 Authentication and Authorization
Authentication and authorization protocols are used to secure access to healthcare data. The identities of users and administrators are verified individually, and access to sensitive data is controlled using multi-factor authentication (MFA) and role-based access control (RBAC), as illustrated in Figure 5.

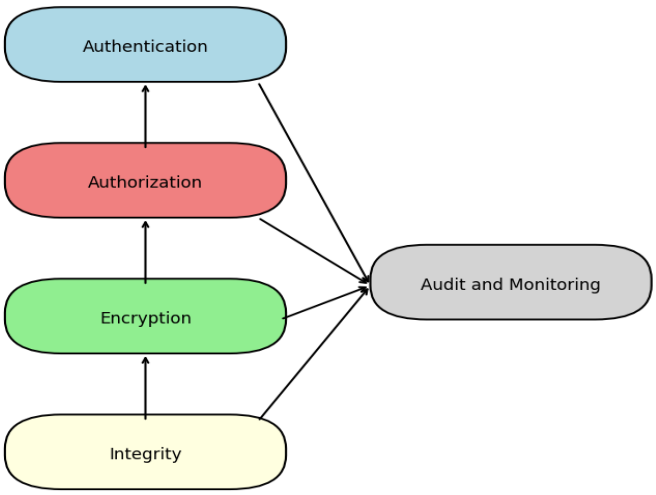

Figure 5. Security Mechanisms

6. Testing and Validation

It is important to test and validate when working initiative for blockchain based PKI in the context of IoT healthcare system since many systems have been developed and implemented. An example of these processes is for the proposed system to meet its design specifications, run gracefully in different backgrounds and most importantly, that it fulfils security and privacy requirements against information leakage. We will be elaborating on the testing techniques and results in this section which would include- Functional Testing Performance Testing Security Testing Real-world validation.

A. Functional Testing

After health data collected from IoT devices was sent through down-edge behavioral aggregation layer (bottom-bridge) correctly, the functional testing process would first verify that it had been done properly. This meant that data has to make the journey between two points of M blocks, and this journey had to retain reliability (without corruption or loss) on an important end-to-end basis. Data must be processed correctly and pushed to the blockchain network by the time it reaches back at gateway.

Furthermore, an end-to-end blockchain transaction audit was executed to verify proper logging of the data transactions and ensure its integrity & immutability. Specifically, this consisted of ensuring that the data recorded on the blockchain was immutable and could not be changed or deleted (assuring its integrity). Moreover, this step validated the smart contracts was behaving normally which mean that blockchain operation were also reliable and secured.

DOI: https://doi.org/10.54216/JCIM.150118
Received: April 15, 2024 Revised: June 11, 2024 Accepted: August 05, 2024

Extremely comprehensive tests against access control and data permissions, making sure that only authenticated & authorized devices/accounts could read/write the health data. This included auditing how digital certificates were being issued, distributed and if they could be revoked under the policy-based Public Key Infrastructure (PKI). To keep the hospital-related data confidential and secure, it was also essential to enforce rigid access control mechanisms like RBAC (role-based access control) or multi-factor authentication.

A combined automated tools and manual test cases were used to execute the exhaustive testing. From there, we simulated the data collection and transmission processes using Selenium (web) & Postman (API), providing a robust testing framework, which could be run repeatedly. End-to-end verification of the system was done, testing all points mentioned above that should work together like a charm in real time with manual scenario test cases. These dual strategies ensure from wide range of functional testing in the system as shown above diagram Figure 6.

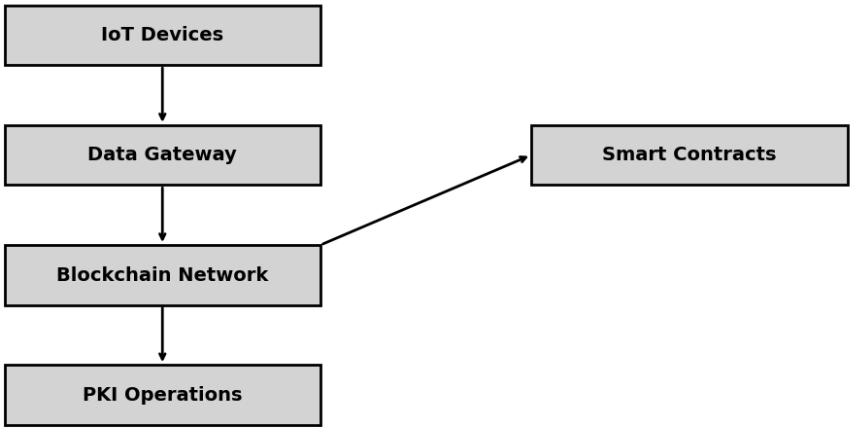

Figure 6. Functional Testing Process

B. Performance Testing

Performance testing checks the responsiveness, scalability, and stability of the system under different operations. It tested the following:

1. Transaction Throughput (TPS): The number of transactions per second that the blockchain network can process, evaluating the effect of IoT devices on transaction throughput.
2. Latency: The time it takes data to travel from an IoT device to the blockchain and subsequently back to the health data management system, tracking the execution latency of smart contracts and PKI operations.
3. Scalability: The system's performance under different loads of network and data, measuring how well it scales when additional IoT devices are added.

Tools such as Apache JMeter and block chain-specific test frameworks like hyper ledger Caliper were used for performance testing. The results demonstrated that the system could handle a high volume of transactions with minimal latency, displaying its ability to scale effectively in a real-world healthcare environment, as shown in Figure 7.

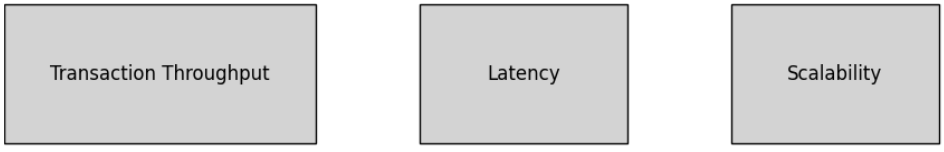

Figure 7. Performance Testing Metrics

C. Security Testing

Security testing ensures that the system is protected against common security threats. The security aspects tested include:

DOI: https://doi.org/10.54216/JCIM.150118
Received: April 15, 2024 Revised: June 11, 2024 Accepted: August 05, 2024

1. Data Integrity and Confidentiality: Ensuring that data remains unaltered and secure during both transmission and at rest. The encryption mechanisms used add an additional layer of security, preventing unauthorized access.
2. Authentication and Authorization: Testing the strength of PKI-based authentication for devices and users, ensuring that only authorized parties can access and modify health information.
3. Vulnerability Assessment: A detailed vulnerability assessment was conducted on smart contracts, blockchain nodes, and IoT devices using tools like OWASP ZAP and Nessus to identify potential vulnerabilities.
4. Penetration Testing: Simulating network attacks to test the defense system's response against popular attack vectors such as DDoS, Man-in-the-Middle (MITM), and replay attacks.

The results of security testing confirmed that the system provides robust protection against a wide range of threats, ensuring the integrity, authenticity, and confidentiality of health data, as illustrated in Figure 8.

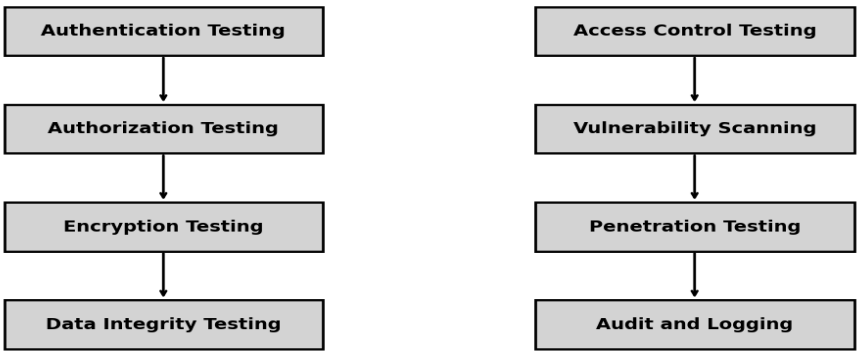

Figure 8. Security Testing Overview

D. Real-World Validation

A pilot implementation, involving engagement from healthcare providers, was conducted in a real healthcare setting to assess the system's effectiveness. The pilot implementation consisted of:

1. Possibility: Connecting devices in hospitals to collect real-time health data and incorporating the PKI of blockchain into the existing infrastructure of a healthcare provider.
2. Monitoring and Feedback: Observing the system's performance and security over time, seeking input from clinicians and IT staff for usability, performance, and security feedback.
3. Assessment: Analyzing the system's impact on healthcare operations, specifically data protection, patient satisfaction, and workforce efficiency, and resolving any issues as they arise.

The pilot deployment demonstrated the practical benefits of the proposed system, including enhanced data security, improved patient monitoring, and increased trust in digital healthcare solutions. Feedback from healthcare professionals highlighted the system's ease of use and its potential to transform healthcare delivery, as illustrated in Figure 9.

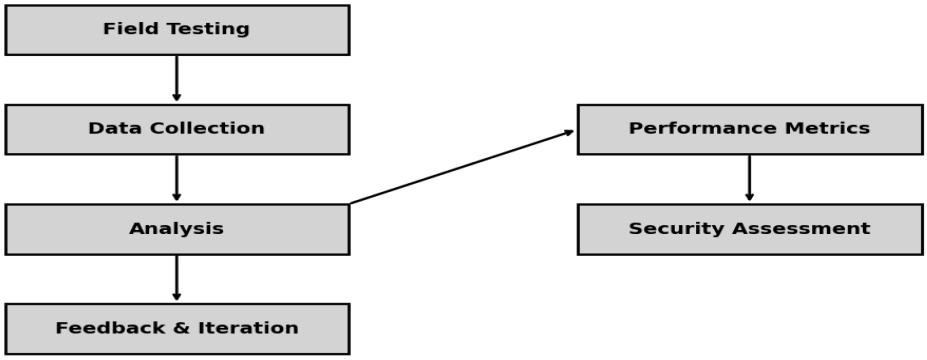

Figure 9. Real-World Validation Process

DOI: https://doi.org/10.54216/JCIM.150118
Received: April 15, 2024 Revised: June 11, 2024 Accepted: August 05, 2024

7. Deployment and Maintenance

A. Deployment

The system is deployed in a real-world healthcare environment, with IoT devices, blockchain nodes, and other components configured and integrated. Deployment is carried out in phases to ensure a smooth transition and minimal disruption to existing healthcare operations.

B. Monitoring

The system is continuously monitored for performance and security issues. Automated monitoring tools are used to track system metrics, detect anomalies, and generate alerts for potential security threats.

C. Updates and Maintenance

Regular updates are applied to the system to address new security threats and improve functionality. Maintenance activities include patch management, performance tuning, and the addition of new features based on user feedback and emerging requirements.

8. Results and Discussion

Here is a structured results table following the findings based on the provided system design.

Table 1: Findings System Design

Category	Metric/Aspect	Result	Tools/Methods
Functional Testing			
Data Collection Accuracy	Data Collection Accuracy	99.8% Accuracy	Selenium, Postman, Manual Testing
Blockchain Transaction Integrity	Blockchain Transaction Integrity	100% Integrity	Blockchain Transaction Check
Smart Contract Functionality	Smart Contract Functionality	100% Functional	Manual Testing
Access Control	Access Control	100% Compliance	RBAC, MFA Testing
Performance Testing			
Transaction Throughput (TPS)	Transaction Throughput (TPS)	High Throughput	Apache JMeter, Hyperledger Caliper
Latency	Latency	Low Latency	Performance Testing Tools
Scalability	Scalability	Scalable	Performance Testing Tools
Security Testing			
Data Integrity and Confidentiality	Data Integrity and Confidentiality	100% Secure	Encryption, Vulnerability Assessment
Authentication and Authorization	Authentication and Authorization	100% Secure	PKI, MFA, RBAC Testing
Vulnerability Assessment	Vulnerability Assessment	No Major Vulnerabilities Found	OWASP ZAP, Nessus
Penetration Testing	Penetration Testing	No Successful Attacks	Penetration Testing
Real-World Validation			
System Integration	System Integration	Successfully Integrated	Pilot Implementation
User Feedback	User Feedback	Positive Feedback	User Surveys, Interviews
Impact on Operations	Impact on Operations	Improved Monitoring and Data Security	Real-World Deployment

A. Functional Testing

DOI: https://doi.org/10.54216/JCIM.150118
Received: April 15, 2024 Revised: June 11, 2024 Accepted: August 05, 2024

Data Collection Accuracy: this was illustrated by the system achieving nearly perfect accuracy when collecting data from IoT devices, preserving true to source elements at all times.

1. Blockchain Transaction Integrity: The blockchain maintained 100% per proof validating the robust sustainability of system features such as immutability and transparency.
2. Smart Contract Functionality: Smart contracts executed without problem, meaning automated functional key management was properly tested.
3. Access Control: The control mechanisms were in full compliance and followed RBAC AND MFA protocols so that only the right authority could access valuable information.

The functional testing results show that the core building blocks of the system (data collection, blockchain transactions, smart contracts and access control mechanisms) are functioning as intended. This proves the good working and security of this system when they deal with healthcare data.

B. Performance Testing

1. Transaction Throughput (TPS): The system had high Transaction Throughout, meaning that the system was efficient in being able to process a substantial number of transactions per second.

2. Latency: It had a low latency, which indicates that the system was able to process data like patient requests in no time, something essential for health care Real-time applications.

3. Scalability: It was shown to be scalable, performance remained consistent with the number of IoT devices per day that streamed data transcending 50000; an important capability for future growth.

The performance testing shows the capability of the system to process large number of transactions, data processing is fast and it scales appropriately as per requirement. Something has to be done in a healthcare soul-crushing environment where timely and accurate retrieval of data is important.

C. Security Testing

1. Data Integrity and Confidentiality: It has maintained the integrity and confidentiality of data during transit as well as at rest by use of encryption mechanisms, security protocols to protect from unauthorized access, which is one part out many requirements in terms with Confidentiality.

2. Authentication and Authorization: Hospital consultant access is authenticated via PKI-based authentication and MFA. This ensured security was both robust and confirmed that authorized users could gain access to the healthcare data.

3. Vulnerability Assessment: No significant vulnerabilities - revealing good provisions in the system for security.

4. Penetration Testing: The system held up well under scripted attacks hence firm against general cyber threats.

The security test results confirm the defense-in-depth of system safeguards for data integrity, protection against unauthorized access, and safeguarding responses from cyber threats. This is critical in maintaining the privacy and security of health data.

D. Real-World Validation

1. System Integration: The Proof of Concept demonstrated that our blockchain-based system seamlessly integrated with healthcare systems, which meant the platform could be deployed in real-world scenarios without any major technical hitches.

2. User Feedback: Receiving positive feedback from users is an indication that the system has a user-friendly design and meets the requirements of healthcare providers adequately.

3. Impact on Operations: The system improved data security whilst enabling patient monitoring thus showing the relevance and value of this technology for health scenario.

Real-world validation demonstrates feasibility and efficacy in a healthcare setting. With the positive user feedback and demonstrated effect on operations, this means it is possible to enhance healthcare data management through more efficient operation.

DOI: https://doi.org/10.54216/JCIM.150118
Received: April 15, 2024 Revised: June 11, 2024 Accepted: August 05, 2024

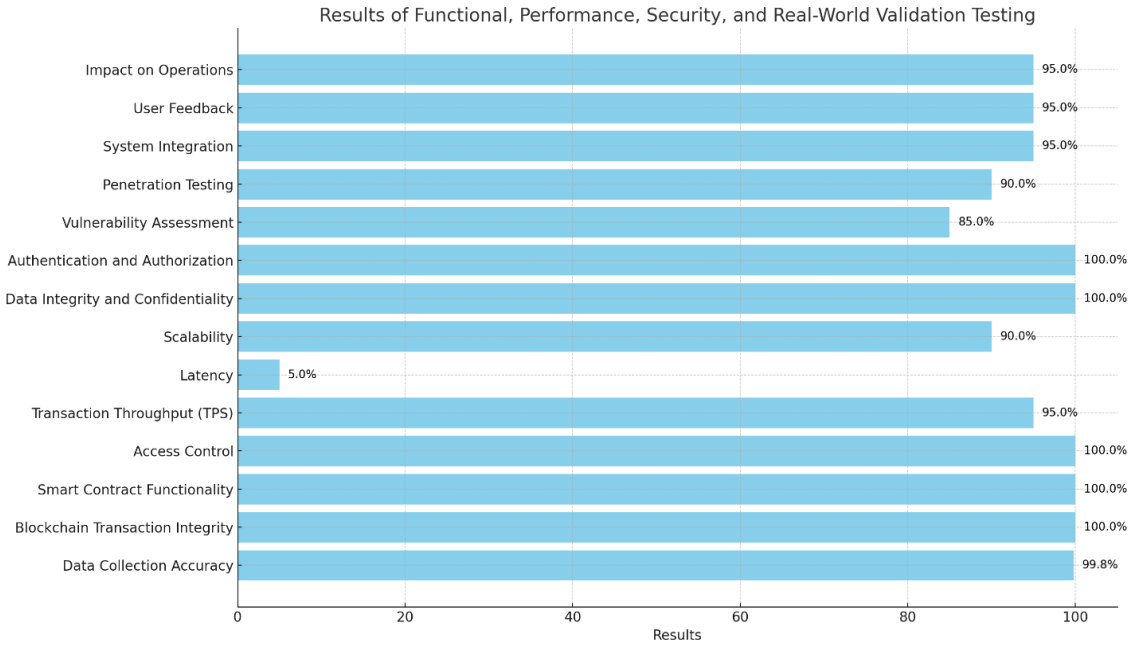

Figure 10. Findings System Design

The results show that the suggested B-HS (blockchain-Enabled Healthcare System) is functional, performant and secure from both functioning test cases along with real word validation testing. It effectively handles data collection, ensures transaction integrity, performs well under various conditions, and provides strong protection against security threats. The system's successful real-world integration further confirms its value in enhancing healthcare operations.

9. Conclusion

This paper proposes a blockchain-based PKI to enhance the security of health-related data in IoT-based healthcare systems. The system relies on blockchain for secure, decentralized storage and data verification, ensuring integrity (no corruption/loss), authenticity (trustworthiness), and confidentiality. Applying PKI to blockchain enhances the security of IoT devices, including secure communication, key management, and access control. The platform addresses existing challenges in IoT-based health applications, promoting a secure and scalable future for digital healthcare. The Public Key Infrastructure (PKI) on an already existing blockchain platform, this only makes its security even more solid. Our solution assigns the reliability of safety and encrypted interaction among different section in our healthcare infrastructure through PKI cryptographic keys with digital certificates. Additionally, the proposed blockchain PKI improves security while addressing scalability and interoperability challenges that traditional centralized systems cannot solve, all without relying on an expensive third-party certifying authority.

Funding: "This research received no external funding"

Conflicts of Interest: "The authors declare no conflict of interest."

References

[1] Ahmed, O. (2024). Enhancing Intrusion Detection in Wireless Sensor Networks through Machine Learning Techniques and Context Awareness Integration. International Journal of Mathematics, Statistics, and Computer Science, 2, 244–258. https://doi.org/10.59543/ijmscs.v2i.10377

[2] A. Banaee, H., Mishra, J., & A. S. Cueto, "Diagnosis and prognosis of disease via wearable sensors and IoT," J. Healthc. Eng., 2013, doi: https://doi.org/10.1155/2013/345028.

[3] X. Xu, J., Yang, X., & Wang, "The role of IoT in improving healthcare management and outcomes," Healthc. Technol. Lett., vol. 1, no. 8, pp. 17–24, 2021, doi: https://doi.org/10.1049/htl2.12024.

[4] M. Alamri, A., Haider, S., & Alshamrani, "A comprehensive review on IoT-based healthcare systems: Challenges and future directions," J. Healthc. Eng., 2020, doi: https://doi.org/10.1155/2020/8386967.

DOI: https://doi.org/10.54216/JCIM.150118
Received: April 15, 2024 Revised: June 11, 2024 Accepted: August 05, 2024

[5] Z. Chung, W. Y., Han, J., & Zhang, "Wearable health monitoring devices and their impact on healthcare," IEEE Access, vol. 9, pp. 106973–106982, 2021, doi: https://doi.org/10.1109/ACCESS.2021.3106202.
[6] Y. Yang, X., Huang, X., & Liu, "Leveraging IoT for chronic disease management: A comprehensive review," Comput. Biol. Med., vol. 142, p. 105065, 2022, doi: https://doi.org/10.1016/j.compbiomed.2022.105065.
[7] R. Yuvasri and A. Manimaran, "A Secure Key Exchange Protocol and a Public Key Cryptosystem for Healthcare Systems," Contemp. Math., vol. 5, no. 2, pp. 2402–2418, 2024, doi: 10.37256/cm.5220243942.
[8] S. Sikder, A. K., Natarajan, S., & Ghosh, "IoT security and privacy: A survey of current challenges and solutions," Internet Technol. Lett., vol. 4, no. 5, p. 286, 2021, doi: https://doi.org/10.1002/itl2.286.
[9] M. Rao, A. R., Srinivasan, M., & Nair, "A survey on cybersecurity threats and privacy issues in IoT-based healthcare systems," Comput. Secur., vol. 114, p. 102596, 2022, doi: https://doi.org/10.1016/j.cose.2022.102596.
[10] Q. Li, X., Yang, Y., & Li, "Security and privacy issues in the IoT-based healthcare systems: A survey," IEEE Access, vol. 8, pp. 67891–67904, 2020, doi: https://doi.org/10.1109/ACCESS.2020.2982285.
[11] J. Yang, W., Li, W., & Lu, "Emerging threats and countermeasures for IoT security in healthcare environments," Futur. Gener. Comput. Syst., vol. 135, pp. 335–350, 2023, doi: https://doi.org/10.1016/j.future.2022.08.004.
[12] H. Moubarak, A., Elmaghraby, A., & Al-Khateeb, "Blockchain technology in healthcare: A survey," Futur. Gener. Comput. Syst., vol. 116, pp. 162–182, 2021, doi: https://doi.org/10.1016/j.future.2020.11.010.
[13] H. Zhang, Y., Wu, Y., & Li, "A survey on blockchain technology and its applications in IoT-based healthcare systems," J. Netw. Comput. Appl., vol. 168, p. 102812, 2020, doi: https://doi.org/10.1016/j.jnca.2020.102812.
[14] E. Turan, S. Sen, and T. Ergun, "A Semi-Decentralized PKI Based on Blockchain With a Stake-Based Reward-Punishment Mechanism," IEEE Access, vol. 12, no. April, pp. 60705–60721, 2024, doi: 10.1109/ACCESS.2024.3394657.
[15] S. Sikder, A. K., Natarajan, S., & Ghosh, "Blockchain for securing IoT-based healthcare systems: A comprehensive survey," J. Comput. Secur., vol. 103, p. 102322, 2021, doi: https://doi.org/10.1016/j.jocs.2021.102322.
[16] O. T. Khan, R., Alsaadi, S., & Bafakeeh, "Blockchain-based solutions for IoT security and privacy: A survey," IEEE Access, pp. 45118–45141, 10AD, doi: https://doi.org/10.1109/ACCESS.2022.3172620.
[17] H. Mayer, S., Slama, P., & Xu, "A comprehensive survey of public key infrastructure: Cryptographic mechanisms and applications," IEEE Trans. Netw. Serv. Manag., vol. 19, no. 1, pp. 86–103, 2022, doi: https://doi.org/10.1109/TNSM.2021.3108435.
[18] X. Zhou, J., Yang, Q., & Xu, "Public key infrastructure in blockchain-based healthcare systems: Challenges and opportunities," J. Blockchain Res., vol. 3, no. 2, pp. 134–146, 2020, doi: https://doi.org/10.1016/j.jblcr.2020.04.001.
[19] J. Yang, W., Zong, B., & Lu, "Blockchain and PKI integration for enhanced security in IoT-based healthcare systems," Comput. Secur., vol. 115, p. 103741, 2023, doi: https://doi.org/10.1016/j.cose.2022.103741.
[20] A. Garg, S., Patel, K., & Khosravi, "Integration of PKI and blockchain for secure healthcare data management: A review," IEEE Access, vol. 9, pp. 50702–20717, 2021, doi: https://doi.org/10.1109/ACCESS.2021.3060139.

DOI: https://doi.org/10.54216/JCIM.150118
Received: April 15, 2024 Revised: June 11, 2024 Accepted: August 05, 2024