Journal of Harbin Engineering University
ISSN: 1006-7043

Vol 46 No. 4
April 2025

Blockchain Based Hybrid Encryption Techniques to Enhance Security in Healthcare Networks

Edna Elizabeth.N[1], Jayashree C G[2], Kavin R B[3], Deepan M[4]

[1, 2,3,4]Department of Electronics and communication Engineering, Sri Sivasubramaniya Nadar College of Engineering, Kalavakkam, Chennai, India

Email:[1]ednaelizabethn@ssn.edu.in,[2]jayashree2110644@ssn.edu.in, [3] kavin2110845@ssn.edu.in

Abstract

Conventional Public Key Infrastructure (PKI) systems, including Log-based PKI and Web-of-Trust PKI, are prone to single points of failure and hence are susceptible to security threats. To overcome these issues, this study suggests a Blockchain-based PKI system for secure data transmission in healthcare networks. The system combines hybrid encryption methods with a trust-based self-organizing network to improve security, minimize energy consumption, and enhance computational efficiency. Node clustering is done through trust calculations for effective certificate authority selection and delivery. Routing attacks are also simulated to test the resilience of the network. Comparison of trust-based clustering and self-observing networks shows increased energy efficiency and security in healthcare transactions based on blockchain. The system proposed ensures decentralized, transparent, and tamper-proof PKI operations, providing better security and resilience to medical data transactions.

Keywords:Blockchain, Healthcare, Trust-based Clustering, Self-Organizing Network, Security, Energy Efficiency

1. Introduction

Blockchain technology has proven to be a revolutionary solution for digital transaction security in many fields, including healthcare. The requirement of secure, scalable, and efficient authentication mechanisms for healthcare networks prompted the investigation into Blockchain-based Public Key Infrastructure (PKI). Log-based PKI and Web-of-Trust PKI models are traditional examples that suffer from single points of failure, making them susceptible to security attacks. In healthcare networks where data integrity, confidentiality, and availability are of utmost importance, these vulnerabilities can result in unauthorized access [1], data breaches, and compromised patient records. Blockchain provides a decentralized and tamper-proof ledger that can remove such vulnerabilities by dispersing trust across nodes, making data transactions secure and transparent. By combining Blockchain with hybrid encryption methods, healthcare networks can provide increased security while maximizing computational efficiency and energy use.

One of the most difficult issues to tackle in the deployment of a Blockchain-based PKI for healthcare is how to manage trustworthiness among nodes in the network. A trust-based clustering that has self-organization can much enhance network efficiency through clustering of nodes in accordance with their trust levels. Dynamically, trust is calculated based on energy consumption, past transaction reliability, and network activities. This method guarantees that, only [2] most reliable nodes are used as certificate authorities, reducing the threats of malicious. The trust-based node clustering process includes specifying nodes in the Blockchain, emulating a healthcare transaction network, establishing a trust threshold, and adjusting trust values according to each node's performance.

Through application of this method, the system minimizes the decision on the certificate authorities, thus lowering the threats of a compromised PKI. Hybrid encryption methods also complement the security offered by Blockchain-based healthcare networks with the benefits of both symmetric and asymmetric cryptography. Symmetric encryption is used for speedy encryption and decryption of data [3], whereas asymmetric encryption is applied to provide key exchange methods safely. Both have a symbiotic relationship in health settings where ample amounts of personal medical data have to be communicated

safely without diminishing performance. Blockchain-based PKI guarantees that patient information is safeguarded against unauthorized access, even when routing attacks or other network weaknesses are present.

Moreover, the use of multiple certificate authorities in the Blockchain eliminates the constraints of traditional PKI models based on a single trusted party. Routing attacks are serious security risks in Blockchain-based networks, especially in situations where healthcare data is sent via the internet. Adversaries can try to disturb the network by redirecting [4] data packets, causing delays in transaction confirmation, or damaging data integrity. In the system proposed herein, trust-based routing is used to thwart attacks. Validator nodes constantly revise trust values for every node from previous interactions so that the network can detect and quarantine possible threats. This preemptive strategy enhances the security of the Blockchain network against attacks and guarantees seamless healthcare data transactions.

A comparison between trust-based clustering and self-observing networks points out the energy efficiency of the proposed system. In traditional networks, computational power is consumed for data authentication and transaction execution, resulting [5] in higher power demand. Through cluster-based node division based on trust and dynamic changes in trust, the system is able to utilize energy efficiently and ensure high levels of security. The self-observing network also improves efficiency by allowing the nodes to change their trust rating independently, hence minimizing the validation processes from external sources. These optimizations render Blockchain-based PKI more appropriate for real-time healthcare applications where resource efficiency is paramount.

The combination of Blockchain-based PKI with hybrid encryption methods and trust-based clustering offers a strong solution for healthcare network security. The system proposed not only overcomes the weaknesses of conventional PKI models but also improves network efficiency, security, and energy management. Through reducing the dangers [6] of single points of failure and channeling attacks, the system provides a dependable and scalable framework for authentication in medical data transactions. This research contributes to advancing secure and efficient Blockchain deployments in healthcare, with future innovations possible in decentralized identity management and encrypted data exchange.

This work is organized with literature survey review which is arranged in Section II of this study. The functioning of the methodology is highlighted in Section III. Results and discussions are presented in Section IV. Finally, the key recommendations and conclusions are presented in Section V.

2. Literature Survey

Blockchain technology has been extensively researched for improving data security in healthcare systems. Its ability to offer a decentralized, tamper-proof ledger for storing and sharing medical records has been explored by researchers. Blockchain's immutability guarantees data integrity, and smart contracts enable automated access control. Different studies emphasize the benefits of implementing Blockchain to prevent data breaches, enhance interoperability, and create a trust framework between patients and healthcare providers. Nonetheless, scalability, transaction latency, and compliance issues continue to pose problems to mass adoption. Optimized consensus algorithms and data management are still key research challenges.

Application of Blockchain in electronic health records has drawn substantial interest because of its capacity to improve security and privacy. Different research investigate how Blockchain can enable a patient-oriented data management system where individuals manage access to their health history. Decentralized identity management guarantees that only the [7] patient can update patient information. Research suggests that storage constraints and processing overhead pose challenges to mass deployment. Development work to introduce Blockchain into cloud storage and off-chain data solutions continues to be implemented to cover such issues as ensuring data integrity and accessibility without losing it within healthcare settings.

The adoption of smart contracts for healthcare Blockchain networks has widely been explored as a means of automating insurance claims, billing, and accessing data. Smart contracts run coded rules, provide transparency, and cut down administrative costs. Studies point out that smart contracts reduce fraudulent [8] behaviour by mandating adherence to healthcare policies. Yet, security flaws in smart contract code are susceptible to exploits and

unintended effects. Research is focused on strong auditing and formal verification methods to avoid errors. Moreover, compliance with healthcare regulation is still a challenge to achieve and is in need of further research into privacy-preserving smart contract frameworks.

Blockchain-based solutions have been suggested to improve drug supply chain management through increased transparency and traceability. Studies analyze how Blockchain facilitates secure tracking of pharmaceutical products from producers [9] to consumers, mitigating the threat of counterfeit drugs. The decentralized ledger tracks all transactions in the supply chain, guaranteeing authenticity and regulatory compliance. Even with these advantages, data privacy, integration with current supply chain systems, and scalability are challenges. Research indicates the integration of Blockchain with Internet of Things (IoT) technologies and sophisticated encryption methods to enhance efficiency and security in pharmaceutical supply chain management.

Research on Blockchain use in medical imaging indicates its potential to advance data sharing and storage. Medical images, including MRI and CT scans, need secure and efficient transfer between healthcare facilities. Research investigates Blockchain's potential to enable decentralized access while maintaining data integrity and privacy. Nonetheless [10], the storage and computational intensity of medical images is challenging for on-chain deployment. Solutions have been proposed in the form of hybrid architectures that have metadata stored on the Blockchain and large image files stored off-chain. Blockchain and artificial intelligence integration for automated diagnosis is also being researched for future developments.

Blockchain-based sharing of healthcare data has also been seen as a solution to interoperability issues between various medical organizations. Research talks about how decentralized management of health records facilitates effortless data sharing with security. Access control and encryption mechanisms are built in to ensure that only authorized individuals [11] can access patient data. Scalability is a problem, though, as Blockchain networks expand, causing transactions to be delayed in validation. Scholars recommend employing sharding to reduce the burden on nodes and Layer 2 scaling services to increase transaction volume and efficiency, enabling mass adoption of Blockchain in healthcare data sharing.

Some studies examine the application of Blockchain in remote patient monitoring platforms. With the growing implementation of wearable sensors and IoT devices in medicine, there is a need for secure and reliable data exchange. Blockchain makes patient-generated health data tamper-proof and traceable. But real-time processing of sensor data is [12] hindered by latency and network traffic. Studies indicate the use of edge computing and light-weight consensus protocols to enhance performance. Further, privacy-preserving methods like homomorphic encryption and zero-knowledge proofs are being investigated to improve security without compromising seamless integration with remote healthcare monitoring systems.

The use of Blockchain in securing clinical trial data to provide transparency and avoid manipulation of data has been studied by researchers. Legacy clinical trial procedures are inefficient, have data inconsistencies, and a lack of trust between parties. Blockchain guarantees an immutable ledger of trial information, such that results cannot be tampered with or manipulated. Research shows the way smart contracts ensure automated management of patient consents [13] and regulation adherence. Despite this, connecting Blockchain to established clinical trial infrastructure is technically and regulatorily problematic. Research continues in developing scalable and privacy preserving Blockchain models to make clinical trial processes more reliable and efficient.

Blockchain has been explored for use in medical insurance for the purposes of deterring fraud and automating claims processing. Research points out how smart contracts facilitate automatic claim validation and payment settlements, eliminating administrative costs and human discrepancies. The openness of Blockchain allows for fraud claims to [14] be easily identified, promoting trust between insurers and policyholders. Data privacy concerns and healthcare regulatory compliance issues are challenges that need to be addressed. Research aims to create privacy-critical solutions that ensure transparency against data protection while maintaining interoperability with standard insurance management systems.

Security of Internet of Medical Things (IoMT) devices has been a subject of concern following weaknesses in conventional data storage systems. Researchers have

advocated for Blockchain as a means of securing IoMT communications and unauthorized access of critical patient information. Blockchain provides decentralized authentication and data integrity of device-generated information. Nevertheless, high energy consumption and latency in transactions are obstacles to real-time IoMT applications. Research indicates [15] lightweight Blockchain architectures and off-chain data processing methods to improve performance. Artificial intelligence-based anomaly detection in IoMT networks is also being researched for improved security.

Blockchain's role in genomic data protection has been studied because of the growing concerns of privacy and illicit access to genetic data. Evidence shows that the conventional centralized databases holding genomic information are vulnerable to cyberattacks and data leaks. Blockchain offers a decentralized and immutable platform for the protection of genetic data while facilitating controlled access [16] for research. Nevertheless, the increased storage and processing requirements of genomic data are formidable barriers to implementing on-chain solutions. Solutions discussed include hybrid designs in which Blockchain hosts metadata, and encrypted cloud storage is utilized for massive storage of genomic information.

Blockchain identity management systems were examined by researchers as a basis for healthcare personnel and patient systems. Conventional systems of identifying entities depend upon central authorities who may be victims of fraud as well as stolen identities. Blockchain facilitates self-sovereign identity management, where users own their credentials and do not depend on intermediaries. Research identifies [17] the application of decentralized identifiers and verifiable credentials to strengthen security and privacy. Interoperability with current healthcare authentication systems and compliance with regulatory requirements are still areas of concern.

Blockchain and artificial intelligence integration has been proposed in healthcare contexts to enhance data security and decision-making. AI algorithms need to access large amounts of medical data for training and inference purposes, compromising data privacy. Blockchain offers a tamper-proof and secure [18] data-sharing model while ensuring that AI processing is done over tamper-proof data. The computational overhead generated by Blockchain transactions, however, can have an effect on AI processing efficiency. Research suggests federated learning and decentralized AI models that utilize Blockchain for safe collaboration while maintaining data privacy in healthcare applications.

Consent management based on Blockchain for sharing healthcare data has been suggested to give patients control over their medical records. Centralized entities are used by traditional consent management systems, and hence they are susceptible to unauthorized access and misuse of data. Blockchain facilitates smart contracts to automate enforcement of consent [19], so that requests for data access adhere to patient preference. Research points to the advantages of transparency and auditability in Blockchain-based consent management. Complying with data protection laws like GDPR and HIPAA is challenging. Research continues to build interoperable and scalable solutions that improve privacy and security in healthcare consent management.

Studies have explored the role of Blockchain in pandemic response management, focusing on secure data sharing and supply chain tracking. The COVID-19 pandemic highlighted the need for real-time data exchange between healthcare organizations, governments, and research institutions. Blockchain provides a transparent and tamper-resistant platform [20] for tracking disease outbreaks, managing vaccine distribution, and ensuring data integrity. Yet, interoperability with current healthcare systems and data privacy issues constrain adoption. Studies indicate the integration of Blockchain with decentralized data-sharing protocols and secure multi-party computation methods to enhance pandemic response effectiveness and public health readiness.

3. Methodology

Public Key Infrastructure (PKI) is important for securing data exchange in healthcare networks, providing authentication, confidentiality, and integrity. Conventional PKI models like Log-based and Web-of-Trust are vulnerable to single points of failure and hence security breaches. Blockchain technology provides a decentralized solution with immutability, transparency, and improved security for PKI transactions. This work combines hybrid encryption methods with blockchain-based PKI to protect medical data transactions. A self-organizing network based on trust is utilized to maximize energy usage and computation. Nodes are clustered in a trusted manner

to provide efficient certificate dissemination while preventing routing attacks and enhancing network stability.

A. Blockchain-Based PKI Initialization

A blockchain network is formed using validator nodes and a Certificate Authority (CA) in charge of issuing digital certificates. Every participant in the network derives a public-private key pair, which is securely stored for authentication. The PKI based on blockchain guarantees certificates are issued in an open and tamper-proof way. A consensus protocol is used to authenticate transactions and ensure ledger integrity. The initialization process establishes the basis for a decentralized PKI system, removing single points of failure. Smart contracts are implemented to automate certificate issuance and revocation, guaranteeing secure operations while minimizing dependence on centralized authority structures within healthcare networks.

B. Certificate Request and Trust Calculation

The participants ask for digital certificates from the CA to verify their identity in the network. Trust scores are computed using pre-defined parameters like energy usage, transaction history, and node behavior. A mathematical trust function is used to ensure dynamic trust over time. Nodes with good energy efficiency and reliable transactions are given higher trust values. The trust model enhances network security by reducing malicious behavior and ensuring only reliable participants are issued certificates. Periodically, the trust scores are refreshed based on node behavior so that real-time assessment of network reliability is possible, and the healthcare data transmission process is secured.

C. Certificate Authority and Ledger Update Selection

A decentralized process chooses the CA based on the highest trust score among the eligible nodes. The chosen CA issues certificates and updates the distributed ledger to ensure transparency. Each issued certificate is recorded on the blockchain ledger, creating an immutable and tamper-proof history of certificates. This removes weaknesses related to centralized PKI models. The process of updating the ledger guarantees that all participants in the network have verified records of certificates, enhancing trust and security. Once the CA is chosen, smart contracts take over certificate management processes like renewal, revocation, and expiration, minimizing human intervention and providing an efficient, secure certification process.

D. Node Clustering Based on Trust

Network nodes are clustered according to trust ratings, maximizing certificate distribution and resource allocation. A threshold is set to qualify clusters to ensure only high-trust nodes are engaged in certificate issuance and validation. Clustering improves network efficiency by eliminating duplicate computations and balancing loads. The leader node manages each cluster and is dynamically elected based on updates in trust values. This process reduces energy costs by spreading the authentication load over trusted nodes. The clustering function provides a scalable, robust, and efficient PKI system ideal for high-load applications like blockchain-based healthcare networks.

E. Secure Data Transmission and Trust-Based Routing

Authenticated nodes securely exchange medical data using hybrid encryption techniques, ensuring confidentiality and integrity. Trust-based routing directs data packets through highly trusted nodes, minimizing exposure to security threats. Each transmission updates trust values, allowing adaptive network behavior. Trust-based routing mitigates risks associated with malicious nodes attempting to disrupt communication. The integration of encryption with trust-aware routing enhances overall security by preventing unauthorized access to medical records. This method maximizes energy usage by choosing the best route for data transfer. The system is flexible and adapts to network changes, providing equal security and performance in healthcare data exchange.

F. Detection and Simulation of Routing Attacks

A simulated routing attack environment tests the robustness of the network against security attacks. Malicious nodes try to intercept or manipulate data transfer by breaking routing routes. The system detects and isolates these nodes on the basis of anomalous behavior and falling trust scores. The blockchain ledger holds an immuable record of routing anomalies, which allows forensic analysis and mitigation of threats. Countermeasures of re-routing through trusted nodes and real-time refresh of trust calculations in attack resistance guarantee resilience against attacks. The simulation measures how blockchain PKI increases network security against routing attacks, showcasing enhanced resilience over

traditional PKI models susceptible to communication infrastructure vulnerabilities.

G. Analysis and Comparison

The performance is measured with regards to energy consumption, trust forwarding, and resistance to security attacks. Performance comparison is made between the trust-based clustered network and the self-organizing network. Energy consumption factors show the effectiveness of trust-aware clustering in preventing computational overhead. The effect of routing attacks on network performance is evaluated, emphasizing the benefits of blockchain in preventing security breaches. Experimental results confirm the efficacy of the proposed system in protecting healthcare data exchanges. The model improves security, scalability, and efficiency through the integration of blockchain, trust-based clustering, and hybrid encryption, making it a potential solution for secure medical data transactions.

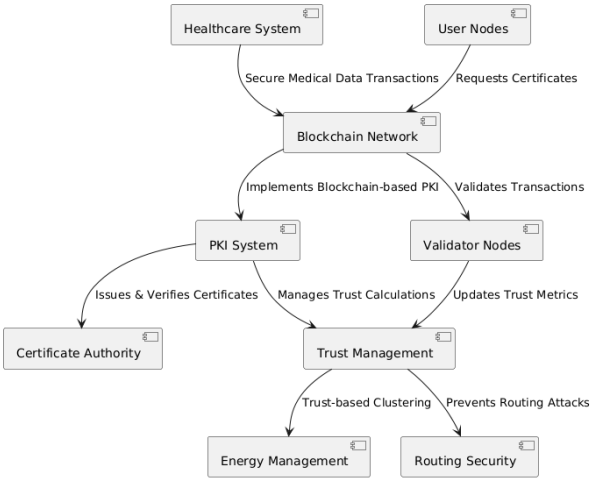


Fig. 1: Architecture Diagram

4. Result And Discussion

The suggested Blockchain-based PKI system was tested in terms of energy consumption, trust management, and routing attack resistance in a healthcare network. The performance of the trust-based clustered network and the self-observing network was compared by simulating data transactions between nodes. The energy consumption of every node was measured in various network scenarios to evaluate the efficiency of the suggested system. The trust-driven clustering mechanism efficiently clustered nodes based on their trust values such that only trustworthy nodes took part in sensitive transactions. The self-monitored network also improved security by dynamically adjusting trust values depending on current interactions, thus minimizing the threat of malicious intentions.

In the trust-driven clustered network, nodes with higher trust values were given higher priorities for certificate issuance and transaction verification, resulting in enhanced security and optimized energy consumption. The self-observing network presented an adaptive mechanism where every node independently assessed its interactions and updated its trust score. This mechanism provided improved resistance against Sybil attacks and illegitimate certificate authorities. The energy consumption analysis indicated that the self-observing network used a bit more power than the trust-based clustered network because of constant trust updates, but this trade-off was worth it in terms of enhanced security and reliability.

Network Observation

A comparison between trust-based node clustered network and self-observing network was done to assess their performance in blockchain-based healthcare environments. The self-observing network updated the trust scores dynamically using real-time interactions, while the trust-based node clustered network clustered nodes using pre-defined trust thresholds. The energy consumption analysis indicated that the self-observing network used a little more power as it recalculated trust more frequently. It did not, however, offer improved adaptability and security. In comparison, the trust-based clustering algorithm maximized energy consumption while ensuring a consistent trust assessment system.

Comparison between Self observing, and Trust based node clustered networks:

Energy and Trust values in Self observing Networks:

```
Energy and Trust values of nodes:
Node 0: Energy = 41 units, Trust = 0.5900 (Trusted)
Node 1: Energy = 40 units, Trust = 0.6000 (Trusted)
Node 2: Energy = 48 units, Trust = 0.5200 (Not Trusted)
Node 3: Energy = 38 units, Trust = 0.6200 (Trusted)
Node 4: Energy = 48 units, Trust = 0.5200 (Not Trusted)
Node 5: Energy = 40 units, Trust = 0.6000 (Trusted)
Node 6: Energy = 48 units, Trust = 0.5200 (Not Trusted)
Node 7: Energy = 46 units, Trust = 0.5400 (Not Trusted)
Node 8: Energy = 40 units, Trust = 0.6000 (Trusted)
Node 9: Energy = 42 units, Trust = 0.5800 (Trusted)
Node 10: Energy = 43 units, Trust = 0.5700 (Trusted)
Node 11: Energy = 44 units, Trust = 0.5600 (Trusted)
Node 12: Energy = 36 units, Trust = 0.6400 (Trusted)
Node 13: Energy = 37 units, Trust = 0.6300 (Trusted)
Node 14: Energy = 39 units, Trust = 0.6100 (Trusted)
```

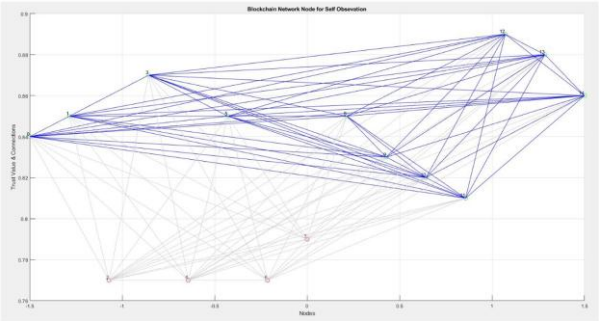
Energy and Trust values in Trust based node clustered Networks:

```
Energy and Trust values of nodes:
Node 0: Energy = 38 units, Trust = 0.6200
Node 1: Energy = 54 units, Trust = 0.4600
Node 2: Energy = 66 units, Trust = 0.3400
Node 3: Energy = 55 units, Trust = 0.4500
Node 4: Energy = 49 units, Trust = 0.5100
Node 5: Energy = 45 units, Trust = 0.5500
Node 6: Energy = 49 units, Trust = 0.5100
Node 7: Energy = 45 units, Trust = 0.5500
Node 8: Energy = 59 units, Trust = 0.4100
Node 9: Energy = 59 units, Trust = 0.4100
Node 10: Energy = 52 units, Trust = 0.4800
Node 11: Energy = 55 units, Trust = 0.4500
Node 12: Energy = 46 units, Trust = 0.5400
Node 13: Energy = 37 units, Trust = 0.6300
Node 14: Energy = 46 units, Trust = 0.5400
```

Trust Levels by Node ID In Self Observing Network

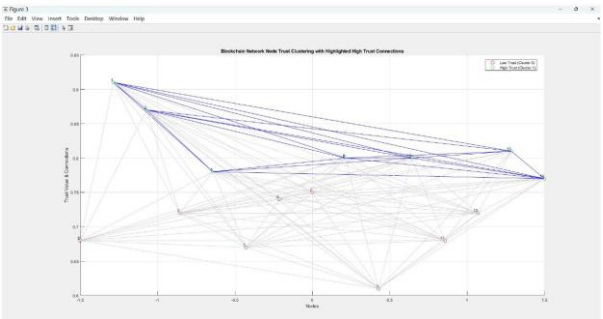
The trust level of each node in the self-observing network was computed and updated dynamically according to its interactions. Nodes with a past of secure and efficient transactions were assigned higher trust scores, while nodes that were engaged in suspicious activities saw their trust decrease. This

adaptive mechanism kept malicious actors from dominating the network. The distribution of trust levels among nodes exhibited a consistent progression, with trustworthy nodes retaining high trust values, providing a secure and robust PKI system.



Trust Levels by Node ID in Trust Based Node Clustered Networks

In the trust-based node clustered network, trust levels were attributed by predefined qualifications, mainly taking energy used and successful transactions into consideration. Nodes were segmented into clusters, and their trust values were constant unless a catastrophic event led to an update. The formal method of doing this made efficient certificate dissemination possible while reducing computational overhead. The findings indicated that trusted nodes did not deviate from stable scores, while the untrusted ones were progressively kept out of security-critical functions to ensure protection without wasteful resource usage.



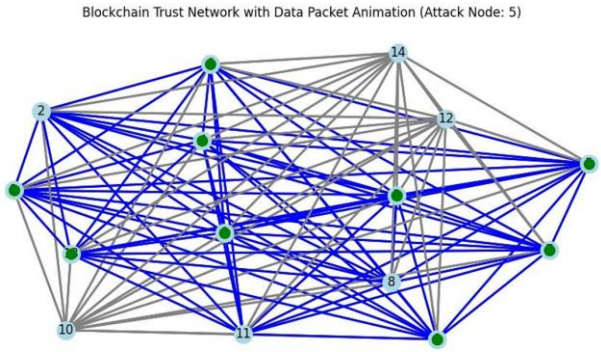
Routing Attack

An analysis of routing attacks was investigated by the presence of malicious nodes that tried to redirect transactions. The nodes had attempted to trick the network facilities by forwarding the data packets to unauthorized addresses. The intensity of the attack rested on whether the faulty nodes induced partial or total data drops. The trust protocols in both network configurations were important in detecting and averting these attacks. The self-monitoring network exhibited quicker detection of faulty nodes, while the trust-based clustered network successfully isolated untrusted nodes using pre-defined trust thresholds.

Network Performance Under Routing Attack

Trust-Based Node Clustered Networks (Partial Drop)

When a partial drop attack was launched, a few data packets were lost but the network was still operational. The trust-based clustering mechanism was able to detect unreliable nodes and mitigate the effects of the attack. The network did suffer some delays as the other nodes had to make up for the lost data.

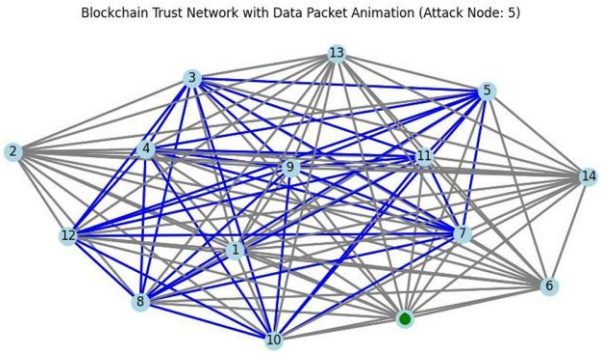



```
Enter the node ID to introduce a routing attack (0-14): 5
Data packet dropped at attacked node!

Node Energy Consumption and Trust Values:
------------------------------------------------
Node 0: Energy = 40, Trust Value = 0.600
Node 1: Energy = 30, Trust Value = 0.700
Node 2: Energy = 48, Trust Value = 0.520
Node 3: Energy = 31, Trust Value = 0.690
Node 4: Energy = 46, Trust Value = 0.540
Node 5: Energy = 49, Trust Value = 0.510
Node 6: Energy = 50, Trust Value = 0.500
Node 7: Energy = 35, Trust Value = 0.650
Node 8: Energy = 47, Trust Value = 0.530
Node 9: Energy = 31, Trust Value = 0.690
Node 10: Energy = 55, Trust Value = 0.450
Node 11: Energy = 35, Trust Value = 0.650
Node 12: Energy = 51, Trust Value = 0.490
Node 13: Energy = 32, Trust Value = 0.680
Node 14: Energy = 59, Trust Value = 0.410
```

Trust-Based Node Clustered Networks (Complete Drop)

In the case of a complete drop, the malicious nodes effectively hindered data transmission, causing substantial interference in network operations. The system needed to be manually intervened or have an external process to resume normal operations. This pointed to the necessity of adaptive trust updates to effectively counter complete drop attacks.

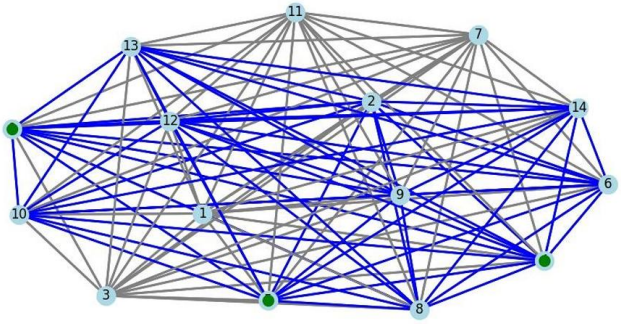



```
Enter the node ID to introduce a routing attack (0-14): 5
Data packet stopped at node 0 due to no available high-trust paths.

Node Energy Consumption and Trust Values:
-------------------------------------------------
Node 0: Energy = 53, Trust Value = 0.470
Node 1: Energy = 56, Trust Value = 0.440
Node 2: Energy = 59, Trust Value = 0.410
Node 3: Energy = 46, Trust Value = 0.540
Node 4: Energy = 47, Trust Value = 0.530
Node 5: Energy = 49, Trust Value = 0.510
Node 6: Energy = 52, Trust Value = 0.480
Node 7: Energy = 47, Trust Value = 0.530
Node 8: Energy = 40, Trust Value = 0.600
Node 9: Energy = 43, Trust Value = 0.570
Node 10: Energy = 49, Trust Value = 0.510
Node 11: Energy = 33, Trust Value = 0.670
Node 12: Energy = 39, Trust Value = 0.610
Node 13: Energy = 57, Trust Value = 0.430
Node 14: Energy = 51, Trust Value = 0.490
```

Self-Observing Network (Partial Drop)

The self-monitoring network responded rapidly to a partial drop attack by dynamically adjusting trust levels. Nodes involved in the attack immediately lost trust, which prevented additional data loss. The system had stable performance with minimal disruption.

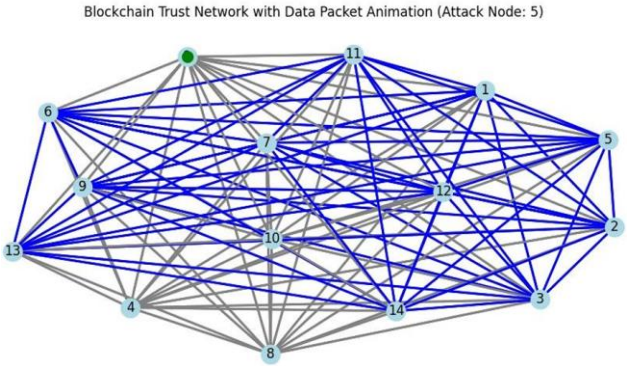



```
Enter the node ID to introduce a routing attack (0-14): 5
Data packet dropped at attacked node!

Node Energy Consumption and Trust Values:
-------------------------------------------------
Node 0: Energy = 35, Trust Value = 0.650
Node 1: Energy = 48, Trust Value = 0.520
Node 2: Energy = 43, Trust Value = 0.570
Node 3: Energy = 47, Trust Value = 0.530
Node 4: Energy = 45, Trust Value = 0.550
Node 5: Energy = 42, Trust Value = 0.580
Node 6: Energy = 44, Trust Value = 0.560
Node 7: Energy = 46, Trust Value = 0.540
Node 8: Energy = 42, Trust Value = 0.580
Node 9: Energy = 36, Trust Value = 0.640
Node 10: Energy = 41, Trust Value = 0.590
Node 11: Energy = 47, Trust Value = 0.530
Node 12: Energy = 38, Trust Value = 0.620
Node 13: Energy = 37, Trust Value = 0.630
Node 14: Energy = 44, Trust Value = 0.560
```

Self-Observing Network (Complete Drop)

In the worst-case drop scenario, the self-monitoring network's ongoing surveillance allowed for immediate detection and response. Infected nodes were rapidly discovered and quarantined, normalizing network activity without the need for external input. This fault tolerance proved the benefit of live trust updates in responding to critical attacks.




```
Enter the node ID to introduce a routing attack (0-14): 5
Data packet stopped at node 0 due to no available high-trust paths.

Node Energy Consumption and Trust Values:
-------------------------------------------------
Node 0: Energy = 48, Trust Value = 0.520
Node 1: Energy = 40, Trust Value = 0.600
Node 2: Energy = 43, Trust Value = 0.570
Node 3: Energy = 39, Trust Value = 0.610
Node 4: Energy = 46, Trust Value = 0.540
Node 5: Energy = 42, Trust Value = 0.580
Node 6: Energy = 45, Trust Value = 0.550
Node 7: Energy = 37, Trust Value = 0.630
Node 8: Energy = 47, Trust Value = 0.530
Node 9: Energy = 35, Trust Value = 0.650
Node 10: Energy = 46, Trust Value = 0.540
Node 11: Energy = 41, Trust Value = 0.590
Node 12: Energy = 37, Trust Value = 0.630
Node 13: Energy = 45, Trust Value = 0.550
Node 14: Energy = 41, Trust Value = 0.590
```

The ultimate outcome is that both network models effectively protected the blockchain-based PKI system for health data transactions. The suggested hybrid encryption methods further enhanced data integrity and confidentiality. Through the combination of blockchain technology and adaptive trust management, the system removed the vulnerabilities of single points of failure in traditional PKI architectures. The research concludes that a hybrid solution integrating trust-based clustering with self-observing mechanisms can considerably improve the security and efficiency of blockchain-based healthcare networks.

5. Conclusion

This paper describes a hybrid encryption-focused Blockchain-PKI system aimed at improving security, trust management, and energy efficiency in healthcare networks. By incorporating trust-based clustering and self-observing features, the proposed system performs

well in addressing some of the major issues with conventional PKI designs, such as single points of failure, poor trust assessment, and susceptibility to routing attacks. The model provides secure sharing of medical information while maintaining the integrity and confidentiality of blockchain-based healthcare systems. The trust-based node clustering algorithm performed well in clustering trusted nodes, saving energy, and facilitating efficient certificate propagation. It offered a formalized trust assessment mechanism to authenticate transactions by trusted nodes. However, its application of fixed trust thresholds made it less dynamic in dynamic network environments. The self-observing network learned in real time by dynamically adapting trust ratings as necessary, thus being more resilient to malicious behaviour. Despite showing a marginally higher energy consumption, it provided a better Sybil attack defence and unauthorized certificate issuance. A detailed examination of routing attacks confirmed that both models could effectively counter network interference and data forgery. The self-monitoring network was more efficient in the detection of threats and responding to them due to its dynamic updates of trust, whereas the trust-based clustering model applied static trust values to isolate malicious nodes. The combination of these two models provides the optimal balance of security and performance, making the hybrid model particularly well suited for use in applications that incorporate blockchain technology in the healthcare sector.

A consumption analysis of energy revealed that the self-observing network utilized higher computational resources because of repeated recalibrations of trust. However, the trade-off was worthwhile in the form of the corresponding security and reliability enhancements. On the other hand, the trust-based clustering model offered a more energy-conserving solution with a steady trust assessment process. However, when the two approaches were compared, the self-observing network performed better on average since its overall energy consumption was lower than that for the trust-based node clustering network. In addition, the integration of blockchain technology improved security by taking advantage of its immutability, transparency, and decentralization properties to ensure that unauthorized modifications were not made. This research concludes that a hybrid approach, which incorporates trust-based clustering and self-adaptive mechanisms, improves the security, reliability, and efficiency of blockchain-based medical networks. Based on adaptive trust management and secure certificate dissemination, the framework proposed in this research provides a secure and scalable medical data transaction solution. Future research can further improve energy consumption and investigate other security improvements to make blockchain-based healthcare systems more robust against the latest cyber-attacks.

References

[1] R. Kumar, R. Chavan, V. S. Shirsath, S. Sanjay Gharat and K. S. Patil, "Blockchain Solutions for Nursing: A New Paradigm in Healthcare Security and Data Management," 2024 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS), Pune, India, 2024, pp. 1-4, doi: 10.1109/ICBDS61829.2024.10837162.

[2] M. Sharma, S. Singh, A. Deep, D. Garg and A. Kumar, "Blockchain's Frontier: Enhancing Data Security and Collaboration for Healthcare," 2024 11th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Noida, India, 2024, pp. 1-6, doi: 10.1109/ICRITO61523.2024.10522385.

[3] A. Kumar, K. Guleria, I. Sharma and A. Khan, "Multichain Blockchain Solutions for Ensuring Trust and Transparency in IoT Healthcare Environment," 2024 7th International Conference on Circuit Power and Computing Technologies (ICCPCT), Kollam, India, 2024, pp. 1314-1318, doi: 10.1109/ICCPCT61902.2024.10672895.

[4] S. Pandey, A. K. De, S. Choudhary and M. Asim, "A Decentralized Blockchain-Based Architecture for Healthcare Industry," 2023 International Conference on Artificial Intelligence for Innovations in Healthcare Industries (ICAIIHI), Raipur, India, 2023, pp. 1-5, doi: 10.1109/ICAIIHI57871.2023.10489491.

[5] H. Ryu, H. Kim, S. Agarwal, D. K. Sharma, B. Kapito and P. Ali, "Data Sovereignty Provision Blockchain for Remote Healthcare Service," 2023 6th International Conference on Information Systems and Computer Networks (ISCON), Mathura, India, 2023, pp. 1-4, doi: 10.1109/ISCON57294.2023.10112016.

[6] S. Swati, R. K. Mishra, A. Kumar and R. Ingle, "Unlocking the Potential of Blockchain Integration in Secured Framework of Mental Health," 2024 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS), Pune, India, 2024, pp. 1-5, doi: 10.1109/ICBDS61829.2024.10837065.

[7] P. Vidap, A. Bhargav, R. Paswan and A. Jewalikar, "Blockchain Solution to Electronic Healthcare

Records," 2023 International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE), Bengaluru, India, 2023, pp. 659-664, doi: 10.1109/IITCEE57236.2023.10090970.

[8] R. Pise, S. Gavkare, S. Patil, S. Patil and S. Shinde, "Empowering Healthcare: Hyperledger Blockchain for Unified Electronic Health Records and Organ Donation Integrity," 2024 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS), Pune, India, 2024, pp. 1-6, doi: 10.1109/ICBDS61829.2024.10837436.

[9] P. Verma and A. K. Jain, "A Comprehensive Study on the Application of Blockchain Technology's Use in Healthcare," 2023 International Conference on Sustainable Computing and Smart Systems (ICSCSS), Coimbatore, India, 2023, pp. 1388-1393, doi: 10.1109/ICSCSS57650.2023.10169250.

[10] V. G. Lindbergh and I. De Morais Barroca Filho, "Trends in Blockchain Applied to Healthcare," 2024 IEEE 12th International Conference on Healthcare Informatics (ICHI), Orlando, FL, USA, 2024, pp. 531-533, doi: 10.1109/ICHI61247.2024.00078.

[11] S. A. Alex, E. L. Chuma, G. C. Vaz and G. G. de Oliveira, "HealthGuard: Blockchain-Powered Healthcare Data Security," 2023 International Conference on Intelligent Computing and Next Generation Networks（ICNGN), Hangzhou, China, 2023, pp. 1-5, doi: 10.1109/ICNGN59831.2023.10396708.

[12] W. Y. Leong, Y. Z. Leong and W. S. Leong, "Enhancing Blockchain Security," 2024 IEEE Symposium on Wireless Technology & Applications (ISWTA), Kuala Lumpur, Malaysia, 2024, pp. 108-112, doi: 10.1109/ISWTA62130.2024.10651753.

[13] S. Baskar and P. V. Gopirajan, "Application of Blockchain in Digital Healthcare," 2023 International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE), Bengaluru, India, 2023, pp. 591-595, doi: 10.1109/IITCEE57236.2023.10091070.

[14] S. Kumar and J. S. Kumar, "Federated Blockchain Based Highly-Available Healthcare System to Protect the Privacy and Security of Users," 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT), Kamand, India, 2024, pp. 1-6, doi: 10.1109/ICCCNT61001.2024.10725386.

[15] A. Butalia, P. Kharat and N. Hatwar, "Blockchain Pervasive Ledger Technology for Healthcare Using Rough Set Theory," 2024 IEEE Pune Section International Conference (PuneCon), Pune, India, 2024, pp. 1-5, doi: 10.1109/PuneCon63413.2024.10895720.

[16] J. Kumar, A. S. Ali, A. Kumar and S. Kumar, "Enhancing Patient Data Security Through Blockchain Adoption in Fiji's Healthcare System," 2023 International Conference on Sustainable Technology and Engineering (i-COSTE), Nadi, Fiji, 2023, pp. 1-6, doi: 10.1109/i-COSTE60462.2023.10500773.

[17] M. Katoch, K. Devi, A. Sharma, P. K. Angra, P. Singh and A. Kumar, "Enhancing the Security of E-Healthcare Transactions Using Hyperledger Fabric Modular Blockchain Framework," 2023 6th International Conference on Contemporary Computing and Informatics (IC3I), Gautam Buddha Nagar, India, 2023, pp. 1344-1348, doi: 10.1109/IC3I59117.2023.10397797.

[18] U. Zukaib, X. Cui, M. Hassan, S. Harris, H. J. Hadi and C. Zheng, "Blockchain and Machine Learning in EHR Security: A Systematic Review," in IEEE Access, vol. 11, pp. 130230-130256, 2023, doi: 10.1109/ACCESS.2023.3333229.

[19] S. Chowdhury and A. D. Jurcut, "Design Requirements for Secured and Cost-Efficient Blockchain-Based Data Exchange Frameworks in Healthcare," 2023 Fifth International Conference on Blockchain Computing and Applications (BCCA), Kuwait, Kuwait, 2023, pp. 474-486, doi: 10.1109/BCCA58897.2023.10338889.

[20] R. Bokde and P. Phutane, "Blockchain Technology in Healthcare for Patient Privacy: Advances and Threats," 2024 International Conference on Healthcare Innovations, Software and Engineering Technologies (HISET), Karad, India, 2024, pp. 300-303, doi: 10.1109/HISET61796.2024.00093.