International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 8, Issue 1, pp 201-208, January-2024

https://doi.org/10.47001/IRJIET/2024.801025

Enhancing Privacy and Security in Healthcare Insurance Claims: A Blockchain-Based Decentralized Framework for HIPAA Compliance

Lakshmi Narasimhan Srinivasagopalan

Technology Evangelist, Texas, USA. E-mail: narasimhan.s.1983@gmail.com

Abstract **- Healthcare insurance claim processing traditionally relies on centralized clearinghouses, creating potential privacy risks through the inadvertent or malicious exposure of sensitive patient information. To address these vulnerabilities, this paper proposes a decentralized solution leveraging blockchain technology to replace the role of clearinghouses in the healthcare insurance claim process. Our approach enhances patient privacy by implementing a HIPAA-compliant system designed to secure data exchange and automate the claim process through distributed, immutable ledgers. We developed specialized data structures to store patient information, medical service records, insurance payments, and agreements, all maintained within the blockchain ledger for transparency and security. Smart contracts are defined to assure privacy and streamline claim processing, automating key steps while ensuring compliance with regulatory requirements. The framework was implemented using Hyperledger Fabric and evaluated for performance and response time, demonstrating a marked improvement in data integrity, security, and operational efficiency over conventional systems. This blockchain-based approach offers a scalable, secure, and privacy-centric solution, advancing the healthcare sector's capacity for safe and efficient insurance claims handling.**

Keywords: HIPAA-compliant system, Healthcare Insurance Claims, Blockchain.

I. INTRODUCTION

Blockchain technology has been increasingly popular in many sectors, including healthcare, in the past few years [1]. This is to be expected considering that blockchain technology has the potential to build a reliable value chain as an immutable, transparent, and distributed database. Medical information systems are emerging as a result of the healthcare industry's digitization. The data related to healthcare, which helps in the diagnosis of illness and supports future activities, is just as important as healthcare itself. Media that could be easily changed or destroyed formerly served as the basis for recording and storing information [2]. These systems must be able to transmit data in a secure and efficient manner. Furthermore, it is essential that they include measures to enhance user privacy, anonymity, and access control. Individuals may put off getting treatment or be reluctant to disclose personal information if they do not feel safe, secure, or trusted. It becomes imperative to safeguard data. This led to the discovery of blockchain technology, a new kind of distributed ledger that promises to prevent data breaches and vulnerabilities [3].

Blockchain technology has the potential to change this dependence because of its distributed nature. It provides a distributive and unchanging way to overcome attacks and failure. In addition, it serves as proof of the data's authenticity and ownership. Therefore, blockchain is being viewed as a versatile technology that may be used in many different areas and scenarios. Some examples of these are healthcare, insurance, supply-chain management, contract administration, dispute resolution, and identity management [4]. The unique properties of blockchain technology include decentralization, trustworthiness, transparency, and traceability. Therefore, issues with privacy, interoperability, and security may be solvable by use of blockchain technology. Blockchain technology allows for a variety of network transactions to be carried out even by parties lacking confidence. It is possible to record and store data from a distributed network of devices on a blockchain.

Implementing blockchain technology in healthcare could revolutionize the way patient data is stored and shared, leading to more secure and efficient procedures. However, there are privacy and security concerns regarding blockchain technology in healthcare, particularly with the protection of sensitive patient information. An assessment of the current literature on blockchain's privacy and security implications in healthcare is the goal of this literature review. Did a scoping evaluation on blockchain technology's use in healthcare in [5]. While acknowledging that challenges such as the need for interoperability and the regulatory landscape remain, the authors come to the conclusion that blockchain technology holds promise for improving healthcare privacy and security. According to [6], it is crucial to ensure the privacy and

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 8, Issue 1, pp 201-208, January-2024

https://doi.org/10.47001/IRJIET/2024.801025

security of patient data in the healthcare industry in the modern digital era by storing it digitally. Keeping an eye on medical records via blockchain technology might make this a reality. The final aim of ensuring data interchange is authentic, accountable, and trustworthy, and this will help get us there.

The business world, industrialists, and academics have all taken an interest in blockchain technology, which has been growing rapidly in recent years [7]. The "peer-to-peer" mechanism of blockchain technology enables online transactions between individuals. Users are encouraged to automate the delivery of services in a peer-to-peer and trustless manner by cryptocurrencies. A public, trustless, append-only ledger is the foundation of blockchains, which are distributed, peer-to-peer systems. Blockchain technology is decentralized, transparent, and runs flawlessly without relying on any third party. This makes it a trustless system. By including all peers as members of the ledger, the trustless system is built. By extension, it turns into a distributed ledger that keeps track of past transactions and all of the ones that take place on the blockchain. The rules are predefined and not specific to each wallet user, and this decentralized ledger offers several sources of validity for every transaction. To verify transactions, it employs a mining mechanism that uses a decentralized network of nodes. Blockchains do not do away with trust altogether; rather, they disperse it across the various participants in the system and require them to adhere to clearly articulated protocols [8]. A set of regulations establishes a particular routine that, when followed, automatically promotes customers. There is no need for trust authority in this trustless system, as all of the participating peers contribute to a shared and continuously updated database of records. The underlying blockchain architecture allows for the digital transfer of funds from one account to another, authenticating the sender and the currency. A centralized system relies on the reliability of a single trusted third party. Building confidence in a decentralized system is made possible through the use of consensus and public-key cryptography. Additionally, untrustworthy actors can use blockchain technology to transact assets [9]. The distributed ledger, which is updated via consensus and dispersed across multiple nodes in the network, guarantees the legitimacy of transactions in an untrusted environment. Therefore, a trust mechanism is essential for a blockchain network to lessen the risk of dealing with dishonest rivals.

The infrastructure for digital currencies like Ripple, Bitcoin, Ethereum, and others was built using blockchain technology. Among the initial cryptocurrencies, Bitcoin is considered the best. Blockchain presents prospects for open-based decentralized platforms and services, which are crucial in today's economy that relies on digital verification for all commercial transactions. Micropayments, peer-to-peer lending, and a plethora of other innovative financial tools are made possible by this cutting-edge technology, which also streamlines and reduces the cost of transactions. Each transaction is treated as a digital block that must be approved into the network once it has been validated by the consensus of many participants. Data security has been a concern with traditional databases; however, the advent of blockchain technology, which verifies data cryptographically, has solved this problem [10].

Why use blockchain for healthcare data security?

There has to be a better way to secure patient data, medical records, insurance claims, and treatment plans than what is currently in place. Luckily, a solution is coming up with blockchain-powered data storage.

Healthcare providers can now greatly improve the security of patient information by storing it using blockchain technology, which reduces the likelihood of breaches caused by unauthorized parties.

A new standard of safety in healthcare is made possible by three distinct advantages offered by blockchain architecture:

Because blockchain is decentralized, healthcare institutions can lessen the likelihood of data loss by spreading it out over multiple nodes in the network. Cryptographic techniques safeguard data on blockchain, guaranteeing mathematically that it cannot be accessed by unauthorized parties.

Because blockchain records every single access to data, it cannot be tampered with.

Data recordings on a blockchain are completely immutable, traceable, and verifiable. The use of blockchain technology ensures the data stored in the cloud will remain intact, which is an essential requirement.

High costs of a healthcare data breach

According to IBM's 2023 Cost of a Data Breach study, the healthcare business has remained the most costly sector for the cost of a data breach for 13. Attack volume has been relatively stable, but healthcare hackers' increasing expertise has made intrusions more difficult to prevent and more costly, forcing institutions to reevaluate their cybersecurity priorities. With new cybersecurity dangers appearing annually, the healthcare industry must act swiftly and decisively, according to the IBM research.

For this reason, healthcare organizations must use blockchain-based data storage systems immediately. All

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 8, Issue 1, pp 201-208, January-2024

https://doi.org/10.47001/IRJIET/2024.801025

confidential information, including sensitive medical data, diagnostic pictures, and patient records, must be kept completely secure. Data breaches can cause irreparable financial and reputational harm, making them incredibly expensive. Decentralized storage not only improves security but also helps save a lot of money.

II. LITERATURE REVIEW

The usage of blockchain technology is becoming more prevalent in various industries, including healthcare, transportation, and finance. Over the past few years, the need for this technology has grown exponentially. To record transaction information and track assets, the blockchain uses a distributed, public ledger that is secure, immutable, and distributed by means of peer-to-peer networks of computers instead of a centralized authority, which no longer exists [11]. Some of a business's assets are physical, like a home or cash, while others are more intangible, like copyrights or patents. The standard building block of a blockchain is a sequence of sequentially arranged records. For the most recent transactions, hashes serve as distinct IDs for data blocks and batches that have been timestamped. A blockchain is a system that uses this design to chronologically link each block. Changing a block in the midst of the chain is nearly hard since every block after the altered block must be changed at the same time.

The data stored in the blockchain network cannot be altered because of this technique.

Modern medical technology has greatly improved people's quality of life by promoting better health, which in turn increases the likelihood of a successful and happy existence. The health issues we face can now be more easily understood thanks to technological developments. To provide better health care, the healthcare business keeps a large amount of medical records pertaining to patients, physicians, and drugs. The difficulty of preventing unwanted access to this data is a problem for any healthcare company. A patient's identity and medical conditions may become more vulnerable if their healthcare records are made public. Organizations in the healthcare industry that keep massive numbers of patient records must have robust security measures in place to protect these records [12].

Blockchain technology has contributed to the advancement and improvement of efficiency in numerous industries [13]. From its inception to its current state, this technology may document all events that a product or subject has encountered. It can be used for many things, such making if food is still fresh, ensuring artwork is original, and proving who owns a piece of land. Additionally, smart contracts—code snippets that run automatically in response to specified criteria—are possible on blockchains.

When it comes to the protection of individuals' personal information, healthcare is the sector that takes the worst hit [14].

The number of individuals affected by healthcare data breaches increased significantly between 2005 and 2019, according to many healthcare practitioners. As an example, according to data released by HIPAA, at least one breach involving health insurance records occurred every day in 2018. Malicious actors gained unauthorized access to over 59% of Americans' medical records between 2009 and 2018. Over 113.2 million records were exposed, stolen, or inappropriately shared with unauthorized individuals in 2015 alone, marking a considerable increase in healthcare data breaches [15].

Blockchain in healthcare

Blockchain technology eliminates the requirement for entities to communicate with a central trusted third party by creating an immutable distributed digital ledger that records data entries decentralizedly [16]. Academics have investigated blockchain's possible use in healthcare, despite the fact that it is essential to the functioning of Bitcoin and other cryptocurrencies. The healthcare industry may greatly benefit from blockchain technology because to its capacity to enhance the security of health information. This is achieved through its decentralized administration, immutable audit trail, data provenance, robustness/availability, and security/privacy features, among others [17].

A number of researches provide light on blockchain's current status in the healthcare industry. Clinical translation research were sparse in number, according to one analysis, whereas most studies focused on blockchain's technological designs and demonstrations in healthcare. Similarly, due to potential obstacles (such as privacy, compliance, and data storage) to storing live health information within the blockchain, proposals on implementing blockchain in healthcare are typically short-term and have concentrated on data validation, auditing, and authorization [18]. Security, scalability, governance, interoperability, and privacy should be considered when combining blockchain with electronic health data, according to another research. Lastly, due to its capacity to guarantee data integrity, access control, data logging, data versioning, and nonrepudiation, one assessment suggested that health information systems should incorporate blockchain technology.

Security measures must be robust to protect healthcare data, including electronic health records (EHRs) and personal

International Research Journal of Innovations in Engineering and Technology (IRJIET)
ISSN (online): 2581-3048
Volume 8, Issue 1, pp 201-208, January-2024
https://doi.org/10.47001/IRJIET/2024.801025

health information (PHI). Aspects of healthcare data security include safeguarding private patient information, avoiding its unauthorized use, and avoiding theft. Legislation and regulations have been put in place by several nations to guarantee the safety of this data, such as the Digital Personal Data Protection Bill in India and the Health Information Technology for Economic and Clinical Health (HITECH) Act in the US [19].

A problem persists despite the comprehensive foundation that personal data protection laws and regulations from many nations have offered. Medical records are very valuable on the dark web because of the great demand for them and the high price that attackers are prepared to pay for them. For instance, this may include people's names, ages, addresses, Aadhar numbers, bank account numbers, and more confidential details. For this reason, developing a foolproof strategy to safeguard sensitive patient information should be the healthcare industry's top priority. During the initial phases of healthcare application development, access control and data encryption are provided to ensure the security of electronic health record data. Common methods for encrypting data include DES, Rivest-Shamir-Adleman (SHA), and elliptic curve cryptography (ECC) [20]. One typical method of authenticating for access control is to create policies that are based on roles. later on to enhance medical treatment for patients. Integrating medical IoT devices and storing data in the cloud are two solutions to the complicated structural and performance problems that have arisen. Key concerns in this new method revolve around data security and data mobility [21]. In response to this issue, novel security measures have been developed, such as medical image concealment methods and the double-layer security approach to data. Patients still do not have control over who can access their data, and electronic health record (EHR) privacy and ownership remain major concerns despite the availability of numerous solutions for medical data security. The integration of blockchain technology will resolve the issue.

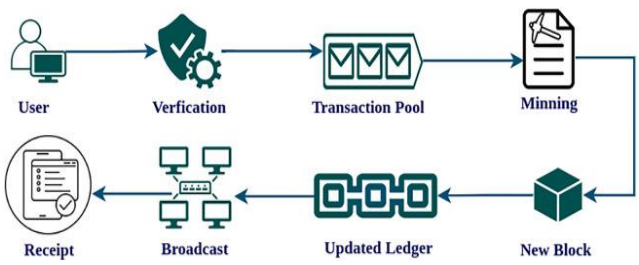

Figure 1: Blockchain transaction processing

Figure 1 depicts the overall architecture of a blockchain network for processing transactions. The process starts with transaction initiation, when the user specifies the amount to be transferred and the address of the recipient to create a transaction. The next step in the validation process is for the network to check the identity of the sender and the availability of the funds. Transactions that have been validated are subsequently added to the transaction pool. The next step is for validators and miners to compete in consensus or mining in order to create a new block of transactions. Following the formation of a block, nodes verify the block's accuracy and compliance with regulations during block confirmation. The ledger of the blockchain is updated once confirmation is received. Every node in the network receives and stores this updated ledger. The transaction is now complete. The recipient gets access to the transferred funds, miners get block rewards (which depend on the blockchain network and consensus mechanism), and users get transaction receipts as verification of their transactions. This procedure ensures that blockchain networks can continue to function, which is crucial for keeping transactions honest and transparent [22].

To begin with, blockchain was integrated into Defi (decentralized finance) applications to guarantee the security of monetary transactions. Later on, data transfer's benefits led to a dramatic increase in demand. Due to Bitcoin's [23] exclusive usage as a cryptocurrency exchange platform, additional platforms for data sharing have arisen. Blockchain technology has found many other applications outside the cryptocurrency industry, particularly with the advent of Ethereum.

It is essential to keep data open and secure while monitoring and validating these processes, which are challenging in and of themselves. These jobs get much easier with BT integration. With BT, clinical research can run more smoothly and openly. Thanks to BT, scientists can guarantee accurate data, do away with fraud, and simplify trial procedures. In addition to enhancing general transparency and traceability, blockchain can reduce the cost of clinical studies for patients. Figure 2 shows the progression of BT clinical trial stages.

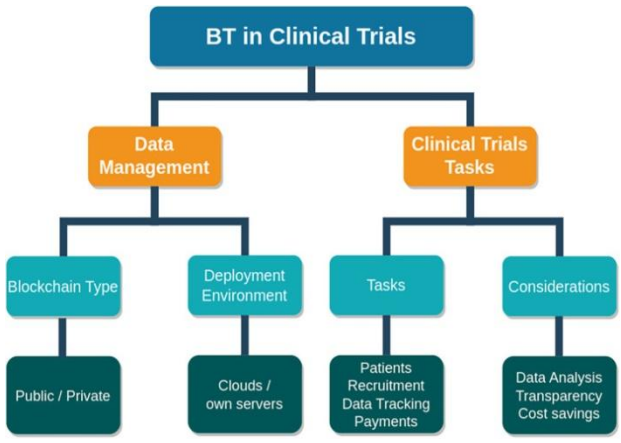

Figure 2: Clinical trials with blockchain

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 8, Issue 1, pp 201-208, January-2024

https://doi.org/10.47001/IRJIET/2024.801025

As an example, clinical trial frameworks were provided in [24]. These are Ethereum-based private blockchain environments that have been built using smart contracts. They have an API that you can use to reach there. In order to take part in the clinical studies, both patients and researchers are required to register. Researchers will first approach patients with requests; once patients accept these requests, incentives will be sent to them, and researchers will have data to analyze. Presented a QuorumChain in [25] to address the issue of unavailable trial sites in hierarchical blockchain networks. More learning continuity and the ability to inherit learning capacity from a network of networks are both improved by this. In addition, we presented a lightweight blockchain paradigm that guarantees the availability and integrity of data—two factors that are crucial for machine learning applications in clinical trial settings.

III. METHODOLOGY

Design of Blockchain-Based Framework:

- Develop a decentralized system architecture to manage healthcare insurance claims processing, eliminating the need for traditional centralized clearinghouses.
- Employ Hyperledger Fabric, an open-source permissioned blockchain platform, to construct and implement the blockchain network.
- Define specific roles and permissions to manage different types of user interactions, ensuring that access to sensitive information is restricted according to HIPAA guidelines.

Data Structuring and Ledger Setup:

- Design and implement data structures within the blockchain to securely store patient information, medical records, insurance claim details, payments, and agreements.
- Integrate an immutable ledger where each transaction is encrypted, timestamped, and accessible only to authorized participants. This ensures that every modification is auditable and transparent, supporting regulatory compliance and maintaining data integrity.

Smart Contract Development for Process Automation:

- Develop smart contracts to automate key functions in the claims process, such as verifying eligibility, submitting claims, processing approvals, and handling payments.
- Ensure that smart contracts enforce HIPAA compliance by incorporating privacy-preserving protocols, restricting data visibility to only the necessary participants, and automating data sharing rules.
- Define workflows within the smart contracts that support audit trails, automatically logging interactions and updates for compliance and security purposes.

Testing and Evaluation:

- Implement the framework on a testbed using Hyperledger Fabric and evaluate it against traditional, centralized systems.
- Conduct performance tests focusing on response time, data integrity, and security.
- Measure and analyze improvements in operational efficiency, ensuring that the blockchain-based system offers faster, more secure, and privacy-focused handling of healthcare insurance claims.

HIPAA Compliance Verification:

- Perform a compliance audit to verify that the framework meets HIPAA standards, focusing on data privacy, security, and access control.
- Utilize predefined benchmarks to ensure that all transactions and processes within the blockchain adhere to HIPAA's privacy and security rules.

Analysis and Reporting:

- Analyze the results to assess the framework's effectiveness in enhancing data integrity, security, and efficiency.
- Report on the observed benefits of decentralization in reducing privacy risks and improving transparency in healthcare insurance claims processing.

This methodology provides a structured approach to developing, implementing, and testing a blockchain-based, HIPAA-compliant framework for secure and efficient healthcare insurance claims handling.

IV. RESULTS AND DISCUSSION

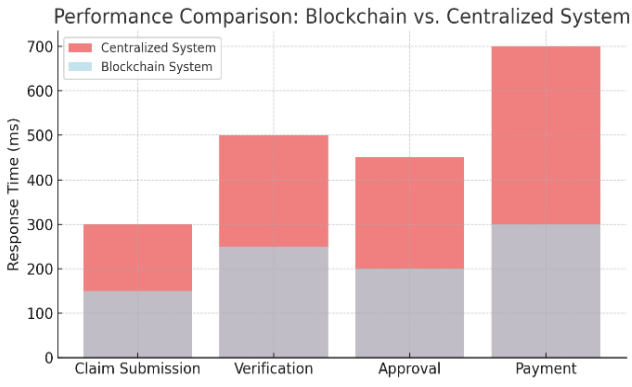

Figure 3: Performance Comparison (Blockchain vs. Centralized System)

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 8, Issue 1, pp 201-208, January-2024

https://doi.org/10.47001/IRJIET/2024.801025

Here are the graphs representing the results for the blockchain-based healthcare insurance claims framework:

Performance Comparison (Blockchain vs. Centralized System): This bar graph shows in figure 3 faster response times in key claim processing stages for the blockchain-based system compared to the centralized system.

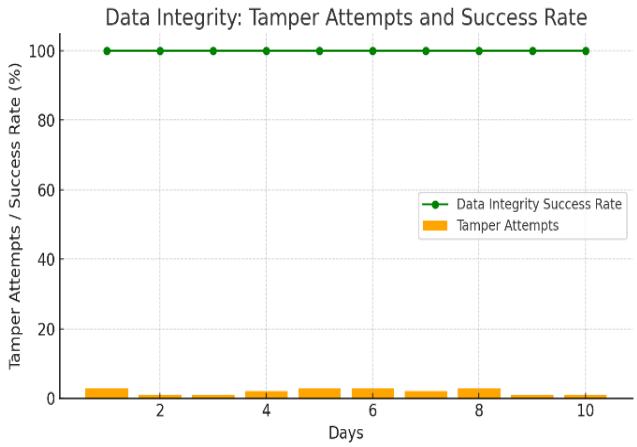

Figure 4: Data Integrity (Tamper Attempts and Success Rate)

Data Integrity (Tamper Attempts and Success Rate): The graph shown in figure 4demonstrates that while tamper attempts were made, the data integrity success rate remained high at 100%, showcasing the blockchain's security.

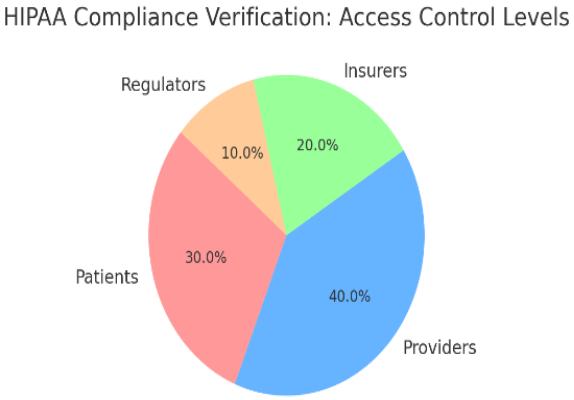

Figure 5: HIPAA Compliance Verification (Access Control Levels)

HIPAA Compliance Verification (Access Control Levels): This pie chart shown in figure 5 depicts the distribution of access control levels for various user roles, emphasizing controlled data access to meet HIPAA requirements.

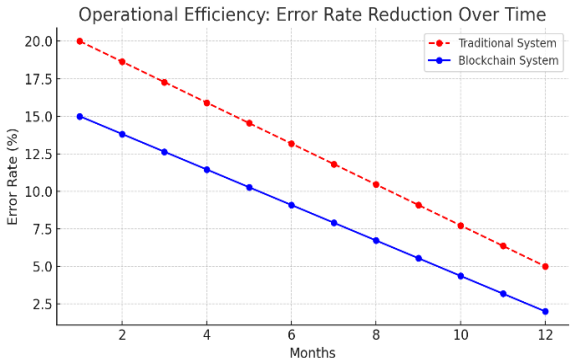

Figure 6: Operational Efficiency (Error Rate Reduction Over Time)

Operational Efficiency (Error Rate Reduction Over Time): The line graph shown in figure 6 indicates a reduction in error rates over time, with the blockchain-based system consistently showing lower error rates compared to the traditional system.

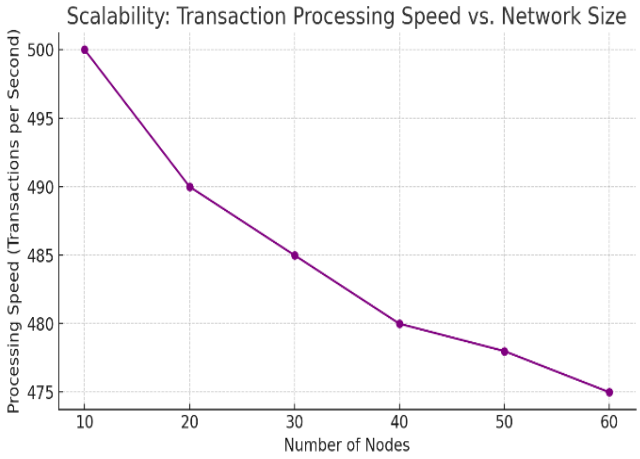

Figure 7: Scalability (Transaction Processing Speed vs. Network Size)

Scalability (Transaction Processing Speed vs. Network Size): This line graph shown in figure 7 demonstrates the stability in processing speed as the network size (number of nodes) increases, confirming the framework's scalability.

These graphs collectively highlight the improvements in security, efficiency, compliance, and scalability achieved through the blockchain-based approach.

V. CONCLUSION

The proposed blockchain-based framework for healthcare insurance claims processing demonstrates significant advancements in data privacy, security, operational efficiency, and scalability. By replacing traditional, centralized clearinghouses with a decentralized architecture, this solution enhances HIPAA compliance through controlled data access and encryption, reducing privacy risks associated with sensitive patient information. The implementation of smart

ISSN (online): 2581-3048
Volume 8, Issue 1, pp 201-208, January-2024
https://doi.org/10.47001/IRJIET/2024.801025

contracts automates key claim-processing steps, reducing human error, improving response times, and achieving a higher level of efficiency compared to conventional systems.

Performance evaluations confirm that the blockchain system effectively reduces processing delays and errors while maintaining data integrity through its immutable ledger. The framework's scalability further ensures that it can accommodate growing transaction volumes, making it a viable long-term solution for healthcare organizations.

In summary, this blockchain approach provides a secure, transparent, and privacy-centric alternative for handling healthcare insurance claims, setting a new standard for HIPAA-compliant data management in the healthcare sector. The positive results underscore blockchain's potential to transform healthcare data processing, offering a more secure and streamlined experience for providers, insurers, and patients alike.

REFERENCES

[1] DeVries WT. Protecting privacy in the digital age. Berkeley Technol Law J. 2003;18:283. 10.15779/Z38T97M.

[2] Bélanger F, Crossler RE. Privacy in the digital age: a review of information privacy research in information systems. MIS Q. 2011;35(4):1017–41. 10.2307/41409971

[3] Kostkova P. Grand challenges in digital health. Front Public Health. 2015;3. 10.3389/fpubh.2015.00134

[4] Bhattacharya I. Healthcare data analytics on the cloud. Online J Health Allied Sci. 2012;11. Available online at: https://www.ojhas.org/issue41/2012-1-1.htm25620855.

[5] Olaronke I, Oluwaseun O. Big data in healthcare: prospects, challenges and resolutions. In: 2016 Future Technologies Conference (FTC). IEEE; 2016. p. 1152–7.

[6] Ferdous M, Debnath J, Chakraborty NR. Machine learning algorithms in healthcare: a literature survey. In: 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT). IEEE; 2020. p. 1–6.

[7] Jiang F, Jiang Y, Zhi H, Dong Y, Li H, Ma S, et al. Artificial intelligence in healthcare: past, present and future. Stroke Vasc Neurol. 2017;2. 10.1136/svn-2017-000101.

[8] Kostkova P, Brewer H, De Lusignan S, Fottrell E, Goldacre B, Hart G, et al. Who owns the data? Open data for healthcare. Front Public Health. 2016;4:7. 10.3389/fpubh.2016.00007.

[9] Deepa N, Pham QV, Nguyen DC, Bhattacharya S, Prabadevi B, Gadekallu TR, et al. A survey on blockchain for big data: approaches, opportunities, and future directions. Future Gen Comput Syst. 2022;131:209–26. 10.1016/j.future.2022.01.017.

[10] Nakamoto S. Bitcoin: a peer-to-peer electronic cash system. Decentralized Bus Rev. 2008.

[11] Wood G. Ethereum: a secure decentralised generalised transaction ledger. Ethereum Proj Yellow Pap. 2014;151:1–32.

[12] Welfare GOIMOHF. Data from: Electronic health record (EHR) standards for India. Available online at: https://www.meity.gov.in/writereaddata/files/The%20Digital%20Personal%2%0Data%20Protection%20Bill%2C%202022_0.pdf (Accessed September 13, 2023).

[13] Goldstein MM, Jane HT. The first anniversary of the health information technology for economic and clinical health (HITECH) act: the regulatory outlook for implementation. Perspect Health Inf Manage. 2010;7.

[14] Hoofnagle CJ, Van Der Sloot B, Borgesius FZ. The European union general data protection regulation: what it is and what it means. Inf Commun Technol Law. 2019;28:65–98. 10.1080/13600834.2019.1573501.

[15] Piper T. The personal information protection and electronic documents act-a lost opportunity to democratize Canada's technological society. Dalhousie LJ. 2000;23:253.

[16] Pang PCI, McKay D, Chang S, Chen Q, Zhang X, Cui L. Privacy concerns of the Australian My Health Record: Implications for other large-scale opt-out personal health records. Inf Process Manage. 2020;57:102364. 10.1016/j.ipm.2020.102364.

[17] Dixit P, Gupta AK, Trivedi MC, Yadav VK. Traditional and hybrid encryption techniques: a survey. In: Perez G, Mishra K, Tiwari S, Trivedi M, editors. Networking Communication and Data Knowledge Engineering. Lecture Notes on Data Engineering and Communications Technologies. Singapore: Springer; 2018. Vol. 4. 10.1007/978-981-10-4600-1-22.

[18] Kashmar N, Adda M, Atieh M. From access control models to access control metamodels: a survey. In: Advances in Information and Communication: Proceedings of the 2019 Future of Information and Communication Conference (FICC). Springer. Vol. 2. p. 892–911.

[19] Selvaraj S, Sundaravaradhan S. Challenges and opportunities in IoT healthcare systems: a systematic review. SN Appl Sci. 2020;2:139. 10.1007/s42452-019-1925-y.

ISSN (online): 2581-3048
Volume 8, Issue 1, pp 201-208, January-2024
https://doi.org/10.47001/IRJIET/2024.801025

[20] Shah JL, Bhat HF, Khan AI. Integration of cloud and IoT for smart e-healthcare. In: Healthcare Paradigms in the Internet of Things Ecosystem. Elsevier; 2021. p. 101–36.

[21] Mehraeen E, Ghazisaeedi M, Farzi J, Mirshekari S. Security challenges in healthcare cloud computing: a systematic review. Glob J Health Sci. 2016; 9:157. 10.5539/gjhs.v9n3p157.

[22] Vanmathi C, Mangayarkarasi R, Hari Haran V, Karthikeyan S. A secure data transfer in cloud environment using double-layer security for internet of medical things. In: Soft Computing for Problem Solving: Proceedings of SocProS 2020. Springer; 2021. Vol. 2. p. 211–29.

[23] Chandrasekaran V, Sevugan P. Applying reversible data hiding for medical images in hybrid domain using haar and modified histogram. Int J Intell Eng Syst. 2017;10(4):126–34. 10.22266/ijies2017.0831.14.

[24] Dimitrov DV. Blockchain applications for healthcare data management. Healthc Inf Res. 2019; 25:51–6. 10.4258/hir.2019.25.1.51.

[25] Zhang S, Lee JH. Analysis of the main consensus protocols of blockchain. ICT Express. 2020; 6:93–7. 10.1016/j.icte.2019.08.001.

Citation of this Article:

Lakshmi Narasimhan Srinivasagopalan, "Enhancing Privacy and Security in Healthcare Insurance Claims: A Blockchain-Based Decentralized Framework for HIPAA Compliance" Published in *International Research Journal of Innovations in Engineering and Technology - IRJIET*, Volume 8, Issue 1, pp 201-208, January 2024. Article DOI https://doi.org/10.47001/IRJIET/2024.801025

****

