Journal of Human Dynamics (JHD)
ISSN: 3007-2816 (E), 3007-2808 (P)

Check for updates

ROOTS PRESS

Research Article

Integrating Blockchain Technology into Healthcare, A Decentralized Ledger That Improves Respect for Patients' Right to Privacy and Confidentiality

Hafiz Gulfam Ahmad Umar[1], Mariam Fareed [2], Sana Rubab[3], Romiza Rubab[4]

[1,2,3,4] *Department of Computer Science & IT, Ghazi University D.G. Khan. Pakistan.*

ABSTRACT

A patient's medical record is an essential tool for treatment and care. However, questions about privacy, interoperability, and data fragmentation have been brought to light by conventional EHR systems. The research here employs blockchain technology to safeguard the transfer and storage of patient data. Since blockchain transactions may be recorded across several computers in a decentralized manner, any future data changes will need updating each subsequent block. The study makes use of tools such as Ganache, Truffle, Metamask, ZKPs, IPFS, and RemixIDE. Blockchain validation is used for patient record retrieval; this procedure generates an encrypted Content ID and a decryption symmetric key. Further assurance of privacy and security is provided by the integration of Zero-Knowledge Proofs (ZKPs), which enable users to demonstrate record access privileges without disclosing sensitive information. In addition to boosting resilience and interoperability across systems, this decentralized strategy increases the confidentiality, integrity, transparency, and access management of healthcare data. The combination of blockchain technology with zero-knowledge proofs (ZKPs) increases the reliability of healthcare transactions by safely confirming data access between nodes.

Index Terms: Access control, Blockchain, Decentralization, Ethereum, Healthcare, Interoperability, patient records, Smart contracts, Solidity.

OPEN ACCESS

Correspondence
Hafiz Gulfam Ahmad Umar
hahmad@gudgk.edu.pk

Article History
Received: October 02, 2024
Accepted: November 14, 2024
Published: November 14, 2024

INTRODUCTION

To offer safe and appropriate care, it is essential to understand a patient's medical history, mental health concerns, and drug consumption. It shares diagnosis, treatment, and care plans to create a whole story for the patient's needs so that medical professionals can provide the right sort of help (li et al., 2023). without any error. Originally, such medical records were documented on paper which was subject to loss and tampering. The last decade has witnessed a significant transformation in the healthcare sector (Argaw et al., 2019). In the early 2000s, manual paperwork processes shifted to centralized electronic device management. Currently, patient data is centered around healthcare facilities and there are concerns about the reliability or accuracy in which those patient data points have been captured. Centralized medical data (usually kept within institutions), is at risk of manipulation, hacking, or getting lost like in a natural disaster causing the patient's info to be tampered with. Long-term reputation damage: Hospitals also suffer significant financial losses for many years due to the damages caused by their name in addition to immediate expenses like patient compensation

(Bani Issa et al., 2020). This access can be used to misuse private health information that can later turn out to be unjust, fraud, or even blackmail. When someone's health information is revealed without their permission, it could have detrimental effects on them. Penalties, fines, and legal costs related to data breaches and privacy violations may cause financial losses for organizations. Expenses for credit monitoring, contacting impacted parties, and putting security upgrades into place could also be incurred during remediation operations (Boiani, 2018). A high-level overview of attacks and data breaches affecting healthcare records that occurred between 2019 and 2024. A few noteworthy occurrences in Figure 1 are summarized by this graph. Given the public domain's susceptibility to healthcare data breaches and the absence of existing security standards, it is crucial to ensure the data's preservation and to offer a secure, feasible, and efficient means of facilitating data exchange and access among various stakeholders (Chen et al., 2019). Data spread among several nodes makes it more difficult for hackers to get all of the information at once. Distributing patient data reduces the likelihood of unauthorized access by making control less central. In this peer-to-peer network, the nodes set up a system where the group must authorize every ledger change (Chen et al., 2018). By using the consensus approach, we can make sure that everyone is on the same page regarding the present state of the system.

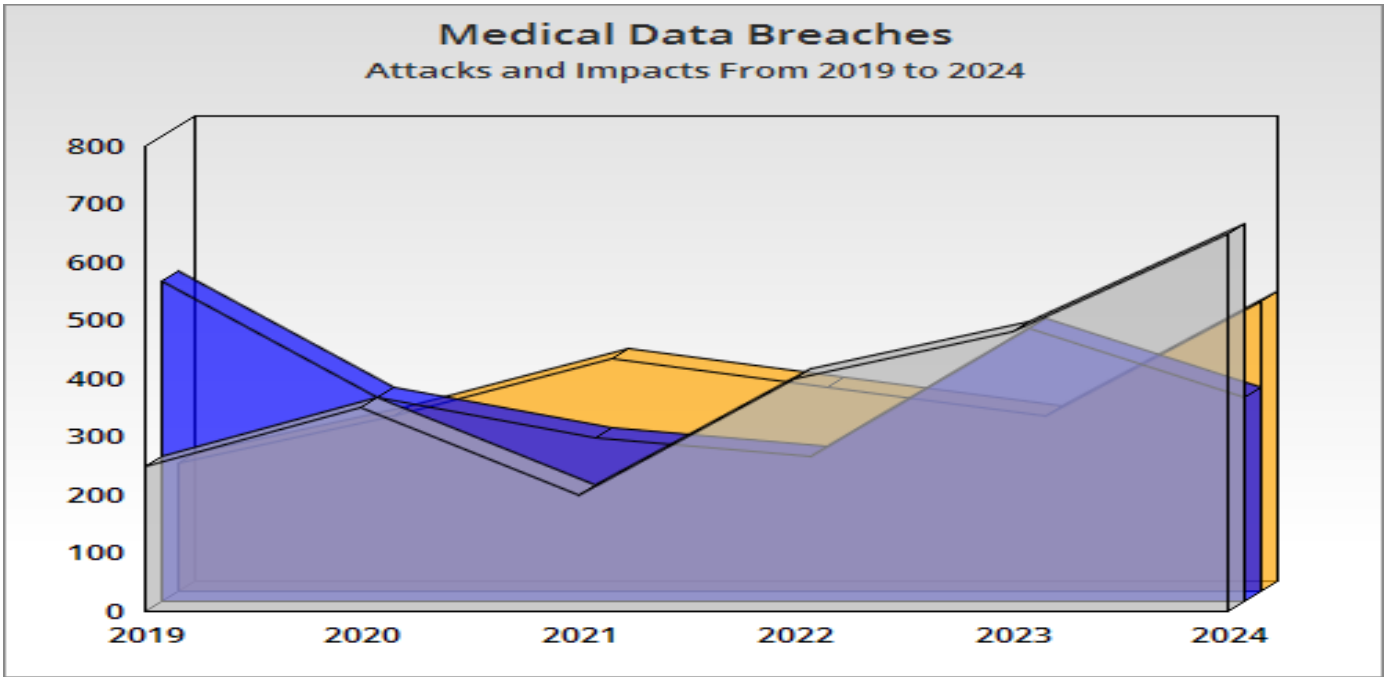

Figure 1. Annual Medical Data Breaches

Blockchain

Blockchain is a technology in which a transaction is recorded and added to a block whenever it occurs between two peers. Blockchain integrates every node to communicate in which many blocks are connected by encrypted hash functions. A revolutionary technology that allows for the safe and automated transmission of records is the blockchain. The creation of a block by one of the participants in a transaction starts the process (Chenthara et al., 2020). Thousands of computers spread out over the network are checking this block. Connecting the block to a chain allows for the creation of a distinct record with its history. So, when all the blocks involved in a blockchain agree via contracts, it's considered a legal transaction. Users must have faith in one another to share keys in a blockchain system since both the technology and trust are decentralized (Choi & Walker, 2019). Since the blockchain is a distributed ledger that may record transactions on several computers, updating any data in the future would need updating all blocks that follow it. Because of this, everyone involved in the blockchain may verify the transactions on their own and make a decent profit (Dagher et al., 2018). A blockchain database may be independently created via a peer-to-peer network. Their authentication has been approved by the majority of the network nodes. As seen in the illustration, a blockchain with this type of design might allow for efficient processing.2. Using a blockchain also fixes the problem of double-spending. Many different scenarios can benefit from blockchain technology (Dimitrov, 2019).
The distributed ledger technology known as blockchain has expanded beyond its initial use case of cryptocurrencies and is now present in a wide variety of other sectors (Dong et al., 2023).

https://doi.org/10.55627/jhd.002.02.0872

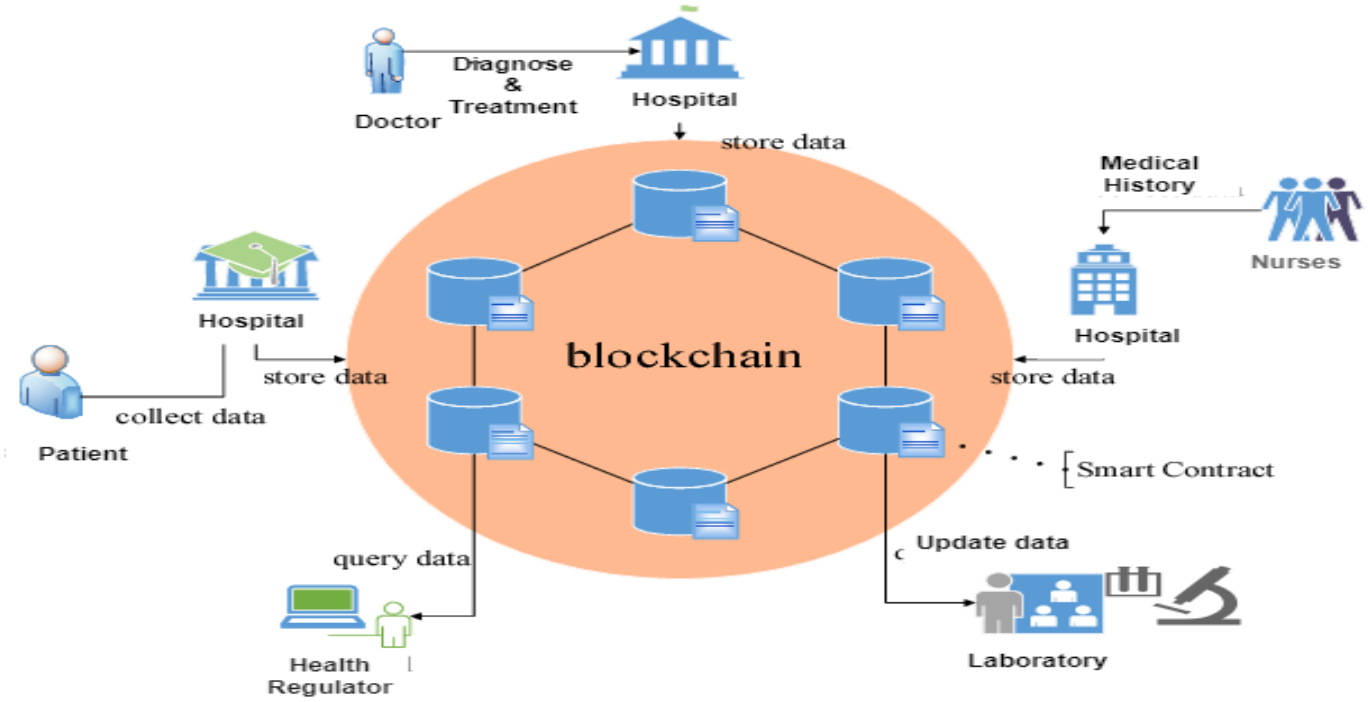

Figure 2. Blockchain Network

Working of Blockchain

In addition to Bitcoin, Ethereum is a significant cryptocurrency that was introduced in 2015. It was developed as a project based on a study that Vitalik Buterin had published two years earlier (Dubovitskaya et al., 2020). Ethereum as a Similar technology to that of Bitcoin was used to create a second blockchain; however, Ethereum added smart contracts, which enable logical code execution on top of the blockchain. A collection of data or transactions can be found in every block in the blockchain. These transactions might be financial transactions, the execution of smart contracts, or ownership records, among other kinds of information (Fiza et al., 2016).

Hash Function

To add new transactions to the blockchain, a new block must first be established. Before being added to the blockchain, a block is hashed. The data in the block is subject to hashing, a cryptographic process that converts inputs into strings of characters of a set length. The hashing algorithm used in blockchain technology generates a distinct hash value depending on the contents of each block (Goldsby& Hanisch, 2023). One way to represent an input, such as a "message," is as an alphabetical list; hashing is the process of transforming it into a string of characters of a defined length. To determine the residual when divided by p, this hash function adds up the ASCII values of each character in the input string. The generated hash value is an integer of a predetermined size. Hashing is a key component of blockchain technology that ensures data is secure, immutable, and intact. The ability to provide unique identifiers to digital assets, transactions, and blocks improves the security and efficiency of data storage and transmission in decentralized networks (Gordon & Catalini, 2018; Ali et al., 2023).

The fundamental steps in the hashing process are shown in Figure 3:

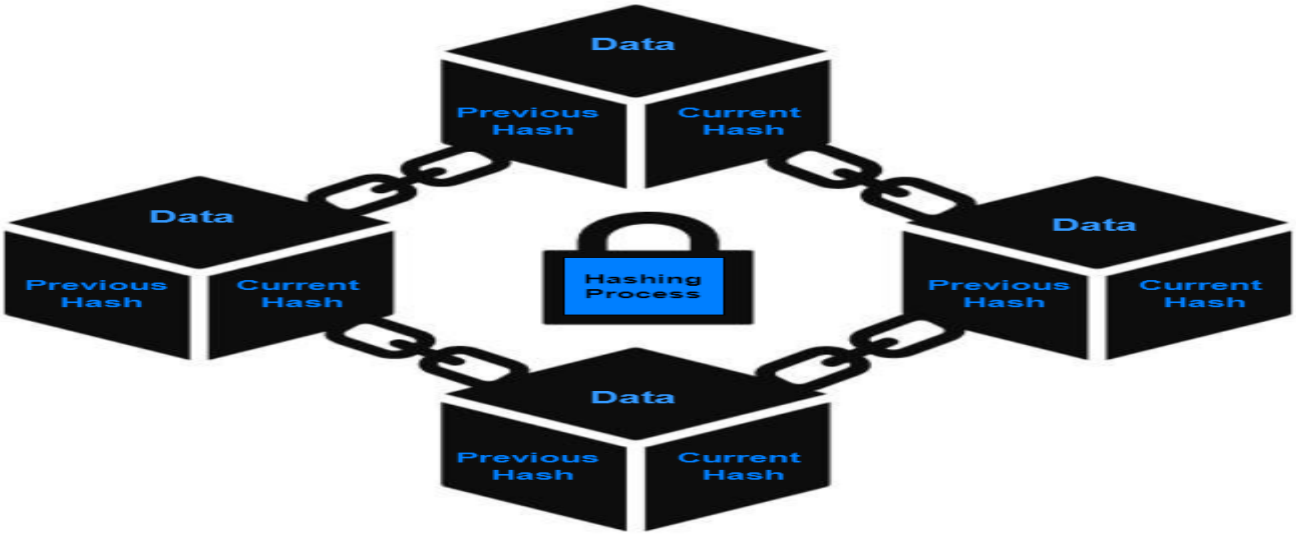

Figure 3**.** Hash Function of Blockchain

RELATED WORK

Encrypting electronic health records is crucial (Zhao et al., 2023) and In attempting to categorize encrypted EHRs, managers encounter a conundrum. Regardless of the encryption method, EHRs are also predictable and guessed. In this research, we offer a safe strategy to help categorize encrypted EHRs based on certain keywords. They focused on risks to EHR predictability posed by storage servers and group administrators guessing. We can see that their strategy is practical and efficient from the trial outcomes. The main objective of this study (Dong et al., 2023) is to create and evaluate a model for a platform for exchanging personal health records (PHRs) that makes use of blockchain technology and offers the necessary degree of privacy, control, and granularity inpatient authorization. Building on their work on a BAC model, they developed a blockchain-enabled PHR sharing platform that gives patients control over the degree of privacy, permission, and confidentiality that is enforced. Health organizations that have access to patients' electronic health records (EHRs) will only do so after patients verify their identities. This study (Wu et al., 2021) uses blockchain technology to effectively apply anti-theft measures and secure information.

Furthermore, a cutting-edge platform is developed, leveraging the power of blockchain technology to securely store private information. To ensure utmost security, cryptographic algorithms are employed for seamless transmission of data. Recently, blockchain in healthcare has been on everyone's lips - and for good reason: the potential uses of this promising technology are generating headlines by nature at a frenetic pace. This research also starts with a systematic literature review of the b as mul pu projects that propose applying blockchain to EHR, but uniquely focused on privacy and security (Shi et al., 2020). Such a review can be very helpful in understanding why EHR or blockchain proprietary systems are highly limited. We also point out many areas for research that entail a wide range of problems and opportunities.

A Possible Solution Thanks to blockchain technology, it may now be time for a reboot of how we think about medical records. A decentralized, peer-to-peer network for exchanging healthcare records based on blockchain technology may change this paradigm and make record exchanges more secure. A new, lightweight blockchain framework is implemented in this study for the secure storage and dissemination of patient level status change information as well as complete disease diagnosis transactions (Thabit et al., 2024). Efficient and Patient-Oriented Electronic Health Care Certification System? -Results from a Survey on Nursing Staff.

It Makes the Security of EHR systems First with Blockchain Technology as they use encryption etc. Central points of failure and attack vectors, which are mostly also avoided due to the decentralized nature of this technology. The goal of this paper (Kiania et al., 2023) is to conduct a systematic review of the literature (SLR) on blockchain technology and its applications in improving the security and privacy of Electronic Health Systems. They elaborate upon the list of points, type of Blockchain, evaluation measures & approaches used by each paper they have selected. Discussion

of outstanding issues, new research directions, and hurdles concludes the essay. Based on blockchain technology, a cyber-physical healthcare sector 4.0 architecture was introduced by Kumar et al. (2023) to facilitate trustworthy and secure data sharing. Various encryption methods such as AES, BigchainDB, Tendermint, IPFS, and MongoDB are utilized in the proposed system to enrich Healthcare 4.0.

The suggested paradigm places the patient in charge of their data and prioritizes security and privacy. However, protecting patients' privacy seems challenging due to the sensitive nature of medical records. Sharing electronic health information can increase diagnosis accuracy, even when there are major systemic issues about privacy and security. The immutability features of blockchain technology have led to its proposal as a possible solution to secure and privately transmit individual health information. According to Naser Alsuqaih et al. (2023), blockchain technology has several advantages, including speed, security, and the ability to significantly lower compute and storage expenses. A thorough comparison of several existing platforms and data storage models is provided by the study of relevant work. Table.1, it is indicated whether or not the smart contract was used in the preceding framework.

Table 1. Analysis of Related WorkThe present research employs ZKP, smart contracts, and off-chain storage to

Author name	Year	Platform	Data Storage Model	Smart contract
Randa kamal	2022	Public	Decentralized	yes
Osama A. Khashan	2023	Hybrid	Decentralized	No
Zhiliang Zhao	2023	Both (private & Hybrids)	Centralized	No
Andrew J	2023	Hybrid	Decentralized	yes
Hanan Naser Alsuqaih	2023	Hybrid	Decentralized	No
Mohit kumar	2023	Hybrid	Decentralized	yes
Kianoush Kiania	2023	All	Decentralized	No

safeguard the transfer and storage of patient records using blockchain technology. Giving patients more power and accessibility, it generates an immutable, sequential, and irreversible record. Better data management leads to cost savings for healthcare providers and payers.

The structure of this research is as follows: Provides works of literature or allied subjects. In Section 3, we go over the functions and tools that were used for this study. In this section, we also go into the research methods that were employed. Section 4 displays the visual results and examines how well this notion improved security, with an emphasis on feature fragmentation and interoperability. The conclusion and next efforts are explained in section 5.

PROBLEM STATEMENT AND PROPOSED SOLUTION

Problem Description

Interoperability in traditional EHR systems suffers from record fragmentation and centralization issues, posing significant challenges to crisis response and disaster management. Most patients lack control over their information, rendering it susceptible to unauthorized access and modification. There is a critical necessity for an enhanced system to improve data security, interoperability, and patient ownership of health records.

Solution Framework

To ensure the safe transfer and preservation of patient information, this makes use of blockchain technology. Since every transaction on the blockchain has an immutable hash signature, it is practically hard to alter the data contained inside. This study makes use of the following tools and functions: RemixIDE, IPFS, truffle, ganache, and ZKP. The combination of these technologies allows for encrypted storage, safe access management, and data integrity, all of which contribute to the security of patient information on a blockchain.

METHODOLOGY

Distributed Ledger Technology and Blockchain

The nodes computers that make up a distributed ledger system are linked in a scattered fashion, much like peer-to-peer networks, making it a decentralized database. Independent ledgers will be maintained by each node in DLT. All of the nodes follow the same security measures and protocols. Nodes validate the deal by reaching a unanimous

decision. With blockchain and other decentralized ledger technologies, any node may keep its records autonomously. Every node in a blockchain uses consensus algorithms to confirm each transaction. Each node in a blockchain maintains its recorder, making it a decentralized ledger.

Smart Contract

Authorized parties can post Solidity-written, self-executing programs called "smart contracts" on channel peers. Among these are the regulations that control certain types of network transactions. Smart contracts address the system's application logic for electronic health record transactions, including data transmission, access management, and request handling. These tasks include updating medical records, allowing doctors to write referrals to other doctors, updating ownership, and electronically sending prescriptions to pharmacists. Medical record access rights may be identified, validated, granted, and changed through user interactions with smart contracts. The benefit of smart contracts is that they are transparent and self-executing; once they are added to the blockchain, they cannot be stopped.

Secure Hash Algorithm 3

Password encryption using the SHA3 algorithm is a cryptographic technique. Because the hash function is deterministic, hashed passwords do not change, even if SHA-3 is a very strong hash algorithm. So long as the inputs remain constant, the outputs will also remain constant. That makes it easier for the attacker to find the password that corresponds to that hash. After the password has been found, it may be used to access any accounts that have the same hash. The use of salt has been implemented to tackle this problem. This is what salt means. To encrypt passwords, we utilized a chaotic map, which is one of the strongest encryption algorithms but also has a highly sensitive beginning condition. Logistic maps, which are two-dimensional and filled with disorder, are a common sort of chaotic map. Several workable ideas for logistic maps have been put forward. There are three requirements for selecting one: a Mixing Property, Robust Chaos, and Large Parameter. A regular logistic map will be used to examine all of the attributes

Consensus algorithms

In a blockchain network, there is no trustworthy central authority. Therefore, a variant of the Byzantine Generals (BG) Problem—getting untrustworthy nodes to agree on these transactions—is a critical issue in dispersed networks. The Byzantine army is told by a group of generals to surround the city; they will not have a chance of victory until they all assault at the same time. Therein is the BG conundrum. However, they do not know whether there are betrayers who may retreat in a scattered situation. This forces them to choose between fighting or retreating. The same problem also affects the blockchain network.

POW (Proof of Work)

To protect the network from hackers, PoW uses a mathematical puzzle. Cryptocurrency is awarded to nodes using PoW, which stands for proof of work. As with P2P file sharing, the process entails adding the block to the Blockchain and updating the data across the network. The wheels are in motion. As soon as the initial user requests a transaction over the blockchain upon login. One of the many nodes that have the block receives the verified transaction and sends it on its way. Nodes verify the transaction using the block and distributed data on the blockchain.

The addition of this validated transaction completes a secure blockchain transaction.

Hash Function

$$\mathrm{H}\,(\mathrm{input}) = \mathrm{Hash\ Output} \quad \lambda \qquad (1)$$

Where input includes the block data and nonce.

Target Difficulty

$$\mathrm{H}\,(\mathrm{Block\ Data} \| \mathrm{Nonce}) \leq \mathrm{T} \qquad (2)$$

Where T is the target threshold set by the network.

Finding a Valid Nonce

Find Nonce such that

H (Block Data ‖ Nonce) ≤ T (3)

Proof of Work Validation

Proof of Work Valid if $\mathbf{H\,(Block\ Data\ \|\ Nonce) \leq T}$ $\mathbf{(4)}$

All the pertinent information from the block is included in Block Data, which is represented by H in these equations,

https://doi.org/10.55627/jhd.002.02.0872

and miners vary Nonce to get a suitable hash. The POW challenge's complexity is defined by the objective T. Web.3, Ganache, Truffle, Metamask, NIZK, IPFS, and RemixIDE are the technologies and functionalities utilized in this thesis.

Web.3

The Hypertext Transfer Protocol (HTTP) connection allows Web3 to access the Ethereum network via an Ethereum node. This Ethereum node has the option to run either locally on the Ethereum wallet or remotely. On the other hand, MetaMask is a browser extension that integrates seamlessly with websites and simplifies the management of Ethereum accounts.

Ganache

You may deploy smart contracts and run tests on Ganache, a local development blockchain that functions like a public blockchain. Ganache provides ten accounts with one hundred Ethereum to trial the smart contracts on the local blockchain nodes.

Truffle

When working with Ethereum smart contracts, a truffle is a useful tool. An integrated smart contract compiler is a feature of the command-line program Truffle. Not only may it be utilized for the aforementioned tasks, but it also offers a platform for testing automated contracts, managing networks and packages, and linking smart contracts.

Metamask

Featuring a graphical user interface (GUI), Metamask is an easy-to-use, open-source solution for Ethereum transactions. You can run an Ethereal Dapp using the framework browser even if you don't have access to a full Ethereum hub. Using Metamask is like plugging a user's browser into the Ethereum network.

Remix ide

When it comes to developing smart contracts, many people prefer using Remix IDE, a popular browser-based IDE.

Solidity

Solidity is a high-level language that focuses on contracts and is ideal for building smart contracts. The high-level statically typed programming language Solidity has reached Turing completeness. Its creators drew inspiration from Python, JavaScript, and C++, and the EVM is its target. Solidity is statically typed, has inheritance, and allows for sophisticated user-defined types. It also supports libraries. Voting, blind auctions, crowdsourcing, multi-signature wallets, and countless other uses are all within Solidity's purview.

Language

Languages such as Next.js, React.js, CSS, and HTML are utilized in the front-end design process of websites. The SHA-3 cryptographic algorithm is written in the Solidity programming language for use in smart contracts. Truffle and Ganache, two tools for building local Ethereum blockchains, were used to design the system.

Zero Knowledge proof

One cryptographic approach that ensures privacy and security is Zero-Knowledge Proof (ZKP). It allows one party to verify another without giving sensitive information. For password authentication and cryptocurrency ownership verification, it is extensively utilized in privacy-oriented protocols and blockchain systems as in Figure 3.

- **NIZK**

Non-Interactive Zero-Knowledge Proof is an additional cryptographic method that allows one side to guarantee another side regarding a certain piece of information without disclosing any knowledge. Data validation without revealing vital details is made possible by NIZKs, which greatly improves the efficiency, privacy, and security of blockchain systems.

By enabling users to validate particular parts of their identity or transaction without revealing personal information, NIZKs solve privacy and scalability problems in blockchain technology. Additionally, by doing away with repeated contacts, decreasing communication costs, and speeding up verification, they improve the scalability of distributed systems.

When it comes to blockchain, NIZKs play a big role in protecting user privacy, guaranteeing scalability, and enhancing security. While zk-STARKs and zk-SNARKs streamline processing and data sharing to make verification easier, zk-SNARKs ensure the proper output from a valid input by expressing computation as a system of polynomials.

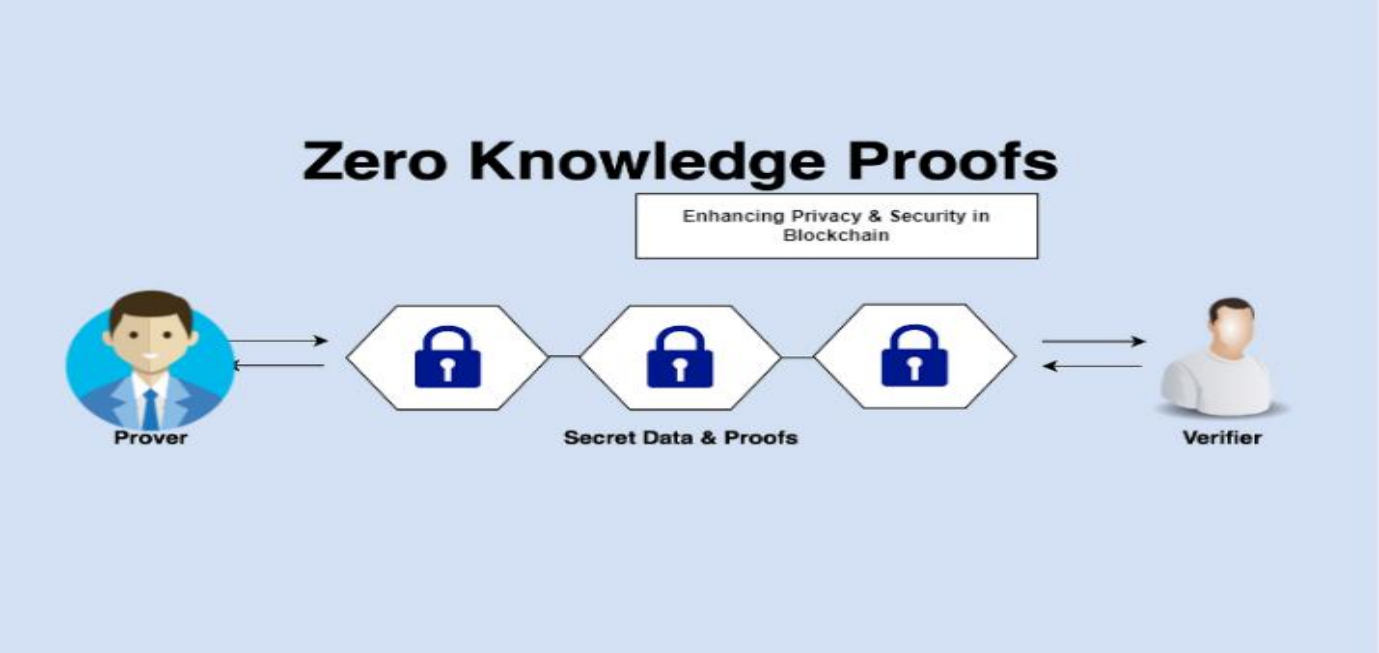

Figure 4. Zero Knowledge proof

The primary QAP equation:

$$P(x) = \sum i = 1 \ ai(x) \cdot b\, i(x) = t(x) \cdot h(x) \quad (5)$$

ai(x)·bi(x) Polynomials denote the inputs and outputs, respectively. The target polynomial is t(x). The quotient polynomial is denoted by h(x).

Elliptic Curve Pairing Equation:

$$e\,(A, B) = e\,(C, D) \quad (6)$$

This is where e represents the bilinear pairing process. Points A, B, C, and D on an elliptic curve are those that result from using public and witness parameters.

Setup Phase: During the setup step, the public parameters pk and vk are generated. A setup's equation looks like this:

$$\text{Assuming key} = \left(G_1^{\alpha}, G_1^{\beta}, G_1^{\gamma}, G_1^{\delta}, \ldots.\right) \quad (7)$$

$$\text{Verification key} = (G_2^{\alpha}, G_2^{\beta}, G_2^{\gamma}, G_2^{\delta}, \ldots.) \quad (8)$$

Assuming that $G1$ and $G2$ are elliptic curve groups α, β, γ, and δ are secret values produced during setup.

Zk-SNARK Proof Generation:

The prover uses elliptic curve operations and a polynomial P(x) to compute a proof:

$$\pi = (A, B, C) \quad (9)$$

where: $A=g^{P(a)}$, $B=g^{P(b)}$, $C=g^{p(c)}$ are the product of g and P(c). a, b, c, and d are witness values, and g is an elliptic curve group generator.

Zk-SNARK Proof Verification: The verifier ensures that the proof and verification key are compatible by checking if the pairing equation is true:

$$e\,(\pi A, \pi B) = e\,(vk\,A, vk\,B) \quad (10)$$

Where π Aand π B are components of the demonstration. vk A,vk B are components of the verification key. Central to the zk-SNARK architecture are these equations, which provide efficient and accurate proof without disclosing any statement specifics.

The steps are shown in Figure 5.

https://doi.org/10.55627/jhd.002.02.0872

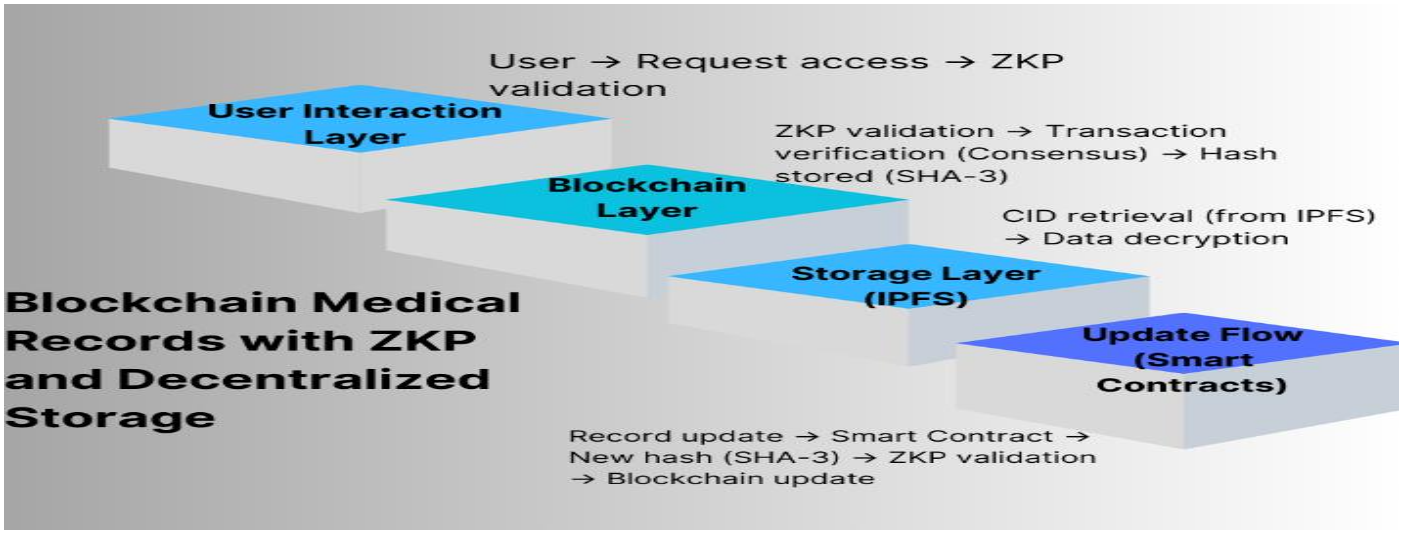

Fig 5**.** Blockchain medical record with ZKP steps

Smart Contract Deployment and Interaction

There is a predetermined procedure for creating smart contracts for blockchain-based patient records. To begin, the platform Remix IDE is used to construct smart contracts using the Solidity language. Compiling the functions and done using the Remix IDE. The Truffle development framework is used to deliver these files. The blockchain will incorporate these smart contracts so that they may be monitored and executed automatically. For the safety of patient records, IPFS (Interplanetary File System) should use Secure Hash Algorithm 3. Using SH-3 and ZKP for validation, we get a one-of-a-kind hash value for the data. The data and hash value are both stored in IPFS. For improved security and privacy, it is recommended to encrypt medical records using SHA-3 and ZKP before uploading them to IPFS. The storage is guaranteed to be safe because it is encrypted and decentralized. An encrypted CID and patient record will be sent to the user when they request and are confirmed by blockchain. As seen in Figure 6, the EHR may be securely retrieved from IPFS and a symmetric key for decryption can be obtained from the server using the CID.

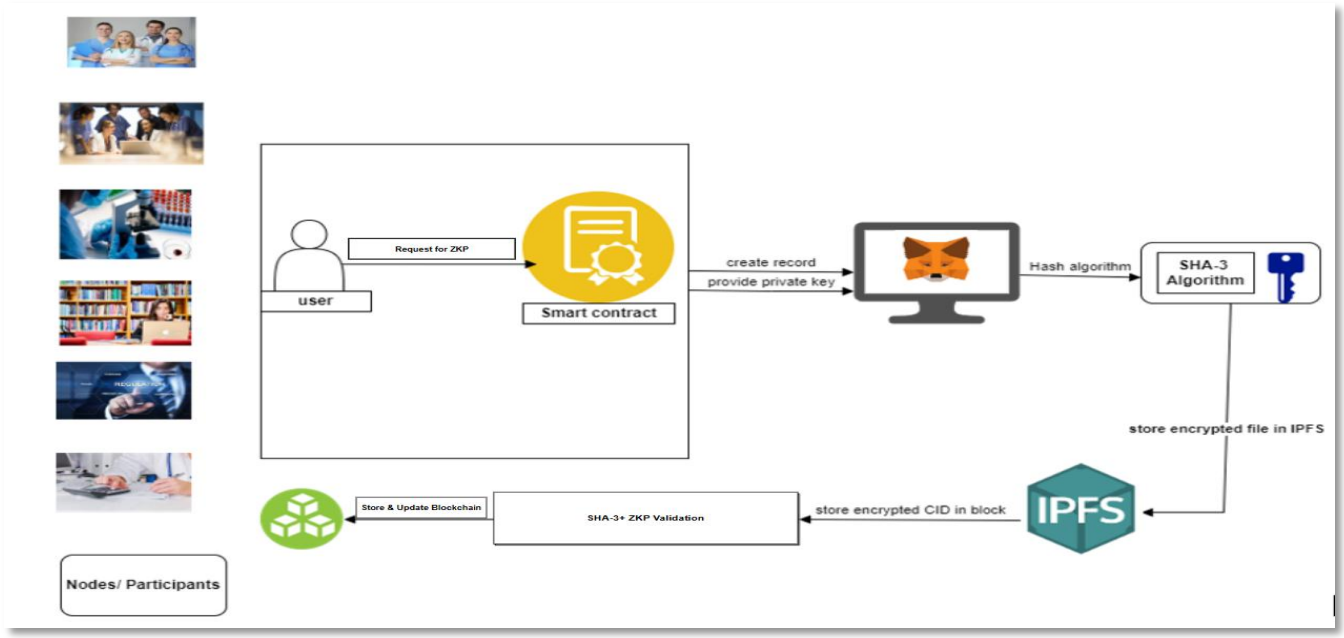

Fig 6. Process of storing patient records on Blockchain

RESULT AND DISCUSSION

Using public keys for encryption and private keys for decryption, the system encrypts sensitive data. Ensuring that just the sender and the recipient possess knowledge of each other's private keys safeguards the communication's

secrecy. Having said that, sharing public keys between several people won't compromise security. The blockchain network processes the transactions, which include the encrypted patient health records and relevant metadata. To ensure that all transactions follow the rules and consensus procedures of the blockchain network, the nodes in the network confirm them. To verify the authenticity of digital signatures on transactions, validators utilize the public keys associated with the sender URL. The semantic and syntactical correctness of transactions is also checked. Multiple security measures are enhanced using blockchain technology for medical patient transactions, as seen in Figure 7 and described in the table.2:

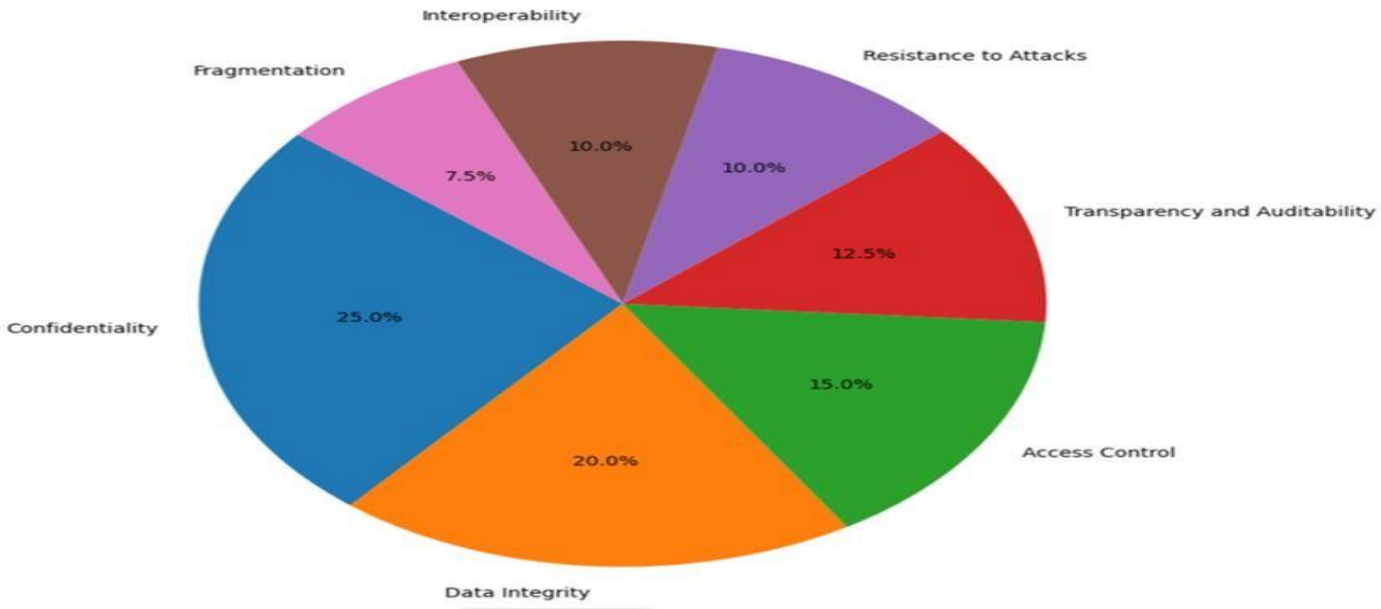

Figure 7. Enhanced features in the proposed methodology

Table 2. Comparison of existing approaches and proposed solution

Features	(3)	Mahajan, (2024)	Shah, V, (2023)	CHELLADURAI, (2021)	Kumar et al., (2023)	Proposed idea
Confidentiality		□	□□	□	□	□
Access control		□	□□	□	□	□
Transparency		□	□□	□	□	□
Data integrity		□	□□	□	□	□
Resilience		□		□ □	□	□
Interoperability		□		□ □	□	□
Fragmented		□		□ □	□	□

Figure 8 shows the resultant graph of the computational problems associated with several healthcare blockchain integration features. On the y-axis, you can see the computational complexity scores that were given to each part. A higher score indicates a more demanding computational or temporal need. The height of each bar represents the difficulty score of that element.

The graph illustrates the relationship between the data size and the time needed to compute the SHA-3 hash within the context of IPFS (Interplanetary File System). As the data size expands along the x-axis, the y-axis shows that the time required for the hashing method also climbs. Computing SHA-3 hashes for larger data sets so requires more computational resources in Figure. 9.

https://doi.org/10.55627/jhd.002.02.0872

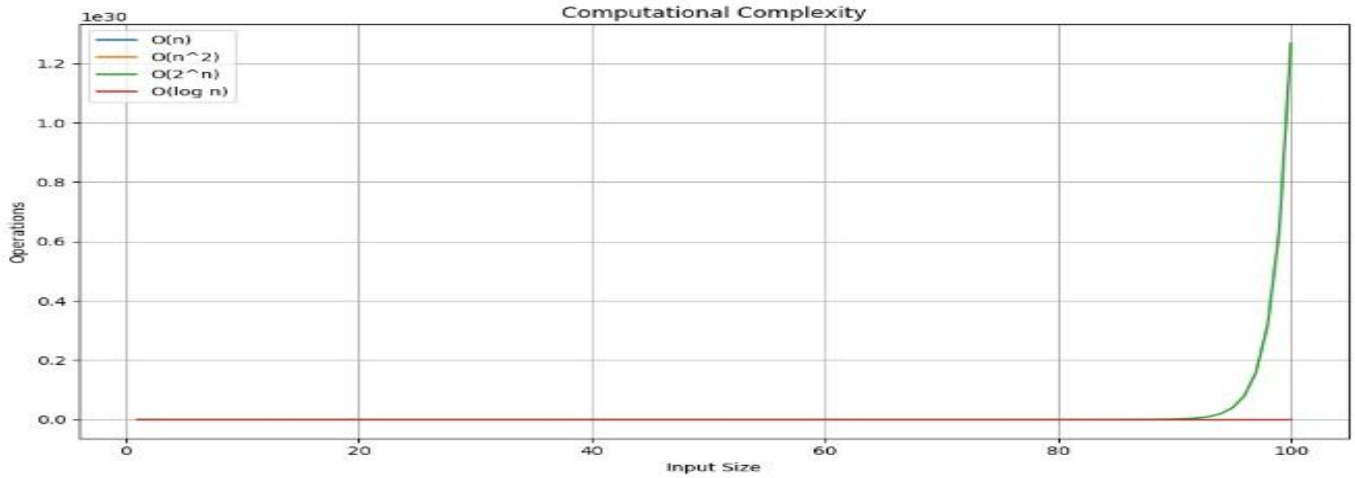

Figure 8. Computational Complexity

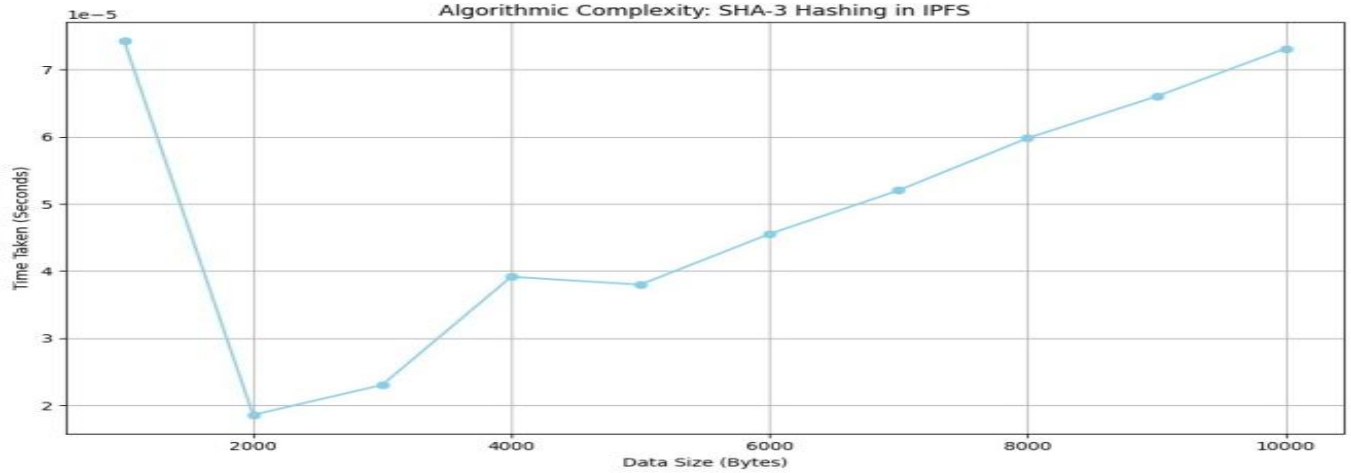

Figure 9. Algorithm Complexity

Figure. 10 is a graph illustrating the relative strengths of several countermeasures in a healthcare blockchain integration system concerning quantum assaults. The range is shown by the height of the bar. A general overview of the system's resilience landscape is offered by the graph, which graphically depicts the distribution of resilience scores. The graph illustrates the system's resistance to several forms of assaults in a healthcare scenario that incorporates blockchain technology. As seen in the graphic, the average success rate of several attack types is shown by each bar. These types include man-in-the-middle attacks, data breaches, quantum assaults, and DDOS malware injection Figure 11. The x-axis of the figure.12 displays the request rate in bps, while the y-axis represents the response time in ms, which is the latency. Consistent with the scenario's projected relationship, the latency decreases as the RC increases. We have highlighted each data point with a circle marker and connected them with a solid line to better visualize the trend.

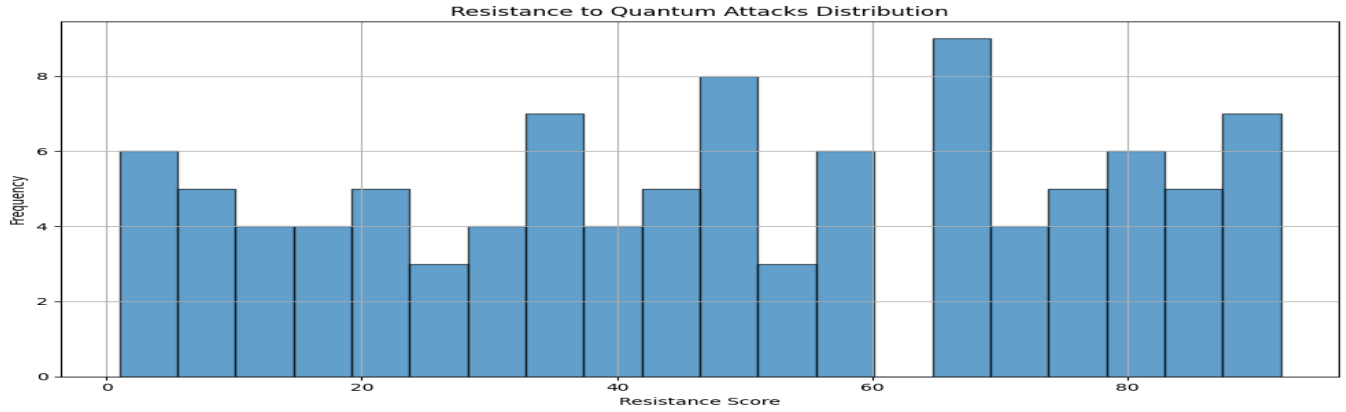

Figure 10. Resistance to Quantum Attacks

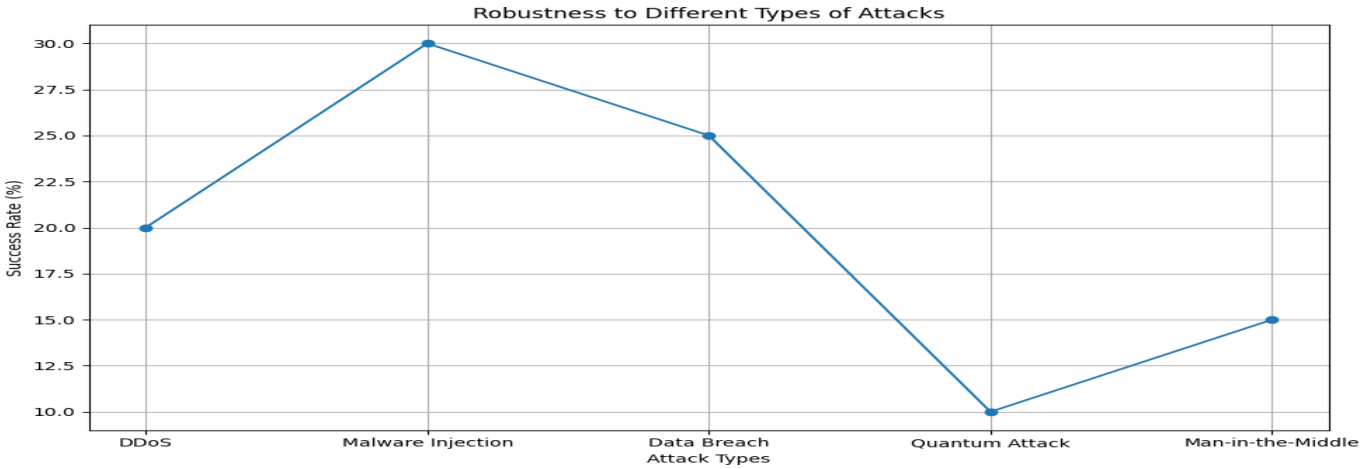

Figure 11. Robustness to Different Types of Attacks

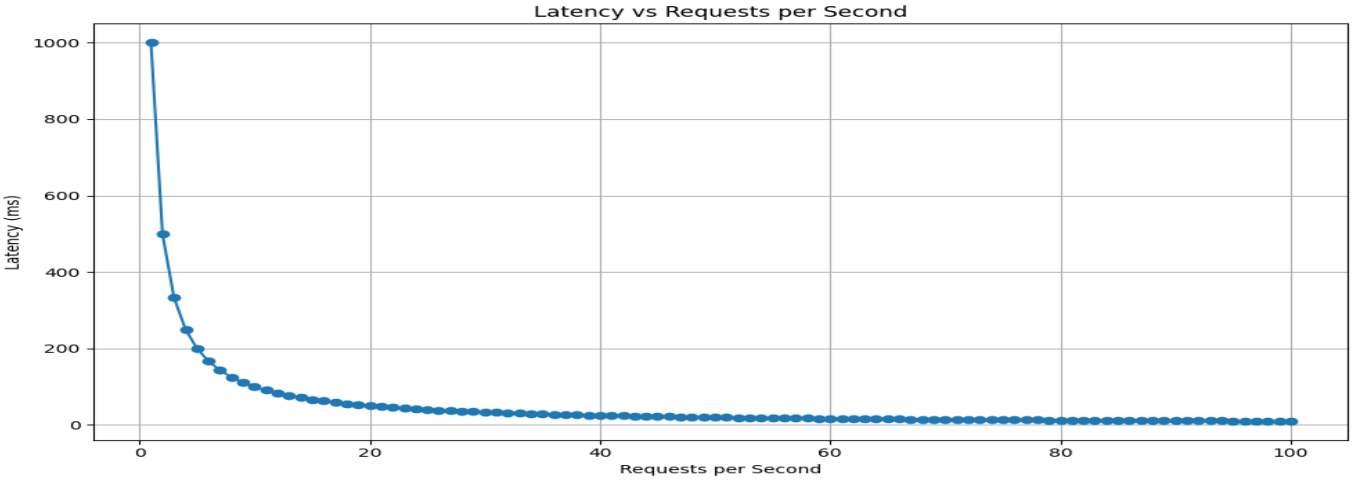

Figure 12. Latency VS Requests Per Seconds

CONCLUSION AND FUTURE WORK

This study presents a decentralized blockchain-based management system that puts patients' interests first by regulating access to their medical information, facilitating cross-blockchain communication between physicians and patients, and securely assigning decision-making authority over data sharing. Our method gives patients the agency to control their health records and other personal information. Patients, including those who are unconscious or experiencing an emergency, may control who has access to their information and when.

With full functionality and complete safety guaranteed, our suggested system maintains decentralization and traceability in every process. In our method, we employ the concept of verifier nodes, which are present in all networks and may establish connections with other nodes across different networks. The security, constraints, problems, and generalizability of our proposed solutions to additional use cases are also reviewed and evaluated. A potential path for future studies might be to develop and deploy complete smart contract algorithms capable of handling a wider range of practical situations. Realistic testing of network latency, response time, execution fees, and gas prices may be achieved by integrating current Oracle node technologies into a public Ethereum testnet and running the built-in smart contracts. For definitive security analysis, use quantitative penetration testing with a robust methodology that can assess attack vectors specific to blockchains.

ACKNOWLEDGMENTS

The authors would like to thank almighty Allah first and then the chairperson of Computer Science and IT, GUDGK, Pakistan, for their support and assistance throughout this study.

https://doi.org/10.55627/jhd.002.02.0872

AUTHORS CONTRIBUTIONS

All the authors equally contributed to this study.

CONFLICT OF INTEREST

The authors declare no conflict of interest and confirm that this work is original and not plagiarized from any other source, i.e., electronic or print media. The information obtained from all of the sources is properly recognized and cited below.

DATA AVAILABILITY STATEMENT

The testing data is available in this paper.

FUNDING

This research received no external funding.

REFERENCES

Ali, H., Shafiq, H., Aisha, Z., Iftikhar, M., Iftikhar, N., Ai, H., (2023). Good Food Score Reflecting Health Status of the Families: A Predicting Approach through Machine Learning. OEconomia, *6*(2), 313-329.

Argaw, S. T., Bempong, N. E., Eshaya-Chauvin, B., & Flahault, A. (2019). The state of research on cyberattacks against hospitals and available best practice recommendations: A scoping review. BMC Medical Informatics and Decision Making, 19(1), 1–11. https://doi.org/10.1186/s12911-018-0724-5

Bani Issa, W., Al Akour, I., Ibrahim, A., Almarzouqi, A., Abbas, S., Hisham, F., & Griffiths, J. (2020). Privacy, confidentiality, security and patient safety concerns about electronic health records. International Nursing Review, 67(2), 218–230. https://doi.org/10.1111/inr.12585

Boiani, F. (2018). Blockchain Based Electronic Health Record Management For Mass Crisis Scenarios. A Feasibility Study. Undefined. Published.

Chen H.S., Jarrell J.T., Carpenter K.A., Cohen D.S, H. X. (2019). Blockchain in Healthcare: A Patient-Centered Model. Biomedical Journal of Scientific & Technical Research, 10(3), 1–10.

Chen, Y., Ding, S., Xu, Z., Zheng, H., & Yang, S. (2018). Blockchain-Based Medical Records Secure Storage and Medical Service Framework. Journal of Medical Systems, 43(1). https://doi.org/10.1007/s10916-018-1121-4

Chenthara, S., Ahmed, K., Wang, H., Whittaker, F., & Chen, Z. (2020). Healthchain: A novel framework on privacy preservation of electronic health records using blockchain technology. In PLoS ONE (Vol. 15, Issue 12 December). https://doi.org/10.1371/journal.pone.0243043

Choi, P., & Walker, R. (2019). Remote Patient Management: Balancing Patient Privacy, Data Security, and Clinical Needs. Contributions to Nephrology, 197, 35–43. https://doi.org/10.1159/000496312

Dagher, G. G., Mohler, J., Milojkovic, M., & Marella, P. B. (2018). Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. Sustainable Cities and Society, 39, 283–297. https://doi.org/10.1016/j.scs.2018.02.014

Dimitrov, D. V. (2019). Blockchain applications for healthcare data management. Healthcare Informatics Research, 25(1), 5156. https://doi.org/10.4258/hir.2019.25.1.51

Dong, Y., Mun, S. K., & Wang, Y. (2023). A blockchain-enabled sharing platform for personal health records. Heliyon, 9(7), e18061. https://doi.org/10.1016/j.heliyon.2023.e18061

Dubovitskaya, A., Baig, F., Xu, Z., Shukla, R., Zambani, P. S., Swaminathan, A., Jahangir, M. M., Chowdhry, K., Lachhani, R., Idnani, N., Schumacher, M., Aberer, K., Stoller, S. D., Ryu, S., & Wang, F. (2020). ACTION-EHR: Patient-centric blockchain-based electronic health record data management for cancer care. Journal of Medical Internet Research, 22(8), 1–15. https://doi.org/10.2196/13598

Fiza, A. R., Lizawati, S., Zuraini, I., & Narayana, S. G. (2016). Safety and privacy issues of electronic medical records. Indian Journal of Science and Technology, 9(42), 1–8. https://doi.org/10.17485/ijst/2016/v9i42/100811

Goldsby, C. M., & Hanisch, M. (2023). Agency in the algorithmic age: The mechanisms and structures of blockchain-based organizing. Journal of Business Research, 168(November 2022), 114195. https://doi.org/10.1016/j.jbusres.2023.114195

Gordon, W. J., & Catalini, C. (2018). Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability. Computational and Structural Biotechnology Journal, 16, 224–230. https://doi.org/10.1016/j.csbj.2018.06.003

Gugueoth, V., Safavat, S., Shetty, S., & Rawat, D. (2023). A review of IoT security and privacy using decentralized blockchain techniques. Computer Science Review, 50, 100585. https://doi.org/10.1016/j.cosrev.2023.100585

Guo, H., & Yu, X. (2022). A survey on blockchain technology and its security. Blockchain: Research and Applications, 3(2), 100067. https://doi.org/10.1016/j.bcra.2022.100067

J, A., Isravel, D. P., Sagayam, K. M., Bhushan, B., Sei, Y., & Eunice, J. (2023). Blockchain for healthcare systems: Architecture, security challenges, trends and future directions. Journal of Network and Computer Applications, 215(September 2022), 103633. https://doi.org/10.1016/j.jnca.2023.103633

Khashan, O. A., & Khafajah, N. M. (2023). Efficient hybrid centralized and blockchain-based authentication architecture for heterogeneous IoT systems. Journal of King Saud University - Computer and Information Sciences, 35(2), 726– 739. https://doi.org/10.1016/j.jksuci.2023.01.011

Kiania, K., Jameii, S. M., & Rahmani, A. M. (2023). Blockchain-based privacy and security preserving in electronic health: a systematic review. Multimedia Tools and Applications, 82(18), 28493–28519. https://doi.org/10.1007/s11042-023-14488-w

Kumar, M., Raj, H., Chaurasia, N., & Gill, S. S. (2023). Blockchain inspired secure and reliable data exchange architecture for cyber-physical healthcare system 4.0. Internet of Things and Cyber-Physical Systems, 3(May), 309– 322. https://doi.org/10.1016/j.iotcps.2023.05.006

li, A. A. M. A., Hazar, M. J., Mabrouk, M., & Zrigui, M. (2023). Proposal of a Modified Hash Algorithm to Increase Blockchain Security. Procedia Computer Science, 225, 3265–3275. https://doi.org/10.1016/j.procs.2023.10.320

Madine, M. M., Battah, A. A., Yaqoob, I., Salah, K., Jayaraman, R., Al-Hammadi, Y., Pesic, S., & Ellahham, S. (2020). Blockchain for Giving Patients Control over Their Medical Records. IEEE Access, 8, 193102–193115. https://doi.org/10.1109/ACCESS.2020.3032553

Shrestha, S., & Panta, S. (2023). Blockchain-based Electronic Health Record Management System. Journal of Artificial Intelligence and Capsule Networks, 5(3), 298–313. https://doi.org/10.36548/jaicn.2023.3.006

Singh, A., Salvi, A., Pawar, K., Prabhu, A., & Bavkar, D. (2022). Blockchain based system to store and retrieve healthcare records. International Research Journal of Engineering and Technology, 2640–2644. www.irjet.net

Thabit, F., Ibrahim, Y., Thabit, T. A., & Yousef, K. (2024). Implementing Blockchain for Secure Electronic Medical Certifications: An Analytical Study. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4714110

Thwin, T. T., & Vasupongayya, S. (2019). Blockchain-Based Access Control Model to Preserve Privacy for Personal Health Record Systems. Security and Communication Networks, 2019. https://doi.org/10.1155/2019/8315614

Tith, D., Lee, J. S., Suzuki, H., Wijesundara, W. M. A. B., Taira, N., Obi, T., & Ohyama, N. (2020). Application of blockchain to maintaining patient records in electronic health record for enhanced privacy, scalability, and availability. Healthcare Informatics Research, 26(1), 3–12. https://doi.org/10.4258/hir.2020.26.1.3

Wu, H., Dwivedi, A. D., & Srivastava, G. (2021). Security and Privacy of Patient Information in Medical Systems Based on Blockchain Technology. ACM Transactions on Multimedia Computing, Communications and Applications, 17(2s). https://doi.org/10.1145/3408321

Zhang, P., White, J., Schmidt, D. C., Lenz, G., & Rosenbloom, S. T. (2018). FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data. Computational and Structural Biotechnology Journal, 16, 267–278. https://doi.org/10.1016/j.csbj.2018.07.004

Zhao, Z., Zeng, S., Cheng, S., & Hao, F. (2023). Efficient and Privacy-Preserving Categorization for Encrypted EMR. Mathematics, 11(3). https://doi.org/10.3390/math11030754