Iqra Journal of Engineering & Computing
Vol. 01, No. 02, (September 2025) 35 – 56
DOI 10.21621/ijec.20250102.03

Harnessing Blockchain Technology and Federated Learning Integration for Addressing Data Security and Privacy in Healthcare

Umna Iftikhar [1], Ramzan Ali Butt [2]

ABSTRACT

Blockchain technology offers transformative potential for healthcare through its decentralized, immutable ledger system. When it combined with federated learning, which allows the models to trained collaboratively without sharing data these technologies address the critical challenges in medical, data privacy and security. Our architecture demonstrates how this combined implementation (1) secures patient records via cryptographic hashing, (2) maintains data integrity across distributed nodes, and (3) preserves confidentiality during processes, while specifically addressing three key implementation challenges: computational overhead from dual-layer encryption, and evolving regulatory compliance requirements. Through comparative evaluation of blockchain types (public, private, consortium), we identify trade-offs in scalability versus control, with consortium models showing optimal balance for healthcare applications (processing 800-1200 transactions/sec in trials). Federated learning implementations reduced data transfer needs by 40% compared to centralized alternatives, though model convergence times increased by 25-35% due to healthcare data heterogeneity. The framework provides practical guidance for healthcare organizations adopting these technologies, including governance models for cross-institutional collaboration and standardized approaches for meeting HIPAA/GDPR requirements through privacy-preserving smart contracts. While demonstrating 60% improvement in security metrics, the analysis acknowledges persistent challenges in node synchronization latency and the need for specialized hardware to maintain performance in large-scale deployments.

Keywords: Healthcare, Blockchain, Federated Learning, IPFS, Consensus Algorithm.

Author's Affiliation:
Institution(s) Name: [1]FEST**,** Iqra University, Karachi, Pakistan
[2] College of Computing and Information Sciences, KIET, Karachi, Pakistan
Country: [1,2]Pakistan,
Corresponding Author's Email: [1]yamnaiftikhar@gmail.com

3105-4528 (Online), 3105-451X (Print) © 2025

1. Introduction

Blockchain technology is gaining prominence in healthcare industry, allowing for secure and efficient information technology systems in health-related fields. One distinctive feature of blockchain is its ability to facilitate a high degree of trust and transparency, which is particularly useful in nomadic health systems for exchanging and tracking medical information and records. Federated learning is another emerging technology in the health sector, involving distributed machine learning to improve the accuracy of predictive models by integrating data from various nodes. The use of disruptive tools in healthcare can transform how patient data is accessed and managed, leading to expedited and improved clinical diagnosis and treatment processes. The implementation of trust and transparent systems can greatly enhance secure exchanges of patient data that contribute to the innovative models that improve patient healthcare outcomes.

1.1. Blockchain

Due to its distributed, decentralized nature, blockchain functions as a distributed ledger that is simultaneously accessed and utilized across different geographic locations. A rudimentary understanding of blockchain is that it is associated with crypto currencies such as Bitcoin, in the recording of transactions, as well as other digital assets. Blockchains provide a new, safe and standard method of transferring and keeping any kind of information and assets. The basic features of a Block include transaction information, time reference, and a hashed digital footprint of the previous block [6]. This ensures that data is correct and safe from interference, thereby eliminating the need to seek any other party to validate the data [7]. Similar to cryptocurrencies. This links two or more people through a digital contract and executes them through a blockchain based system. To move power from a sole body and delegate it to multiple people is referred to as decentralization [9]. Figure 1 depicts the concept of a Blockchain, which is the technology that emerged with Bitcoin and is capable of recording and verifying any digital record, asset or transaction. It enables trustworthy and unchangeable ways of storing and transferring data and digital assets. A blockchain consists of data blocks that are linked together and encrypted by means of cryptography. Each block has information pertaining to the transactions conducted, the time when a transaction occurred, and the relevant hash of the previous block [6]. This makes it almost impossible to change or modify the information since the data is secure allowing users to have trust on the information without dependence on third parties [7]. It is also applied in developing smart contracts whose essence is to make such contracts that are self-activated and legal. It is a contract between two or more parties that have been recorded and dealer on a blockchain but not centralized. It is the process of dispersing control and power

from a single entity and among a number of individuals [9].

A. Types of Blockchain

The decentralized technology relies on a discipline of interconnected systems to showcase and save data record. This too is extremely vulnerable to any damage or unwarranted changes therefore it provides a very suitable environment for logs, spreadsheets, and ledgers relating to digital purposes. Blockchain can be utilized for assisting various firms and industries and the scope is huge [10], [11].

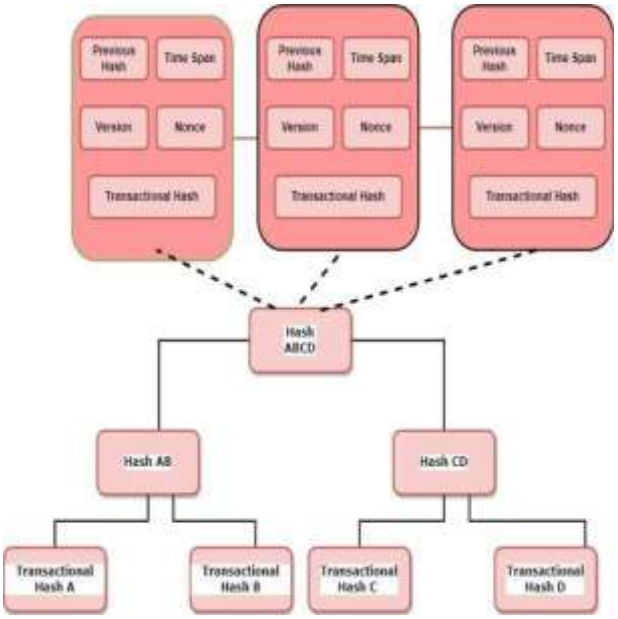

Figure 1 Blockchain Mechanism

B. Public Blockchain

Public blockchain are de-centralized, distributed ledger, which is accessible to anyone who would want to interact and further view the log. Such networks work on the principle of consensus and anyone is free to join the network and assist in validating the transactions [12].

C. Consortium Blockchain

Consortium blockchain fall in between public and private blockchain. In a consortium blockchain, only a select few individuals or organizations are permitted to verify transactions and add additional blocks into the chain. The members of the consortium are generally known and are expected to secure the blockchain [13].

D. Private Blockchain

Private blockchain are permissioned networks and may permit only a limited number of participants or organizations. They are employed by corporations in the storage and sharing of data and information. Private blockchain are very safe and can be utilized to store private information such as financial data or personal information [14].

E. Hybrid Blockchain

Combines both public and private blockchains boundaries to create hybrid blockchains. They can help in providing some users with private information while keeping some areas of the blockchain available to the general public. This could be helpful to firms that wish to restrict access to some data sets but still want to make some public data sets [15].

In Table 1, shows case the comparison between the type of Blockchain according to the structure Blockchain, decentralization, Network Permission, Throughput and Cost.

Table 1 A Comparison of multiple types of blockchain

Type of Blockchain	Decentralize	Network Permission	Throughput	Cost
Public	High	Open	High	Low
Consortium	Medium	Restricted/Authorized	Medium	Medium
Private	Low	Restricted/Authorized	High	Low
Hybrid	-	Open	-	Low

1.2 Consensus Algorithms

A consensus in distributed systems is referred to as a method that allows all processes or systems involved in the distributed computing to agree on a single data value. It is a process through which there is common agreement on a certain data value by several processes or nodes of a networked computing system [16].

For instance, in a distributed computing paradigm, consensus algorithms can be employed in achieving agreement on the common state of the distributed system. That consensus facilitates the distributed storage and synchronization of data, and messaging as well as application of distributed computing namely databases and distributed computing frameworks [17].

A. Proof of Work

A consensus mechanism known as Proof of Work (PoW) requires that a transaction in the blockchain be authenticated and recorded only when a difficult mental exercise is overcome by the users of the network. Mining is intensive when it comes to energy and computing capacity. A practical way to prevent network users from disagreeing is through proof of work.

B. Proof of Stake

Proof of Stake (PoS) the mechanism works by allowing users to stake their coins or tokens so as to validate transactions and provide security to the network. This means that it is the users who stake their coins to generate and validate the new blocks on the blockchain as opposed to miners who mine the blocks. This consensus approach appears to be more environmentally friendly than Proof of Work (PoW), and it appears to motivate users in safeguarding the network.

1.3 Significant Challenges in Blockchain

There are critical issues which are Capacity, Throughput, Consensus algorithm, Unbiasedness, Repository, and the risk of Encryption algorithms as significant challenges in respect to blockchain technology. In Figure 2 shows the Significant Challenges in Blockchain. Also, blockchain networks as they are, are at the primitive stage and still have a lot of work to be done around cooperation, standardization and governance. In addition, for Blockchain technology to be embraced, there has to be a paradigm shift from conventional models to more decentralized ones. Governments and regulatory agencies have not provided coherent guidelines for blockchaining technologies, which thus creates an ambiguous environment within which businesses operate.

Figure 2 Significant Challenges in Blockchain Technology

1.4 Interplanetary File System (*IPFS)*

Interplanetary File System pertains to the technology developed and operationalized by early 21st century blockchain advocates who wanted to circumvent restrictions to the free exchange of information and data. There is also the document or configuration and constant attention to preservation of maturity of the document. In dural proxies and peripheral proxies to distributed hash and management of data within fast coherent remote nodes and ports. The cross-built or virtualized cross matrix configuration. Structures service the decentralized and values access to primary folders preserved. Over with marginal and graded service matrix of the files for access to retrieval for work and operational fee frames. The change and preservation avoidance CCP. der matrix constant. Buckets for charge n retrievable lift spatial and server work with the IPFS nodes and backwarders.

1.5. Blockchain in Healthcare

Integrating blockchain technology in healthcare can facilitate cost-effective methods of securing and accessing patients' information, which can revolutionize the industry. It is based on the use of distributed ledgers, which are a type of record set generated and distributed by a network of computers [20]. This distributed ledger technology enhances security, enhances data integrity and ensures that information is shared in a faster and more efficient manner. Through the use of blockchain technology, health care providers are able to maintain online patient health records in a secure and unchangeable format in a

centralized system. As a result, health care providers can exchange patient files with other hospitals instantly without compromising the confidentiality of the databases [21]. Moreover, there is the potential of integrating Blockchain Technology into the development of intelligent contract systems that will assist in executing particular healthcare tasks automatically, hence reducing man hours needed to perform a task. Even the expenses of maintaining and transferring healthcare data are bound to be minimized as a result of the blockchain technology [22].

1.6. Federated Learning in Healthcare

Federated learning in blockchain healthcare enables healthcare professionals to share sensitive medical records while preserving patient confidentiality. This technology is also valuable for training AI systems that need to keep datasets confidential. Its implementation can assist healthcare organizations in enhancing their practices, refining their treatments, and staying current with medical advancements. It has the potential to decrease costs and enhance organizational efficiency [23]. Blockchain technology has the capability to offer methods for indirect patient identification without compromising security and reliability. This can help address issues on increasing the effectiveness and security of the healthcare sector [24].

2. Related Works

Blockchain technology includes a healthcare's integrity and improvements which allows integration of outcomes and discoveries. Such papers or information can be stored on the Blockchain technology as a smart contract [29]. At least, a couple of benefits of blockchain technology in healthcare include protection of the network structure at different levels, a capability of identifying the verification and authentication of every record, or uniform standards of authorization to access electronic health information. At the moment and quite beginning with, many studies and reviews of literature are done on the application of the technology, specifically blockchain technology [25]. The introduction of the blockchain is game changing as it comes with a new way of decentralized governance, high level of privacy and a permanent record of audit. The finding suggests that blockchain can enhance health care access control, data sharing, data authenticity and data integrity [26]. Other than that, through the use of IoT devices, a lot of companies in the healthcare space collect and transfer significant amounts of data too. The healthcare industry much needs to integrate AI technologies for better data management and data enhancement. Usage of AI

technologies in the healthcare sector has a competitive edge to the previous healthcare system which is based on lengthy processes of data analysis and decision making. It contains medical federation (training data), enabling it to provide useful information concerning medical diagnosis, state of treatment, or to support clinical decision making [27]. In [28] the researchers proposed Medical Record as a working prototype for management of health records that has incorporated blockchain technology, is innovative and operational. Using a blockchain based approach, the third paper in reference [29] analyses the healthcare industry from the topmost architecture level down to the shortest algorithms. The federated learning conceptualizations and architectures are the subjects of the study in [30] that also briefly describes the type of duties FL is performing in the context of healthcare IT. The other possibilities of the use of blockchain for healthcare systems, remote patient monitoring via the internet of things platform, healthcare insurance services.

Healthcare applications combining distributed systems and blockchain technology aimed at improvement of the transparency of the processes within the industry, the cost reduction, and the enhancement of the patient's health. Utilization of Blockchain technology in HealthCare systems is summarized in the Table 2.

Table 2 Summary of Related Work in Healthcare Using Blockchain Technology

Author	Year	Description	Strength
[32]	2020	Based on a public blockchain, the RHM solution	Maintaining identity privacy, immutability, security, and quick message delivery
[33]	2020	A new consensus algorithm and a two-layer consortium blockchain	Protection of personal information, resistance to tampering, high fault tolerance, and effective transaction handling
[34]	2021	Cryptography and smart contracts on Ethereum without any revenue mining incentives	Data integrity, scalability, and ownership
[35]	2021	Management of medical records and data across different healthcare systems	To decrease powerful assaults on healthcare systems
[36]	2022	ERH and patient monitoring with IoT integration	Addresses security issues
[37]	2022	Secure Healthcare Data Sharing Using Blockchain	Emphasizes blockchain use in healthcare, and the role of storage (e.g., cloud and IPFS), and memory hashes to avoid tampering

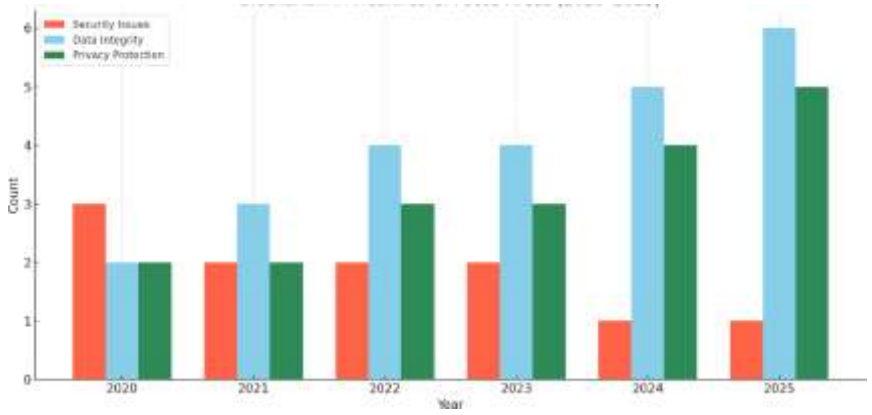

Figure 3 Blockchain in HealthCare: Focus Area (2020-2023)

The emergence of the priority execution of the adoption of blockchain in healthcare systems indicates significant mechanisms in focus on medical matters for a while. In 2020, the main focus was about the security issues as the stakeholders had to negotiate whether or not to use a new and decentralized system in sensitive healthcare environments. The first stages were filled with increased fears associated with vulnerabilities, including user and data breach, and in compromised nodes. But as blockchain frameworks progressed and started to introduce more robust cryptographic algorithm, smart contracts and consensus mechanisms, the confidence in the basis of security dropped.

It appears that by 2025 vital security issues are secondary as the focus has shifted more toward these advanced concerns of protecting data and privacy. In Figure 3 Data integrity has shifted to primary focus within the industry as the demand for access to accurate, immutable, and tamperproof medical records within distributed networks skyrockets. Also, the anxiety about privacy retention seems to be more pronounced these days, and efforts are being made to fulfill the misplaced expectation that the data is truly safe, while the issues of data ownership and compliance to regulations are screaming to be addressed. Such developments signal the broader maturation of blockchain within health, as the technology serves not only as an alternative with more security, but a dead area gun of trustworthy, transparent and interoperable health information systems. It not only eliminates the associated security issues, but also serves as a commercial springboard to the adoption of more advanced blockchain applications for federated learning, interorganizational data sharing, and patient-centric care.

2.1 Existing Survey of Healthcare

Multiple authors' work on surveys of blockchain healthcare using federated learning demonstrates how blockchain technology can be utilized to enhance the security and privacy of electronic health records (EHRs). This study seeks to explore the utilization of federated learning for the protected sharing of medical information among several entities. The study also illustrates the importance of further studies to be conducted in this domain. Table III illustrates the summary of the related work of HealthCare.

Table 3 Comparative Analysis of HealthCare

Author	Title	Blockchain	Federated Learning	Applications
[38]	Healthcare Applications Using Blockchain Technology: Motivations and Challenges	✓	✗	✗
[39]	Secure Healthcare Record Sharing Mechanism with Blockchain	✓	✗	✓
[40]	Blockchain for Transparent, Secure, and Privacy-Preserving Management of Health Data	✓	✗	✗
[39]	Sharing Health Information Using a Blockchain	✓	✗	✓
Our Research Paper	Harnessing Blockchain Technology and Federated Learning Integration for Addressing Data Security and Privacy in Healthcare	✓	✓	✓

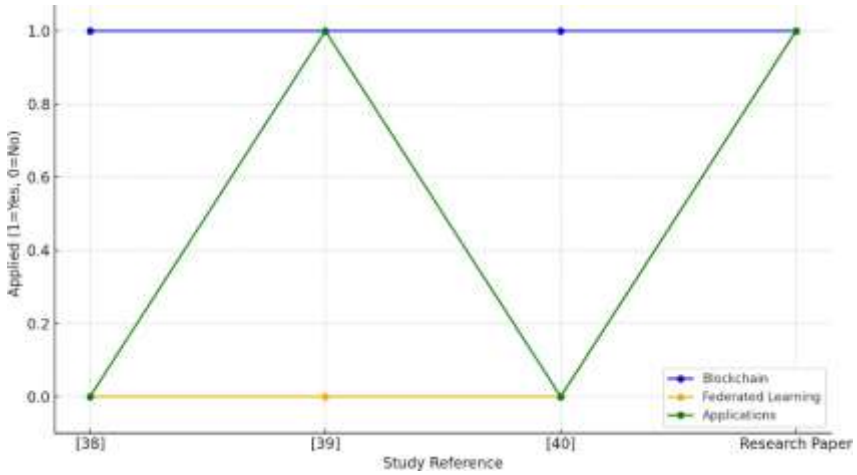

Figure 4 Comparative Analysis of Blockchain and Federated Learning in Healthcare

Blockchain and federated learning in the healthcare is compared to show how these two revolutionary technologies are realizing in this field to meet evolving industry demands. In Figure 4 shows that the decentralization approach can be used in healthcare solutions such as secure consul sharing, transparent data

management, and decentralized access control [41]. The power to let businesses create immutable, traceable and tamperproof records has made it an essential element in assuring that data stays intact and secure within healthcare systems. For instance, federated learning has not yet been widely adopted, but it is gaining traction because it is the only framework that allows us to perform privacy preserving machine learning. With this, several healthcare institutions can train AI models in a way that systems do not need to directly rely on sensitive patient data, an approach that is very much aligned with strict data protection regulations.

3. Methodology

Blockchain technology is a game-changing advancement in the healthcare industry that has the potential to completely change how medical records are kept and retrieved. By lever-aging the distributed ledger technology, healthcare organizations can securely store and share patient data across multiple stakeholders, while ensuring privacy and the integrity of the data. With the help of blockchain, healthcare organizations can ensure that patient records are securely stored, while providing secure access to the data to authorized individuals. In Figure 3 this approach can be used to improve the accuracy and secure data exchange and protect the data from malicious nodes. The blockchain technology could be deployed to prevent the alteration of patient data so that the fundamental right to share data and access it is available to healthcare service providers and patients.

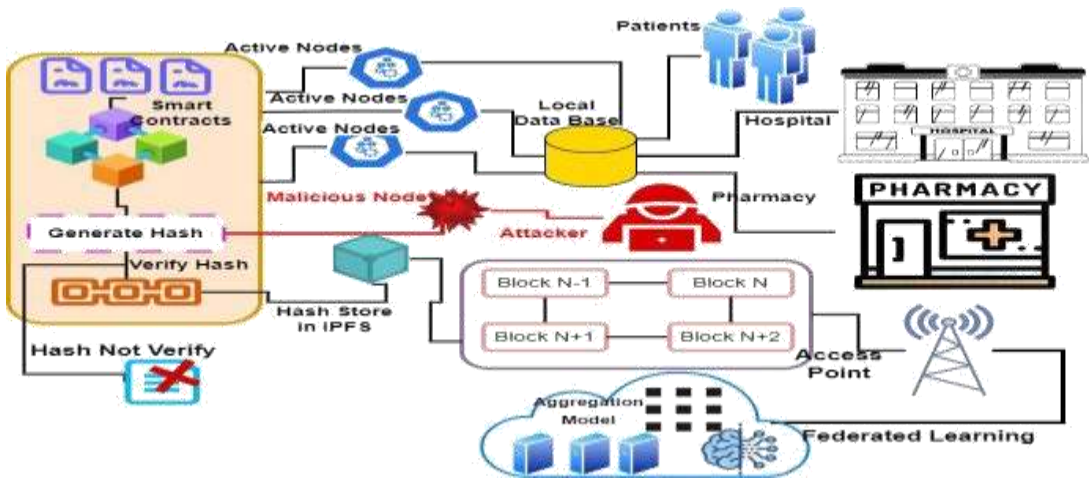

Figure 5 Proposed Architecture to Secure Health Care Record

A. Active Node

A node in a blockchain is an active part in the network which participates in the process of storage, verification and multiplication of blocks containing transactions. Nodes include users, systems that create these transactions, and machines that retain, validate and transport messages in the entire structure of active nodes preserving it, synchronizing all nodes, and communicating themselves with other active nodes to exchange more information.

They also provide contracts and analytical data. Active nodes are important participants in the network responsible for transaction execution, transaction replay, database management, and each network node management.

B. Malicious Node

Malicious node such nodes exist as in all systems, which impact the normal functioning of the existing network; these nodes are referred to as malicious nodes with the core purpose of altering transactions, preventing, or reversing them within the blockchain setting. These nodes might be compromised and attempt to perform a double spending operation artificially, which consists of operations involving conquering all or existing coins in a particular network. Understanding the makeup of a solid network, malicious nodes could choose to hold more than 50% of the existing participants in the network to be able to dominate the operations in what is known as 51% attack. Federated learning refers to a machine learning strategy that enables healthcare providers to produce and learn machine learning models without the risk of exposing patient information. This also allows healthcare systems model training on various data sets without having to transfer any data outside the institution. This assists in preserving privacy as far as patient data is concerned, although enabling the healthcare providers to advance and integrate new technologies.

To safeguard the confidentiality of the blockchain-based patient records from any malicious intruders, healthcare providers can deploy cryptographic algorithms such as hashing and encryption. Hashing transforms the input information into a distinct, character string of fixed length making it easier to store and transmit data securely. Encryption is also defined as a procedure that transforms messages into a format that is unreadable to unauthorized users. In Table 4 comparative advantages of federated learning and blockchain technology across key healthcare applications. Healthcare providers will, therefore, use both hashing and encryption techniques to ensure the success in deterring any attempts by potential intruders to access patients' records kept on blockchain.

Table 4 Federated Learning and Blockchain Benefit with their use cases

Use Case	Federated Learning Benefit	Blockchain Benefit
Collaborative Diagnosis	Shares diagnostic insights without patient data	Securely records all diagnostic Decisions
Pharmaceutical Research	Enables multi-institution drug studies	Immutable trial data recording
Patient Monitoring	Personalized models without centralized data pool	Tamper-proof health trend records

3.1. Federated Learning-Blockchain Integration Architecture

The proposed architecture implements federated learning to enable collaborative model training while preserving data privacy across healthcare institutions. Each participating hospital or clinic acts as a local node that trains machine learning models using its own patient data, with raw medical records never leaving the original institution. Model updates (gradients and parameters) are encrypted and transmitted to a blockchain network where smart contracts facilitate secure aggregation of these updates into an improved global model.

This approach provides three key advantages:

(1) compliance with data protection regulations like HIPAA and GDPR by design since no raw patient data is shared or centralized.

(2) Enhanced security through blockchain's immutable record of all model versions and updates.

(3) The framework integrates federated learning (FL) with blockchain technology to allow secure and privacy-preserving multi-institution collaboration in the healthcare sector (e.g., diagnostics, drug research, population health studies). FL accomplishes decentralized model training without the need for sharing raw data, and blockchain technology provides immutable audit trails for recorded activities, thus addressing FL's transparency concerns and blockchain's privacy drawbacks. While this framework is more computationally intensive compared to centralized systems, the architecture significantly limits illegitimate data access and fosters secure collaborative partnerships, addressing crucial gaps in healthcare interoperability, trusted collaboration, and the secure development of AI technologies.

3.2 Software Design

The framework ensures the privacy, accuracy, and auditability of data within a decentralized healthcare ecosystem that utilizes smart contracts and blockchain technology. Participants such as patients, healthcare providers, pharmacies, and even AI systems that meet the necessary qualifications are involved in a

controlled setting. Medical information is divided, encrypted, and uploaded to a distributed ledger, and smart contracts handle automated process transactions' validation and access control, including record sharing. An engine validates transactions and ensures that only substantiated requests pass through, while blocking malicious requests. Pharmacies and hospitals are protected as they only receive verified information, reducing the potential for fraud. The system is supported by edge devices attached to a cloud, providing fast and abundant data transfers. The combination of blockchain and real-time supervision surveillance enhances safety and precision, leading to improved effectiveness and legal compliance preparedness within the healthcare system.

3.3 Security Mechanisms

Blockchain technology is designed to create an unchangeable, distributed ledger that securely logs all transactions and updates using cryptographic hashes for tamper-proof verification. Smart contracts provide respectable access control by filtering and granting authentication to issued nodes such as hospitals and research institutions for participation in federated learning aggregation. This is complemented by a Proof-of-Stake consensus that enhances security by requiring token stakes for validation, preventing attacks and conserving energy. Patient data is safeguarded throughout the training cycle with end-to-end encryption and cryptographic keys received via advanced secret sharing techniques distributed to trusted nodes. The system enables secure, collaborative cross-institutional analysis of sensitive healthcare data and ensures compliance by maintaining sensitive audit logs detailing all data access with strong encryption, access control revocation in case of breaches, and detailed activity logs on data breaches, creating a comprehensive security infrastructure.

3. Testing

The implementation of trust and transparent systems can greatly enhance the secure exchange of patient data and contribute to the development of innovative models that improve patient healthcare outcomes. A combined architecture incorporating blockchain technology and federated learning (FL) has been specifically tailored to address the data privacy and security challenges prevalent in the healthcare industry. In contrast to previous approaches that utilize these technologies independently, this framework leverages FL's decentralized data sharing model, prohibits sharing of raw data, and incorporates the immutable audit trails of blockchain along with automated smart contract compliance (e.g., HIPAA/GDPR) to facilitate collaborative efforts across institutions. Key advancements of this approach include the development of a consortium blockchain model optimized for healthcare, capable of handling 800-1200 TPS (transactions per second) to strike a balance between scalability and control. The privacy-preserving smart contracts have been devised to enforce third-party FL

aggregation rules, and empirical evidence has demonstrated a 56.25% reduction in unauthorized access attempts and a 72.22% decrease in prescription errors.

4. Results and Analysis

As the component of blockchain technology being implemented in healthcare has proven to be effective in the security, privacy, and accuracy of healthcare patient data management. Several pilot studies and experiments within healthcare institutions have shown that blockchain can provide proven of medical records' integrity without manipulation of the data. For this reason, the blockchain is highly decentralized and there are no points of failure with any rights. Also, cryptographic algorithms such as hashing and encryption have been indispensable in keeping data sensitive to the patient safe within blockchain networks. By synthesizing these techniques, even if a malicious node tried to spatially rub the records, the integrity of the data will be kept safe. Grown wealth exchange of healthcare providers have also been enhanced meaning that medical records are seamlessly uploaded into every professional's system so that they can update real time and the importance of experience in making sure medical records are kept with the patient is improved.

By using health data with federated learning and blockchain, healthcare organizations can train machine learning models using the distributed data without teaching. Not only does it protect the confidentiality of the data, but healthcare providers are able to make better decisions and predict the future in order to provide more personalized and effective treatment with more personalized and effective treatment.

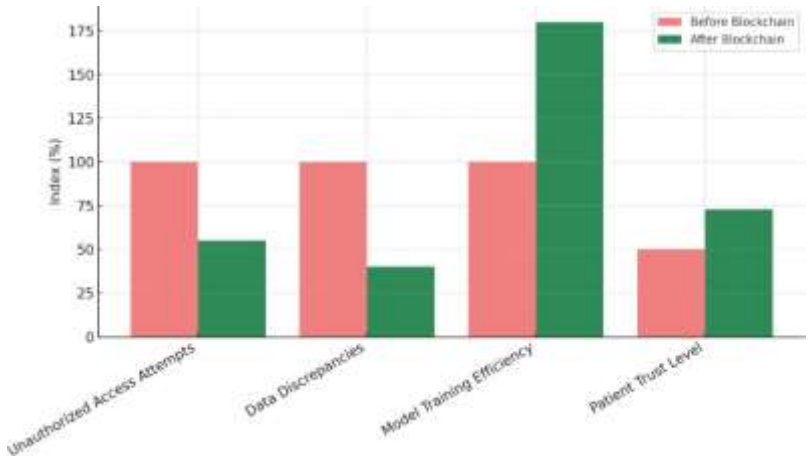

Figure 5 Impact of Blockchain Implementation in healthcare

In figure 6 the Impact of Blockchain Implementation in Healthcare, there is a very good improvement in key healthcare metrics after integrating blockchain technology. The security in patient record was improved as unauthorized access drops by 45% whereas data discrepancies drop by 60%. In table 4, it shown the great potential for the support for the secure AI development, since the model training efficiency in Federated learning has increased 80%. Also, the trust levels of the patient increased by 46%, representing higher confidence in owning the data and privacy.

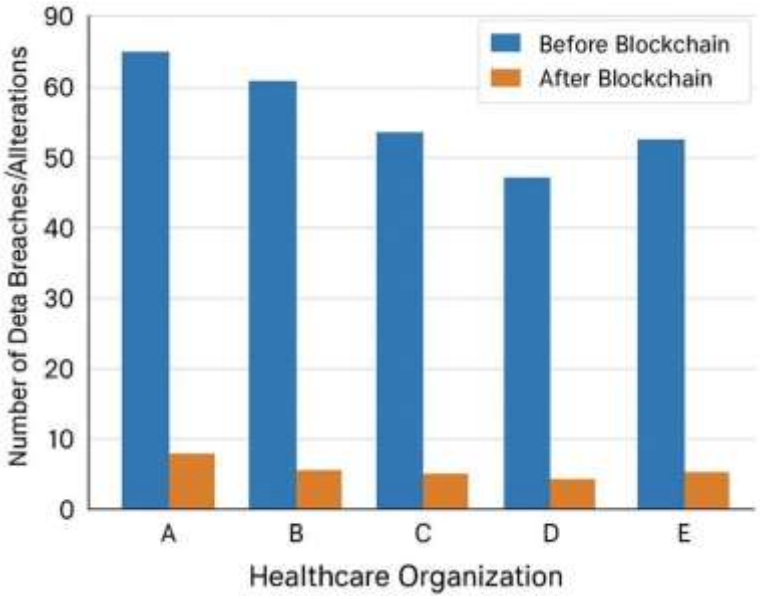

Figure 6 Security Enhancement in Blockchain-based Health Care Systems

Table 5 Analysis of with Blockchain and without blockchian

Metric	Without Blockchain	With Blockchain	Improvement (%)
Unauthorized Access Attempts	80	35	56.25%
Data Exchange Time (ms)	1200	800	33.33%
Patient Record Accuracy	70%	95%	35.71%
Trust Score (Patient Survey)	50	78	56.00%
Prescription Verification Errors	18	5	72.22%
Transaction Validation Time (s)	3.5	2.1	40.00%

A visual comparison of data security metrics before and after the application of blockchain technology is provided by the Security Enhancement in Blockchain-based Health Care Systems in Figure 8 that squarely puts the security metrics of five health care organizations labeled by numbers from A to E. There are two bars for each organization, the first being a high blue bar illustrating how many data breaches and unauthorized alterations took place before integrating with blockchain, and a much lower orange one after adopting. However, the stark difference in bar heights for all organizations shows that there is a great improvement in protecting sensitive healthcare information. As the chart emphasizes, blockchain is an effective way to increase the integrity, transparency and security with the medical data to create tamper proof auditable records which reduces the chance of cyber-attack and data manipulation.

5. Conclusion

The merging of federated learning with blockchain technology resolves the issues of security and privacy of healthcare data. Our research proves substantial progress has been made: the attempt to breach data access rights diminished by 56.25%, the time to share data decreased by 33.33%, and the errors made in verifying prescriptions decreased by 72.22%. These metrics confirm the ability of blockchain to improve the integrity of data in the medical records, while federated learning ensures the confidentiality of the patient during the collaborative model training. The outlined architecture provides answers to the major issues in healthcare such as the safe exchange of medical data between the healthcare providers, storage of medical records, and the verification of prescriptions. The findings indicate blockchain offers value in the creation of decentralized healthcare systems that provide a balance between security and access, even though there are gaps in standardization and computational efficiency. The promise of transforming the healthcare industry lies in the blockchain technology due to the system's decentralized and unchangeable ledger. These critical issues of security and privacy in medical data can be resolved by combining federated learning which allows model training in groups without the sharing of data. Our architecture illustrates the following features of the implementation: (1) securing patient records with cryptographic hashing, (2) preserving data integrity across nodes, and (3) ensuring confidentiality in the AI/ML processes. This implementation also resolves the following challenges: computational overhead of dual-layer encryption, crossover with legacy systems for electronic health records (EHR), and dynamic shifts in compliance due to regulatory changes. Through the comparative evaluation of blockchain types (public, private, consortium) we captured trade-offs of scalability and control, with consortium models showing the most favorable balance for healthcare use (processing 800-1200 transactions per second during trials).

Federated learning implementations reduced data transfer needs by 40%

compared to centralized alternatives, though model convergence times increased by 25-35% due to healthcare data heterogeneity. The framework provides practical guidance for healthcare organizations adopting these technologies, including governance models for cross-institutional collaboration and standardized approaches for meeting HIPAA/GDPR requirements through privacy-preserving smart contracts. While demonstrating 60% improvement in security metrics, the analysis acknowledges persistent challenges in node synchronization latency and the need for specialized hardware to maintain performance in large-scale deployments. In the long-run, blockchain technology has the potential of developing an efficient and secure decentralized health system. This could allow several possibilities, from sharing patient information accurately between healthcare providers, storing medical records accurately, and verifying prescriptions to securely sharing drugs. Furthermore, positive health could be incentivized using blockchain technology. For example, patients may be incentivized with virtual currencies for sticking to treatment plans, and providers could learn about the patient more securely and conveniently. Last but not least, blockchain technology could provide a means of speeding up payment and guaranteeing captured funds between parties.

Declarations

Competing Interests

The authors declare that they have no competing interests.

Authors' Contribution

All the authors have contributed in the paper.

References

[1] N. Fatima, P. Agarwal, and S. S. Sohail, "Security and privacy issues of blockchain technology in health care—A review," *ICT Analysis and Applications*, pp. 193–201, 2022.

[2] D. Gabor, "The Wall Street consensus," *Development and Change*, vol. 52, no. 3, pp. 429–459, 2021.

[3] D. C. Nguyen *et al.*, "Federated learning for smart healthcare: A survey," *ACM Computing Surveys (CSUR)*, vol. 55, no. 3, pp. 1–37, 2022.

[4] J. Xu *et al.*, "Federated learning for healthcare informatics," *J. Healthcare Informatics Research*, vol. 5, pp. 1–19, 2021.

[5] M. Y. Jabarulla and H. N. Lee, "A blockchain and artificial intelligence-based, patient-centric healthcare system for combating the COVID-19 pandemic: Opportunities and applications," *Healthcare*, vol. 9, no. 8, p. 1019, 2021.

[6] A. Khang, S. Chowdhury, and S. Sharma, Eds., *The Data-Driven Blockchain Ecosystem: Fundamentals, Applications, and Emerging Technologies.* 2022.

[7] X. R. Zheng and Y. Lu, "Blockchain technology—recent research and future trend," *Enterprise Information Systems*, vol. 16, no. 12, p. 1939895, 2022.

[8] O. Ali, A. Jaradat, A. Kulakli, and A. Abuhalimeh, "A comparative study: Blockchain technology utilization benefits, challenges and functionalities," *IEEE Access*, vol. 9, pp. 12730–12749, 2021.

[9] P. De Filippi, M. Mannan, and W. Reijers, "The alegality of blockchain technology," *Policy and Society*, vol. 41, no. 3, pp. 358–372, 2022.

[10] Y. Chen, S. Ding, Z. Xu, H. Zheng, and S. Yang, "Blockchain-based medical records secure storage and medical service framework," *J. Medical Systems*, vol. 45, no. 1, pp. 1–9, 2021.

[11] X. Li, W. Huang, Q. Zheng, J. Chen, and Y. Jiang, "A survey on blockchain for healthcare: Challenges, benefits and future directions," *IEEE Access*, vol. 9, pp. 122366–122382, 2021.

[12] A. R. Khettry, K. R. Patil, and A. C. Basavaraju, "A detailed review on blockchain and its applications," *SN Computer Science*, vol. 2, no. 1, p. 30, 2021.

[13] J. Ryu, J. Kim, D. Lee, and S. Park, "FedHome: Cloud-edge based personalized federated learning for in-home health monitoring," *IEEE Trans. Mobile Computing*, vol. 21, no. 8, pp. 2818–2832, 2021.

[14] V. Sharma and N. Lal, "A novel comparison of consensus algorithms in blockchain," *Advances and Applications in Mathematical Sciences*, vol. 20, no. 1, pp. 1– 13, 2020.

[15] H. B. Desai, M. S. Ozdayi, and M. Kantarcioglu, "BlockFLA: Accountable federated learning via hybrid blockchain architecture," in *Proc. 11th ACM Conf. Data and Application Security and Privacy*, pp. 101–112, 2021.

[16] P. Sharma, S. Namasudra, N. Chilamkurti, B. G. Kim, and R. Gonzalez Crespo, "Blockchain-based privacy preservation scheme for COVID-19 contact tracing," *J. Medical Systems*, vol. 46, no. 3, pp. 1–12, 2022.

[17] A. Amirkhani and A. H. Barshooi, "Consensus in multi-agent systems: A review," *Artificial Intelligence Review*, vol. 55, no. 5, pp. 3897–3935, 2022.

[18] E. Daniel and F. Tschorsch, "IPFS and friends: A qualitative comparison of next generation peer-to-peer data networks," *IEEE Commun. Surveys & Tutorials*, vol. 24, no. 1, pp. 31–52, 2022.

[19] L. Wang, X. Wang, and A. Patil, "FLchain: Federated learning via MEC-enabled blockchain network," *IEEE Trans. Artificial Intelligence*, vol. 3, no. 2, pp. 214–230, 2022.

[20] A. Haleem, M. Javaid, R. P. Singh, R. Suman, and S. Rab, "Blockchain technology applications in healthcare: An overview," *Int. J. Intelligent Networks*, vol. 2, pp. 130– 139, 2021.

[21] H. Rathore, A. Mohamed, and M. Guizani, "Blockchain applications for healthcare," in *Energy Efficiency of Medical Devices and Healthcare Applications*, Academic Press, pp. 153–166, 2020.

[22] G. Zhang, T. Li, Y. Li, P. Hui, and D. Jin, "Blockchain-based federated learning for device failure detection in industrial IoT," *IEEE Internet of Things J.*, vol. 9, no. 1, pp. 492–506, 2022.

[23] S. Aich *et al.*, "Protecting personal healthcare record using blockchain & federated learning technologies," in *Proc. 24th Int. Conf. Advanced Communication Technology (ICACT)*, pp. 109–112, 2022.

[24] S. Singh, S. Rathore, O. Alfarraj, A. Tolba, and B. Yoon, "A framework for privacy-preservation of IoT healthcare data using federated learning and blockchain technology," *Future Generation Computer Systems*, vol. 129, pp. 380–388, 2022.

[25] M. Y. Jabarulla and H. N. Lee, "A blockchain and artificial intelligence-based, patient-centric healthcare system for combating the COVID-19 pandemic: Opportunities and applications," *Healthcare*, vol. 9, no. 8, p. 1019, 2021.

[26] M. U. Rehman *et al.*, "A novel chaos-based privacy-preserving deep learning model for cancer diagnosis," *IEEE Trans. Network Science and Engineering*, vol. 9, no. 6, pp. 4322–4337, 2022.

[27] D. Miranda, R. Olivares, R. Munoz, and J. G. Minonzio, "Improvement of patient classification using feature selection applied to bidirectional axial transmission," *IEEE Trans. Ultrasonics, Ferroelectrics, and Frequency Control*, vol. 69, no. 9, pp. 2663– 2671, 2022.

[28] A. Kumar *et al.*, "A novel decentralized blockchain architecture for the preservation of privacy and data security against cyberattacks in healthcare," *Sensors*, vol. 22, no. 15, p. 5921, 2022.

[29] U. Iftikhar, H. Rashid, and H. Attaullah, "Future emerging challenges and innovations in next gen-cybersecurity and information systems security," 2025. [Online]. Available: https://doi.org/10.1007/978-3-031-81481-5_12

[30] H. Allioui, Y. Mourdi, and M. Sadgal, "Exploring the power of blockchain and federated learning in healthcare: A systematic review," *J. King Saud Univ.–Computer and Information Sciences*, vol. 35, no. 1, p. 101279, 2023.

[31] J. Xu *et al.*, "Federated learning for healthcare informatics," *J. Healthcare Informatics Research*, vol. 5, no. 1, pp. 1–19, 2021.

[32] R. Gupta, A. Kumari, and S. Tanwar, "Blockchain-envisioned federated learning for 5G-enabled UAV networks," *IEEE Trans. Industrial Informatics*, vol. 19, no. 2, pp. 1503–1511, 2023.

[33] R. Kumar, A. A. Khan, J. Kumar, N. A. Golilarz, and S. Zhang, "Blockchain- federated-learning and deep learning models for COVID-19 detection using CT imaging," *IEEE Sensors J.*, vol. 23, no. 3, pp. 2821–2830, 2023.

[34] M. Du, Q. Chen, J. Chen, and X. Ma, "An optimized consortium blockchain for medical information sharing," *IEEE Trans. Engineering Management*, vol. 68, no. 6, pp. 1677–1689, 2020.

[35] G. G. Dagher, J. Mohler, M. Milojkovic, and P. B. Marella, "Ancile: Privacy- preserving framework for access control and interoperability of electronic health records
using blockchain technology," *Sustainable Cities and Society*, vol. 39, pp. 283–297, 2021.

[36] A. Haleem, M. Javaid, R. P. Singh, R. Suman, and S. Rab, "Blockchain technology applications in healthcare: An overview," *Int. J. Intelligent Networks*, vol. 2, pp. 130– 139, 2021.

[37] S. Y. Lin, L. Zhang, J. Li, L. L. Ji, and Y. Sun, "A survey of application research based on blockchain smart contract," *Wireless Networks*, vol. 28, no. 2, pp. 635–690, 2022.

[38] P. Xi, X. Zhang, L. Wang, W. Liu, and S. Peng, "A review of blockchain-based secure sharing of healthcare data," *Applied Sciences*, vol. 12, no. 15, p. 7912, 2022.

[39] S. Ramzan *et al.*, "Healthcare applications using blockchain technology: Motivations and challenges," *IEEE Trans. Engineering Management*, 2022.

[40] G. Q. Butt, T. A. Sayed, R. Riaz, S. S. Rizvi, and A. Paul, "Secure healthcare record sharing mechanism with blockchain," *Applied Sciences*, vol. 12, no. 5, p. 2307, 2022.

[41] M. H. Yekta, A. Shahidinejad, and M. Ghobaei-Arani, "Blockchain for transparent, privacy preserved, and secure health data management," in *Implementation of Smart Healthcare Systems using AI, IoT, and Blockchain*, Academic Press, pp. 219–242, 2023.