International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 1, 2025
https://www.theaspd.com/ijes.php

Secure Patient Data Management Using Blockchain Technology

[1]Dr. V Srinadh, [2]E U Iniyan, [3]Dr. Archana Bhat, [4]Archana Ratnaparkhi , [5]Siva Sankar Namani,[6*]Dr. R.Senthamil Selvan

[1]Associate Professor, Department of CSE-AIML,GMR Institute of Technology,Rajam, Andhrapradesh
[2] Assistant Professor ,Department of ECE, Prathyusha Engineering college,Tiruvallur,Tamilnadu
[3]Assistant professor ,Department of AI & ML,BMS Institute of Technology and Management ,Bengaluru , Karnataka
[4]Assistant Professor, Department of Electronics and Telecommunications Engineering, Vishwakarma Institute of Technology, Pune, Maharashtra ,India
[5]Assistant Professor, Department of CSE (AI & ML),G Narayanamma Institute of Technology and Science (GNITS), Shaikpet, Hyderabad.
[6*]Associate Professor,Department of ECE,Annamacharya Institute of Technology and Sciences,Tirupati,Andhar Pradesh
Email ID: [1]srinadh.v@gmrit.edu.in ,[2] iniyan2540@gmail.com ,[3] archanabhat@bmsit.in ,[4] archana.ratnaparkhi@gmail.com , [5]sivagnits@gmail.com , [6]*selvasenthamil2614@gmail.com

Abstract

Modern healthcare systems keep track of patient data effectively that are safe, effective and simple to access. The conventional method of Electronic Medical Record (EMR) platforms have a lot of issues like problems with integration, problems with information security, risks to confidentiality and the ability to be hacked, especially when storage is centrally placed. Furthermore the massive storage requirements of server-based healthcare administration technologies restrict their scalability. Blockchain technology addresses these problems by allowing people store and swiftly access health information without depending on a single source. Utilizing distributed digital records for smart contracts for storing data, the study proposes a blockchain-based approach to secured data management for real-time patient health monitoring. By combining medical records into a decentralized system, this blockchain technology complies to healthcare standards while improving safety, reliability and cost. Security of data has been improved and authorized user access information is made simpler with the combination of cryptographic methods with decentralized consensus mechanisms. Health care professionals are able to safely exchange patient information utilizing this method, which optimizes both decisions regarding health care and the treatment results of the patient. The proposed strategy increases the effectiveness of operations, legal compliance along with certainty regarding health care data management by implementing an integrated distributed framework that links healthcare data.

Keywords: *Electronic Medical Record systems, Decentralized network, Blockchain technology, Cryptographic methods, Healthcare data.*

1.INTRODUCTION

Patient data management has been greatly modified by the healthcare sector's fast digital evolution. The availability of data & efficiency in operation are getting better for health care organizations as a result of the increasing popularity in server-based patient management platforms & Electronic Medical Records [1]. But these traditional systems frequently face significant problems regarding privacy, compatibility, adaptability as well as protection. Issues regarding confidentiality of patients & compliance to medical regulations have been raised by the simple fact that almost all available healthcare data storage facilities are centralized making them highly susceptible to cyberattacks, illegal access, and data thefts [2-4]. Additionally, medical professionals have difficulty in exchanging data effortlessly across organizations, which complicates efficient decision-making & organized patient care [5].

Healthcare information requires the use of rigorous safety protocols [6-9] to protect against unauthorized entry and to ensure conformity to laws such the Insurance Convenience & Accountability Act as well as the Worldwide Data Protection Regulations. Patient data are at risk, particularly from unauthorised alterations and detached points of failure associated with centralized storage [10-12]. Additionally, traditional server-based health care management systems have a demand for significant storage capabilities, resulting in operational inefficiency and higher costs. considering the increasing number of healthcare data, a data management method that is adaptable, reliable, as well as secure is absolutely necessary[13].

By facilitating decentralized, transparent & unalterable storage of information, blockchain technology has developed a revolutionary approach for solving these issues. Blockchain technology removes the hazards that is related to centrally stored data by working on an open ledger procedure which differs from traditional database systems [14-16]. Data is preserved across multiple nodes in this system. This decentralized technique enables unchangeable records, protects the confidentiality of information & provides safety. The proposed blockchain technology provides an excellent solution for managing healthcare information as it utilizes cryptographic methods and consensus processes to avoid unwanted modifications.

The applications of blockchain technology are investigated, as it deals with the healthcare data systems. It focuses, how distributed databases, electronic contracts & cryptographic safety features may assist to mitigate the limitations of conventional EMR systems. Through the implementation of blockchain-based technology, this research intends to showcase, how a distributed approach could transform medical information's ensuring greater safety, compatibility as well as personalized care for patients [17].

The study will carry out an in-depth analysis of the functionalities of blockchain, its integration with current healthcare facilities and possible challenges to follow. The paper will additionally investigate the impact of blockchain-based medical technologies on security of data, patient confidentiality and healthcare effectiveness in real-world applications [18]. This study contributes the active endeavours to boost digital healthcare environments by suggesting a safe and scalable system, which will create a healthier and safer path in medical data handling system [19].

2.METHODOLOGY

A systematic strategy is employed to create a blockchain based technology in health care information management system. The strategy consists of: The main objective evaluation is to find the primary issues with modern healthcare information systems and establishing the goals that require for blockchain integration. The system is set to operate as an independent body utilizing blockchain technology, digital safety, access control and smart contracts. In order to make sure that data management is safe and effective. For the delivery phase, technologies like Hyperledger Fabric & Ethereum are employed to create and set up the blockchain architecture. This assures consistency and permits future enhancement if necessary. Subsequently, the system has been deployed in a location where it performs an extensive assessment and testing process to validate its safety, compatibility, and speed. This evaluation step assesses the reliability of the system, security and compliance with health care laws like HIPAA and GDPR. This comprehensive strategy ensures that the recommended blockchain-based patient records management tool is both trustworthy and efficiently providing solutions that directly address all the difficulties associated with the organization & transfer of healthcare data.

2.1 The Patient Management System's architecture

A multi-layered architecture ensures efficiency, interoperability & security based on blockchain technology patient management system. Clients in the healthcare industry, especially medical professionals and patients, interact with the system during the User Stage. In order to avoid outsiders from obtaining or manipulating patient data, robust authentication methods & role-based limitations on

access have been implemented in place. The Applications Stage enables seamless patient record management through offering needed interfaces for input of data, record recovery, as well as report output. At this stage, the system can be integrated with IoT devices that enable remote patient monitoring in real time, which has become a huge boon to healthcare professionals.

Using advanced cryptographic techniques—including digitally signed documents, encryption, and hashing—the Security Stage assures compliance with healthcare regulations. These methods ensure the safety, genuineness, and reliability of patient data, thereby decreasing the risks connected with online threats and illegal access to data. A secure quick and easy as well as interoperable remedy for patient information management is provided by the blockchain-based health care system by incorporating these stages.

This architecture provides a decentralized, scalable, and reliable method of maintaining patient data as shown in figure1**.**

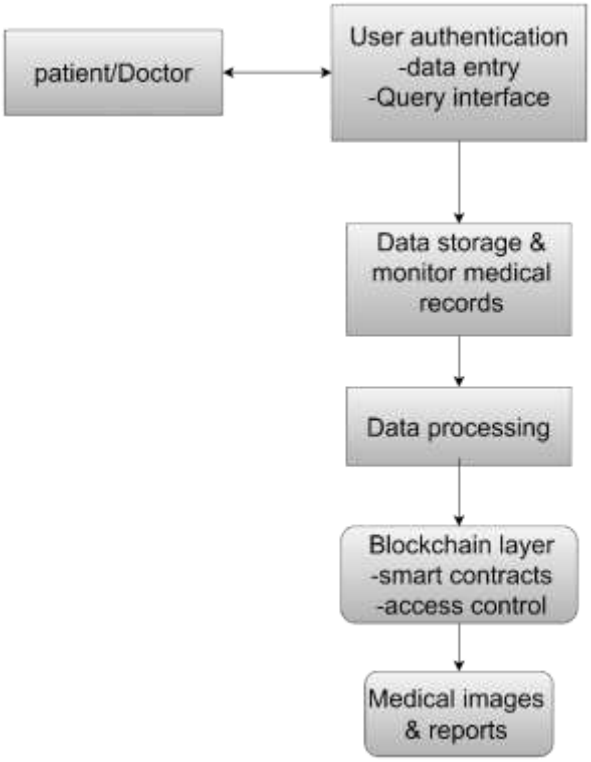

Figure1 Architectural diagram for patient Management system

2.2 The techniques employed

2.2.1 Blockchain Technology: Blockchain technology provides safe and consistent recording of events using a distributed record of transactions that is not maintained. To deal with the demand for a centralized authority, blockchain technology facilitates the protected storage of patient data in the medical sector. Cryptographic hashing maintains data accuracy and openness by connecting each transaction to the earlier block and capturing it in a block. The use of this technology is ideal for keeping patient data secure since it reduces the chance of illegal modifications.

2.2.2 Blockchain working model:

Blockchain is an integrated network of nodes which stores information. This type of technology is excellent for maintaining private information securely in the system. There is not a single entity that

controls the Blockchain. Instead, it is built up of nodes, which are standalone computers that maintain records of present and past along with transaction data. Everyone who uses the network can store and share data. Blockchain is a system made up of three key concepts: blocks, nodes & miners. Blockchain does not maintain all of its data in one place. A network of computing devices instead stores and shares the Blockchain. A new block gets added to the Blockchain whenever a device on a network changes its Blockchain. Figure 2 shows the basic working model Blockchain technology.

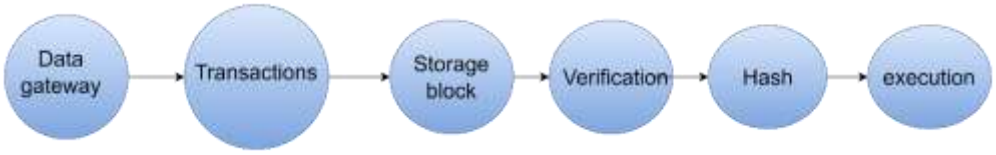

Figure2 Blockchain working model

2.2.3. Cryptographic Hashing: A method to improve the integrity and security of data. Patient data based on a healthcare systems has been transformed into a fixed-length hashing value before being stored. This assures that even small changes generate a completely distinct hash, which allows tracking of illegal changes. Common hashing methods include SHA-256, that is often used for secured medical data storage.

2.2.4. Smart contracts: Smart contracts are based on a self implementing tasks with predetermined terms. Smart contracts protect the confidentiality of medical records in patient management systems, permitting only physicians & hospital staff to access or modify them. These contracts maintain healthcare rules, safeguard information & minimize intermediaries**.**

2.2.5. Consensus Mechanism: The consensus process is a key feature that ensures network members compliance & assurance. Proof-of-Work (PoW) & Proof-of-Stake (PoS) are two types of consensus techniques that healthcare blockchains employ for verifying transactions as well as prevent fraud. The reliability and safety of patient data maintained on the blockchain are guaranteed by these processes, that make sure only valid transactions are made.

2.2.6. Access Control Models: Patient management systems based on the blockchain technology utilizes Role-Based Access Control (RBAC) to stop outsiders from accessing it. Through the implementation of role-based access control, only authorized users including healthcare professionals will be permitted to see or perform modifications to patients' medical records. In accordance with healthcare rules that include GDPR & HIPAA, this method increases data privacy & prevents hacking of data. The flowchart for the Blockchain technology is shown in figure3.

International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 1, 2025
https://www.theaspd.com/ijes.php

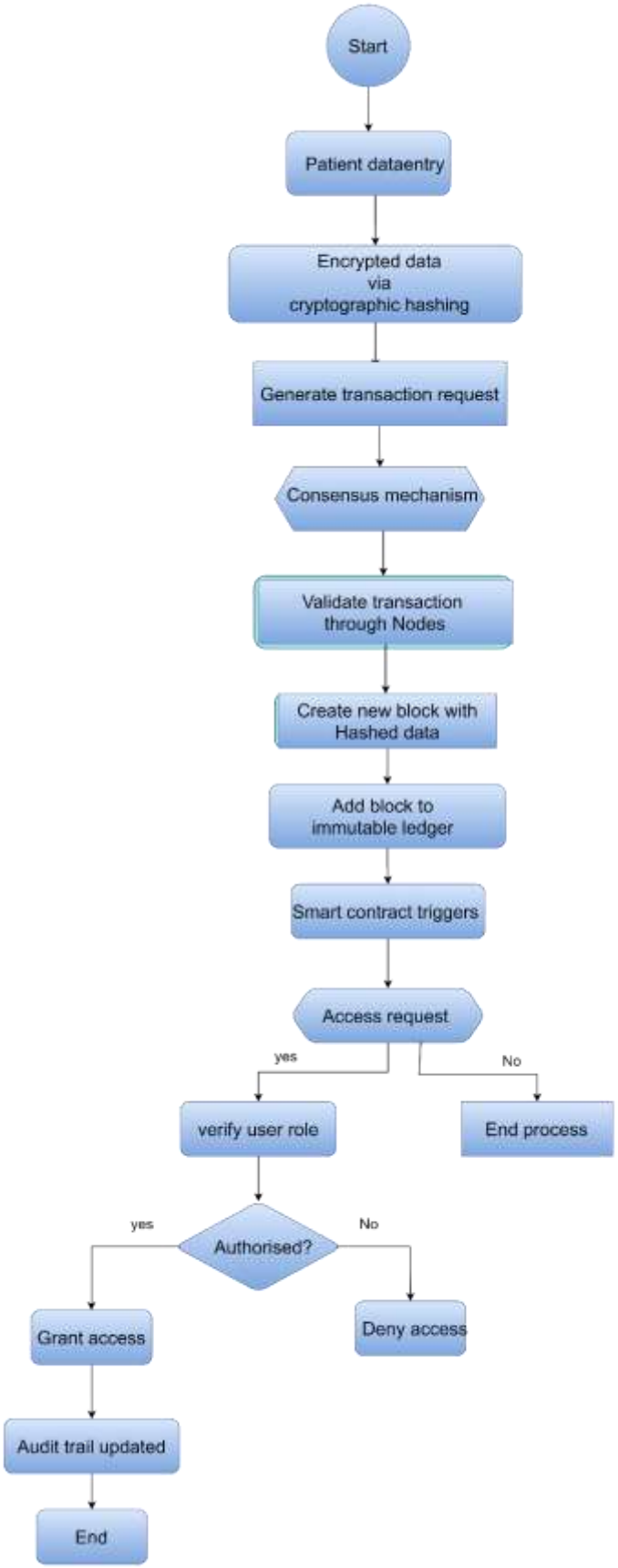

Figure3 Block chain technology flowchart

2.3. Mathematical model Analysis for Blockchain technology

The cryptographic hash of data d is represented by H(d).

The data integrity is given by

$$H(d) = H(d') \quad (1)$$

In Access Control the user authentication follows

$$A_{cont} = f(u_i, p_i) \quad (2)$$

where U_i is user ID and P_i is permissions

The Blockchain Validation using Merkle Tree that ensures secure block verification

is given by

$$M = H(H(L1) \| H(L2)) \quad (3)$$

Valid transaction assures that all block will remain tamper proof

$$T_{vaid} = \sum_{i=1}^{n} H(b_i) \quad (4)$$

Mechanism for encryption is given by

$$C = E_k(D) \quad (5)$$

where C is encrypted data & E_k is the encryption function with key k.

2.4 Algorithm for Safe Data Storage and Recovery

The key elements of the algorithm include cryptographic hashing, blockchain storage, access control, data recovery and decryption are shown in algorithm1. The aim is to protect the confidentiality and safety of patient information by converting it into a hash value of a specific size. A cryptographic hash method such as SHA-256 is employed to encrypt patient data D. and this ensures tamper detection by creating an entirely new hash even for tiny changes to D.

In Distributed ledger technology the blockchain captures the encrypted information as a transaction with the hash value H(D). For the purpose of the auditing process, each financial transaction is given an individual Transaction ID (TID) which prevents unauthorized alterations. The purpose of smart contracts with access control to automate authorization and verification processes. The smart contract examines the user's identities when they need data. The smart contract obtains H(D) through the blockchain if it is permissible. Access will be restricted if it is not permissible, maintaining compliance to confidentiality regulations.

The system recovers H(D) from the blockchain, which contains encrypted data. Using a safe key the user decodes the information. The smart contract maintains secured data by refusing access.

Algorithm1

Algorithm1 demonstrates Safe Data Storage & Recovery using Blockchain.

```
Input: Patient Data D, User Request R

Output: Encrypted & Stored Data or Retrieved Data

STEP1:Begin

STEP2:Encrypt Data D using cryptographic hashing → H(D)

STEP3:Generate Unique Transaction ID TID

STEP4:Store H(D)on Blockchain with TID

STEP5:If User Requests Data:

STEP6:Verify Authentication via Smart Contract

STEP7If Authorized: Retrieve  and Decrypt Data

STEP6:Else: Access Denied

End
```

3.RESULTS & DISCUSSION

The proposed blockchain technology was implemented and tested in a simulated healthcare platform. The Key performance indicators include transaction speed, security resilience and effectiveness of access control were determined. In table1 the following metrics are evaluated as shown.

Table1 Performance Comparison Proposed Vs Conventional Method

Metrics	Proposed blockchain method	Conventional method
Encryption time	0.5 sec	0.1 sec
Transaction speed	2.1 sec	0.3 sec
Access verification	1.2 sec	2.5 sec
Data integrity	100%	95%
Unauthorised access blocked attempts	98%	70%

3.1 Healthcare data management using blockchain technology:

By implementing blockchain technology to healthcare data management, it solves significant issues like security of information, accessibility, as well as sharing thereby rendering the process far more effective. Centralized storage is frequently employed in old healthcare data systems, however it can be slow, accessible to hackers, and difficult to expand. Through the use of blockchain, hospitals and medical centres are able to maintain patient data securely while making sure that they are always accessible with restricted access.

3.2 Rapid access with protection

Blockchain-based healthcare data management provides faster retrieval of information & restricted protection. Blockchain employs distributed ledger system for retrieving data more quickly than centralized storage approaches, which are frequently delayed by server workload and congestion in the network. This enables medical professionals to quickly obtain necessary patient records, enhancing the

care of patients & decision-making. Blockchain safeguards the transfer of information through encrypted hashing & smart contracts. Cryptographic hashing maintains the patient data immutable and digital contracts facilitate access verification to minimize risk. Blockchain works well for dealing with confidential healthcare information due to its safety and efficacy.

3.3 Healthcare Administrative Interoperability

Contemporary health care data management relies on interoperability, which is very important. In the past, clinics and hospitals use distinct electronic medical record networks, which complicates seamless sharing of patient data. Blockchain overcomes this problem by providing a uniform as well as established method of storing information.

Blockchain-based healthcare systems allows numerous entities to securely share data and access information about patients without depending on centralized intermediaries. This enhances interaction among physicians, therefore ensuring increased evaluation, planning of treatment as well as patient monitoring. In addition, the decentralized traits of blockchain gets rid of single points of breakdown, thus improving reliability of the system substantially more.

3.4 The graph depicting Time taken to Retrieve Data vs. User Base

The efficient operation of blockchain in comparison to centralized storage techniques is demonstrated by the graph which illustrates data retrieval time with user count. Conventional central databases often become slower when more users request data about patients due to congestion in the network & server computing constraints. Blockchain-based storage, on the contrary hand shares data across numerous nodes in order to maintain a constant recovery time. This improved efficiency assures that healthcare professionals can quickly access information about patients regardless of rising amount of users, increasing overall health care results & medical response times. Healthcare providers could transform digital healthcare management through the application of blockchain technology to find an acceptable compromise among privacy of data, availability and effectiveness.

The figure4 depicts the relationship between the amount of time taken to retrieve data and the number of users for both centrally maintained storage & blockchain storage. When user counts increases, the graph indicates that blockchain storage substantially improves productivity, consequently decreasing the amount of time needed for retrieving data.

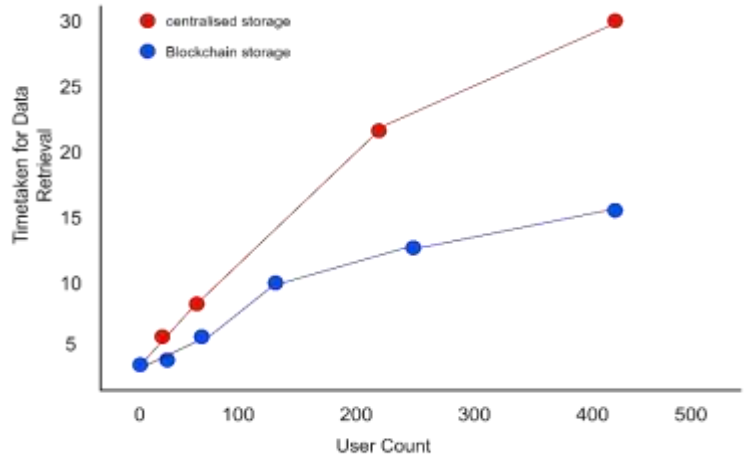

Figure4 User Count Vs Time taken for Data Retrieval

3.5 Evaluating the Levels of Privacy and Security

3.5.1. Preventing Data Leakage: Encryption renders data inaccessible even in case of a data breach. Intrusion Detection & Prevention Systems (IDPS) keep monitoring on data from networks to identify and stop activities that appear strange. The process of data tokenization improves security more effectively by altering private data with exclusive codes that cannot be utilized towards the owner if they move away. While data is transmitted from one system to a different one, network security methods like VPN firewalls and encrypted communication methods such as SSL/TLS keeps it secure. Finally, performing regular safety and security checks helps to identify the areas of weakness while making sure that healthcare data protection guidelines are being followed. By implementing these steps, healthcare communities may significantly reduce the chance of data breaches, safeguarding the security and confidentiality of patient data.

3.5.2. Tampering Resistance: Cryptographic hashing in blockchain offers tampering resistance by ensuring that any alteration in recorded data is instantly evident. Every single block in a blockchain has a unique hash created from its information. Each change, even the smallest one generates a totally new hash. Changing any information would disrupt the chain as each subsequent block is connected to the earlier one by hashing resulting in simple detection of modification. The decentralized design of blockchain assures that, many copies of the records are distributed across various nodes, thus preventing illegal changes from being undetected. Blockchain is an excellent method to secure sensitive patient information from cyber assaults along with unauthorized access, as advanced hashing algorithms that use SHA-256 offers excellent data integrity. Table2 shows the security comparison of blockchain & traditional methods.

Table2 Security Comparison between blockchain & traditional database.

Characteristics	Blockchain Database	Traditional Database
Immutable Records	Yes	No
Decentralized data	Yes	No
Auditability	High	Low
encryption	End to end	Limited

Using significant performance metrics including scalability, interoperability, data security, tamper resistance and efficiency, the figure5 compares the blockchain-based methods to traditional methods in safety management. Blockchain-based applications outperform other alternatives on every measure to its decentralized & cryptographically secure architecture. Cryptography hashing as well as decentralized storage makes blockchain 95% safer than standard systems. This is because they reduce the risks of information theft and illegal access. Interoperability is a major issue for conventional healthcare systems, but blockchain's constant accessible data-sharing mechanisms makes it 90% smoother. Conventional systems get only 65% for scalability as they have problem with limited storage as well as rising transaction workloads. Blockchain on the contrary hand, achieves 85% because it utilizes spread storage along with consensus techniques to handle increasing information counts more effectively.

Moreover, blockchain-based management systems have been 88% more efficient than conventional ones. Smart contracts made this change possible because they simplify access to data and evidence, curbing down on the requirement for human action as well as delays. Finally, blockchain has the greatest benefit when it comes to intrusion resistance which is an important aspect of safe data management. It ranks 98% when compared to 50% for traditional systems, since cryptographic hashing along with immutability makes it extremely difficult for people who aren't meant to make modifications.

International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 1, 2025
https://www.theaspd.com/ijes.php

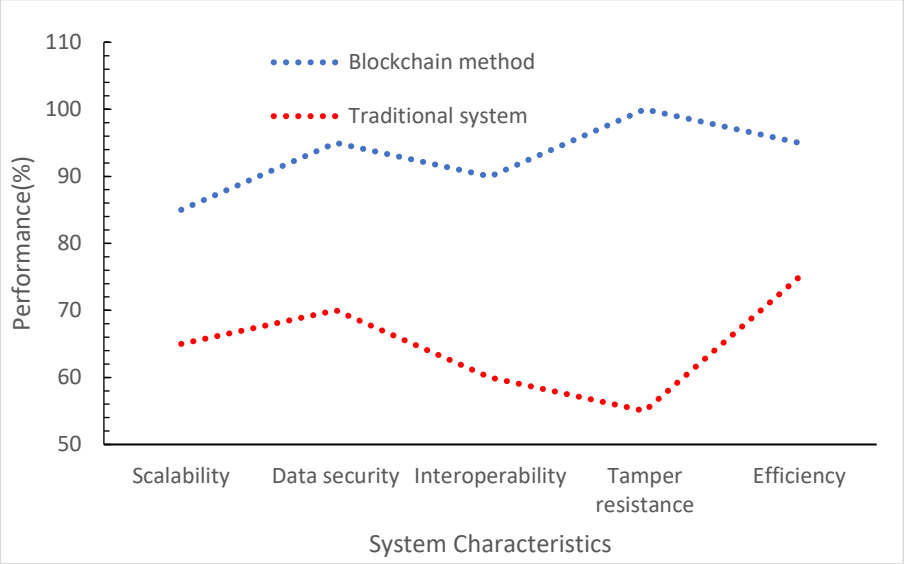

Figure5 Performance characteristics of blockchain and traditional methods

3.6 Problems and Boundaries

3.6.1. Adaptability: As more transactions take place, blockchain systems (like Ethereum) might encounter slower performance. One of the primary concerns when employing blockchain in healthcare management of data is scalability. The efficient operation of blockchain system might be affected as an increasing number of users & increase in transactions. The use of consensus methods like Proof-of-Stake or Proof-of-Work in public blockchain platforms like Ethereum could result in slower processing times when handling huge amounts of medical data. Ethereum handles transactions in blocks, network congestion could result in delays in retrieving information & verification during peak times. Applications for real-time healthcare such as live patient monitoring or quick access to medical records might be affected by this delay. Healthcare blockchain technologies frequently examine scaling methods like rollups, sharding & sidechains to overcome these challenges. These approaches may boost the volume of transactions while protecting security as well as decentralization.

3.6.2. Storage expenses: The cost of storing data is another significant issue for healthcare systems which utilize blockchain. It is not possible to save large medical files including X-rays, MRI scans as well as high-resolution clinical images instantly on the blockchain as it is too expensive and has less storage spaces. Blockchain networks operate effectively while they are used to store shorter records of transactions instead of huge amounts of data. It might become more costly to save massive medical data.

3.7 Future Enhancements

3.7.1. IoT integration: IoT integration has become crucial role for enhancing healthcare as it makes safe exchange of information & real-time monitoring feasible. Essential health parameters including blood pressure, heart rate and glucose levels are continuously recorded by wearable health gadgets like fitness trackers, medical sensors and smartwatches. These gadgets provide secure, impermeable storage while maintaining patient privacy by authenticating and transferring medical data immediately to the blockchain. The internet of things offers medical professionals access to real-time information about patients, enabling remote monitoring & quick responses. In addition, smart contracts have the capacity to automatically execute reactions based on the information collected such us emailing out notifications for unexpected medical circumstances. While ensuring privacy and compliance to medical data regulations, this seamless interaction promotes patient care, reduces human error and increases overall healthcare productivity.

3.7.2. Access Control Based on Artificial Intelligence: This AI-based security system uses algorithms based on machine learning is used to identify errors in requests for access & block illegal entry. Access control mechanisms that use AI detect patterns for unsuccessful logins, the location and gadget use. If a suspicious time of access or gadget is detected, the system could trigger temporary access limitations or multi-factor authentication (MFA). AI permits access according to risk levels & adapts from previous access patterns for improving accuracy. AI increases protection, error detection and efficient access control is given by combining behavioral analytics, real-time threat detection and biometric authentication. Table3 depicts the current performance with future enhancement method.

Table3 Proposed Enhancement

Field	Current performance	Future Enhancement
Transaction speed	2.1 sec	Sharding for faster processing
Storage cost	High	IPFS for off-chain storage
Smart contracts	Rule based	AI powered dynamic policies

4.CONCLUSION

Healthcare storage of information, accessibility and protection have gone through a fundamental shift with the arrival of blockchain technology into patient data management systems. Difficulties with conventional medical data management systems includes lack of transparency, interoperability, centralized imperfections, and data thefts. By incorporating automated access control, cryptographic security as well as decentralization, blockchain offers a reliable alternative that significantly boosts the security, efficacy and reliability of healthcare data administration. The capability of blockchain technology to provide data immutability and consistency represents one of its most important advantages. Health information are kept safe and reliable as patient records cannot be changed or manipulated, once they have been saved on the blockchain. Since it ensures that patient information is valid, this function is very important for legal and regulatory purposes. Furthermore, the utilization of cryptographic hashing assures that the privacy of data remains unchanged even when it is circulated across numerous companies.

The implementation of blockchain technology in handling medical records seems to have an optimistic outlook. Advancement in federated learning, secure multi-party computing & AI-driven analytics are going to boost the potential of blockchain technology as it expands. These advancements will eventually transform the administration and utilization of medical records through enabling more effective exchange of information, real-time monitoring of patients as well as forecasting medical insights.

REFERENCES:

1. Zaabar, Bessem, et al. "HealthBlock: A secure blockchain-based healthcare data management system." Computer Networks 200 (2021): 108500.
2. Tariq, Muhammad Usman. "Revolutionizing health data management with blockchain technology: Enhancing security and efficiency in a digital era." Emerging technologies for health literacy and medical practice. IGI Global Scientific Publishing, 2024. 153-175.
3. Mewada, S., Saroliya, A., Chandramouli, N., Kumar, T. R., Lakshmi, M., Mary, S. S. C., & Jayakumar, M. (2022). Smart diagnostic expert system for defect in forging process by using machine learning process. Journal of Nanomaterials, 2022(1), 2567194.
4. Hovorushchenko, Tetiana, Artem Moskalenko, and Vitaliy Osyadlyi. "Methods of medical data management based on blockchain technologies." Journal of Reliable Intelligent Environments 9.1 (2023): 5-16.

5. Yaqoob, Ibrar, et al. "Blockchain for healthcare data management: opportunities, challenges, and future recommendations." Neural Computing and Applications (2022): 1-16.
6. Adeghe, Ehizogie Paul, Chioma Anthonia Okolo, and Olumuyiwa Tolulope Ojeyinka. "Evaluating the impact of blockchain technology in healthcare data management: A review of security, privacy, and patient outcomes." Open Access Research Journal of Science and Technology 10.2 (2024): 013-020.
7. Taloba, Ahmed I., et al. "A framework for secure healthcare data management using blockchain technology." International Journal of Advanced Computer Science and Applications 12.12 (2021).
8. Adeghe, Ehizogie Paul, Chioma Anthonia Okolo, and Olumuyiwa Tolulope Ojeyinka. "Evaluating the impact of blockchain technology in healthcare data management: A review of security, privacy, and patient outcomes." Open Access Research Journal of Science and Technology 10.2 (2024): 013-020.
9. BramahHazela, J. Hymavathi, T. Rajasanthosh Kumar, S. Kavitha, D. Deepa, Sachin Lalar, and Prabakaran Karunakaran. "Machine Learning: Supervised Algorithms to Determine the Defect in High-Precision Foundry Operation." Journal of Nanomaterials 2022, no. 1 (2022): 1732441.
10. Singh, Suruchi, et al. "Blockchain technology for efficient data management in healthcare system: Opportunity, challenges and future perspectives." Materials Today: Proceedings 62 (2022): 5042-5046.
11. Wang, Haoxiang. "IoT based clinical sensor data management and transfer using blockchain technology." Journal of ISMAC 2.03 (2020): 154-159.
12. Saif, Sohail, Suparna Biswas, and Samiran Chattopadhyay. "Intelligent, secure big health data management using deep learning and blockchain technology: an overview." Deep Learning Techniques for Biomedical and Health Informatics (2020): 187-209.
13. Saif, Sohail, Suparna Biswas, and Samiran Chattopadhyay. "Intelligent, secure big health data management using deep learning and blockchain technology: an overview." Deep Learning Techniques for Biomedical and Health Informatics (2020): 187-209.
14. Tian, Haibo, Jiejie He, and Yong Ding. "Medical data management on blockchain with privacy." Journal of medical systems 43 (2019): 1-6.
15. Abbas, Asad, et al. "Blockchain-assisted secured data management framework for health information analysis based on Internet of Medical Things." Personal and ubiquitous computing 28.1 (2024): 59-72.
16. Azbeg, Kebira, Ouail Ouchetto, and Said Jai Andaloussi. "BlockMedCare: A healthcare system based on IoT, Blockchain and IPFS for data management security." Egyptian informatics journal 23.2 (2022): 329-343.
17. Bittins, Soeren, et al. "Healthcare data management by using blockchain technology." Applications of blockchain in healthcare (2021): 1-27.
18. Attaran, Mohsen. "Blockchain technology in healthcare: Challenges and opportunities." International Journal of Healthcare Management 15.1 (2022): 70-83.
19. Siyal, Asad Ali, et al. "Applications of blockchain technology in medicine and healthcare: Challenges and future perspectives." Cryptography 3.1 (2019): 3.
20. R.Senthamil Selvan “Implementing Machine Learning Techniques for the Anticipation of Maintenance Requirements in Naval Assets” by 2024 Second International Conference Computational and Characterization Techniques in Engineering & Sciences (IC3TES), 15-16 November 2024,ISSN:0018-9219,E-ISSN:1558-2256, 17 February 2025, DOI: 10.1109/IC3TES62412.2024.10877593
21. R.Senthamil Selvan “Optimising IoT-Enabled Healthcare Systems with Deep Learning: sensors Data Fusion, Prognostic Modelling, and Smart Management” by 2024 Second International Conference Computational and Characterization Techniques in Engineering & Sciences (IC3TES), 15-16 November 2024,ISSN:0018-9219,E-ISSN:1558-2256, 17 February 2025, DOI: 10.1109/IC3TES62412.2024.10877558
22. R.Senthamil Selvan “Evaluation and Implementation of Optimal Classification Algorithms for Credit Card Fraud Detection” by 2024 Second International Conference Computational and Characterization Techniques in Engineering & Sciences (IC3TES), 15-16 November 2024,ISSN:0018-9219,E-ISSN:1558-2256, 17 February 2025, DOI: 10.1109/IC3TES62412.2024.10877521
23. R.Senthamil Selvan “Classification and Signal Detection in Shared Spectrum Using a Deep Learning Method” by 2024 Second International Conference Computational and Characterization Techniques in Engineering & Sciences (IC3TES), 15-16 November 2024,ISSN:0018-9219,E-ISSN:1558-2256, 17 February 2025, DOI: 10.1109/IC3TES62412.2024.10877437
24. R.Senthamil Selvan “Adoption and Acceptance of Tele health Technologies in Mental Health Services during COVID-19” by 2024 Second International Conference Computational and Characterization Techniques in Engineering & Sciences (IC3TES), 15-16 November 2024,ISSN:0018-9219,E-ISSN:1558-2256, 17 February 2025, DOI: 10.1109/IC3TES62412.2024.