A Blockchain-Enabled Tamper-Proof Approach For Enhanced Medical Data Integrity And Access

S.Sreeja Reddy [1], Y.Mahisri Reddy [2], T.Varditha Reddy [3], M.Swetha [4],
[1,2,3] UG Scholar, Department of Computer Science and Engineering, St. Martins Engineering College, Secunderabad, Telangana, India, 500100
[4]Assistant Professor, Department of Computer Science and Engineering, St. Martins Engineering College, Secunderabad, Telangana, India, 500100

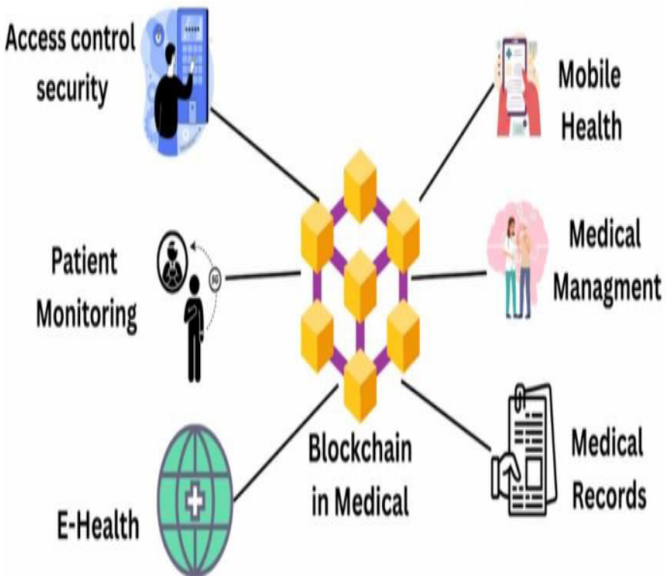
Abstract

The healthcare industry has seen significant advancements over the past few decades, but issues related to data integrity and access control remain critical concerns. In India, the healthcare sector has experienced rapid growth, with a market size expected to reach $372 billion by 2022. Blockchain technology has emerged as a transformative solution for enhancing the integrity and access control of medical data. Its decentralized and tamper-proof nature ensures that patient information remains secure, accessible only to authorized individuals while maintaining transparency and traceability. Our main objective is to enhance the integrity and security of medical data through a decentralized blockchain approach and to improve access control mechanisms to ensure that only authorized personnel can access sensitive medical information. Traditional healthcare systems relied on centralized databases, where patient records were stored and managed by a single entity, such as hospitals or clinics. Traditional healthcare systems face significant challenges in maintaining data integrity and security due to their centralized nature, which makes them vulnerable to unauthorized access, data breaches, and manipulation.. With increasing concerns about data privacy and security, there is a pressing demand for innovative solutions that leverage blockchain technology to ensure that medical data remains secure, accurate, and accessible only to authorized users. The proposed decentralized blockchain model enhances medical data integrity and access control by creating a secure and transparent platform for managing patient records. Each patient's data is stored on a blockchain as a unique record, which cannot be altered without consensus from the network. This tamper-proof nature of blockchain ensures that any unauthorized attempts to manipulate data can be detected and prevented.

ywords: Healthcare industry, Transparency, Security, Data Integrity, Access Control, Tamper-Proof, Patient Records.

1.INTRODUCTION

The healthcare industry in India is growing rapidly, but with this expansion comes the increasing need to secure and protect the vast amounts of sensitive patient data generated daily. As of 2022, the healthcare market in India was valued at $372 billion, driven by advancements in technology and the government's push toward digital healthcare services. However, traditional systems for managing medical data, which rely on centralized databases, face significant challenges in maintaining data integrity, privacy, and security. Cybersecurity issues in Indian healthcare have escalated, with a 125% increase in data breaches over the past five years, exposing millions of patient records. These breaches often lead to unauthorized access, data manipulation, and even identity theft. Blockchain technology, with its decentralized, transparent, and immutable nature, has emerged as a transformative solution to address these issues.



By

storing medical data in a tamper-proof ledger, remains immutable, safeguarding the integrity of medical records. This is especially

critical in India, where multiple stakeholders, from hospitals to insurance companies, handle sensitive patient information, often leading to vulnerabilities. Blockchain-enabled systems are designed to revolutionize healthcare by securing patient data and ensuring accurate, tamper-proof records. The decentralized nature of blockchain makes it impossible for any single entity to manipulate data, thus ensuring transparency. Additionally, blockchain allows for better patient data management across multiple healthcare providers, enhancing care coordination. Its applications include securely sharing electronic health records (EHRs), ensuring data privacy in clinical trials, and enabling secure insurance claim processes, preventing fraud.

2.LITERATURE SURVEY

Cui et al. [1] proposed a blockchain-based framework for supply chain provenance, which ensures the traceability and authenticity of data through a decentralized approach. Their research highlights the advantages of using blockchain for secure provenance in various sectors by addressing the issues of data manipulation and unauthorized modifications. The framework ensures tamper-proof records and facilitates trust among different stakeholders by leveraging blockchain's immutable ledger.Hardin and Kotz [2] introduced Amanuensis, a framework for ensuring information provenance in health-data systems. Their work emphasizes the critical need for secure data lineage in healthcare to maintain data accuracy and reliability. The framework offers a mechanism to track the origin and transformation of health data, thereby improving patient safety and data security. They further discuss the challenges faced in integrating provenance systems into existing healthcare architectures.

Harley and Cooper [3] explored the concept of information integrity and its relevance in contemporary data management systems. Their comprehensive survey on integrity frameworks addresses key concerns such as data authenticity and trustworthiness. They identify gaps in current solutions and propose strategies for achieving robust information integrity, with a focus on applying blockchain for immutable and verifiable records. Hasan et al. [4] presented a solution for preventing history forgery with secure provenance mechanisms. Their work introduces a method to secure data history in storage systems, ensuring that no unauthorized changes can be made without detection. By combining cryptographic techniques with provenance, they aim to build trust in data storage systems and prevent malicious attacks on historical recorJaigirdar et al. [5] discussed the concerns of physicians regarding the trustworthiness of medical data in IoT-based health architectures. Their study highlights the risks associated with decentralized IoT health systems and the potential for data breaches

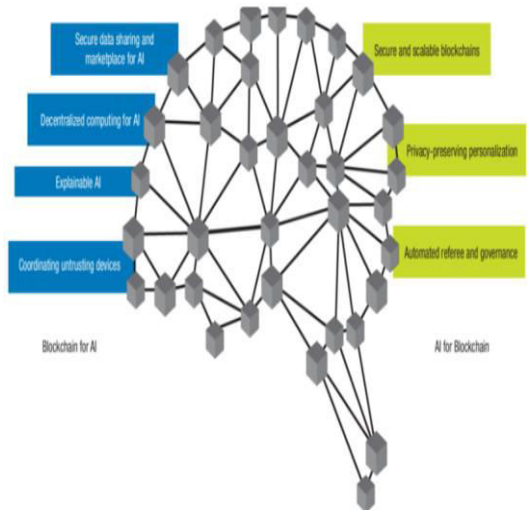
Kaur et al. [6] proposed a blockchain-based solution for managing heterogeneous medicare data in a cloud environment. Their work addresses the interoperability issues between different healthcare systems and presents a future direction for secure and reliable data sharing. By leveraging blockchain, they ensure data integrity, confidentiality, and improved collaboration among healthcare providers, thereby reducing the risks associated with traditional centralized systems. Kumar Lilhore et al. [7] explored cloud performance evaluation using hybrid load balancing models based on modified particle swarm optimization and improved metaheuristic firefly algorithms. Although primarily focused on cloud computing, their research has implications for medical data storage, emphasizing the importance of efficient resource allocation and performance optimization in cloud-based healthcare systems.Lei et al. [8] introduced a novel EMR integrity management approach using a blockchain platform in hospitals. Their model ensures secure storage and tamper-proof management of electronic medical records. By integrating blockchain technology with hospital systems, they aim to enhance the reliability of patient data, reduce fraud, and improve overall data management in healthcare. Toosi et al. [9] examined interconnected cloud computing environments, identifying challenges, taxonomies, and future directions. Their survey provides a comprehensive overview of multi-cloud environments and the associated risks of data loss and security breaches. The study proposes secure data management practices that align with blockchain's decentralized features for improved data integrity and access control. Vishwa and Hussain [10] proposed a blockchain-based approach for multimedia privacy protection and provenance. Their research focuses on safeguarding multimedia data by preventing unauthorized access and manipulation. The blockchain-based system ensures data authenticity and provides a reliable mechanism for tracing data origins and modifications. Yang et al. [11] presented a blockchain-based framework for big data networking that ensures data sharing and tamper-proofing. Their work highlights the importance of securing large datasets in decentralized networks while maintaining data privacy and integrity. The proposed framework leverages blockchain to create a secure, transparent environment for big data management. Yaqoob et al. [12] provided an extensive review of blockchain for healthcare data management, discussing its opportunities, challenges, and future recommendations. Their research emphasizes the potential of blockchain to address security and interoperability issues in healthcare, while also providing a roadmap for future developments in this field.

Zafar et al. [13] conducted a comprehensive survey on secure provenance schemes, offering a taxonomy of trustworthy data management. Their study categorizes existing provenance mechanisms and highlights the need for blockchain technology to overcome limitations in traditional data provenance approaches. They propose a future direction focused on building robust, verifiable data systems. Zheng et al. [14] provided an overview of blockchain technology, covering its architecture, consensus mechanisms, and future trends. Their research serves as a foundational reference for understanding the core concepts of blockchain and its application across industries, including healthcare. The study identifies the potential of blockchain to revolutionize data integrity and access control in medical data management systems.

Patel.R.&Zhao, L.[15] Proposed a patient-centered data management system using blockchain, focusing on secure data sharing, access control &improved data integrity.

3.PROPOSED METHODOLOGY

Blockchain is a decentralized digital ledger that securely records transactions across a network of computers. Each block contains a list of transactions and links to the previous block, forming a chain. This structure ensures that once data is recorded, it becomes extremely difficult to alter, promoting transparency and security. When a transaction is initiated, it undergoes validation through consensus mechanisms like Proof of Work or Proof of Stake. Once validated, the transaction is grouped with others into a block, which is then added to the existing blockchain in a way that is permanent and unalterable. This decentralized validation and storage eliminate the need for a central authority. A blockchain consists of a series of blocks, each containing a cryptographic hash of the previous block, a timestamp, and transaction data. The decentralized nodes in the network maintain and validate the blockchain, ensuring consistency and security across the system. After coding, rigorously test the contract to identify and fix potential vulnerabilities. Once validated, deploy the smart contract onto the blockchain network, where it will operate autonomously, executing transactions when specified conditions are met.



ADVANTAGES:

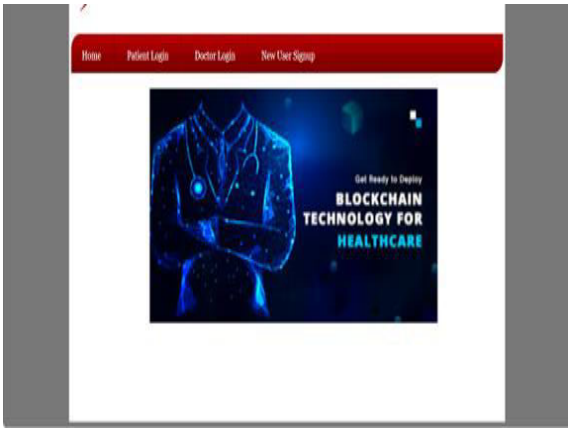
- **Security:** The decentralized and cryptographic nature of blockchain makes it resistant to tampering and fraud.
- **Transparency:** All transactions are recorded on a public ledger, promoting openness.
- **Immutability:** Once information is added, it cannot be altered, ensuring a reliable record of transactions.
- **Efficiency:** Automated processes, such as smart contracts, streamline and expedite transactions by eliminating intermediary

4.EXPERIMENTAL ANALYSIS

Integrating blockchain and artificial intelligence (AI) in cybersecurity fortifies data protection and enhances threat detection. Blockchain's decentralized ledger ensures data integrity and transparency, while AI's advanced algorithms analyze vast datasets to identify anomalies and predict potential threats.

Implementation Steps:

- **Data Integrity Assurance:** Utilize blockchain's immutable ledger to securely store and verify the authenticity of data, ensuring it remains unaltered and trustworthy.
- **Decentralized Identity Management:** Implement blockchain for secure identity verification, reducing reliance on centralized authorities and minimizing single points of failure.
- **AI-Driven Threat Detection:** Deploy AI algorithms to monitor network traffic and user behavior, identifying patterns indicative of cyber threats in real-time.
- **Smart Contract Automation:** Use blockchain-based smart contracts to automate security protocols, ensuring consistent and tamper-proof execution of cybersecurity policies.
- **Secure Data Sharing:** Facilitate encrypted and transparent data exchange between entities using blockchain, with AI monitoring for unauthorized access or anomalies.
- **Benefits:**
- **Enhanced Security:** The combination of blockchain's tamper-proof records and AI's predictive capabilities creates a robust defense against cyber threats.
- **Improved Efficiency:** Automated processes reduce manual intervention, allowing cybersecurity professionals to focus on complex challenges.
- **Scalability:** The integrated system can adapt to growing data volumes and evolving threats, maintaining performance and security standards.



The Figure Show the Home Page of the Helathcare with the text "Home Patient Login ,Doctor Login New User Signup at the top and BLOCKCHAIN TECHNOLOGY FOR HEALTHCARE in the center.

Contact No: XXXXXXX

- **Email ID:** XXXX@gmall.com
- **Address:** XXXXXX
- **Self Description:** 25 years suffering from headache
- **Identification No:** #####
- **User Type:** A dropdown menu with "Doctor" selected, and "Patient" as the other option.

Login Screen

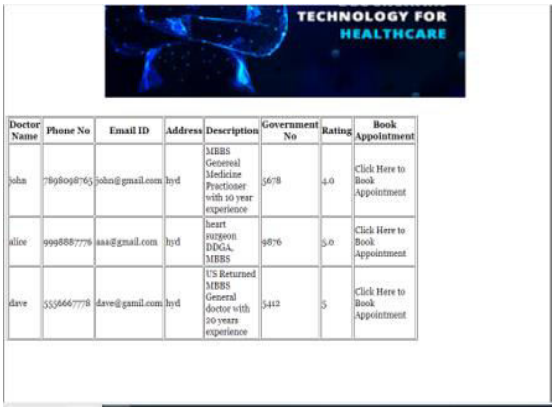
The Figure shows a **Patient Login Screen**:

- **Title:** "Patient Login Screen" clearly labels the page's purpose.
- **Username Field:** Filled with "suresh".
- **Password Field:** Masked with dots for security.
- **Login Button:** A button labeled "Login" to submit credentials.

Patient home screen

This image depicts a patient's logged-in screen of healthcare platform utilizing blockchain technology.

- **View Doctors List:** Allows the patient to browse available doctors.
- **View Prescriptions:** Enables the patient to access their prescribed medications.
- **Feedback & Ratings:** Likely a section to provide feedback on doctors or services and view ratings.
- **Logout:** Provides a way to securely exit the platform.



Doctor List

The Figure shows a Doctor List:

- **Doctor Name:** The name of the doctor (e.g., John, Alice, Dave).
- **Phone No:** The doctor's phone number.
- **Email ID:** The doctor's email address.
- **Address:** The doctor's location (e.g., hyd, indicating Hyderabad).
- **Description:** A brief description of the doctor's qualifications, specialization, and experience (e.g., "MBBS General Medicine Practitioner with 10 years experience").
- **Government No:** Likely a registration or license number.
- **Rating:** The doctor's rating (e.g., 4.0, 5.0).
- **Book Appointment:** A button or link to book an appointment with the doctor

Book History of appointment

The Figure shows that screen provides a record of the patient's interaction with the healthcare system, including their submitted report. It also allows them to view their prescription

5.CONCLUSION

The integration of Artificial Intelligence (AI) and blockchain technology has emerged as a transformative approach in enhancing cybersecurity measures. AI's advanced capabilities in data analysis and pattern recognition, when combined with blockchain's decentralized and immutable ledger system, offer a robust framework for securing digital infrastructures. This synergy not only fortifies data integrity and confidentiality but also provides automated, real-time responses to potential threats, thereby significantly reducing the risk of cyber-attacks. The collaborative application of these technologies has demonstrated substantial improvements in identifying anomalies, preventing unauthorized access, and ensuring the authenticity of transactions across various sectors. The proposed decentralized blockchain model enhances medical data integrity and access control by creating a secure and transparent platform for managing patient records. Additionally, integrating quantum computing with AI and blockchain could unlock unprecedented levels of security and processing power, enabling the handling of complex cryptographic challenges and vast datasets more efficiently. As these technologies continue to mature, their combined application is expected to lead to more autonomous and intelligent security systems, capable of self-healing and adaptation in the face of new cyber threats. As cyber threats continue to evolve in complexity, the AI-blockchain amalgamation stands as a promising solution to proactively address and mitigate security challenges, paving the way for more resilient and trustworthy digital ecosystems.

REFERENCES

[1]Cui, P., Dixon, J., Guin, U., & Dimase, D. (2019). A blockchain-based framework for supply chain provenance. IEEE Access, p. 7, 157113–157125.

[2]Hardin, T., & Kotz, D. (2021). Amanuensis: Information provenance for health-data systems. Information Processing & Management, 58(2), 102460.

[3]. Harley, K., & Cooper, R. (2021). Information Integrity: Are We There Yet?. ACM Computing Surveys (CSUR), 54(2), 1-35.

[4]. Hasan, R., Sion, R., & Winslett, M. (2009). Preventing history forgery with secure provenance. ACM Transactions on Storage (TOS), 5(4), 1-43.

[5]. Jaigirdar, F. T., Rudolph, C., & Bain, C. (2019, January). Can I trust the data I see? A Physician's concern on medical data in IoT health architectures. In Proceedings of the Australasian computer science week multiconference (pp. 1-10).

[6]. Kaur, H., Alam, M. A., Jameel, R., Mourya, A. K., & Chang, V. (2018). A proposed solution and future direction for blockchain-based heterogeneous medicare data in cloud environment. Journal of medical systems, 42, 1-11.

[7]. Kumar Lilhore, Dr & Simaiya, Sarita & Maheshwari, Shikha & Manhar, Advin & Kumar, Santosh & Chitkara,. (2020). Cloud Performance Evaluation: Hybrid Load Balancing Model Based on Modified Particle Swarm Optimization and Improved Metaheuristic Firefly Algorithms. Engineering Science and Technology an International Journal. 12315-12331.

[8]. Lei Hang, Eunchang Choi & Do-Hyeun Kim 1. (2019, April 25). A novel EMR integrity management based on a medical blockchain platform in hospital.MDPI.

[9]. Toosi, A. N., Calheiros, R. N., & Buyya, R. (2014). Interconnected cloud computing environments: Challenges, taxonomy, and survey. ACM Computing Surveys (CSUR), 47(1), 1-47.

[10]. Vishwa, A., & Hussain, F. K. (2018, November). A blockchain based approach for multimedia privacy protection and provenance. In 2018 IEEE symposium series on computational intelligence (SSCI) (pp. 1941-1945). IEEE.

[11].Yang, J., Wen, J., Jiang, B., & Wang, H. (2020). Blockchain-based sharing and tamper-proof framework of big data networking. IEEE Network, 34(4), 62-67.

[12]. Yaqoob, I., Salah, K., Jayaraman, R., & AlHammadi, Y. (2022). Blockchain for healthcare data management: opportunities, challenges, and future recommendations. Neural Computing and Applications, 1-16.

[13]. Zafar, F., Khan, A., Suhail, S., Ahmed, I., Hameed, K., Khan, H. M., ... & Anjum, A.(2017). Trustworthy data: A survey, taxonomy and future trends of secure provenance schemes. Journal of network and computer applications, 94, 50-68.

[14].Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017, June). An overview of blockchain technology: Architecture, consensus, and future trends. In 2017 IEEE international congress on big data (BigData congress) (pp. 557-564). Ieee.