Review paper on healthcare record management system using blockchain technology

Khushi Lawankar[1], Swapnil Sawalkar[2]
[1,2] *Sipna college of engineering and technology amravati*

***Abstract*—In the current medical insurance claims process, there are problems of low efficiency and complex services. When a patient applies for medical insurance claims, he/she must go to the hospital to apply for a diagnosis certificate and receipt and then send the relevant application documents to the insurance company. The patient will not receive compensation until the company completes the verification with the patient's hospital. However, we can improve the current dilemma through blockchain technology. Blockchain technology can effectively open up the information channels of the insurance industry and medical institutions, promote industry integration, and enhance the ability of insurance companies to obtain information.In this project we proposed an integrated healthcare system in which all the hospitals and insurance companies will be able to do registration in our system. The patient's health record eg medical bills, reports, admit cards etc will be maintained on blockchain servers in encrypted format and patient will be able to claim the insurance. The insurance company will be able to review all the bills and reports. As all data is maintained on blockchain servers there is no possibility of manipulation in bills and reports hence transparency will be maintained and security of the claims processing will be increased.**

This blockchain-based approach offers significant improvements in data privacy, security, and efficiency, and has the potential to revolutionize the management of healthcare records by ensuring that all critical healthcare information—patient data, medical documents, and insurance records—are securely and transparently handled in a unified systemThe integration of these three key data sets within a single blockchain framework ensures seamless interaction and verification of records across all stakeholders. The use of a decentralized ledger enhances data security, reduces fraud, and provides an auditable trail of all transactions, ensuring accountability. Furthermore, the system allows for faster claims processing, minimizes administrative overhead, and improves the accuracy of medical treatments by ensuring that accurate and up-to-date patient information is always available.[3]

.

1. INTRODUCTION

The blockchain-based healthcare record management system is a modern solution designed to address the challenges of traditional medical record-keeping and insurance claim processes. In the current system, patient data is often scattered across different hospitals and insurance providers, leading to delays, inefficiencies, and risks of data tampering or loss. By using blockchain technology, this system enables secure, decentralized, and tamper-proof storage of patient health records such as medical reports, bills, and admission details. All participating hospitals and insurance companies are connected through a unified network, allowing authorized users to access and verify data in real time. This not only enhances data privacy and security but also speeds up insurance claim processing, reduces administrative workload, and ensures transparency across all parties involved. Ultimately, the integration of blockchain in healthcare record management aims to build a more efficient, trustworthy, and patient-centered healthcare ecosystem.

In Blockchain like a distributed ledger, singular transactions are encrypted into blocks by the applicable encryption, added to the ledger and never deleted. The information in Blockchain is verified fundamentally by a linked list of encoded exchanges that utilizes a hash. The hash function generates a hash by encrypting the information fed in Blockchain. It shapes the foundation of a decentralized medicinal service stage shared by the patients and suppliers, acting as an interface to the patient's record. Blockchain is a cryptographically secured, immutable, write once, read anywhere type data structure. It consists of blocks and theses blocks are linked together using an unmodifiable key referencing mechanism.

The Blockchain data structure consists of the following components: • The Blockchain network has secured list of blocks which contains the useful information. • A peer-to-peer network which contains identical examples of the Blockchain data structure • A consensus mechanism which secures the harmonized growth of Blockchain. • A security mechanism that ensures that the data stored in the Blockchain network is immutable. 1.2 Problem Statement Currently, there are a huge amount of separate health information systems, which hold the data of the individual patients in huge silos of health information. These information systems are organized by different ways. The ways of organizing data depend on the goals of the health care provider's business. It is totally different in case of a diagnostic center or in case of a general practitioner. Anyway, in both cases ultimately (name, value) pairs describe the results of an encounter and different structuring procedures integrate the data into EHR records. The (name, value) pairs are implicitly always extended by several essentials' attributes, where the time of the event represents a crucial role. In order to integrate these isolated data silos a series of interfaces are built and maintained continuously. To resolve the problem of interfacing the different health data recording systems a wide range of protocols have emerged.

In this model, dual Blockchain structure is used, the first part grants access to health data and is built using the Hyperledger Fabric. The second part of the structure works on Ethereum and performs all application and services. Medical information is very sensitive and personal so a closed Blockchain such as Hyperledger Fabric helps in retaining necessary privacy required. Majorly blockchains are classified as public Blockchains and permissioned Blockchains. This can be explained by considering the example of a user wants who to sell a book to person with some rebate and does not intend to talk about this to general public, the seller then can employ permissioned Blockchain to hide the information about the offer from the public. This model uses a double encryption mechanism on a permission-based Blockchain. The security that is provided by this model which uses Blockchain is beyond and far more advanced than any other centralized security system being used.
The health data is secured between the patient and the authorized doctor. When the authorised doctor adds additional information to the patients record history, the system will automatically update it. Only those clinicians who have authorized access can view the updates. None of the doctors are given permanent authorization, the access for the doctor ends when the patient wants so that the doctor can no longer update the record or access it. In emergency situations when the patient is unconscious and unable to provide any sort of input on his health, it would be vital to have access to the patients' health records. This information while performing lifesaving surgeries as history of past medications and illnesses are crucial before performing any sort of major surgery. There are two steps in building a new Machine learning model. The first step is to take in the dataset and adjust the model weights to increase the accuracy of the model. The second step is testing the Machine learning model on independent or new datasets for the accuracy of the model and thus validate the model and prevent overfitting of the model. An over fitted model is very good at a given dataset but is bad at hypothesizing for the given problem

2. LITERATURE SURVEY

Author: Chen, Y.; Ding, S.; Xu, Z.; Zheng, H.; Yang, S. Abstract: Accurate and complete medical data are one valuable asset for patients. Privacy protection and the secure storage of medical data are crucial issues during medical services. Secure storage and making full use of personal medical records has always been a concern for the general population. The emergence of blockchain technology brings a new idea to solve this problem. As a hash chain with the characteristics of decentralization, verifiability and immutability, blockchain technology can be used to securely store personal medical data. In this paper, we design a storage scheme to manage personal medical data based on blockchain and cloud storage. Furthermore, a service framework for sharing medical records is described. In addition, the characteristics of the medical blockchain are presented and analyzed through a comparison with traditional systems. The proposed storage and sharing scheme do not depend on any third-party and no single party has absolute power to affect the processing. Limitation: It requires large amount of resources

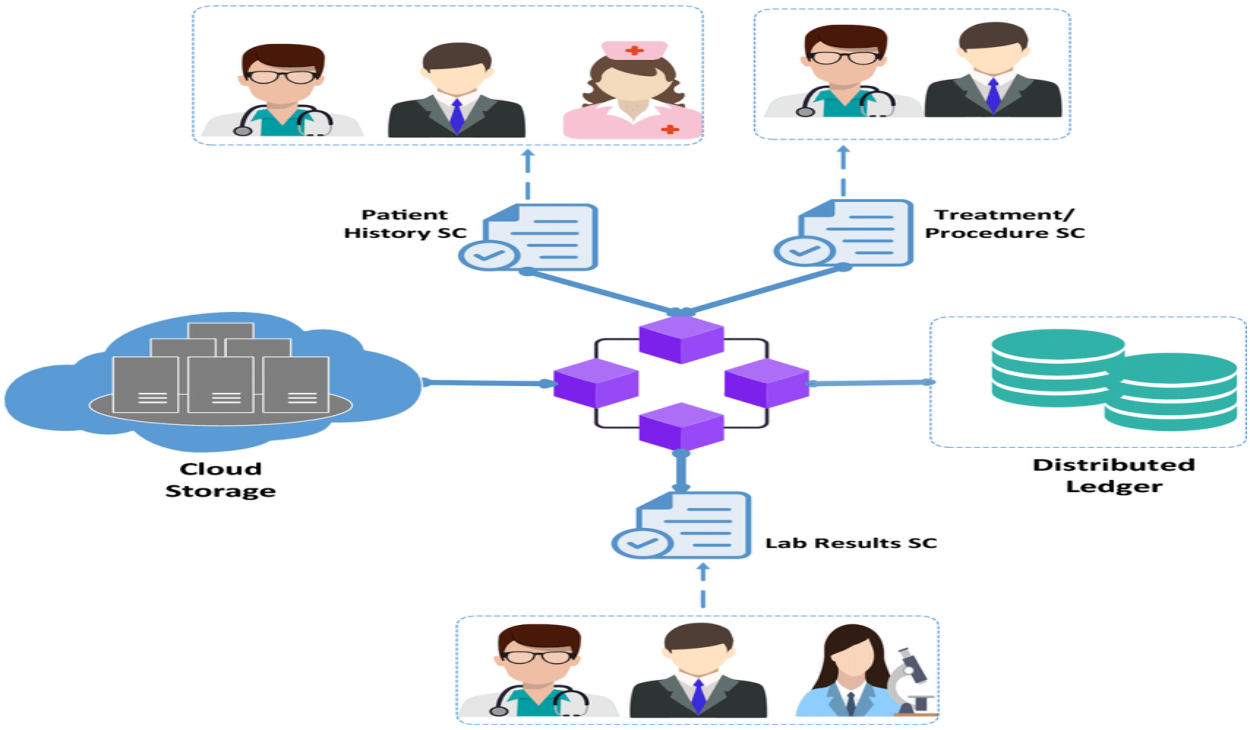
Author: G.Magyar Abstract: A blockchain powered Health information ecosystem can solve a frequently discussed problem of the lifelong recorded patient health data, which seriously could hurdle the privacy of the patients and the growing data hunger of the research and policy maker institutions. On one side the general availability of the data is vital in emergency situations and supports heavily the different research, population health management and development activities, on the other side using the same data can lead to serious social and ethical problems caused by malicious actors. Currently, the regulation of the privacy data varies all over the world, however underlying principles are always defensive and protective towards patient privacy against general availability. Limitation: It requires large number of resources.

This system entails the utilization of an emergency bracelet that caregivers can scan to access critical patient information when the patient is incapacitated or unable to provide consent. blockchain technology holds significant promise for transforming Electronic Health Record (EHR) management systems. It offers decentralized, secure, and transparent solutions for EHR sharing patient control, data integrity, and interoperability. Various blockchain models like Ethereum, Hyperledger, Corda, and Tendermint have been proposed, providing advantages like improved privacy, data security, patient empowerment, and access control [8] . However, addressing scalability, performance, and emergency access backup systems remains crucial for practical blockchain-based health record management.

EMRChain and PHD-Chain. EMRChain manages Electronic Medical Records (EMRs) by combining off-chain storage and on-chain verification techniques. On the other hand, PHD-Chain is specifically designed for housing personal healthcare data generated by patients themselves. Their proposed consensus algorithm is built upon Proof of Work and features a modified transaction processing method. This approach has shown a commendable throughput of 46 transactions per second, surpassing the capabilities of both Ethereum and Bitcoin. However, it's important to note that the platform's scalability and performance during high-stress and crisis situations still require further testing and evaluation [10].

3. METHODOLOGY

We proposed blockchain technology to keep healthcare records transparently and securely on blockchain servers in encrypted format. It is essential to implement robust security measures to protect the devices and the data they collect. Blockchain has emerged as the most reliable decentralized platform due to its ability to facilitate transactions without an agent and its strict guidelines against data modification, which safeguard private information. if blockchain technology is used70. People, medical researchers, and healthcare providers can all benefit from developing a website that keeps track of personal information, records health data, and offers users dependable access to data. By enabling correct data viewing, blockchain technology also provides this benefit. Information exchange between healthcare entities was one of the most significant responsibilities during the global outbreak. Research regarding the benefits and drawbacks of the epidemic may now be conducted more quickly due to the increased worldwide connectivity and data available. Global communication becomes more natural for everyone, and patients have greater freedom when there is no longer a requirement for a central server or for authorities to stand between patients and their data. Blockchain technology generally gives people more power. It becomes possible for hospitals and patients to communicate effectively and decentralize relevant data and information. The system that gathers, transfers, and saves data is also made incredibly easy to maintain and open for inspection by anybody by utilizing a blockchain.



The Advanced Encryption Standard (AES) is a symmetric block cipher chosen by the U.S. government to protect classified information.AES is implemented in software and hardware throughout the world to encrypt sensitive data. It is essential for government computer security, cybersecurity and electronic data protection.The National Institute of Standards and Technology (NIST) started development of AES in 1997 when it announced the need for an alternative to the Data Encryption Standard (DES), which was starting to become vulnerable to brute-force attacks.

The AES encryption algorithm defines numerous transformations that are to be performed on data stored in an array. The first step of the cipher is to put the data into an array, after which the cipher transformations are repeated over multiple encryption rounds.The first transformation in the AES encryption cipher is substitution of data using a substitution table. The second transformation shifts data rows. The third mixes columns. The last transformation is performed on each column using a different part of the encryption key. Longer keys need more rounds to complete.

Choosing the new AES algorithm

Fifteen competing symmetric algorithm designs were subjected to preliminary analysis by the world cryptographic community, including the National Security Agency (NSA).

- speed and reliability in the encryption and decryption processes;
- key and algorithm setup time; and
- resistance to various attacks -- both in hardware- and software-centric systems.

Detailed analyses were conducted by members of the global cryptographic community, including some teams that tried to break their own submissions.After much feedback, debate and analysis, the Rijndael cipher was selected as the proposed algorithm for AES in October 2000. It was published by NIST as U.S. Federal Information Processing Standards (FIPS) PUB 197, which was accepted by the secretary of commerce in December 2001.

AES became effective as a federal government standard in 2002. It is also included in the International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 18033-3 standard, which specifies block ciphers for the purpose of data confidentiality.

In June 2003, the U.S. government announced that AES could be used to protect classified information. AES soon became the default encryption algorithm for protecting classified information, as well as the first publicly accessible and open cipher approved by the NSA for Top Secret information. The NSA chose AES as one of the cryptographic algorithms to be used by

its Information Assurance Directorate to protect national security systems.

The successful use of AES by the U.S. government led to the algorithm's widespread use in the private sector. AES has become the most popular algorithm used in symmetric key cryptography. The transparent selection process established by NIST helped create a high level of confidence in AES among security and cryptography experts.

Triple DES Algorithm Description

Triple DES (3DES) is a symmetric key encryption algorithm that enhances the security of the original Data Encryption Standard (DES) by applying the encryption process three times. This algorithm is widely used for securing sensitive information in financial and other secure communications systems.

Triple DES Modes of Operation

The core of 3DES involves encrypting, decrypting, and then encrypting the data again. The process uses the DES algorithm in the following steps:

1. Encryption with Key 1 (K1): The plaintext is encrypted using DES and the first key.
2. Decryption with Key 2 (K2): The output from the first step is decrypted using DES and the second key. Decrypting here is deliberate, to add complexity and avoid weaknesses in DES.Encryption with Key 3 (K3): The result from the second step is encrypted again using DES and the third key.

Strengths of Triple DES

- Increased Security: The triple-layered process makes it much harder to crack compared to DES.
- Backward Compatibility: Can interoperate with systems designed for DES by setting K1=K2=K3K1 = K2 = K3K1=K2=K3.Widely Tested: Longstanding use has exposed and fixed vulnerabilities, making it well-understood.

4.SYSTEM REQUIREMENTS AND SPECIFICATION

System Requirement Specification System Requirement Specification (SRS) is a central report, which frames the establishment of the product advancement process. It records the necessities of a framework as well as has a depiction of its significant highlight. An SRS is essentially an association's seeing (in composing) of a client or potential customer's frame work necessities and conditions at a specific point in time (generally) before any genuine configuration or improvement work. It's a two-way protection approach that guarantees that both the customer and the association comprehend alternate's necessities from that viewpoint at a given point in time.

Specific Requirement

- Software Specification: ¬ Java IDE: The system is developed using Java as the primary development language to implement the backend functionality.
- SQL Workbench: SQL Workbench is used to manage and interact with the database, ensuring the structured storage of data such as patient details, claims, and other medical records.
- AIVEN Cloud Platform: The system integrates with AIVEN Cloud, a cloud platform used to store and manage the SQL data securely

Functional Requirements:

This section describes the functional requirements of the system for those requirements which are expressed in the natural language style. 1. Create a web application which contains the following user’s data owner, doctor, admin. 2. Data owner will upload his/her medical records to our system. 3. System will convert to blocks and stores in the distributer environment. 4. Medical data will have stored in Ethereum using blockchain technology. 5. Doctor will login to our application and selects patients’ records. 6. System will use the KNN algorithm to provide efficient access control of medical data. 7. Application should efficiently provide secure data access control.

Non-Functional Requirements:

These are requirements that are not functional in nature, that is, these are constraints within which the system must work. • The program must be self-contained so that it can easily be moved from one Computer to another. It is assumed that network connection will be available on the computer on which the program resides. • Capacity, scalability and availability. The system shall achieve 100 per cent availability at all times. The system shall be scalable to support additional clients and volunteers. • Maintainability. The system should be optimized for supportability, or ease of maintenance as far as possible. This may be achieved through the use documentation of coding standards, naming conventions, class libraries and abstraction. •

Randomness, verifiability and load balancing. The system should be optimized for supportability, or ease of maintenance as far as possible. This may be achieved through the use documentation of coding standards, naming conventions, class libraries and abstraction. It should have randomness to check the nodes and should be load balanced. 3.5 Performance Requirement 1. Quality and efficiency of patient care 2. Cost of healthcare services 3. Disparities

Objectives

- To develop an online secure healthcare web application
- To implement blockchain technology for EHR storage
- To implement AES and SHA algorithms for blockchain data/document storage
- To share and manage patient health records securely
- To develop insurance company, medical stores and pathology modules

5. ADVANTAGES

1.Data Security & Integrity

- Blockchain's immutable ledger ensures that records cannot be altered or deleted without detection.
- Strong encryption protects sensitive health data from breaches.

2. Patient-Centric Control

- Patients have ownership of their data and can grant/revoke access via private keys or smart contracts.
- Encourages transparency and accountability in healthcare services.

3. Interoperability

- Facilitates data sharing across different healthcare providers and systems regardless of platform.
- Improves continuity of care, especially in emergencies.

4. Auditability & Transparency

- All actions (view, update, access) are logged on the blockchain, providing a full audit trail.
- Useful for compliance with regulations (e.g., HIPAA, GDPR).

6. Smart Contracts for Automation

- Automates tasks like insurance claims, data access permissions, and billing**.**
- Reduces administrative overhead and speeds up processes.

6. DISADVANTAGES

1. Scalability Issues

- Public blockchains can face latency and performance issues when dealing with large volumes of data.

2. Integration with Legacy Systems

- Difficult to integrate with existing hospital information systems which were not built for blockchain.

3. Regulatory and Legal Barriers

- Lack of global standards and regulations for blockchain in health.

7. CONCLUSION

In this project Proposed the significant increase in health data breach through hacking, and application of Blockchain for security becomes important and imperative. It will encourage advancement of Machine Learning, Blockchain and other data-based techniques in various sectors including Healthcare. Continuous efforts are being made to increase the accuracy of wearable health tracking devices and if these data could provide more accurate and reliable results there will be brighter chances of integrating these devices with the health records to provide more information and also share some of these medical data securely with authorized doctor without actually visiting. we are developing an online healthcare documents management system for insurance claims. As we are using blockchain to store medical transactions, transparency and security of the medical transactions for insurance claims will be increased. Blockchain transactions will be maintained in encrypted format and patient or any other user will not be able to edit those transactions. At the conclusion of this project, it's evident that we are at the forefront of healthcare technology transformation, demonstrating how blockchain can optimize healthcare, making it more efficient, secure, and patient-centered. We Believe that Our Data Management System of Patients Based on Hospital Health Record Can Be Used as Future Record for Any Patients If Required.

8. FUTURE SCOPE

In future we can add hybrid cryptography and steganography concept for document encryption to increase the security of the EHR documents. One of the main challenges facing blockchain in healthcare is scalability. Current blockchain systems like Bitcoin and Ethereum struggle with transaction throughput, which can become problematic when handling the massive amounts of healthcare data generated daily. There is further scope of improvising this idea by implementing Artificial Intelligence (AI), Internet of things (IoT) and much more available technology to develop a more comprehensive health care model in future

Integration with Artificial Intelligence (AI) and Machine Learning (ML)

The integration of blockchain with AI and ML can significantly enhance healthcare applications:

- Predictive Analytics and Decision Support: AI models that analyze healthcare data stored on a blockchain could provide real-time insights into patient health, predicting medical conditions or suggesting treatments based on historical data.
- Personalized Healthcare: Blockchain can ensure that patient data is securely shared across healthcare providers, while AI can analyze this data to create personalized treatment plans, identify rare diseases, and recommend the most effective therapies based on individual medical histories.
- Automated Diagnosis: Blockchain-based systems could store diagnostic results securely, while AI models process and cross-reference this data for more accurate and timely diagnoses.

Research and Data Analytics

- Blockchain can allow anonymized data sharing for research without compromising individual privacy.
- Useful for epidemiological studies, AI-based diagnostics, and clinical trials.

Long-Term Vision

- Global health ID systems based on blockchain for international travelers.
- Decentralized Autonomous Organizations (DAOs) in healthcare for decision-making and resource allocation.
- Integration with Web3 technologies for decentralized healthcare ecosystems.

Enhanced Data Security and Privacy

- Blockchain provides decentralized and tamper-proof record-keeping, reducing the risk of data breaches.
- Patients can control who accesses their records via private keys and smart contracts, ensuring privacy compliance.

REFERENCES

[1] Chen, Y.; Ding, S.; Xu, Z.; Zheng, H.; Yang, S. "Blockchain-Based Medical Records Secure Storage and Medical Service Framework", Journal of Medical Systems, vol.43, no. 5, 2018.

[2] G. Magyar,Blockchain: Solving the privacy and research availability tradeoff for EHR data: A new disruptive technology in health data management, Budapest, Hungary,24-25 Nov. 2017.

[3] Zack Whittaker (2019, March), “A huge trove of medical records and prescriptions found exposed.”,

[4] Jin, H.; Luo, Y.; Li, P.; Mathew, J. A Review of Secure and Privacy-Preserving Medical Data Sharing. IEEE Access 2019, 7, 29656–29669.

[5] Soltanisehat, L.; Alizadeh, R.; Hao, H.; Choo, K.K.R. Technical, Temporal, and Spatial Research Challenges and Opportunities in Blockchain-Based Healthcare: A Systematic Literature Review. IEEE Trans. Eng. Manag. 2020, 1–16.

[6] Saha, A.; Amin, R.; Kunal, S.; Vollala, S.; Dwivedi, S.K. Review on “Blockchain technology based medical healthcare system with privacy issues”. Secur. Priv. 2019, 2, e83. [CrossRef]

[7] Abu-elezz, I.; Hassan, A.; Nazeemudeen, A.; Househ, M.; Abd-alrazaq, A. The benefits and threats of blockchain technology in healthcare: A scoping review. Int. J. Med. Inform. 2020, 124, 102396.

[8] Hasselgren, A.; Kralevska, K.; Gligoroski, D.; Pedersen, S.A.; Faxvaag, A. Blockchain in healthcare and health sciences—A scoping review. Int. J. Med. Inform. 2020, 134, 102222.

[9] Dubovitskaya, A.; Novotny, P.; Xu, Z.; Wang, F. Applications of Blockchain Technology for Data-

Sharing in Oncology: Results from a Systematic Literature Review. Oncology 2020, 98, 223–231.
[10] Agbo, C.C.; Mahmoud, Q.H.; Eklund, J.M. Blockchain Technology in Healthcare: A Systematic Review. Healthcare 2019, 7, 56.