Protecting Personal Healthcare Record Using Block chain & Federated Learning Technologies

Mrs.B.Mamatha[1], Ramaram Sneha[2], M Abhishek Reddy[2], Bandela Praveen Kumar[2],S Sai Chanakya Sharma[2]
[1]Asst.Professor,Computer Science and Engineering, CMR Engineering College, medchal, T.S, India,
[2] BTech, Computer Science and Engineering,CMR Engineering College,medchal, T.S,India

Abstract: Health and medicine are undeniably important to human existence in the modern world. Due to their centralised architecture, traditional and current Electronic Health Records (EHR) systems that are used to exchange information between medical stakeholders (patients, physicians, insurance companies, pharmaceutical companies, medical researchers, etc.) have security and privacy flaws. The use of encryption in blockchain technology assures the security and privacy of EHR systems. Additionally, this technology avoids central failure and central attack points because of its decentralised nature.

In this research, an SLR is presented to analyse the current Blockchain-based methods for enhancing security and privacy in electronic health systems. There are explanations of the search query, paper selection procedure, and research methodology. 51 publications that met our search criteria and were released between 2018 and December 2022 are examined. Each chosen paper's key concepts, blockchain type, assessment criteria, and tools are covered in depth. Finally, various difficulties, open tasks, and prospective research directions are presented.

1. INTRODUCTION

Today, healthcare is regarded as one of the most crucial issues facing people. Healthcare-related data are regularly created, saved, and reused in large quantities. Electronic Health Records (EHR) are one of the most crucial parts of healthcare systems. Healthcare stakeholders have a wide range of options thanks to electronic patient records. For instance, it enables patients to access medical information and steers clear of pricey testing, radiography, and recurrent imaging. Additionally, doctors working in all of those medical centres can access the patient's records using EHR even if they are located far away from one another and the patient is being treated in hospitals or different medical centres in different cities, provinces, or other countries. Access to a patient's medication use history is another benefit of adopting an EHR[1]; this information will aid doctors when they are recommending a new

prescription for a patient. The utilisation of patient medical information for research and developing new treatment techniques is another benefit of adopting EHR.

A Description Of The Project: How to protect a patient's privacy while utilising an EHR in healthcare is one of the fundamental difficulties. Patients' privacy is a significant problem since healthcare records are widely accessible[2].The fact that the patient's data is not their own and is instead owned by the medical centres presents another difficulty for EHR. One facet of the patient's privacy is that doctors and researchers may access a patient's EHR without the patient's permission to utilise these data for treatment and study. Utilising EHR presents the following security challenges: First, frequent usage of wearable sensors and the Internet of Things (IoT) to detect a patient's condition and enter data into their medical file might raise the danger of assaults.

This might have an impact on the doctor's treatment plan for the illness and put the patient's life in peril. Fraud detection is the second security concern[3]. There have been several instances when physicians have given a patient a medication that is not essential for him or her just because it is offered at the hospital pharmacy or the medical facility where the doctor practises. As a consequence, the patient's health can be put at risk, and/or the patient would have to pay needless expenses. Counterfeit medications provide another security risk. Many people die from the use of illegal drugs or experience severe side effects from doing so. To solve this problem, a medicine supply chain with easy access to vital data must be established. The drug's manufacturer's name, the location and method of storage, the distributor who delivered the medication to the pharmacy, the date of distribution, and other details must all be included in this information[4]. Block chain technology may be used to solve the aforementioned issues. Block chain’s distributed ledger offers a distributable characteristic that lowers the possibility of an assault on an integrated centre. Additionally, neither the transactions recorded in this distributed ledger nor its state can be altered. Additionally, by having both their private key and public key, only the patient can give permission for a third party to read or modify their data.

2. LITERATURE SURVEY

2.1 Existing System

The Blockchain architecture exemplifies a genuine peer-to-peer network that helps its members maintain a shared, trustworthy, and decentralised database[5]. A Blockchain may be conceptualised as a continually expanding list of data kept in blocks that is resistant to alteration and manipulation thanks to the most recent cryptographic techniques [6]. A typical Blockchain system is made up of a number of blocks linked in a certain sequence. The word "blockchain" is derived from this linked depiction. The system's users, often referred to as "nodes," are responsible for validating and storing the data in blocks. Proof of Work (PoW) algorithm is the name of the consensus method that is used to validate transactions and add new blocks to the chain. The essential components of each block in the chain are a cryptographic hash of the previous block, transaction-related data, and a timestamp [7].

Starting with the Genesis block, this continual process establishes the validity of the previous block [8]. The following is a list of Blockchain's numerous security benefits.

2.2 Proposed System

Blockchain-based healthcare privacy

This section aims to respond to RQ2: How can Blockchain ensure patient privacy in EHR?

The privacy of health data may be balanced with access to such data thanks to blockchain technology. The privacy policy's goal is to safeguard patient privacy while providing PHI2. Here, four things must be accomplished: 1. Giving patients complete control over their EHRs. 2. Deciding who has access to and control over the materials. 3. Making it feasible for the records to be transferred securely. 4- Reducing the likelihood that PHI will be obtained by unauthorised parties. Using blockchain technology, these four objectives can be accomplished[9].

An efficient and secure Blockchain-based architecture for accessing medical information called Ancile was suggested by the authors in [10]. In this framework, data misuse was controlled and prevented using smart contracts. Additionally, cutting-edge encryption methods were used to increase security. This essay's focus is on security and privacy concerns in healthcare. This paradigm put a lot of emphasis on patient data ownership rights. The patient is the owner of the data, and parental or carer control is offered.

2.2 Securing healthcare data by using the Blockchain

Patient involvement is a significant issue in contemporary healthcare systems, according to paper [11]. This article proposed location sharing for e-health systems using a blockchain. Decentralisation, privacy, and reliability are among the fundamental requirements for Blockchain-based location sharing that are defined in the first stage. Then, a Blockchain-based privacy-preserving scheme called BMPLS was proposed for Location Sharing3 using Merkel's cryptography and root. The findings demonstrated that this strategy satisfies the relevant criteria. Finally, the project's outputs and the analysis's findings support the notion that the field of medical care will benefit from and be able to implement this project. In essence, the plan might be utilised to communicate Blockchain-based medical information securely for telecare.

A large-scale Blockchain-based health data privacy initiative called Healthchain was described in another research [12], where health data were encrypted to manage micro-access. With the launch of the Healthchain, IoT data and medical diagnostics are impervious to deletion and manipulation. The idea made by Healthchain seems to be applicable to the smart healthcare system, according to security analysis and experimental findings. The following are some key themes raised in this essay: 1- A healthchain, or blockchain-based healthcare system, is advised to safeguard the privacy of extensive health data. Users may get IoT data from the Healthchain and get comments from doctors. After that, doctors may view data and submit feedback. 2- For lowering the computational burden and maintaining security, in the Healthchain privacy, data is encrypted and stored in the IPFS4 . 3- In addition, by transferring updated transactions, Healthchain allows users to revoke physicians' access at any time

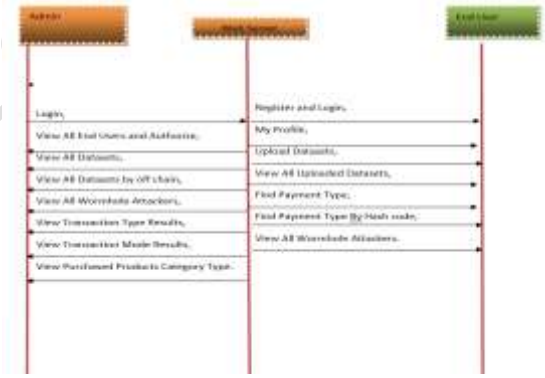

Fig 1: System Flow

3. SYSTEM ANALYSIS & DESIGN

3.1 Privacy Protection

Blockchain adopts Peer to Peer networking system which eliminates the need of a centralized database for storing confidential information[13]. This in turn eliminates centralized points that a hacker might target and steal valuable information. Similarly, a Blockchain does not have a central point of failure making it more robust than centralized networking systems. Blockchains employ Asymmetric Cryptography wherein each user has 2 keys: a public key that is visible to everyone on the network and is used to encrypt messages/transactions for the particular user as well as a private key which can only be used to decrypt the message encrypted via the user's public key. A user's public key has no relation to his/her public address and, computing a user's private key from his/her public key is an impossible task. Thus, Blockchain maintains user anonymity and privacy.

Keeping Data Manipulation at Bay

Blockchain features a special data writing technique that prohibits data from being changed once it has been put in a block. As soon as a new record is produced, this process generates a timestamp. [14]Data modification is no longer permitted. Additionally, a consensus mechanism is used to decide whether to record a new transaction. This mechanism typically requires the consent of more than 50% of network users.

3.3 System Architecture:

Management of Patient Billing and Claims

Aside from electronic health records, patient billing management systems are currently in use and are extremely susceptible to fraud and manipulation[16]. According to estimates, over 50% of all expenses for healthcare are fraudulent because of either excessive billing or invoicing for services that weren't used. For instance, in the US alone, healthcare fraud caused losses of almost $30 million in 2016 . Further research revealed that inefficient financial systems were mostly to blame for the 80% of total spending on activities linked to billing and insurance [15].It is anticipated that the introduction of Blockchain-powered healthcare systems would significantly reduce the losses brought on by fraudulent medical invoicing. Automating the settlement of payments and associated processes, including the creation of receipts, may achieve this. Additionally, Blockchain-based systems can reduce administrative costs and give suppliers and customers more time by eliminating

intermediaries. GemOS, a Blockchain-based system to handle healthcare claims, was created as a consequence of the recent partnership between Gem Health and Capital One Bank.

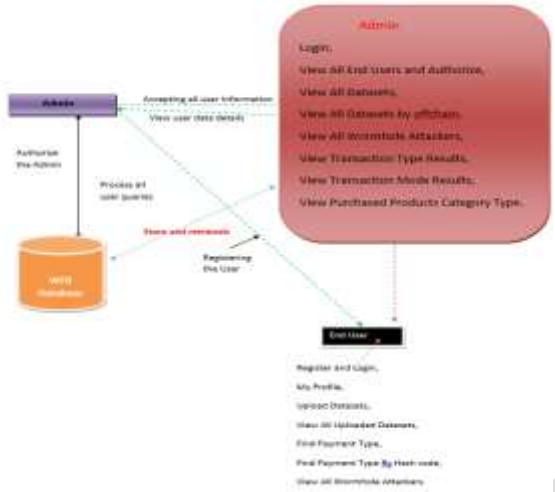

Fig 2 : System Architecture

3.4 Data Flow Diagram : Whenever a new system is developed, user training is required to educate them about the working of the system so that it can be put to efficient use by those for whom the system has been primarily designed. For this purpose the normal working of the project was demonstrated to the prospective users. Its working is easily understandable and since the expected users are people who have good knowledge of computers, the use of this system is very easy.

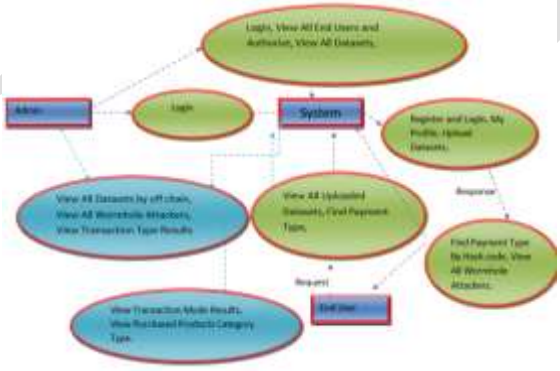

Fig 3: Data Flow Diagram

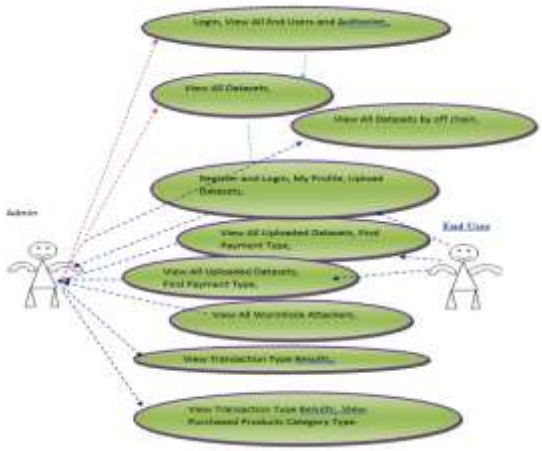

Fig 4 Use Case UML Diagrams

5. CONCLUSION

This article provided a comprehensive examination of the existing Blockchain-based approaches being utilised to attempt to safeguard patient security and privacy. The explanation of Blockchain and its properties were followed by an investigation into electronic health records and the potential role that Blockchain may play in maintaining security and privacy in this industry. We selected and assessed current publications from reputable scientific resources. The advantages and disadvantages of using blockchain technology in healthcare as compared to traditional methods were examined. The aforementioned query resulted in the discovery of 331 journal articles and 156 conference papers in all of the aforementioned databases. Finally, we selected 51 papers that were published between December 2018 and December 2022 using the previously mentioned paper selection process. We discussed the main idea, evaluation criteria, tools or structure, and Blockchain type for each selected article.

Integrity (10%), access control (8%), security (25%), privacy (17%), availability (6%), latency (4%), scalability (10%), performance (16%), and cost (4%), among others, were utilised as assessment criteria in the papers that were examined. It was discovered that 43% of the papers used public blockchains, 35% used private blockchains, 10% used hybrid blockchains, and 12% used consortium blockchains.

6. FUTURE SCOPE

The secret to preventing data breaches, fraudulent billing, and improving patient privacy and healthcare facilities internationally is correct application of Blockchain technology. It would make it easier for those involved to safely and securely share patient data. Additionally, it would guarantee that patients and pharmacies receive real medications and are not harmed by the rising prevalence of fake medications and false billings. Blockchain is the first step towards a safer, more open healthcare sector. Blockchain can thus revolutionise the healthcare industry by enabling private, secure, and quick payments, as well as reliable and accessible medical information.

7. REFERENCES

1. Abbas AF, Qureshi NA, Khan N, Chandio R, Ali J (2022) The blockchain technologies in healthcare: prospects, obstacles, and future recommendations; lessons learned from digitalization. Int J Online Biomedical Eng 18(9):2–12

2. Abid A, Cheikhrouhou S, Kallel S, Jmaiel M (2022) NovidChain: blockchain-based privacy-preserving platform for COVID-19 test/vaccine certificates. Softw Pract Exp 52(4):1–24

3. Abou-Nassar E, Iliyasu AM, El-Kafrawy PM, Song O-Y, Bashir AK, Abd El-Latif AA (2020) DITrust chain: towards blockchain-based trust models for sustainable healthcare IoT systems. IEEE Access 8:1–13

4. Shrivastava Rajeev, Tiwari Rajesh, Mehta Kamal and Bano Sarifta, "Various Olap Technologies and Their Impact on Decision Making" (April 23, 2021). Available at SSRN: https://ssrn.com/abstract=3832711 or http://dx.doi.org/10.2139/ssrn.3832711.

5. Akbar MA, Leiva V, Rafi S, Qadri SF, Mahmood S, Alsanad A (2022) Towards roadmap to implement blockchain in healthcare systems based on a maturity model. Journal of Software:

6. Ali A, Almaiah MA, Hajjej F, Pasha MF, Fang OH, Khan R, Zakarya M (2022) An industrial IoT-based blockchain-enabled secure searchable encryption approach for healthcare systems using neural network. Sensors 22(2):2–18

7. Alonso SG, Arambarri J, López-Coronado M, de la Torre Díez I (2019) Proposing new blockchain challenges in ehealth. J Med Syst 43(3):1–5

8. Alsayegh M, Moulahi T, Alabdulatif A, Lorenz P (2022) Towards secure searchable electronic health records using consortium blockchain. Network 2(2).

9. Vinit Kumar Gunjan, Sheo Kumar, Mohd Dilshad Ansari & Yellasiri Vijayalata , Prediction of Agriculture Yields Using Machine Learning Algorithms, January 2022, DOI:10.1007/978-981-16-6407-6_2, 10 January 2022, Lecture Notes in Networks and Systems book series (LNNS,volume 237

10. P Shivani, TR Singh, P Ravali, MD Rafeeq, Verification of Query Results Over Secure Cloud Data.

11. Chen L, Lee W-K, Chang C-C, Choo K-KR, Zhang N (2019) Blockchain based searchable encryption for electronic health record sharing. Future Gener Comput Syst 95:2–5

12. Dagher GG, Mohler J, Milojkovic M, Marella PB (2018) Ancile: privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. Sustain Cities Soc 39:1–11

13. Fan K, Wang S, Ren Y, Li H, Yang Y (2018) Medblock: efficient and secure medical data sharing via blockchain. J Med Syst 42(8):1–8

14. MD Rafeeq, CS Kumar, NS Chandra
International Journal for Innovative Engineering & Management Research 8. A Novel Approach Approaches for Load Balancing in Cloud Environment and Detection of Duplication Data.

15. A Brain-Inspired Cognitive Control Framework for Artificial Intelligence Dynamic System. In: Kumar, A., Mozar, S., Haase, J. (eds) Advances in Cognitive Science and Communications. ICCCE 2023. Cognitive Science and Technology. Springer, Singapore. https://doi.org/10.1007/978-981-19-8086-2_70 An Overview of Various Security Issues and Application Challenges of the Attacks in Field of Blockchain Technology. In: Kumar, A., Mozar, S. (eds) ICCCE 2021. Lecture Notes in Electrical Engineering, vol 828. Springer,Singapore. https://doi.org/10.1007/978-981-16-7985-8_38.

16. Rajesh Tiwari, Manisha Sharma and Kamal K. Mehta “IoT based Parallel Framework for Measurement of Heat Distribution in Metallic Sheets”, Solid State Technology, Vol. 63, Issue 06, 2020, pp 7294 – 7302, ISSN: 0038-111X.