International Journal of Communication Networks and Information Security
ISSN: 2073-607X, 2076-0930
Volume 14 Issue 1s Year 2022 Page 177:188

A Review of Blockchain Technology Based Techniques to Preserve Privacy and to Secure for Electronic Health Records

Arulmozhi.B
Research Scholar, Department of Computer Science and Engineering, Puducherry Technologial University, Puducherry-605014, India ammuarulmozhi@gmail.com
J.I Sheeba
Assistant Professor, Department of Computer Science and Engineering, Puducherry Technologial University, Puducherry-605014, India. sheeba@ptuniv.edu.in
S. Pradeep Devaneyan
Professor, Department of Mechanical Engineering, Sri Venkateshwaraa College of Engineering and Technology, Puducherry-605012, India pr.signs@gmail.com

Article History

Received: 13 July 2022
Revised: 20 September 2022
Accepted: 26 October 2022

Abstract

Research has been done to broaden the block chain's use cases outside of finance since Bitcoin introduced it. One sector where block chain is anticipated to have a big influence is healthcare. Researchers and practitioners in health informatics constantly struggle to keep up with the advancement of this field's new but quickly expanding body of research. This paper provides a thorough analysis of recent studies looking into the application of block chain-based technology within the healthcare sector. Electronic health records (EHRs) are becoming a crucial tool for health care practitioners in achieving these objectives and providing high-quality treatment. Technology and regulatory barriers, such as concerns about results and privacy issues, make it difficult to use these technologies. Despite the fact that a variety of efforts have been introduced to focus on the specific privacy and security needs of future applications with functional parameters, there is still a need for research into the application, security and privacy complexities, and requirements of block chain-based healthcare applications, as well as possible security threats and countermeasures. The primary objective of this article is to determine how to safeguard electronic health records (EHRs) using block chain technology in healthcare applications. It discusses contemporary Hyperledger fabrics techniques, Interplanar file storage systems with block chain capabilities, privacy preservation techniques for EHRs, and recommender systems.

Keywords: Electronic Health Records, block chain, recommender system, privacy, file storage

1. Introduction

Technology's recent advancement is changing how we use and perceive things, which has an impact on every aspect of human life. The healthcare sector is looking for new ways to improve, just as how technology has improved a variety of other areas of life [1]. Security, customer experience, and other improvements are among the primary benefits that technological innovations are providing to the healthcare sector. Electronic Medical Record (EMR) and Electronic Health Record (EHR) systems provided these advantages. They still encounter issues with user ownership, data integrity, and medical record security, though [2]. Utilizing a cutting-edge system like block chain could be the answer to these problems. Health files and other information pertaining to healthcare would be preserved on a safe, secure website with the usage of this technology [3]. The healthcare sector used a document system, or a written approach, to keep health records before the emergence of modern technology. This system of maintaining medical records on paper was inefficient, risky, unorganized, but not temper-proof. This issue also developed as a result of the patient's health files being redundant and replicated across all of the institutes the patient attended. A trend towards EHR systems, which integrate computerised and paper-based medical records, was present in the healthcare industry (EMR).In their many components, these systems were used to store testing results and clinical notes [4]. By reducing mistakes and enhancing information availability, they were proposed as a way to enhance the sufferers' safety [5]. The purpose of EHR systems was to develop an effective system that would change the situation of the healthcare industry and to address the issues with paper-based medical records. The use of EHR systems in hospitals around the world is widespread because to its benefits, particularly the increased security and cost-effectiveness they provide. They are regarded as an essential component of the healthcare industry since they give healthcare a lot of functionality [6].These functions include scheduling appointments for patients, handling invoices and accounts, ordering tests, and electronically storing medical records. Many of the Electronic health records employed in the healthcare industry have access to these. The main goal is to deliver stable, secure, and transportable medical records across many platforms. EHR systems were introduced into healthcare facilities and other institutions with the intention of raising treatment quality; nevertheless, these systems encountered a number of issues and failed to live up to expectations.

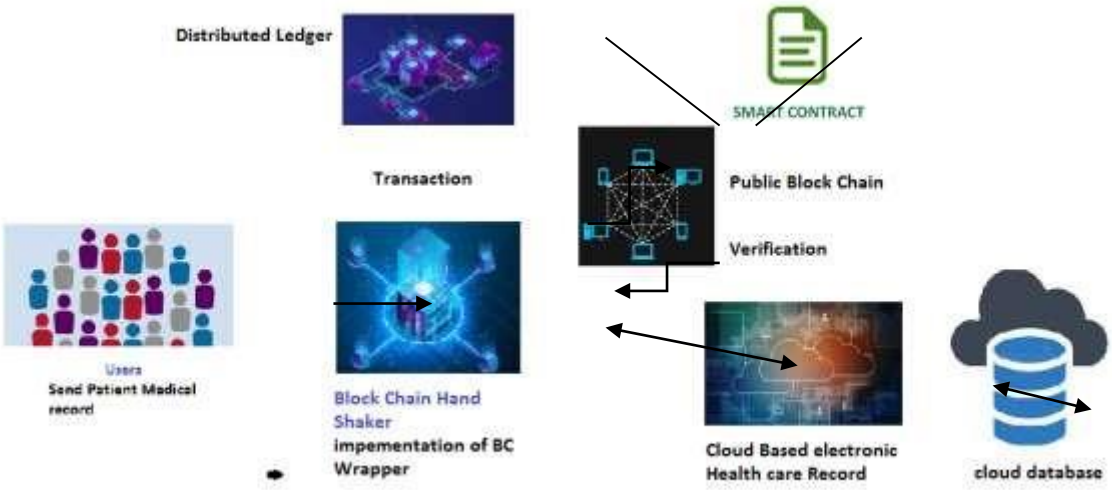

Figure 1. Architecture of Block chain-based Electronic Health Record Management Systems

The off-chain scaling solution combined with block chain solves the scalability issue by storing the data on the underlying media, which improves security and privacy in EHR. Figure 1 depicts the architecture [12]. Our suggested architecture consists of four essential parts: a user application, a block chain hand shaker, a cloud, and a public block chain network. Nakamoto [7] for his well-known advent of digital money or symmetric encryption, namely, bitcoin, developed this technique. Nakamoto used block chain technology to fix the double spending problem in bitcoin, but shortly this cutting edge technology was being used in many other applications. As new transactions are entered on the blocks, the network of

connecting blocks known as a block chain continues to grow. This platform uses a distributed method that allows for the sharing of ownership over each dispersed piece of data as well as the distribution of information. Peer-to-peer networks control block chains, which store batches of hashed transactions that are secured by the technology [8,9].

A block chain offers advantages including security, privacy, and data integrity without outside interference. Because of these advantages, it makes sense to keep patient medical information on it.

Thanks to technological advancements patient health information security in the healthcare industry has become a major concern. Additionally, some academics have determined that using block chain technology to the healthcare industry would be a workable approach.

Public, private, and consortium block chains are the three basic forms of block chain networks shown in Table 1. Each of these systems has advantages, disadvantages, and perfect applications.

Table 1. Categorization of block chain networks

parameters	**Public (e.g.bitcoin)**	**private**	**Consortium/ permissioned (e.g. EHRs)**
Type of the network	decentralised	Partially decentralized	Between private and public block chains that are only partially decentralised
uses	On the network, anyone can read and publish from anywhere in the world. Every member of the network verifies the data, making it extremely secure.	One "highly trustworthy" organization—the block chain's owner—controls access to read or write data on the block chain.	permissions for a select number of specified nodes to validate read and write operations on the blockchain. Every organization on the blockchain may have an unique set of preset nodes.
benefits	• It is transparent since all transactions take place public with individual anonymity • It is secure because the entire network validates transactions.	• Secure because only the block chain's owner can verify transactions; • Private because the owner may regulate who has permission to read and write just on blockchain	Private since read and write operations can only be controlled by the predefined nodes Efficient since relatively smaller nodes verify transactions

A digital ledger that stores data in blocks is known as a block chain. These blocks are distributed among the network's nodes and are decentralised. Data is also kept in a conventional database, such as a NoSQL database or an RDMS. Although not every database is a block chain, they are all a sort of database. Block chains are capable of maintaining a digital ledger of transactions. Operations are limited to read and create only. Different forms of data may be stored in databases, which also offer update and delete operations.

A block chain is slower than other types of databases because each block must be signed and authenticated. Table-2 compares the pros and disadvantages of block chain and database technologies under the headings "problem," "block chain," "central database," and "benefits".

Table 2. Comparison between block chain and database technology

Issue	**block chain**	**Central database**

Trust Development	can function without any reliable third party	Need a dependable central figure
Information Privacy	The data is visible to all nodes.	It only allows authorised people access.
Robustness/Fault Tolerance	Nodes share data among themselves	Information is kept in a central database.
Endurance	Consensus is reached slowly.	immediately carry out/update
Span	Every participating node has the most recent version.	Copy only exists in the central party.
protection	Utilize cryptography safeguards	employs customary access control

In the above section, basic introduction about Block chain-based Electronic Health Record Management Systems is given. Moreover, three basic types of block chain such as Public, private, and consortium are discussed with its advantages, disadvantages and applications. The major comparison between blockchain and database technology is also explained. We can conclude that, both blockchain and database technology has equal advantages and disadvantages. But, when concerning security blockchain is the best.

2. Evolution of Block Chain Technology

This section divides the development of blockchain technology into three categories.

Blockchain 1.0 (Cryptocurrencies): The Blockchain 1.0 technology that powers Bitcoin is linked to an unidentified entity from 2008 with the tag "Satoshi Nakamoto" [10]. Blockchain 1.0 was utilised by Bitcoin to address long-standing issues with double spending of virtual currency and the execution of virtual transactions without a trustworthy third party's assistance. To efficiently store the digital financial between two parties, a blockchain technology is employed. The transactions are kept in "Blocks," which are a growing collection of data. These blocks may be verified in a permanent manner and are impervious to alteration. The verification of the ledger records is often managed by a group of users connected by a P2P network. A majority of the network's users must agree on any modifications to be made inside blocks in order to do so.

Blockchain 2.0 (smart contracts): It was the subsequent significant stage in the growth of the blockchain sector and is known as "Smart Contracts." Beyond digital money, It is a theory that supports the transference of many various types of assets, such as shares, securities, loans, mortgages, home automation, etc., as well as the broad democratization of markets [11]. Similar to traditional business contracts, it was developed as a way of effectively enforcing the regulations decided upon by parties having an interest. Technology advancements have made it evident that Blockchain might revolutionise not only marketplaces, payments, and financial services, but also all economic sectors. Similarly, the concept of "contracts" is not fresh and has been discussed in written since 1994. A computerised transaction protocol that carries out a contract's provisions is how it is described. The idea was to transform legal provisions (such as collateral, bonding, etc.) into computer code and implement them as hardware or software so they would enforce themselves with little assistance from trusted intermediates [12]. A smart contract on the Blockchain automatically upholds agreements made by two parties or more without the aid of a dependable mediator. These smart contracts are built into Blockchain technologies like Ethereum and Hyperledger as computer programmes Members can connect to the network and request the execution of a certain contract for a transfer in the Block chain P2P network, depending on the type of Blockchain. Similar to how digital currencies are recorded, the history of these transactions

is also stored in Blockchain. The order of transactions on the Blockchain determines the condition of the contract and the assets of participants [13].

Blockchain 3.0 (blockchain application): This technology has applications outside of the financial markets, such as in the domains of governance, health, literature, and culture [14]. Beyond the financial markets, block chain 3.0 provides a platform for creating distributed and secure applications. By connecting to web technologies, it provides a universal and worldwide scope and size. It is seen as a platform to aid in the development of the "Smart World," especially for allocation of resources of both people and physical resources. In the literature, an architectural pattern for building distributed apps is how a general block chain design is depicted in Figure 2.

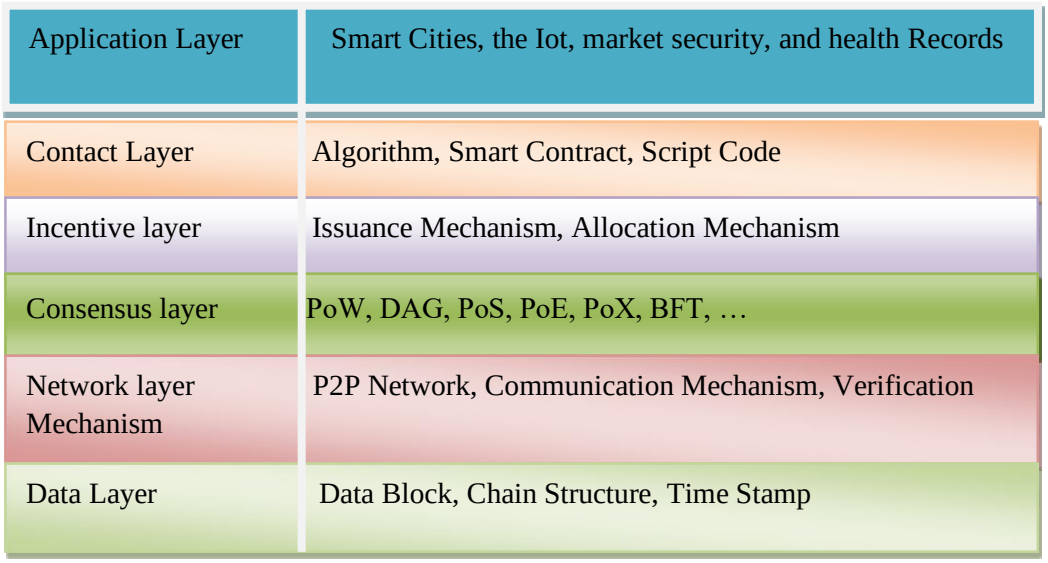

Figure 2. A general Block chain Layered Architecture

The above figure shows the usage of each layer, where the data layer is used for creating data block, chain structure and time stamp. Network layer is used for P2P network, Intelligence, Markets Security, Internet of Things, and Health Consensus layer is acquired for proof process, incentive layer is using for issuance process and allocation process. Finally, application layer is usable for real time applications.

3. Challenges of EHR Management with Block Chain

The biggest obstacles to the widespread implementation of block chain in healthcare data management systems are presented in this section. We describe the underlying reasons for these difficulties and offer pointers to future researchers in the field.

One of the primary obstacles to the widespread use of public block chains in the healthcare sector is scalability. Evidently, thousands of transactions may be processed every second using conventional transaction networks. Visa, for instance, can handle about 1700–2000 transactions per second. Ethereum blockchains, on the other hand, can only handle about 20 transactions per second, considerably behind other blockchains in terms of transaction speeds [15]. Durability is less of a concern with private blockchains because the processing nodes are managed by trusted parties. The scalability issue might be handled using many tactics. One of the potential solutions is the lightning network that aims to extend the primary blockchain network by adding a second layer to enable faster transactions.

Interoperability: In order to fully realise the benefits of blockchain technology in the healthcare industry, interoperability-related issues must be resolved. Interoperability is essential for enabling communication across various blockchain networks. Although the lack of standards in blockchain helps developers, the lack of interoperability creates significant communication issues. The existence of many blockchain networks, each of which is based on a separate consensus model, transaction mechanism, and smart

contract functionality, poses a serious obstacle to interoperability. Utilizing current blockchain network standards is one approach that might be taken to address this issue.

Tokenization: In the existing healthcare system, the majority of businesses, hospitals, and pharmaceutical companies do not divulge patient information. Additionally, it is quite challenging for patients to confirm the data's correctness. The healthcare business may undergo a change thanks to the tokenization of patient data. It is a procedure that enables the creation of digital representations of healthcare data and the granting of certain usage rights for a selection of healthcare services. Users are able to view and recover their medical information thanks to this feature without having to first encrypt or re-encrypt it.

The immutability of blockchain technology is one of its key benefits for ensuring the accuracy of medical record data. The integrity of the health records that must be transferred to the blockchain must be guaranteed as a result [16]. Healthcare organisations are looking to implement blockchain-based solutions in one of three scenarios, such as maintaining a paper registration, a virtual registry, or a registration that was destroyed.

Due to a number of reasons, including price inequality, insurance competition, human and administrative error, and tax avoidance, the majority of the existing healthcare data registries are inaccurate. Therefore, before putting data on blockchains, the healthcare data registries need to be updated and sanitised.

4. Survey on HyperLedger Fabrics

Melo et al., [17] provides an analysis of the effectiveness of an infrastructure that underpins a blockchain-based application. While keeping an eye on the system, we noted a little rise in resource use, which may be related to software ageing problems within the hyperledger fabric framework or its fundamental parts. The impact of this capacity increase on the probability that the system would work has also been evaluated.

Wang et al., [18] The Hyperledger architecture was adopted because of its improved privacy security features and enterprise-grade capabilities for data processing. In addition to a Fabric's built-in privacypreserving capabilities, universal health care smart contracts featuring hierarchical access control were created to strengthen privacy protection in data exchange. The goal of the proposed healthcare datasharing framework is to enhance, not replace, the current data management approaches. It is based on Australian medical practises.

Kumar et al., [19] outlines a cutting-edge, Hyperledger Fabric-based system for exchanging medical data that protects privacy, called MedHypChain uses a Personality broadcasting group signcryption approach to secure each transaction. We proved that the marked by a series, transparency, confidentiality, and anonymity of MedHypChain are all achieved. Additionally, we standardized the MedHypChain to implement the PCI healthcare system, where the patient keeps track of their healthrelated data in the blockchain that can be viewed by the implemented by various.

Kothariet al., [20] employed blockchain principles to offer patients ownership over their own data and the freedom to pick which specific medical professionals they wish to share it with. Based on the hyperledger fabric paradigm, we have created a substantial information architecture to access EHRs. The core network of edge computing, which may be seen as vectorized decentralised edge computing, can be built up using the distributed ledger of the blockchain node.

Since Hyperledger Fabric is still in its early stages of development, problems developed during the project's lifespan. Understanding the framework's development and implementation takes some time due to the documentation's complexity and ongoing growth. The absence of instructions for deploying a Hyperledger fabric blockchain remotely and the cryptic error messages made things difficult and time-consuming.

5. Survey on Blockchain Enabled Interplanary File Storage System

Zaabar et al., [21] presents a novel architecture that utilises decentralised databases to prevent problems with centralised storage. The decentralised OrbitDB with Interplanetary File System database is used to store patient electronic health records (IPFS). Additionally, we have established a blockchain network based on the Hyperledger by using Hyperledger composition to store hashes of recorded data and control permission when retrieving it. The suggested Blockchain-based architecture is intended to improve the

sturdiness of healthcare management systems and to get around known security flaws in existing systems for smart healthcare.

Subathra et al., [22] intends to develop decentralised consensus blockchain and data aggregation based on the Interplanetary File System (IPFS) for efficient data classification and storage. The attack is identified through using meta-hyperparameter random forest (MHP-RF) classifier. The transaction data is securely saved on a server once the attack has been identified using a blockchain technology that is based on smart contracts. The transaction processing stage categorises the transaction type as normal or abnormal, and then executes business logic via a smart contract, adding the blockchain transaction to the network cloud. Using a PoW-enabled approach linked with Elgamal-based data aggregation, the consensus blockchain technique is used.

Khan et al., [23], We suggest TREAD, a blockchain-based system composed of smart contracts, to keep this movement data on the a distributed ledger so that many peers may access and use it in different place apps while disclosing users' sensitive personal information. However, storing a lot of continuously created trajectories in a scalable manner is difficult. To solve this problem, We make use of the distributed database peer-to-peer system for data storage known as IPFS (InterPlanetary File System). In order to stop users from adding harmful or false trajectories into the ledger, we develop efficient consensus mechanisms for the participants to check the retrieval and storage operation in a distributed manner.

Chenet al.,[24] introduces a system for detecting diabetes using Blockchain that uses a variety of machine learning classification algorithms to identify the condition sooner and securely preserves patient EHRs. Wearable sensor devices are utilised to collect patient health data, and our EHRs sharing platform blends side effect illness predictions, Blockchain, and the interplanetary file system (IPFS).

Batchu et al., [25] created a proof-of-concept smart contract that maintains information on patients with brain tumours, including their name, diagnosis, grade, chemotherapy treatments, and Karnofsky score. The picture files were efficiently saved in the InterPlanetary file system, and the associated content identification hashes were kept in the smart contracts.

The technique proposed by Wang et al., in [26] Providing attribute-based encryption, IPFS, and Ethereum together allows for granular access control for data There is no need for an external key generator, according to the authors. Data owners can offer fine-grained access control by data encryption using secret key and access controls.

The IPFS software implements an access control smart contract created by the Ethereum-enabled IPFS version, according to Sun et al., [27]. A user's file is uploaded, IPFS divides it into smaller pieces. These elements each contain a content identification for the smart contract (CID). The transaction is also verified by the permission to ensure that it is not vacant or held by the same individual, check the storage against the CID. Control switches back to IPFS after the file has been correctly confirmed. A request for access to a data file is made to the data owner, who utilises smart contracts to approve or reject access. Their strategy ignores cloud data transfer and the related authorization constraints. Users may choose to restrict access to a file they submitted to the network, even on a private IPFS network. They could want that the file be accessible exclusively to specific members of the private network. Consider a situation where management in an organisation wants to restrict access to particular files for other employees or lower level management while granting higher level management access to the same file. Such a rule cannot currently be created in IPFS by an organisation for accessing the system according to their own IPFS network. If a file intended for highlevel management only is shared on the network, anybody with access to the file's hash on the organization's IPFS network may easily access it. Despite this, the IPFS does not offer any traceability tools for monitoring and auditing network file access.

6. Survey on Privacy Preservation Methods for EHRs

As stated by the current security algorithms, there are still certain security flaws and the health care system will not be happy with the integrity and consistency of the data transfer from one vendor to another. Additionally, it greatly increases side channel hacking and IP spoofing. Hacking incidents are rising along with internet usage, particularly in the health care industry.

Grover et al., [28] the e-healthcare cloud's block chain and anonymized ring signatures enhance the protection of patient health data's personal information, making it suitable for real-time applications. Yanet al., [29] A versatile modelling technique for multi continuous or linked data that considers

sitelevel variability is Fed-GLMM, or federated generalised linear mixed models. Fed-GLMM can be applied to both federalised and consolidated research networks to provide data integration while protecting privacy and increase computational efficiency. Fed-GLMM can produce findings that are nearly identical to those of the gold-standard method, in which the GLMM is explicitly fit to the pooled dataset, but with much less summary data.

Kadam et al., [30] A system called an electronic health record (EHR) gathers digital health information about patients and makes it accessible to other healthcare practitioners in the cloud. The system must guarantee response accuracy and dependability because the EHR includes a significant amount of sensitive data about patients. For users who must rely on assets, the verifiable database (VDB) is recommended as a productive updatable distributed storage strategy. In this method, a user transfers his enormous data set to a cloud employee and queries when he needs particular information. Most modern VDB designs demonstrate the accuracy of the enquiry findings by increasing efficiency through confirmation reuse and proof refreshing techniques.

Tina et al., [31] In order to preserve consumer privacy and such that verified signatures, it uses a revolutionary technique to generate accumulated understanding of data security and data refreshment in the cloud theme. Privacy and data protection for the cloud-based public auditing of shared data (HARS) In order to ensure that customers receive up-to-date information, the tree overlay rule is used. The information in the cloud is also audited by the Third Party Auditor (TPA). Without disclosing the users' identities, you must be able to track the CSP's confidence. The problem is that it is impossible to detect malicious user activity. Increased traceability is a defect in the system that makes it impossible for anyone other than the authorised user to monitor the identity of the signator and prevent the destructive behaviour carried out by user in the group.

Rongxing et al., [32] In the Big Data age, effective and secure computer preservation The Big Data era's efficiency and privacy requirements for data mining led to the development of the efficient and confidentiality cosine similarity (PCSC) computing protocol. The privacy is protected while also being effectively protected by the PCSC protocol. Big Data analytics benefit greatly from it. When n is large, the gain of the suggested PCSC protocol increases due to the computation overhead. The drawback is that specific privacy requirements for some big data analyses. To offer full and distinctive security in the age of huge data, protocols like data protection computers have been introduced.

This assessment revealed a number of study issues with regard to the privacy and security of e-health data. We discovered that in order to protect client privacy and sovereignty and ensure the privacy and security of patient data in e-health systems, it is urgently necessary to increase network security.

7. Survey on Recommender Systems in Block Chain

The Encyclopaedia on Machine Learning provides the following definition of a recommendation systems: "The objective of a recommender system is to make relevant suggestions to the a group of users for products or services that would interest them." A blockchain is frequently a publicly accessible record of data built on the basis of the internet and accumulated through a sizable network. Bhardwaj et al., [33] The algorithm known as Health Mudra was created to provide protocols to avoid diabetes, the most difficult disease in the healthcare industry. Based on block chain technology, Health Mudra incorporates the proper machine learning algorithms and optimization techniques. Filtering makes use of suggestions. By treating symptoms as directed by experts, diabetes can be prevented. Blockchain is a decentralised database that may be used to hold information on how to lessen the symptoms of diabetes that has been sourced from a big number of physicians.

Yeh et al.,[34] Research on Blockchain and recommendation systems requires creative and sophisticated investigation. By integrating smart contracts with the core block chain protocol, we want to create a safe and trust-based system that takes use of the benefits of block chain supported secure multiparty computing. Online actions are made more private and safer by fusing block chain technology with recommendation algorithms. A method is developed allowing businesses to use smart contract technologies to cooperatively create a safe dataset and host a model that is updated frequently. Hai et al.,[35] offers a platform that combines federated deep learning with the block chain to deliver a customised recommended system. Focus of the work is on two phases of block chain based electronic health record storage, where the block chain makes use of a Hyperledger network and is able to follow alterations to the data continually.

Decentralized RSs have been developed in order to address issues with traditional RSs that are controlled entirely by a central authority by delegating some of that authority and responsibility to the users. However, when it comes to disagreements or inappropriate behaviour, this might raise major issues.

As a result, it is crucial to identify any possible unfair trades that can take place during activity between two or more users and to design suitable solutions that might produce fair processes, example as the adoption of atomic swaps, a block chain legacy. The energy use of block chain when used in RSs is a significant concern as well.

8. Proposed Framework

Based on the above literature survey, some of the problems are considered. Including infrastructure costs, vendor acceptance, and technology constraints. These restrictions need to be removed in order to implement a block chain based global and completely interoperable EHR. The existing Hyperledger fabrics based block chain is more cost to construct. Moreover, while constructing the blocks the existing methods may be complex to hold multi-dimensional data. The Interplanary file storage system has the issue of data de-duplication. Finally, the recommender system have the issue of false prediction and calculating similarity index. To overcome come those issues the below architecture is constructed

In Figure 3, the private block chain architecture is established, the patients have direct communication with a healthcare provider, and the patients' families are also shown to be in direct touch with the healthcare provider. In a private block chain architecture, a smart contract is implemented using Hyper ledger fabrics. The Graph-based Dual Mode technique enables the blocks to hold both text and picture data. With access to an interplanetary file storage system, this private architecture may also function as a decentralised architecture. The huge files that are contributed to IPFS are divided up into a variety of smaller data chunks and resolved to a list of IPFS links that lead to the original data's broken up components. In the IPFS network, this kind of addressing makes guarantee that the request will always go to the same file at the provided address. The original information can be decrypted using an encryption engine on a local machine whenever a data user requires to access data which the owner has uploaded.

HypreLedger Fabrics- It serves as a base for creating solutions or applications with a modular design.

Healthcare Provider- It is someone or something that offers medical assistance or therapy. Healthcare professionals includes physicians, registered nurses, midwife, radiologist, labs, hospital, acute medical clinics, medicine supply companies, and other professions, facilities, and organisations that provide such services.

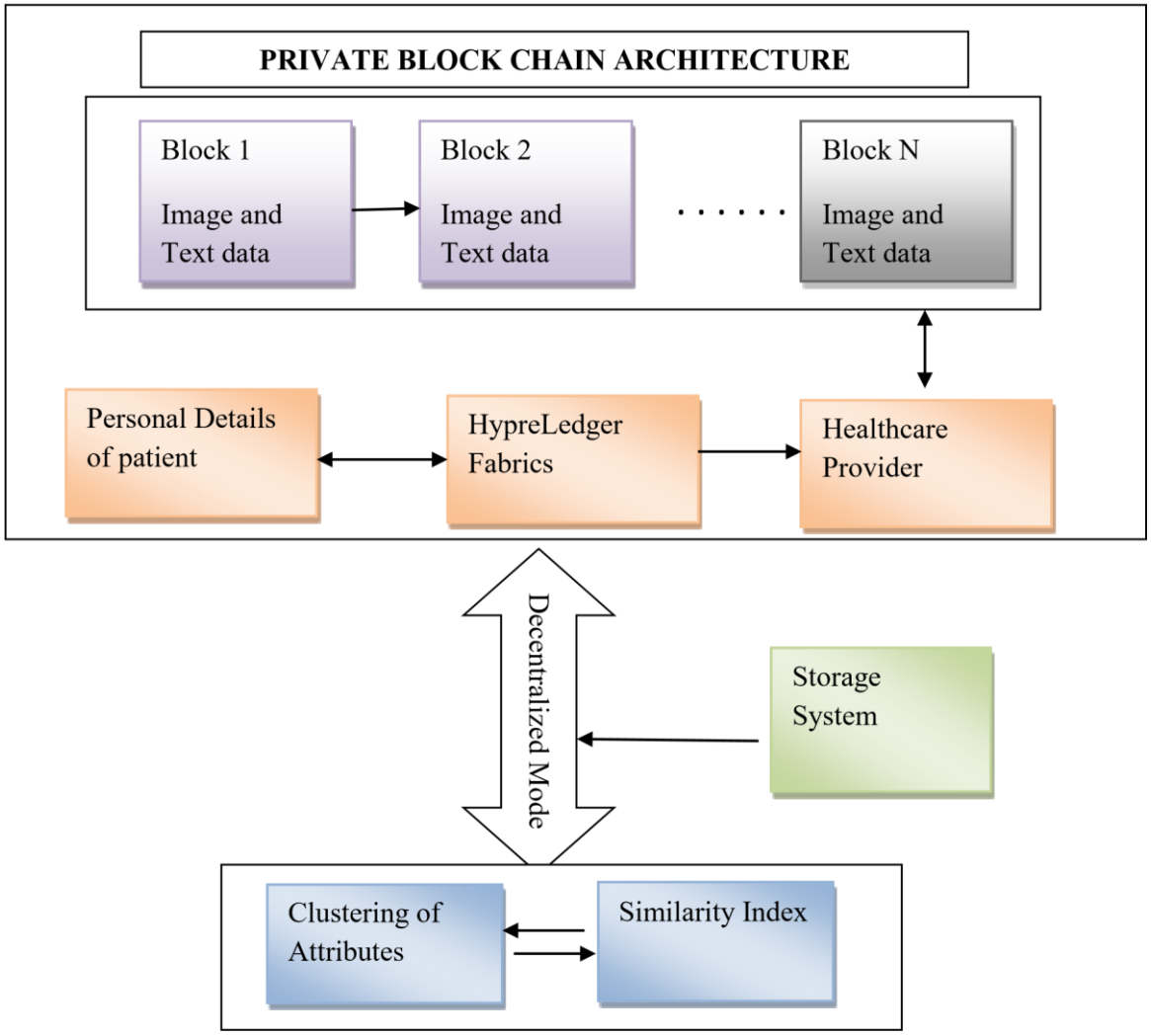

Figure 3. Architecture of block chain with recommender systems

Decentralized storage system- Encrypted data and stored across several places, or node, that are managed by people or organisations who charge a fee to share their spare disc space. The secret encryption key is only in the possession of the data's owner; storage companies cannot access the data. Finally, the recommender system is equipped to provide the patients with appropriate recommendations. A specific item is recommended through various stages of this Health Recommender System (HRS). These include the training phase, the procedure for creating patient profiles, the sentiment analysis phase, the privacy preservation phase, and the recommender phase. A healthcare dataset must first be gathered before we can apply a feature selection and classification approach on it. A crucial part of this HRS is the development of the personal medical record (PHR) and client database. PHR is a significant worry when used as data by the recommender engine to forecast and suggest treatments to the patients. For feature selection, we draw meaningful data from the patient database that is linked to the PHR. The knowledge is then classified and kept in a repository using a classification technique.

9. Conclusion

In order to identify and evaluate the key problems, obstacles, and potential advantages of block chain adoption in the healthcare industry, a systematic literature review of EHRs inside a block chain was undertaken in this study. We have discussed Block chain's promise for the healthcare sector and how its

use has gone beyond the confines of that industry, but we have also made clear that adoption of the new technology within the healthcare ecosystem is still crucial to its success.After analysing the findings from the literature review, we come to the conclusion that block chain technology may one day be a suitable solution for issues with the healthcare industry, such as EHR interoperability, building trust between healthcare providers, auditability, privacy, and allowing patients to grant access control to their health data, allowing them to choose who they want to share their medical records with. Prior to implementing block chain technology on a broad scale in healthcare, however, further study, trials, and experiments are required to verify that a safe and reliable system is put in place. This is because a patient's health data are private, extremely sensitive, and vital information. The focus of the next work is on doing analytical systematic studies with a year-by-year component.

References

[1] G. Jetley and H. Zhang, ‘‘Electronic health records in IS research: Quality issues, essential thresholds and remedial actions,’’ Decis. Support Syst., vol. 126, pp. 113–137, Nov. 2019

[2] K. Wisner, A. Lyndon, and C. A. Chesla, ‘‘The electronic health record’s impact on nurses’ cognitive work: An integrative review,’’ Int. J. Nursing Stud., vol. 94, pp. 74–84, Jun. 2019.

[3] M. Hochman, ‘‘Electronic health records: A ‘‘Quadruple win,’’ a ‘‘quadruple failure,’’ or simply time for a reboot?’’ J. Gen. Int. Med., vol. 33, no. 4, pp. 397–399, Apr. 2018.

[4] S. T. Argaw, N. E. Bempong, B. Eshaya-Chauvin, and A. Flahault, ‘‘The state of research on cyberattacks against hospitals and available best practice recommendations: A scoping review,’’ BMC Med. Inform. Decis. Making, vol. 19, no. 1, p. 10, Dec. 2019

[5] Neal D. Choosing an electronic health records system: professional liability considerations. InnovClinNeurosci. 2011 Jun;8(6):43–5

[6] Narayanan A, Bonneau J, Felten E. Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton, New Jersey, United States: Princeton University Press;

[7] S. Nakamoto, Bitcoin: A Peer-to-Peer Electrnic Cash System. 2008, pp. 1–9

[8] W. J. Gordon and C. Catalini, ‘‘Blockchain technology for healthcare: Facilitating the transition to patient-driven interoperability,’’ Comput. Struct. Biotechnol. J., vol. 16, pp. 224– 230, Jan. 2018

[9] James, Febin John. 2018. "How to Validate If Your Ideas Need a Blockchain." We Think Ideas, February 12. Accessed 2018-03-27.

[10] Colomo_Palacios, R., Sánchez_Gordón, M., & Arias_Aranda, D. (2020). A critical review on blockchain assessment initiatives: A technology evolution viewpoint. Journal of Software: evolution and process, 32(11), e2272.

[11] Buitenhek, M. (2016). Understanding and applying blockchain technology in banking: Evolution or revolution?. Journal of Digital Banking, 1(2), 111-119.

[12] Ertemel, Adnan Veysel. "Implications of blockchain technology on marketing." Journal of international trade, logistics and law 4, no. 2 (2018): 35-44.

[13] K. Christidis and M. Devetsikiotis, ‘‘Blockchains and smart contracts for the Internet of Things,’’ IEEE Access, vol. 4, pp. 2292–2303, 2016, doi: 10.1109/ACCESS.2016.2566339

[14] Hussein, D. M. E. D. M., Taha, M. H. N., & Khalifa, N. E. M. (2018). A blockchain technology evolution between business process management (BPM) and Internet-of-Things (IoT). International Journal of Advanced Computer Science and Applications, 9(8).

[15] Mazlan AA, Daud SM, Sam SM, Abas H, Rasid SZA, Yusof MF (2020) Scalability challenges in healthcare blockchain system—a systematic review. IEEE Access 8:23663– 23673

[16] Tanwar S, Parekh K, Evans R (2020) Blockchain-based electronic healthcare record system for healthcare 4.0 applications. J InfSecurAppl 50:102407

[17] Melo, C., Oliveira, F., Dantas, J., Araujo, J., Pereira, P., Maciel, R., &Maciel, P. (2022). Performance and availability evaluation of the blockchain platform hyperledger fabric. The Journal of Supercomputing, 1-23.

[18] Wang, Q., & Qin, S. (2021). A Hyperledger Fabric-Based System Framework for Healthcare Data Management. Applied Sciences, 11(24), 11693.

[19] Kumar, M., & Chand, S. (2021). MedHypChain: A patient-centered interoperability hyperledger-based medical healthcare system: Regulation in COVID-19 pandemic. Journal of Network and Computer Applications, 179, 102975.

[20] Kothari, S., Tazrin, T., Desai, D., Parveen, A., Fouda, M. M., &Fadlullah, Z. M. (2021). On securing electronic healthcare records using hyperledger fabric across the network edge. In Secure Edge Computing (pp. 155-176). CRC Press.

[21] Zaabar, B., Cheikhrouhou, O., Jamil, F., Ammi, M., &Abid, M. (2021). HealthBlock: A secure blockchain-based healthcare data management system. Computer Networks, 200, 108500.

[22] Subathra, G., Antonidoss, A., & Singh, B. K. (2022). Decentralized Consensus Blockchain and IPFS-Based Data Aggregation for Efficient Data Storage Scheme. Security and Communication Networks, 2022.

[23] Khan, J. A., Bangalore, K. U., Kurkcu, A., &Ozbay, K. (2022). TREAD: privacy preserving incentivized connected vehicle mobility data storage on interplanetary-file-system-enabled blockchain. Transportation research record, 2676(2), 680-691.

[24] Chen, M., Malook, T., Rehman, A. U., Muhammad, Y., Alshehri, M. D., Akbar, A., ...& Khan, M. A. (2021). Blockchain-Enabled healthcare system for detection of diabetes. Journal of Information Security and Applications, 58, 102771.

[25] Batchu, S., Henry, O. S., & Hakim, A. A. (2021). A novel decentralized model for storing and sharing neuroimaging data using ethereumblockchain and the interplanetary file system. International Journal of Information Technology, 13(6), 2145-2151.

[26] S. Wang, Y. Zhang, and Y. Zhang, "A blockchain-based framework for data sharing with finegrained access control in decentralized storage systems," IEEE Access, vol. 6, pp. 38437–38450, 2018.

[27] J. Sun, X. Yao, S. Wang, and Y. Wu, "Non-repudiation storage and access control scheme of insurance data based on blockchain in IPFS," IEEE Access, vol. 8, pp. 155145–155155, 2020.

[28] Grover, B., & Kushwaha, D. K. (2022). Authorization and privacy preservation in cloud-based distributed ehr system using blockchain technology and anonymous digital ring signature. Health Services and Outcomes Research Methodology, 1-14.

[29] Yan, Z., Zachrison, K. S., Schwamm, L. H., Estrada, J. J., &Duan, R. (2022). Fed-GLMM: A Privacy-Preserving and Computation-Efficient Federated Algorithm for Generalized Linear Mixed Models to Analyze Correlated Electronic Health Records Data. medRxiv.

[30] Kadam, M. A., & Navale, V. (2021). EFFICIENT PRIVACY-PRESERVING INTEGRITY AUDITING SYSTEM FOR ELECTRONIC HEALTH RECORDS USING SECURE ENCRYPTION ALGORITHMS. INTERNATIONAL JOURNAL, 6(6).

[31] Tina Esther Trueman, P.Narayanasamy "Ensuring privacy and data freshness for public auditing of Shared data in cloud," 2018:

[32] Rongxing Lu, Hui Zhu, Ximeng Liu, Joseph K. Liu, Jun Shao , "Toward Efficient and Privacy-Preserving Computing in Big Data Era "July/August 2019

[33] Bhardwaj, R., & Datta, D. (2020). Development of a recommender system HealthMudra using blockchain for prevention of diabetes. Recommender System with Machine Learning and Artificial Intelligence: Practical Tools and Applications in Medical, Agricultural and Other Industries, 313-327.

[34] Yeh, T. Y., & Kashef, R. (2020). Trust-Based collaborative filtering recommendation systems on the blockchain. Advances in Internet of Things, 10(4), 37-56.

[35] Hai, T., Zhou, J., Srividhya, S. R., Jain, S. K., Young, P., & Agrawal, S. (2022). BVFLEMR: An Integrated Federated Learning and Blockchain Technology for Cloud-based Medical Records Recommendation System.