# Secure E-Health Record Sharing using Blockchain: A Comparative Analysis Study

**Conference Paper** · June 2022

DOI: 10.1109/ICICCS53718.2022.9788462

Moses Dayanand
Karunya University

Andrew Onesimu
Manipal Institute of Technology

2022 6th International Conference on Intelligent Computing and Control Systems (ICICCS) | 978-1-6654-1035-9/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICICCS53718.2022.9788462

# *Secure E-Health Record Sharing using Blockchain: A Comparative Analysis Study*

Moses Dayanand Kondepogu
*Computer Science and Engineering*
*Karunya Institue of Technology and Sciences*
Coimbatore, India
kondepogumoses@karunya.edu.in

Andrew J*
*Computer Science and Engineering*
*Manipal Institue of Technology*
*Manipal Academy of Higher Education*
Manipal, India
andrewj.research@gmail.com

***Abstract*— Blockchain is a digital ledger where the data entries are recorded in a decentralized fashion that cannot be altered. This is likely to prosper in a variety of industries, including healthcare. According to a survey, 70% of healthcare professionals believe that blockchain has the largest influence on clinical report management, regulating documents, and creating a framework for sharing electronic health records (EHR) in the healthcare industry. Even though blockchain technology is having real potential for improving health information systems, the rise of this technology has also led to innovative proposals and applications. This review mainly focuses on EHR data exchange between the patient and the hospital entities like doctors, record verifiers, insurance companies, pharmaceuticals, etc. The proposed research study has also discussed about the techniques used in these models to counter the problems present in the traditionally used server-client model like a data breach, Unauthorized access, centralized data management, etc., and improvisation of the blockchain-based models. Further, a comparative analysis has been provided on various blockchain-based systems for hosting a secure EHR sharing.**

***Keywords—Blockchain, IPFS, Smart Contracts, cloud, EHR, PHR, encryption, Authentication, User-centric model.***

## I. Introduction

Electronic Health Records (EHR) are a collection of medical information such as a person's health condition, medicine, lab reports, and personal information. Security and privacy are two of the most difficult concerns to address. The requirement to preserve the privacy of EHRs is the mechanism that allows only the user to perform special operations because EHRs include essential personal medical-related data. In general, a variety of approaches, such as identification, authentication, and authorization of the user, can be used to construct an access control scheme.

The current system is centralized, with complete control of the entire structure held by a single organization or individual. Accessibility and se curity are two big issues with EHR, both of which can be addressed, to a large extent using the innovative Blockchain Technology. Using Blockchain helps to keep the system more secure because of its characteristics like immutability, traceability, and decentralization. Since the demand for this technology in the sector of health care is growing by the day, as data security has become one of the most pressing concerns in the field of information technology (IT). Furthermore, the current system is opaque to the patients, necessitating the development of a patient-centric model. Some of these concerns are solved by blockchain, however, it is limited by its limits, such as scalability, latency, resource management, and storage.

Many difficulties, however, have persisted despite continued interventions, eluding attempts to overcome them. Information security, confidentiality, and interoperability are only a few of them. There is presently no rule for what procedures and/or processing are allowed to be performed on the requested data.

This review aims to describe the current state of blockchain-based health records management, as well as design decisions, constraints, and future directions. The section-wise summary is as follows: Section II discusses the types of research in healthcare blockchain and discusses the techniques used in the state-of-the-art literature. Section III discusses the challenges and research gaps studied in this review. Finally, Section IV concludes the paper with insights observed and the need for blockchain in healthcare.

## II. Blockchain for Healthcare

### *A. Blockchain Overview*

Bitcoin is a decentralized ledger that transfers data between nodes using peer-to-peer networks. A growing number of irreversible documents are being added to the blockchain network. As a result, several blockchain-based systems ensure that payments are safely transferred among untrustworthy clients. Instead of being stored within a single organization, blockchain is spread across the network. The compromise of a blockchain-based system is extremely tough since adversaries must employ more computer power to exploit it. To crack the SHA-256 cryptographic hash, a large amount of processing power is required to tackle a big and complex mathematical problem, which is not currently possible with present technology.

The four basic properties of blockchain are verifiability, efficiency, immutability, and transparency. Verifiability arises from the fact that the public blockchain is nothing but a public record, allowing transactions to be inspected and reviewed at any time. Efficient because it takes a lot of computational effort to add a block to the blockchain, but once it's done, verifying the transaction is incredibly simple. Transactions are published to the blockchain using a consensus algorithm, making them immutable. Different blockchains use various algorithms to achieve consensus. This agreement is intended to ensure that every network node must have the same version of the ledger. A distributed blockchain is transparent by its very nature, and anyone who is part of the blockchain can see which transactions are supported to maintain a single copy of the ledger across all clients.

### B. *Blockchain in the Healthcare Industry*

Because of the powerful features present in blockchain, it is used in many sectors like supply-chain, healthcare, IoT, and data management. Blockchain for health care is emerging very fast with more and more enhancements every day. Some of the blockchain frameworks and models are discussed in the below sections. Blockchain for healthcare is implemented using existing technologies and also some innovative techniques. It has been implemented with IoT and wearable devices which are used for patient monitoring. Some models were also implemented with cloud services as off-chain storage models. Few others used simple blockchain models and other local databases, data lake models, symmetric and asymmetric encryption algorithms, and authentication techniques to answer problems like confidentiality, secure data exchange between entities, integrity, and authentication problems. Table I shows the important applications of blockchain in healthcare.

TABLE I. HEALTHCARE APPLICATIONS OF BLOCKCHAIN

| Healthcare Blockchain Applications | Description | Technology Used |
|---|---|---|
| Patient Data Management | Ability of the patient to control their personal data being shared for research and medical purposes | Smart contracts and private blockchain |
| Clinical Adjudication | Unanimous verification of drug discovery between stakeholders and developers | Hyperledger blockchain |
| Claims Adjudication | Unanimous verification of claims of hospital bills and medical insurance | Private blockchain with consensus algorithm |
| Drug Supply Chain | Ability of the stakeholder to check the origin of the drug and its entirety | Ethereum-based blockchain |

### C. *Blockchain and Interplanetary File System (IPFS) based systems.*

EHR has many uses like preventing diseases, getting accurate results, giving the precise cure, and helping the pharmaceutical companies in manufacturing the drugs. Due to the swift development of information analysis techniques and network enhancing technologies in recent years, an increasing number of medical reports have been replaced by digital documents for sharing and transmitting. Medical records that are transmitted over public networks, on the other hand, may be vulnerable to security attacks and privacy threats. Because of its unique properties such as anonymity, verifiability, immutability, and decentralization, blockchain technology has received a lot of attention in a variety of fields. To protect patients' privacy and provide more tailored healthcare services, there are a lot of security-related problems like integrity, confidentiality, and availability. Li et al., [1] used ciphertext policy attribute-based encryption systems and IPFS in addition to blockchain. Here the data are stored on an Attribute-based encryption model. Some of the limitations are Chosen Keyword Attack (CKA) and computational time for key generation.

Ragavendra et al., [2] proposed a system in combination with Blockchain, IPFS, and Cloud storage to secure data and maintain its integrity and confidentiality. He focuses on sharing the data among different entities like doctors, insurance companies, researchers, and pharmaceuticals. This model is a User-centric Model which focuses on user data privacy. Data is viewed using Smart contracts and Jmeter. The computation cost is more and since they used the SHA 256 algorithm it takes more time compared to AES. Time complexity is O(log2n) for IPFS. An increase in the number of records is proportional to Latency Rate.

Ray et al., [3] developed a system that mainly focuses on remote patient monitoring. Used IoT Virtual Nodes, Ethereum blockchain, GnuPG, IPFS, and Swarm Exchange Scheme for implementing the model. GnuPG is a free and open-source program that encrypts and decrypts data. The suggested privacy-preserving system's UML activities help to understand how the system's various entities undertake different activities to deliver security and privacy services to IoT-healthcare networks. Small EHR files had less swarm exchange time during upload, whereas EHR files ranging from 3.3 to 4.6 MB used the least amount of time to upload.

Sun et al.,[4] mainly focus on the data that is being stored in the traditional database which can be accessed by unauthorized means which violates integrity, confidentiality, and other security factors. Ciphertext policy-based attribute encryption scheme which is used for secure storing of data on to IPFS and storing the Reference on the blockchain which thereby cannot be accessed by anyone who does not have the particular credentials. Attribute-based encryption (ABE) can be divided into the key-policy attribute-based encryption (KP-ABE) and the ciphertext-policy attribute-based encryption (CP-ABE). The Computational cost has been calculated as OE0 in group G0 and OE0 in Group G1.

In the past, many researchers tried to implement Electronic Health care Systems using techniques and methods like Local storage, Software-defined networks, Cloud-based computing, and other things. These methods are very centralized and are not efficient in terms of security which is the most invested thing in present days because of the attacks and data leaks that happen on a large scale these days. A new Proof of Consensus algorithm is used to achieve consensus among the nodes. This is a strict Patient-centric algorithm [5] that stores data on Interplanetary File System (IPFS). Access to the data is allowed only after verifying the asymmetric key credentials that are assigned during the registration. Gas Consumption and Block Size versus Number of Transactions of the PCAC-SC functions shows that Gas points are less required when the number of transactions grows and reaches a certain stage.

EHR are vulnerable to issues such as data breaches, interoperability, and information asymmetry, resulting in limited access to a patient's information. Medical background The focus of this work is on the implementation of By providing a permission blockchain in EHR governance, The environment is decentralized, cost-effective, and secure. The goal of the architecture [6] is to increase the scalability of the system. Blockchain is being used in EHR to enable improved access to patient data. The model uses IPFS, Ethereum Blockchain, and Node.Js to implement this model. The transaction costs are very low and work well in low latency situations.

People's health depends on having a personal health record (PHR) system that updates the records in real-time. In e-Health, achieving a trustworthy PHR system is a potential challenge due to data integration from various EHRs, interoperability of data, and ensuring that access to data is completely within the control of the patient. Alamri et al., [7]proposed an electronic health wallet (EHW) system that employs emerging decentralized technologies such as blockchain and IPFS, as well as health data interoperability standards and technologies such as FHIR's APIs, to address these issues. For IoT-based PHR systems, the EHW relies on a GDPR-compliant framework that assures both privacy and interoperability of data. The performance is evaluated with Hyperledger Caliper.

Electronic health records (EHR) are becoming increasingly widespread around the world. The present EHR systems, on the other hand, have their share of privacy and security issues. The authors have proposed a mechanism that addresses the majority of these issues. The use of a permissioned Ethereum blockchain allows hospitals and patients all around the world to connect. To provide secure storage and authorized access to records, by utilizing a combination of symmetric and asymmetric key encryption. It provides patients complete control over their health records which can be authorized or canceled access to their records by a hospital. Reen et al., [8] have used IPFS for securely storing records which has the benefit of being distributed and guarantees the integrity of records.

### *D. Fully Blockchain-based system*

The Electronic Health Record (EHR) not only has a high value but also infers a high level of personal privacy of the patient. To address security issues such as data counterfeit and interfering in the EHR data sharing process, Yang et al., [9] proposed a blockchain-based EHR data searchable scheme for calculating and applying EHR data in a distributed system. Here the EHR data ciphertext is stored in the cloud and the EHR data keyword index in the blockchain. The data of visitors' search results on the chain is generated using the data identifier's blind value. The token for downloading ciphertext data in the cloud not only improves system storage efficiency, but it also improves the security of the data. but also ensures the EHR data index's integrity, immutability, and traceability. The access control of cloud data is comprehended using the attribute encryption mechanism, and attribute signature technology is used to verify the legitimacy of the EHR data source. Regardless of the number of attributes, the encryption and search complexity of this scheme is persistent.

Huang et al., [10] tend to focus on New Zealand Health Systems and tried to implement the Electronic Health Records System on Blockchain which is well adapted because of its characteristics. The team developed MedBloc a framework that can be used to store, retrieve, and transmit data while preserving its integrity, confidentiality, and availability. Huang et al. used Permissioned Blockchain to implement this model. This model has two Internal limitations Insider attacks and External attacks that can manipulate the data. More access control rules are proportional to more transactions per second. Medbloc achieved good encryption and decryption rates that is 163ms and 188ms.

Jaiman et al., [11] focuses on providing security to healthcare records in large Spectrums. Data governance mechanisms due to the necessity to specify and monitor data sharing and data use cases. Jaiman et al., [9] implemented a blockchain-based data-sharing model for access control over individual health records. The consent models are Data Use Ontology (DUO) which is based on the individual consent of users, and Automatable Discovery Access Matrix (ADA-M). This system is built on top of Ethereum Blockchain. Smart contracts are used for data sharing between entities. Cost of Storing data on Ethereum blockchain costs gas points and overhead may result if the number of users in the blockchain increases. This model had been deployed and tested in LUCE.

Madine et al., [12] suggest that patients need to be given the authority to have control over the data that belong to them so they proposed a model which uses Ethereum Blockchain, Smart contracts, Interplanetary File System, trusted reputation-based re-encryption oracles, and Proxy Re-encryption. The records need to be traceable, Trustable, and reliable. The Smart Contracts used in this model are adapted from GitHub and are implemented on Ethereum Virtual Machines. The cost of each traction is 20Gwei which is pretty very high compared to the traditional model. Smart Contract Upgradability and Interoperability are limitations of this model. This Model can be implemented both on Permissioned and Permissionless Blockchain.

Randhir et al., [13] wanted to improve the existing Traditional Electronic health Records system which lacks a lot of characteristics like Confidentiality, Privacy. So, it has been Implemented on IPFS in addition to a web UI and Blockchain. Uses proof of work as a consensus algorithm. Proof of Identity for identification of peers. The mining process is done by the miners who are recognized in the network. Peer verification is done in the consortium network. The execution time is based on the MB of data that is being uploaded and the mining time. Data uploaded is proportional to mining time. Uses SHA256 for hashing the data. This model does not rely on Cloud-based Systems

Jiang et al., [14] focuses on security related to Healthcare Information exchange (HIE) which can provide security as well as eliminate the limitation present in the traditional model. Jiang et al. implemented a unique model BlocHIE – Healthcare Information Exchange is a blockchain-based network that uses two loosely coupled blockchains to handle different sorts of data. PHD-Chain for personal healthcare data and EMR-Chain for electronic medical records. To improve the model's efficiency, two fairness-based packing techniques are applied. The model uses a proof-of-work consensus technique to approve transactions. They obtain a 2.9x and 2.6x increase in fairness, respectively.

Shen et al., [15] to improve eliminate the third-party entities present in the cloud-based Electronic Health Care Records system. Shen et al., discuss the data that is stored in the cloud which is used for health care analysis and big data analytics without the consent of the data owner. So, a model based on Ethereum Blockchain. PBFT is common in consortium blockchain and has been applied to Hyperledger. By influencing consortium blockchain, the blockchain application in different clouds delivers services, ensuring that sharing is secure and trustworthy. The data provided in the platform is not anonymous, and this scheme has a problem with transparent propagation. The well-designed collaboration model incorporates innovations that recognise the dynamic revenue allocation based on Shapley value.

To achieve an efficient healthcare records management system, it should be having characteristics such as integrity, non-repudiation, and confidentiality. Kleinaki et al., [16] mainly focused on the things and proposed to implement a blockchain-based system in addition to the database which is known as PubMed for evaluating medical conditions. Data versioning has also been implemented to track the changes in the data. Kleinaki et al. used Ethereum Hyper Ledger to implement the model and used smart contracts for sharing the data to entities upon request by them. The communication between the blockchain and the Knowledge database is achieved by using an API configuration.

Data transfer across health institutions and portals for medical services are the most common concern in the country's medical services. Individuals to gain access to their medical records Issues that are specific arise, such as the sharing of health records between institutions or Hospitals have issues with data misuse after it has been shared, as well as a lack of protection. The Framework for Electronic Health Records (EHR) on These concerns is addressed by blockchain, which is the product of a distributed ledger technology. All parties concerned must work together. Vardhini et al., [17] investigates the likelihood of depicting medical records to ensure that data is accurate. For the sake of privacy, data accessibility, and data interoperability, a scenario relating to health care. A network architecture has been constructed, and the smart contract has been deployed (Model File, Acl File, Logic, and Query File).

### *E. Blockchain and Cloud-based systems*

Health Information exchanges are prevalent for some time, and their benefits are well understood and widely researched. A survey[18] conducted by the Centers for Disease Control and Prevention tells 72% of the office-based physicians had a certified electronic health record (EHR) system defined by the U.S. Department of Health and Human Services. Despite their usefulness in increasing provider efficiency, One persistent challenge has been the reduction of administrative costs. The data owner cannot control data after it has been transmitted. In a centralized system, the data is controlled by a single entity that is Hospital[19]. The absence of technical mechanisms for effective patient control by combining user-generated suitable use policies with smart contracts for secure control of PHR in a health information exchange Amofa et al., [20] highlights the benefits of this system, its user-centric approach, and showed experimental results alongside. They designed a mechanism for post-controlled data sharing, the framework introduces minimal risk to data. They used Cloud Storage, Blockchain, and local querying engines. By implementing this framework, health care providers will be able to provide a greater guarantee for data management is currently possible with existing systems.

Jiang et al., [21] talks about the health care system which gives importance to the privacy of the patients. It addresses problems like decentralization, immutability, and authorization and focuses on preventing the data from being lost, manipulated, and losing its confidentiality. The authors developed a separate system known as PESchain which stores and encrypts the data in the local cloud. This project is made on the top of Ethereum Blockchain name Ganache. The main Limitation of the PESchain is caused in the Registration Phase when transaction and certificate calculation is done. Apart from a Stealth authorization is also added. This system works well with AES 128 Encryption but lags when it uses SHA 256.

Nugen et al., [22] talks about the recent trend in technology that is being used for electronic health care record management. It criticizes the existing model for its lack of privacy and data handling. Nugen et al. proposed an Electronic Health Records sharing framework which used Blockchain and Interplanetary File System (IPFS) on a mobile cloud platform. This uses Ethereum as blockchain and for the mobile cloud platform, Amazon Web services are being used. It also works well with the Internet of Medical Things (IOMT).

Chukwu et al.,[23] focuses on decentralization, power failures, and attacks failures, and data exchange custodians majorly focus on trustless and secure exchange of data. Chukwu et al., [8] proposed Preferred Reporting Item for Systematic – Meta-Analysis (PRISM) methodology to implement the system. The model focuses on decentralization using private blockchains like Hyperledger. Built the model based on HIPPA and GDPR related Guidelines. This model has been implemented on Ethereum blockchain and Amazon web Services for testing and found that the average participant spent $283 for storing data. The cost computation is the bottleneck of this system.

Patel et al., [24] implemented cross-domain image sharing that uses blockchain for storing the data. Thus, eliminating the third-party interference in the health records and protecting them from unauthorized entities. Patel et al. also implemented User-Managed Access (UMA) for data sharing. Uses Proof of Stake as a consensus algorithm. Though this model does work fine certain things like Privacy and other security model-related things are unclear and need enhancements. Data lakes and other third-party applications and infrastructures are eliminated from this model to ensure no third party gets access to the data. Moreover, a pair of asymmetric keys are assigned to each participant who is recognized in the consortium.

Uddin et al., [25] discuss the innovative ideas or models which disrupt the traditional Electronic Health care records system. It uses the Internet of Things (IoT), Blockchain, Machine to machine or Cyber-Physical systems, and Wireless Sensor Networks. Use Byzantine Fault Tolerance, Proof of Stake, and Proof of work for different consensus. Used blockchain, network, and node metrics to evaluate the performance of the model. Uses Federated two-way peg communication between networks. The entities are verified by using the assigned private and public key pair which are created during the registration phase in the consortium. IoT devices have limited computing power and memory, whereas Blockchain technology necessitates a large amount of storage and processing power.

Upadhyay et al., [26] focuses mainly on Cyber-Physical system and protect data using the blockchain Fog of things, and the Internet of Things. Proof of work has been eliminated since it consumes a lot of energy and computational resources and has high latency. Proof of Stake has been implemented to verify transactions. To avoid these issues, smart contracts are uploaded into CPS to guarantee data correctness. Byzantine fault is one limitation of the model. The dimension of this CPS device-level security place adds more complexity to the overall CPS interaction. It is easy to deploy the microservices and securely execute the micro-payments in the CPS. The suggested blockchain-enabled cyber-physical society framework aids players in strategizing the development and deployment of the cyber-physical system, as well as driving the cyber-physical society forward.

Wang et al., [27] proposed a framework to effectively maintain Electronic Health Records. The proposed and implemented model consists of Parallel Healthcare Systems (PHS), Parallel Execution (ACP), Artificial Intelligence, and Blockchain. Ethereum Blockchain is used and smart contracts are implemented for data transactions. The PHS focuses to break such “information isolated islands” because the blockchain will mitigate the storage issues by safely integrating the medical data dispersed in various parts. The blockchain uses substitute proof of stake (DPoS) mechanism to achieve consensus among nodes. DPoS is a fast, efficient, and flexible consensus model. The Smart contract help in viewing and sharing the data between entities.

Akkaoui et al., [28] focus on sharing data among different entities like patients, doctors, researchers, and pharmaceuticals genuinely. To accomplish this, he proposed a framework named EdgeMediChain which can perform secure and competent data management. This framework is based on Ethereum Blockchain. Smart contracts deployed on the global-blockchain network which define a set of permissions and AC policies. Smart contracts are used for both data sharing and data reviewing. The observations show the effectiveness of EdgeMediChain in terms of run time with a reduction of nearly 84.75% for 2000 simultaneous transactions. EdgeMediChain also uses an off-chain storage system by adopting Interplanetary File System (IPFS). The MIoT devices used by patients are also verified by using a mechanism called Eth-Identifier along with MIOT-Edge-Manager and certain open authorization protocols are implemented.

In the medical industry, there is a pressing need to address issues such as secure storage, access control management, and privacy preservation, reliable sharing. In this research, Li et al., [29] presented EHR Chain, a blockchain-based EHR system that solves the challenges above using an attribute-based and homomorphic cryptosystem. Li et al. implemented a secure medical record storage framework. Based on blockchain technology and IPFS, a high volume of medical data storage and secure sharing are possible. Second, SHDPCPC-CP-ABE is an improved cryptography primitive. It performs semi-policy activities. At the same time, dynamic permission changes based on partial ciphertext are hidden. This system employs homomorphic encryption the Paillier cryptosystem, which has been improved for patient privacy.

Bhattacharya et al., proposed HeaL [30], a lightweight blockchain (BC)-envisioned architecture that enables secure and trusted EHR exchange over public networks with negligible encryption and signature overheads. HeaL works in two stages. To construct a wireless body area network, proximity sensor nodes (PSN) are installed over the patient in the first phase (WBAN). Based on resource capabilities to forward data to the gateway, nodes elect a cluster-head (CH) in their neighborhood. With EHR meta-information, sensor nodes (GSN) in WBAN. GSN then conducts a lightweight encryption technique in the second phase, which combines data encryption with signing among authorized participants. The data is transmitted over public network and can only be accessed by authorized individuals who have obtained secure keys from interplanetary file systems (IPFS). To address the same, an energy-competent consensus mechanism should be proposed with reduced computational limitations. The transactions cost decreases increase in blocks.

Although because of concerns about confidentiality, interoperability, and integrity, the digitization of health records has greatly accelerated Health Information Exchange (HIE) activities among different practitioners, which has lagged behind the implementation of Electronic Health Records for a variety of reasons. In this work [31], a Blockchain-as-a-Service (BaaS-HIE) based HIE solution is used. This design effort entails the usage of a private Blockchain and smart contracts to achieve access control management. All health data is encrypted and saved in an InterPlanetary File System (IPFS), and the output of the assets URL is stored in the blockchain, to maintain effective levels of applications performance and make them economically viable. The typical response times required to retract and issue authorizations are comparable; the grant transaction takes 0.32s on average, on the other hand the retract transaction takes 0.21s on average. Registration takes an average of 3.7 seconds. It takes only 1.3 seconds to log in.

Patients’ private information, such as their names, addresses, and diseases, is regularly breached in today's smart cities and houses, which is indirectly tied to the security of electronic health records (EHRs). The current state-of-the-art security measures for EHRs have rendered data inaccessible to patients in most cases. Because it shares data in a decentralized and transactional manner, blockchain technology addresses the aforementioned difficulties. This can be used in the healthcare industry to strike a compromise between EHR privacy and accessibility. Vora et al., [5], [32] used Proxy nodes, Ethereum Blockchain, and EHR database. He proposed the BHEEM framework to implement this model. Unauthorized access by various actors is further reduced, and a sense of decentralization is achieved by combining certain nodes with improvised authority.

TABLE II. COMPARATIVE ANALYSIS OF STATE-OF-THE-ART HEALTHCARE BLOCKCHAIN LITERATURE

| Name of Author | Technologies used | Confidentiality | Integrity | Availability | Non - Repudiation |
|---|---|---|---|---|---|
| Li et al., [1] | Blockchain, APHR Search System | ✓ | ✓ | ✓ | ✓ |
| Ragavendra et al., [2] | IPFS, Ethereum blockchain, Local Query engine | ✓ | ✓ | | |
| Yang et al., [9] | Blockchain, Cloud Storage, Data Pool, Local Storage | ✓ | ✓ | | |
| Ray et al., [3] | Blockchain, IOT, Swarm Exchange Infrastructure | ✓ | ✓ | ✓ | |
| Sun et al., [4] | IPFS, Blockchain | ✓ | ✓ | ✓ | |
| Jabarulla et al., [5] | IPFS, Ethereum Hyper Ledger | ✓ | ✓ | ✓ | \ |
| Mukherji et al., [6] | IPFS, Hyper Ledger | ✓ | ✓ | ✓ | |
| Alamri et al., [7] | IPFS, Hyper Ledger Fabric, HL7FHIR | ✓ | ✓ | ✓ | |
| Reen et al., [8] | IPFS, Blockchain, INFURA | ✓ | ✓ | ✓ | |
| Huang et al., [10] | Ethereum Blockchain | ✓ | ✓ | | |
| Jaiman et al., [11] | Ethereum Blockchain, Customized Consent Model, | ✓ | ✓ | ✓ | |
| Madine et al., [12] | Hyperledger, Re-encryption oracles, IPFS | ✓ | ✓ | ✓ | |
| Patel et al., [22] | Blockchain, Cloud Storage | | ✓ | ✓ | |
| Randhir et al., [13] | Ethereum Blockchain, IPFS, | ✓ | ✓ | ✓ | |
| Jiang et al., [14] | Blockchain, Local Cloud | ✓ | ✓ | ✓ | |
| Shen et al., [15] | Blockchain, Multiple Cloud Servers | ✓ | ✓ | ✓ | ✓ |
| Kleinaki et al., [16] | Blockchain, Local Database, Hash Tree | ✓ | ✓ | ✓ | |
| Vardhini et al., [17] | Blockchain, Hyper Ledger | ✓ | ✓ | ✓ | |
| Amofa et al., [18] | Cloud Storage, Blockchain, Local Storage | ✓ | ✓ | ✓ | |
| Jiang et al., [19] | Blockchain, Cloud Storage | ✓ | ✓ | ✓ | |
| Nugen et al., [20] | Hyper Ledger, Blockchain, Cloud Storage | ✓ | ✓ | | |
| Chukwu et al., [21] | Blockchain, PRISMA framework | ✓ | ✓ | | ✓ |
| Uddin et al., [23] | Blockchain, Decentralized Application, DAG Network | ✓ | ✓ | ✓ | |
| Upadhyay et al., [24] | Blockchain, Cloud services, IoT | ✓ | ✓ | ✓ | ✓ |
| Wang et al., [25] | Blockchain, Artificial Intelligence, Parallel Execution (ACP) | ✓ | ✓ | ✓ | |
| Akkaoui et al., [26] | Blockchain, IPFS, Data Repositories | ✓ | ✓ | ✓ | |
| Li et al., [27] | IPFS, Local Database | ✓ | ✓ | ✓ | |
| Bhattacharya et al., [28] | IPFS, Wireless Body Area Network, Gated Sensor Nodes | ✓ | ✓ | ✓ | |
| Buzachis et al., [29] | Truffle Framework, IPFS, Ethereum | ✓ | ✓ | ✓ | |
| Vora et al., [30] | Blockchain, HER Database, Proxy Nodes | ✓ | ✓ | ✓ | |

## III. Discussion

Healthcare records protection and distribution using blockchain and other sidekick technologies help in maintaining the privacy, availability, and integrity of the data. But Blockchain when combined with Interplanetary File System gives us more flexibility, Integrity, availability, and confidentiality. In addition to this anonymity can also be achieved. Further use of hashing function incorporated with other techniques and encryption algorithms can also be used to achieve more security. Interplanetary file systems and blockchain combined give good results compared to purely blockchain-based models and hybrid models which use clouds, data lakes, others, etc.

Techniques like privacy-preserving-based data sharing[33], [34] can be enhanced to produce good results. Some of the papers discussed were more efficient by not only focusing on data sharing but also an integration of the MIoT, data exchange between hospitals to achieve the goals of security very widely. Though the usage of other technologies was present they tried to solve the problems like Unauthorized access, less patient-centric ness, internal attacks, and EHR ownership.

TABLE III. Merits and Demerits of Healthcare Blockchain Techniques

| Blockchain Technology | Merits | Demerits |
|---|---|---|
| Ethereum Blockchain | Transaction are confidential | High Ethereum Gas Price |
| server-client model using Blockchain | Data can be accessed and stored easily | Malware, Non-availability, Data Breach |
| Cloud integrated Blockchain | Storage flexibility and easy access | Data Breach and Data Availability |
| Blockchain with IPFS | Very secure provides confidentiality and integrity of data | Social Engineering Attacks |

Since 2016, the Ethereum blockchain has been hacked numerous times as a result of third-party involvement in assaults. With time, the Ethereum blockchain has received numerous updates in the form of milestones, ensuring that it remains trustworthy and safe for its users. Many blockchain projects are still built on the Ethereum platform, making it the development environment of choice. For the time being, Ethereum's future appears to be solid, especially with new improvements for Ethereum 2.0. Gas cost is very high which is the current problem. There are numerous methods a blockchain may be attacked. Performing those assaults which includes Finney attack, race attack, 51% attack, eclipse attack, Sybil attack, DDoS, routing attack, DAO attack, parity multisig parity attack on a blockchain will become extra hard as extra computing electricity is brought to the network.. Some of these attacks have been mitigated and other problems persist. The comparative analysis of various blockchain based EHR data sharing literature is provided in Table II. The comparative analysis is based on the CIA triad such as confidentiality, integrity, availability and non-repudiation. Table III discusses the merits and demerits of the healthcare blockchain technologies.

## IV. Conclusions

The application of blockchain in healthcare is currently recognized as an academic topic, with an increase in the number and quality of publications. Healthcare institutions are in desperate need of new and enhanced trust-preserving solutions due to the overarching need of retaining confidence while satisfying the constant demand for data sharing in the healthcare ecosystem. According to the findings of this review, blockchain-based frameworks are presently being used in a few EHR, PHR. This study provides an in-depth review of various state-of-the-art research using blockchain for the healthcare industry. We explored the advantages of IPFS based mechanism for secure EHR data sharing. Further, we provided a comparative analysis based on CIA triads to compare the efficiency of the recent research. Finally, we perceive that the research agenda should be expanded to include these specific topics, and the search for blockchain-based solutions that build trust by reducing threats both inside and outside the healthcare industry.

## References

[1] C. T. Li, D. H. Shih, C. C. Wang, C. L. Chen, and C. C. Lee, “A blockchain based data aggregation and group authentication scheme for electronic medical system,” *IEEE Access*, vol. 8, pp. 173904–173917, 2020, doi: 10.1109/ACCESS.2020.3025898.

[2] R. K. Marangappanavar and K. Kiran, “Inter-Planetary File System Enabled Blockchain Solution for Securing Healthcare Records,” *ISEA-ISAP 2020 - Proceedings of the 3rd ISEA International Conference on Security and Privacy 2020*, pp. 171–178, Feb. 2020, doi: 10.1109/ISEA-ISAP49340.2020.235016.

[3] P. P. Ray, B. Chowhan, N. Kumar, and A. Almogren, “BIoTHR: Electronic Health Record Servicing Scheme in IoT-Blockchain Ecosystem,” *IEEE Internet of Things Journal*, vol. 8, no. 13, pp. 10857–10872, Jul. 2021, doi: 10.1109/JIOT.2021.3050703.

[4] J. Sun, X. Yao, S. Wang, and Y. Wu, “Blockchain-Based Secure Storage and Access Scheme for Electronic Medical Records in IPFS,” *IEEE Access*, vol. 8, pp. 59389–59401, 2020, doi: 10.1109/ACCESS.2020.2982964.

[5] M. Y. Jabarulla and H. N. Lee, “Blockchain-based distributed patient-centric image management system,” *Applied Sciences (Switzerland)*, vol. 11, no. 1, pp. 1–20, Jan. 2021, doi: 10.3390/app11010196.

[6] A. Mukherji and N. Ganguli, “Efficient and Scalable Electronic Health Record Management using Permissioned Blockchain Technology,” Oct. 2020. doi: 10.1109/IEMENTech51367.2020.9270106.

[7] B. Alamri, I. T. Javed, and T. Margaria, “A GDPR-Compliant Framework for IoT-Based Personal Health Records Using Blockchain,” Apr. 2021. doi: 10.1109/NTMS49979.2021.9432661.

[8] G. Reen, M. Mohandas, and S. Venkatesan, “Decentralized Patient Centric e-Health Record Management System using Blockchain and IPFS,” *2019 IEEE Conference on Information and Communication Technology, CICT 2019*, Sep. 2020, doi: 10.1109/CICT48419.2019.9066212.

[9] X. Yang, T. Li, R. Liu, and M. Wang, “Blockchain-based secure and searchable EHR sharing scheme,” *Proceedings - 2019 4th International Conference on Mechanical, Control and Computer Engineering, ICMCCE 2019*, pp. 822–825, Oct. 2019, doi: 10.1109/ICMCCE48743.2019.00188.

[10] J. Huang, Y. W. Qi, M. R. Asghar, A. Meads, and Y. C. Tu, “MedBloc: A blockchain-based secure EHR system for sharing and accessing medical data,” *Proceedings - 2019 18th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/13th IEEE International Conference on Big Data Science and Engineering,*

*TrustCom/BigDataSE 2019*, pp. 594–601, Aug. 2019, doi: 10.1109/TRUSTCOM/BIGDATASE.2019.00085.

[11] V. Jaiman and V. Urovi, "A Consent Model for Blockchain-based Distributed Data Sharing Platforms," Jul. 2020, doi: 10.1109/ACCESS.2020.3014565.

[12] M. M. Madine *et al.*, "Blockchain for Giving Patients Control over Their Medical Records," *IEEE Access*, vol. 8, pp. 193102–193115, 2020, doi: 10.1109/ACCESS.2020.3032553.

[13] R. Kumar, N. Marchang, and R. Tripathi, "Distributed Off-Chain Storage of Patient Diagnostic Reports in Healthcare System Using IPFS and Blockchain," *2020 International Conference on COMmunication Systems and NETworkS, COMSNETS 2020*, pp. 1–5, Jan. 2020, doi: 10.1109/COMSNETS48256.2020.9027313.

[14] S. Jiang, J. Cao, H. Wu, Y. Yang, M. Ma, and J. He, "Blochie: A blockchain-based platform for healthcare information exchange," in *Proceedings - 2018 IEEE International Conference on Smart Computing, SMARTCOMP 2018*, Jul. 2018, pp. 49–56. doi: 10.1109/SMARTCOMP.2018.00073.

[15] M. Shen, J. Duan, L. Zhu, J. Zhang, X. Du, and M. Guizani, "Blockchain-based incentives for secure and collaborative data sharing in multiple clouds," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 6, pp. 1229–1241, Jun. 2020, doi: 10.1109/JSAC.2020.2986619.

[16] A. S. Kleinaki, P. Mytis-Gkometh, G. Drosatos, P. S. Efraimidis, and E. Kaldoudi, "A Blockchain-Based Notarization Service for Biomedical Knowledge Retrieval," *Computational and Structural Biotechnology Journal*, vol. 16, pp. 288–297, Jan. 2018, doi: 10.1016/j.csbj.2018.08.002.

[17] Vardhini, S. N. Dass, Sahana, and R. Chinnaiyan, "A Blockchain based Electronic Medical Health Records Framework using Smart Contracts," Jan. 2021. doi: 10.1109/ICCCI50826.2021.9402689.

[18] "QuickStats: Management of Patient Health Information Functions Among Office-Based Physicians With and Without a Certified Electronic Health Record (EHR) System — National Electronic Health Records Survey, United States, 2018," *MMWR. Morbidity and Mortality Weekly Report*, vol. 69, no. 38, p. 1381, Sep. 2020, doi: 10.15585/MMWR.MM6938A8.

[19] B. Bhushan, P. Sinha, K. M. Sagayam, and A. J, "Untangling blockchain technology: A survey on state of the art, security threats, privacy services, applications and future research directions," *Computers & Electrical Engineering*, vol. 90, p. 106897, Mar. 2021, doi: 10.1016/J.COMPELECENG.2020.106897.

[20] S. Amofa *et al.*, "A blockchain-based architecture framework for secure sharing of personal health data," *2018 IEEE 20th International Conference on e-Health Networking, Applications and Services, Healthcom 2018*, Nov. 2018, doi: 10.1109/HEALTHCOM.2018.8531160.

[21] S. Jiang, H. Wu, and L. Wang, "Patients-controlled secure and privacy-preserving EHRs sharing scheme based on consortium blockchain," *2019 IEEE Global Communications Conference, GLOBECOM 2019 - Proceedings*, Dec. 2019, doi: 10.1109/GLOBECOM38437.2019.9013220.

[22] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Blockchain for Secure EHRs Sharing of Mobile Cloud Based E-Health Systems," *IEEE Access*, vol. 7, pp. 66792–66806, 2019, doi: 10.1109/ACCESS.2019.2917555.

[23] E. Chukwu and L. Garg, "A systematic review of blockchain in healthcare: Frameworks, prototypes, and implementations," *IEEE Access*, vol. 8, pp. 21196–21214, 2020, doi: 10.1109/ACCESS.2020.2969881.

[24] V. Patel, "A framework for secure and decentralized sharing of medical imaging data via blockchain consensus," *Health Informatics Journal*, vol. 25, no. 4, pp. 1398–1411, Dec. 2019, doi: 10.1177/1460458218769699.

[25] M. A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian, "A survey on the adoption of blockchain in IoT: challenges and solutions," *Blockchain: Research and Applications*, vol. 2, no. 2, p. 100006, Jun. 2021, doi: 10.1016/j.bcra.2021.100006.

[26] N. Upadhyay, "Blockchain Enabled Cyber-Physical Society Framework," in *Procedia Computer Science*, 2019, vol. 162, pp. 53–58. doi: 10.1016/j.procs.2019.11.257.

[27] S. Wang *et al.*, "Blockchain-Powered Parallel Healthcare Systems Based on the ACP Approach," *IEEE Transactions on Computational Social Systems*, vol. 5, no. 4, pp. 942–950, Dec. 2018, doi: 10.1109/TCSS.2018.2865526.

[28] R. Akkaoui, X. Hei, and W. Cheng, "EdgeMediChain: A Hybrid Edge Blockchain-Based Framework for Health Data Exchange," *IEEE Access*, vol. 8, pp. 113467–113486, 2020, doi: 10.1109/ACCESS.2020.3003575.

[29] F. Li, K. Liu, L. Zhang, S. Huang, and Q. Wu, "EHRChain: A Blockchain-based EHR System Using Attribute-Based and Homomorphic Cryptosystem," *IEEE Transactions on Services Computing*, 2021, doi: 10.1109/TSC.2021.3078119.

[30] P. Bhattacharya, P. Mehta, S. Tanwar, M. S. Obaidat, and K. F. Hsiao, "HeaL: A blockchain-envisioned signcryption scheme for healthcare IoT ecosystems," Nov. 2020. doi: 10.1109/CCCI49893.2020.9256705.

[31] A. Buzachis, A. Celesti, M. Fazio, and M. Villari, "On the Design of a Blockchain-as-a-Service-Based Health Information Exchange (BaaS-HIE) System for Patient Monitoring," *Proceedings - IEEE Symposium on Computers and Communications*, vol. 2019-June, Jun. 2019, doi: 10.1109/ISCC47284.2019.8969718.

[32] J. Vora *et al.*, "BHEEM: A Blockchain-Based Framework for Securing Electronic Health Records," *2018 IEEE Globecom Workshops, GC Wkshps 2018 - Proceedings*, Feb. 2019, doi: 10.1109/GLOCOMW.2018.8644088.

[33] J. A. Onesimu, J. Karthikeyan, and Y. Sei, "An efficient clustering-based anonymization scheme for privacy-preserving data collection in IoT based healthcare services," *Peer-to-Peer Networking and Applications 2021 14:3*, vol. 14, no. 3, pp. 1629–1649, Feb. 2021, doi: 10.1007/S12083-021-01077-7.

[34] J. Andrew and J. Karthikeyan, "Privacy-Preserving Big Data Publication: (K, L) Anonymity," *Advances in Intelligent Systems and Computing*, vol. 1167, pp. 77–88, 2021, doi: 10.1007/978-981-15-5285-4_7.