Blockchain Based Secure Architecture for Electronic Healthcare Record Management

Susmita Mondal[1], Mehak Shafi[2], Sumeet Gupta[2], and Sachin Kumar Gupta[2,*]

ARTICLE INFO

Article history:
Received: 17 July 2021
Revised: 6 September 2021
Accepted: 15 September 2021

Keywords:
Blockchain
Healthcare
Cryptography
EHRs
Data Security
Multi signature Stamp
Channel

ABSTRACT

Blockchain technology is a fast-growing field of interest to provide a secure framework for storing encrypted data in several sectors. It is a quite popular technology to enter a new realm, largely due to the emergence of cryptocurrencies. Blockchain technology has a great potential in the healthcare domain, emerging from a patient-centered approach to the integration of decentralized networks, which includes the precision of Electronic Healthcare Records (EHRs). It allows both transparent and an open system for health record management. For accessing EHRs, Blockchain technology does not require any centralized control. The security is based on individual blocks; it is safe and reliable with the cryptographical hash links. Only the verified EHRs are added to the Blockchain after being approved by miners through a consensus mechanism and then it is distributed (or replicated) among the networks. But certainly, there is a need for efficiently managing the numerous amounts of electronically generated data. This paper proposes an EHR management system by integrating a Blockchain multi-signature stamp with a private channel framework. Multi-signature stamps tackle the question of data ownership and authority. This approach assists the construction of a correct protocol for retracing a user's database. A channel guarantees that all parties obey a common rule to preserve the Blockchain ledger. This paper also summarizes several related works and discusses the technical background of the technology. Data decentralization through Blockchain will improve accessibility and protection of data while overturning the healthcare bureaucracy and building a new framework for patients to administer their own health.

1. INTRODUCTION

Healthcare has always been essential for society. The healthcare sector involves many parties like hospitals, doctors, patients, insurance companies, and pharmaceutical companies. Illness, injuries, and crises occur every day and it is important to identify, control, and cure the illnesses and diseases suffered [1]. Healthcare is a data-intensive environment that generates, disseminates, stores, and accesses a vast volume of data every day [2]. Both medical documents such as insurance reports and health data obtained by body sensors, may be used as health information. This leads to the transition of medical information from paper to digital medium, enhancing the security and privacy requirements for the healthcare records. Performance improvement of conventional medical services continues to be huge comparing to modern digitized technologies. There is a need of reliable, cost-effective, and all-time available healthcare networks that tracks, stores, and provides secured patient's data as input when needed [3]. Blockchain is a wiser step in developing the worldwide pragmatic data-based healthcare network.

A Blockchain is a distributed transaction log that enables each node of a P2P (peer-to-peer) network to own a similar copy of a particular ledger. The ledger is verified and synchronized with the creation of a new block through a consensus protocol. The consensus protocol introduced by a distributed P2P Blockchain network eliminates the requirement of a centralized node or a trustworthy entity, such as a government agency [4]. This booming technology is a revolution in every aspect of human lives, be it in the industries, healthcare, real estate, or banking. It has evolved at an incredible rate to provide users with transparency. Even when IoT devices are infiltrated by several intruders, Blockchain can guarantee security and transparency to the users. It also enables information to be monitored, coordinated, and stored from various devices. All the operations do not always require federal cloud

[1]*Department of Computer Science and Engineering, Indian Institute of Technology Gandhinagar, Palaj, Gurarat-382355, India*
[2]*School of Electronics and Communication Engineering, Shri Mata Vaishno Devi University, Katra-182320, Jammu & Kashmir, India*
**Corresponding author:* Sachin Kumar Gupta; Email: sachin.gupta@smvdu.ac.in.

computing strategy. The Blockchain technique restricts data modification (like update or delete) once a block is created. Moreover, gaining some accessibility on the data requires a user to be authorized with the Blockchain network.

Blockchain technology is a feasible technique in the real-time environment, providing confidentiality and security on the patient's data [5]. Due to the shift to Blockchain, the healthcare industry has seen a tremendous transformation in the past few years [6]. Besides, the Blockchain-based EHRs allow a robust, interoperable, and safe sharing of patient records [4]. Some of the significant characteristics that have revolutionized the healthcare industry with Blockchain integration are as follows [7]:

- Decentralization: Replicate ledger throughout the network, supporting interoperability.
- Authentication: Approved parties are given some accessibility to the Blockchain.
- Immutable: Tampering with the data is prevented.
- Transparent: The ledger is visible to everyone, but modification is not permissible.

Blockchain can be implemented with the Wireless Body Area Networks (WBANs), IoT (Internet of Things) devices, Big Data, Cloud, and Machine Learning. The Blockchain technology and WBAN together ensures secure data transfer in a shorter-range communication [3]. To provide confidentiality and accountability for each transitional operation, IoT devices are used in the Blockchain network [5]. Big data offers unlimited possibilities for research and development, medical treatments, and monitoring personal health [8]. Blockchain and cloud can meet the requirements for large-scale health information storage, analysis, and management [4]. The system of Machine Learning uses the data generated by the patient to detect abnormalities in the data [9]. The medical sector is currently the most complex, significant, and rapidly expanding area of digital communication which enhances the standard of patient-doctor interaction.

Healthcare organizations around the world are transforming into more effective, organized, and patient-centered networks in today's era [5]. In health care, the main concerns like data security and data management are still in the developing phase [2]. To address these concerns, the author proposes a decentralized healthcare data framework based on Blockchain technology. This study suggests a concept of incorporating a multi-signature stamp with a private channel. These methodologies together will provide a Blockchain-based security and data management system for EHRs.

In the conventional systems, the medical data is managed by a centralized repository. The data can be destroyed, corrupted, obscured, or exploited by bribing the person who is updating it. Records are not secure neither they provide immutability, or transparency. The data is not spread across all repositories since traditional methods do not permit this. Blockchain aims to restore confidence in modern medical records when conventional approaches struggle to apply such pre-requisites on the healthcare data. Blockchain is one of the growing innovations for offering a smart way of handling EHRs through an accessible, secure, confidential, and decentralized consensus [10].

The objective of this study is to discuss the context and characteristics of Blockchain technology and why it is used in healthcare. A literature review is presented that influenced the development of this article. To address the data management and security issue as a research gap, the proposed methodology incorporates Blockchain with multi-signature stamps and the notion a private channel. Discussing several segments and comparing other systems with Blockchain-based healthcare, gives a brief idea about where the healthcare is heading towards. The paper is concluded after exchanging views upon the restrictions and the challenges with this Blockchain-based technology.

The following is the article's outline. Section 2 discusses the related work. Section 3 deals with Blockchain technology preliminary study. Section 4 presents the technical background of Blockchain technology in the healthcare sector. Section 5 describes the proposed model for healthcare. Further, the major challenges and discussion of Blockchain in the healthcare system have been discussed in Section 6. Finally, the article is concluded with the future direction in Section 7.

2. RELATED WORK

Several scientists, researchers, and authors have published articles on data management applications and Blockchain-based EHR. The informative and precise outline of the EHR management in healthcare applications based on Blockchain technology is elaborated in this portion [5].

MedRec [11] technology is built to provide decentralization, utilizing the properties of Blockchain technology. The patient centric API is designed to include interoperability for the aggregation of the databases. A cryptographic hash is used to ensure that the data is not manipulated. Smart contracts in the Ethereum network are used for data collection and access permission. Proof of identity, a DNS-like model is used to connect a unique Ethereum address to a particular patient ID. A syncing algorithm enables the management of off-chain data sharing between the supplier and the patient's database. To prevent a common point of failure MedRec depends on several participants. The system offers convenient access to immutable and robust medical information resources through care providers and services. However, the model does not have scalability and encryption over smarts contracts. MedBlock [12] proposed a Blockchain-based data management framework that improves the hybrid-consensus platform to resolve network latency and high energy consumption problems where DPoS and PBFT are not sufficient. The consensus process functions like a

committee voting, where one node is elected as the influencer to operate on behalf of several other nodes inside a network. To demonstrate strong and reliable identity, MedBlock incorporates symmetric cryptography with custom access control. The system enables quick data transfer to prevent network overload by executing several tasks in a single period for the patient. Compared to other methods, the Bread Crumb mechanism provides less access time and continuous data transfer at various intervals, which addresses the issue of exchanging information and data storage in broad networks. But EHRs are held in hospital servers, they lack the idea of Blockchain decentralization to prevent being exploited by malicious hackers.

MeDShare [13] is another powerful Blockchain-based management framework that has been developed for cloud storage to handle shared medical information and data across large-scale medical institutions. The proposed framework uses encryption keys to ensure data authenticity, confidentiality, auditing, and user validation. The framework for exchanging data with MedShare is divided into four groups, including the consumer, data application, data structuring and provenance, and an integrated network layer for databases. For a user wanting to enter a database, must produce a private key and sign it digitally. The query method would then forward the data-structuring request to the provenance layer. A smart contract to exchange data between cloud service providers must then be implemented. The downside of this method is that it overlooks concerns regarding data disclosure. ModelChain [14] system has been developed as a cross-institutional study that interacts with healthcare related data. This research implemented a private Blockchain platform to handle the details relevant to safety of metadata. This research utilized both Blockchain technology and machine learning to promote Patient-Centered Outcomes Research (PCOR) and cooperation between institutions. To boost performance and accuracy, a modern proof-of-information algorithm is being built to evaluate the mechanism. But this system needs further improvement in security by encrypting information from transactions and utilizing a Virtual Private Network (VPN).

Peterson et al. [15] proposed a medical information sharing system that has a community-based network design. This study suggested a framework where data can only be viewed on a given node if the community members accept and support the semantics. Ultimately, patient monitors the protected data exchange and their enforcement. But the biggest downside is the direct storage of personal data. SMEAD [16] is a modern healthcare model built for patients with diabetes in a safe end-to-end network. The suggested model involves three wearable tools (neckband, shoes, and wristband) to track the status of the patient and anticipate the condition. They also introduced MEDIBOX (an auto-served and shared network) to act as a tool for patients to warn and recall. Using smart contracts, Blockchain provides encryption and access control of data to trusted parties. The proposed framework is built together with medication, IoT, wearable devices, and cloud storage. The use of public-key cryptography preserves the data authentication. Through protecting transactions, smart contracts are being used to resolve the privacy problem. This system focuses primarily on the constant supervision of patients and alerts people if something is unusual. However, the feature does not define security for the mobile application controlled by the number of parties concerned.

Salahuddin et al. [17] proposed a Machine-to-Machine (M2M) data management framework by an innovative protocol-based beacon. The proposed architecture allows the use of IoT sensors based on Field-Programmable Gate Array (FPGA) for tracking medical data. Heterogeneous groups including authorities, retailers, staff, doctors, insurance providers, and hospitals may handle the deployed systems. Blockchain and IoT-based cloud gateway is used to restrict data manipulation, where data fusion, and decision fusion is applied. While the system offers cost-effectiveness, low latency, and end-user local execution, it also requires some development in IoT software, security, and privacy. Conceicao et al. [18] addressed a solution regarding transparency and protection using Ethereum based smart contracts. The information is only held by the patient and no one other than that (like health organizations). Smart contracts monitor health transactions, store EHR, and store public-private key pairs of users. Wallets are used as a tool to accelerate the information search. Three categories of transactions are defined: New Record, Notification, and Request Access. If a user misplaced their private key, they will not be able to access their wallet anymore. Data is not maintained in a secured database so data recovery mechanisms would be a problem.

Dubovitskaya et al. [19] allow Blockchain to tackle three key goals: patient care, data collection for research purposes, and better treatment by linking various health-care organizations together. The architecture consists of several nodes for achieving network unity, repositories for managing off-chain information, membership support, and user APIs. The system is responsible for registering participants and can be used to describe the chain-code features. Patient records are held in two separate systems that are local storage, and a cloud-based server. Consensus nodes work through a peer validating based on Hyperledger and the Practical Byzantine Fault Tolerance (PBFT) consensus algorithm. The structure seeks to improve the processing period and decrease operating expenses whilst strengthening procedures for decision-making. To have some effective storage systems, data sensitivity should also be considered.

The data stored in the EHRs are commonly viewed as a

potential treasure for medical research. The security and management of EHRs are still a major concern. Since researchers have given different ideas related to Blockchain in EHR, there are still multiple issues affecting data security and management. To address these issues, this paper proposes a model introducing the multi-signature stamp and private channel with the Blockchain technology for the authentication and confidentiality purpose.

3. PRELIMINARY STUDY

This segment addresses the preliminary Blockchain studies. Also, the attributes, categories, consensus, and short overview of the technology is illustrated in this section.

3.1. Blockchain Technology

In 2008, Satoshi Nakamoto first proposed the idea of Bitcoin cryptocurrency as a decentralized P2P public system. Blockchain technology has been the foundation behind Bitcoin that functions as a transactional ledger. Blockchain technology is a digital innovation that has the potential to significantly impact trusted computing activists. Blockchain provides transparency. The features of the Blockchain technology attracted many researchers to explore the architecture and find out potential use cases. The diversity of Blockchain technology in the application domain has faced rapid growth. The type of application is not restricted to financial transactions only. Figure 1 demonstrates the different implementations of Blockchain technology in multiple fields including healthcare.

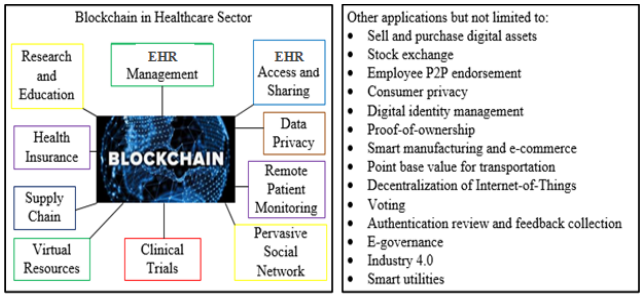

Fig. 1. The applications of blockchain technology.

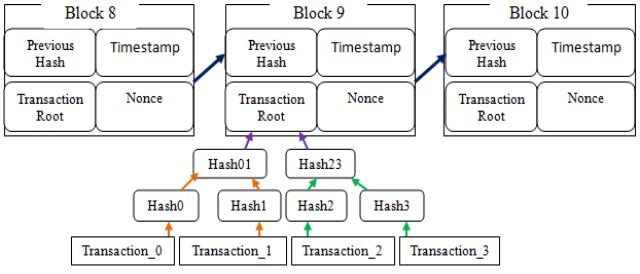

Fig. 2. Hashing in a Blockchain [Each block hash is previously attached to all other block hashes; transaction root follows the principle of "Merkle tree"].

Blockchain is a linked list that is distributed, consistently maintained by consensus, cryptographically linked, and cryptographically assures the integrity of data [20]. A linked list is a set of blocks that are connected by some link. In Blockchain for linking the tamper-resistant blocks cryptographic hashing is used. So, it is called hash linking. Blockchain commonly uses the Secure Hash Algorithm (SHA) 256 for hash linking. A pictorial hashing diagram and is shown in Figure 2.

Table 1. Blockchain Consensus Algorithms

Algo-rithm	Working Principle	Core Feature	Advantage	Disad-vantage
PoW	Nodes perform a calculation to generate the correct hash of the block header.	Solving hash-puzzles using expensive computational power.	• Decentralization of power. • Secure Network.	High power and electricity consumption.
PoS	Nodes allocate a specific amount of stake in the Blockchain.	Network holds the stake amount to ensure the trust of mining.	• Energy-efficient. • Faster processing of transactions.	Less decentralization and less secure than PoW.
DPoS	Chosen nodes will change intervals and block size.	Instead of stakeholders, certain delegates are responsible.	Faster than PoW & PoS. Energy-efficient.	More open to attacks; Richer people dominate the network.
PBFT	At least 2/3 of all nodes will accept block validation to link it to the Blockchain.	Every block generation selects one leader and is responsible for ordering transactions.	Signifying a decrease in energy use. Ability to make a transaction without confirmation.	Works only in small group size; Hard to establish the validity of third-party communications.
Ripple	Nodes create a subset connected to a specific server.	Trusted nodes determine network consensus to reduce latency.	• Fast transactions • Path dependent. • No capacity limit on transaction.	Unique Node Lists (UNLs) must be maintained.

3.1.1. Blockchain Consensus Algorithms

The idea of consensus was formulated based on the Byzantine general problem. Byzantine generals commanded an empire over a single town during the battle. The Byzantine General Problem appears when certain generals must decide to launch an assault or not.

Blockchain introduced distributed consensus algorithms to improve data accuracy and durability [20]. A consensus algorithm is a mechanism where all peers agree on a common state of the distributed ledger. The consistency of the data is maintained by mining (nodes validating transactions and creating blocks) after having the consensus. The consensus means that most of the peers agree on the data that is going in the block. The consensus protocols widely used are Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), PBFT, Ripple, etc. [7]. Table 1 describes the common Blockchain algorithms with their working principles, core features along with their advantages and disadvantages. Consensus mechanisms listed here are irrespective of public and private Blockchain scenarios, as the focus is mainly decentralization.

3.1.2. Features of Blockchain

Blockchain is a less complex approach for encrypting ledger-based transactions across networks. The technology interacts with hosts having various processing capabilities. Ranging from a few to several network nodes, the technology has incredibly efficient computation speed [21]. Figure 3 defines the fundamental operating stages of a Blockchain. First, people perform a transaction or share a query. A network of nodes affiliated with certain roles, validates the transactions. After successful hashing and agreement for the consensus algorithm from each group concerned, a single block is officially announced. The block is eventually added to the current Blockchain [7].

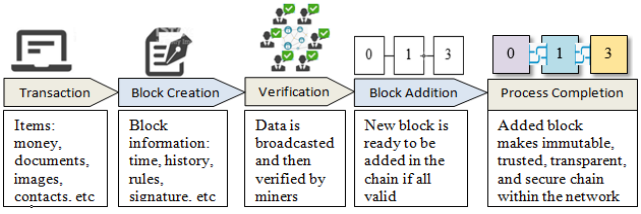

Fig. 3. Basic working principle of Blockchain.

Blockchain includes multiple techniques and have some properties like:

- Integrity: Integrity of the data is maintained because of the cryptographic hash link.
- Immutable: Tamper-proof log of data with limited access.
- Distributed: Blockchain is a distributed system with replicated copies, in contrast to the traditional systems for data management which requires records to be updated on the central server.
- Authenticity: Complete information including data history can be searched on the decentralized network only if the user is authenticated.
- Cryptographically hashed: Uses hash (SHA 256) linking. Hash algorithms provide functions like one-way cryptography, faster deterministic calculation, avalanche effect, and collision resistance. There is a public-private key pair under which the private key used for block signature and the public key is used to test the signature's validity.
- Smart contracts: The codes are time-framed and generated on a distributed ledger framework where all the entities are required to follow the same set of rules.
- Mining: Miners use nonce in the blocks to calculate desired hash-values. This requires a high speed of calculation (and computational power) to obtain the reward for block mining.
- Consensus: The consistency of the connected ledger is maintained through this mechanism. Every party should go through some stages of verification under the thumb rule of certain protocols. This is the backbone of the algorithm for making the technology secure.

Hence, connected data to a ledger at one place can be shared throughout the specific network located in different places (geographically). Such capacity helps data to be exchanged simultaneously with several researchers, affiliate institutions, or other involved organizations, e.g., insurance companies [21].

3.1.3. Classification of Blockchain

The deployment of Blockchain can be public or private. Everyone can participate in a public Blockchain i.e., available to all. Participants in a private Blockchain are known to each other. Bitcoin is the most famous example of a public Blockchain. The private Blockchain network operates by limiting the membership. An example of a private Blockchain would be to grant licenses to a registrar for network participation [10]. Consortium (or federated) Blockchain is a sort of network where the infrastructure is operated by several organizations. In Table 2, a short Blockchain classification has been presented for better understanding.

Table 2. Types of Blockchain

Comparison	Public Blockchain	Private Blockchain	Consortium Blockchain
Permission	Public	Private	Public or private
Organization	Decentralized	Partially decentralized	Almost centralized
Security	High	Medium	Medium
Cost	High	Medium	Low
Identity	Anonymous	Identified	Identified
Example	Bitcoin, Ethereum	Company internal	Hyperledger, Corda

4. TECHNICAL BACKGROUND OF BLOCKCHAIN IN HEALTHCARE SECTOR

People interact with healthcare information in day-to-day life. There should be a location where the personal healthcare records of patients are to be kept. The data might include highly confidential details like, how the patient would be treated and diagnosed. The digitization of data has made it harder to recover, as cyber attackers can easily hack several documents purposely. This has been a potential research gap for newer technologies. There is tremendous scope to establish access specific EHRs through Blockchain technology having the properties like immutability, transparency, and decentralization [5].

Blockchain platform has immense potential to change the whole healthcare industry, placing patients at the heart of the healthcare environment. It improves the safety, protection, and interoperability of health records. Within a standard hosting system, a variety of transactions take place regularly. There is patient identification, the outcome of treatment, health indexes, billing, account monitoring, and expenses. These are being continuously tracked. Every member of the program may be connected to their own electronic ledger with the attributes distinguishable from the others. Figure 4 explains the EHR connectivity of centralized versus decentralized environment. A numerous amount of ledger accounts for mistakes, inefficiency, and theft. For Blockchain technologies, every machine in the network has an accessible copy of the ledger [4]. Data can be conveniently tested and confirmed among all other peers. The established back-end mechanism stores the data to a specific Blockchain after acquisition, analysis, and verification through smart contracts. Now multiple devices can access the saved data using APIs specially built for users [22] for that particular network.

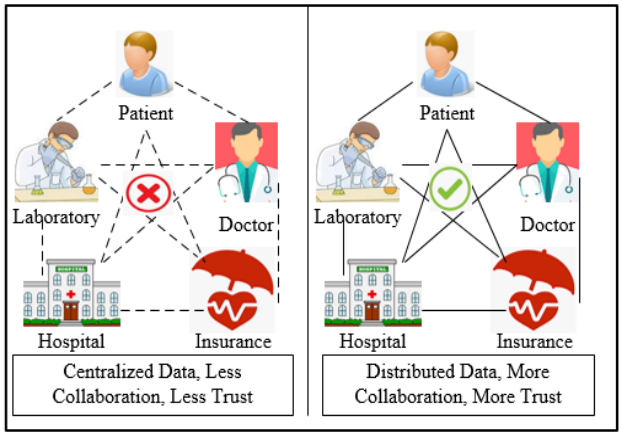

Fig. 4. EHR Connectivity.

4.1. Electronic Healthcare Records (EHRs)

An EHR is a digital version of the medical history of patients. The medical history typically contains clinical data (visual imaging, insurance information, medical advice, and laboratory reports), data on health control (blood pressure, cholesterol level, heartbeat), and other medical records [23]. EHRs are the next stage in the ongoing advancement of health care, which will improve patient-clinical relationships. Many healthcare centers agree on the implementation and application of EHRs. It can typically minimize administrative costs, decrease error rates and enhance patient outcomes. Fast acceptance of EHR has contributed to the large amount of data into the digital world. A critical issue is to manage these healthcare data to improve patient outcomes [24]. Through advancements in electronic data collection leads to safety issues, data resources are growing too fast to regulate and to provide accessibility for viewing and exchanging [25]. It is also difficult to regularly monitor and store health data. Figure 5 illustrates the usual forms of current EMRs in the healthcare industry.

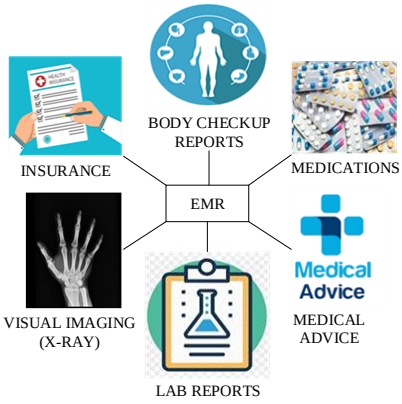

Fig. 5. Types of EMRs.

4.2. Health Information Exchange (HIE)

The features of Blockchain makes it well suited for HIE and clinical trials. It Includes decentralized authentication of transactions, the provenance and sharing of data, and data management. HIE is a mechanism for sharing EHR of the patients [22]. A Blockchain-based medical information system will resolve the problems of supplying trustworthy medications, consultancy, and sensor data to the medical professionals, hospitals, insurance companies, and patients. The health and wellness of a system is not obstructed by faulty information [3]. HIE allows physicians, clinicians, pharmacists, other health care providers, and patients to access and share the essential medical records. It aims to ensure that medical safety, consistency, and efficiency is enhanced electronically. HIE across healthcare organizations have been shown tremendous growth in recent years. First, HIE stimulates the awareness of an individual clinical study. Second, by reviewing a lot of clinical trials the researchers can gain testable theories. Third, the compatibility of expertise in healthcare between laboratory, research organizations, and product developers has been improved [1]. Figure 6 shows the HIE scenario between different parties.

Table 3. Divergences in Healthcare Applications based on Blockchain

Applications	Example	Contribution	Framework	Advantage	Limitation	Remarks
EHR Management	BlockHIE [1]	Privacy and storage enhancement using loosely coupled Blockchain namely EMR-Chain and PHD-Chain.	PoW based algorithms: TP&FAIR, and FAIR-FIRST; Communication layer is coded by GRPC-Python.	Effectiveness and practicability. Dependency on cloud removed by EMR-Chain.	Complex access control: System performance assumes the existence of few time delays.	Combines off-chain storage and on-chain verification methods.
EHR Access and Sharing	OmniPHR 27]	Access to update data, even when it is stored in a different location.	Chord algorithm-based P2P network with Blockchain.	Easy sharing of patient records.	Scalability: Specific data standard fit.	Uniform record keeping.
Data Privacy	MediBchain 28]	Two-level patient: centric data control with Graphical User Interface (GUI).	Elliptic Curve Cryptography (ECC) is used with Blockchain.	Pseudonymity of patient. The patient controls his own data.	The encryption algorithm may expose data content.	The Architecture includes Registration Unit (RU) and Private Accessible Unit (PAU).
Remote Patient Monitoring (RPM)	Pham et al. [29]	Provide Wireless Body Area Network (WBAN) based RPM.	Ethereum, Remix-IDE, and TestRPC based smart Contract (RHS-SC).	Global Positioning System (GPS) based working principle.	Small-scale-based implementation.	Include three parties-patient, doctor, and hospital.
Pervasive Social Network(PSN) based Healthcare	Zhang et al. [30]	PSN based data sharing where WBAN provides authentication.	SHA-512, Elliptic Curve Digital Signature Algorithm (ECDSA), and Raspberry Pi are used along with Blockchain.	Reduces computational load on sensor.	Addresses the challenges for only the PSN network.	Only specific nodes are powerful.
Clinical Trials	Benchoufi et l. [31]	Control of the permission matter to trial, and tracking consent collection.	PoC and Chainscript which uses Stratumn SAS.	Raising openness, auditing, and responsibility.	Low enrolment rate.	Consent-related data has verifiable Fingerprint.
Virtual Resources	Samaniego et l. [32]	Designed for storing health care data, multi-tenancy support, and distribution of shift load using IoT devices	IBM Bluemix and AES are used.	Low latency. Safe, secure, and persistent data storage.	Scalability issue and no experimental setup for key replacement.	Micro-services are hosted closer to the edge and possible to create any number of virtual IoT.
Supply Chain	Modum.io AG [33]	Publically accessible but immutable temperature records fo pharmaceutical products while transportation	Ethereum, JSON, and PostgreSQL databases are used.	Quality controlled temperature is verified and achieved.	No access control or data security based upon digital signature.	Off-line features have been taken into count.
Health Insurance	MIStore [34]	Blockchain-based medical insurance storage system.	Ethereum smart contract and transaction simulator.	Secure and effective verification of data.	Limited efficiency is dependent upon the platform.	Verification between the hospital, patient, and insurance server.
Research and Education	Mytis-Gkometh et al. [35]	Proposes a notary test for users of biomedical data.	Ethereum, JavaScript, Ajax have been used.	Ensures non-repudiation and data integrity.	Query results may not give appropriate information.	Seals query and the result.

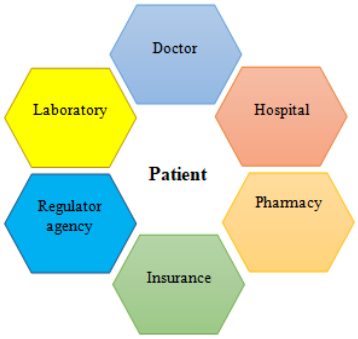

Fig. 6. HIE Scenario.

4.3. Need for EHR Management

Ever since the advent of the e-Health revolution, healthcare services have become increasingly reliant on intelligent technology. These systems help to manage and treat medical illnesses possibly by sending, obtaining, and compiling medical details in the health records [21]. The amount of generated EHR is rising at an exponential pace. Around 63.0% of people manage health-related data online from which 62.4% trust their doctors to share and manage their health details. To properly analyze and coordinate patient's data, many studies need a digital trust management system for modern healthcare technologies. The Blockchain system can build a transparent network between the digital and physical world [7]. Blockchain supports EHR management more safely and can protect patient-centered systems very efficiently [20]. The Blockchain provides an intricate but secure data management system, utilizing smart contracts, consensus, and decentralization.

4.4. Blockchain-Based Radical Changes in Healthcare

There are numerous Blockchain divergences in healthcare offering major alternatives to traditional data-related issues. Through such implementations, Blockchain database is modified in real-time to identify, track and manage medical knowledge. Blockchain-based healthcare data management systems build utilities for patients, physicians, and healthcare organizations in the context of patient information. It further restricts the unauthorized users, comparing conflicting details with healthcare organizations [26]. Table 3 compiles existing healthcare Blockchain implementations to promote incremental and creative development. But the study focuses mainly on the EHR management strategies via Blockchain in contrast with the traditional systems.

5. PROPOSED MODEL

The study proposes a decentralized, Blockchain-based framework for healthcare security and data management. This system enables patients to take full control of their own EHR while giving hospitals and doctors easy access. There are multiple signatures (patient, doctor, and hospital management team) for authentication and non-repudiation of the EHRs as several parties are involved in each chunk of patients' data. The identification of each individual and the recommended medication by physicians are checked via consensus process of the hospital management committee (team of doctors and hospital staff), and verified data is linked to the hospital's main Blockchain. After the data has been validated and added to the Blockchain, a time-stamped hash must be generated. Any modification on the stored data would generate a new hash to be added to the main database, requesting permission from the authorized personnel. This notification will be an alert in case the modification request is not through accredited members. The channel of Blockchain is used to connect different hospitals to rely on the same protocol for successful EHR management. The channel also helps to privatize the digital control of EHRs within the organizations that participated in the Blockchain network.

5.1. Components of Proposed System: Security and Data Management of EHRs

The proposed methodology relies primarily on two strategies: multi-signature stamp and private channel. The key problem which still exists in healthcare is data security and data management Security of Blockchain depends upon the consensus mechanism and algorithm integrated into it. Using it as a research gap, the following procedures with supporting diagrams are discussed in this subsection. It is expected that the proposed architecture will offer a possible approach to this problem and promising outcome in the immediate future.

5.1.1. Security: Multi-Signature Stamp

The security aspect of technology revolves around the CIA rule. "C" stands for confidentiality, "I" stands for integrity, and "A" stands for availability (and authentication). Non-repudiation provides proof of a message as well as the established communication. Here, confidentiality signifies that the message should only be visible to the person intended. The data integrity is to maintain the originality of the data. Availability of machines, networks, and communication links is necessary while the exchange is happening. Authentication is verified identity of a sender and a receiver. In the case of non-repudiation, a party (sender or a receiver) cannot deny their participation in the communication. The data integrity of a Blockchain is remained intact with the help of hashing. The proposed model focuses on the authentication and non-repudiation part with the help of a multi-signature stamp.

The utilization of multi-signature stamps is to solve the data ownership and control issue. Medical information of every patient is placed within a block, generating a unique identification number (Patient ID). The hospital management system verifies the identity of the patient, generates private key-public key pair, and attaches the block to the hospital's database completing the

identification stage. Each patient may review their own profile with the ID after signing it digitally. They are not allowed to search any other profile. The consulted doctor signs the medication after diagnosis, digitally confirming the validity. All other doctors within the hospital verify the prescribed medication or diagnosis by the doctor. The notification is sent to the Patient ID after entire process is done. This multi-signature stamp removes the non-repudiation attack on the EHR. A multi-signature stamp requires private keys to sign a block and public keys to verify that signature. The patient can permit the doctor, the hospital authority, the pharmacy, or the laboratory to communicate. The patient takes full control over their data in case of sharing, storing, and viewing. Blocks are added to the chain after each update. Figure 7 demonstrates the multi-signature structure for data sharing within a Blockchain network.

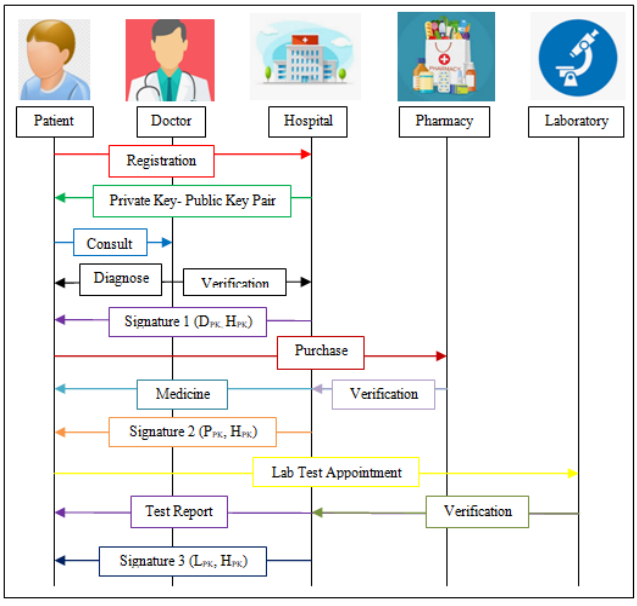

Fig. 7.: Multi-Signature Method.

The diagram shows that the method uses three different signatures for three different parties. Scalability is not an issue here because managing keys is very easy through user application programs. The patient initiates a query and gives access to the consulting party for a limited time. The consulting party goes through a verification process before reaching the patient again. This verification signifies that the result is true and useful for the patient. In the end, each party signs their activity with their private key, and this proves the authentication. Further, parties do not deny upon their communication as the signature is saved with a timestamp and is added to the Blockchain making it secure (tamper-proof) by hash links. The brief pictorial diagram of a patient's Blockchain after the first consultancy is shown in Figure 8. The D_{PK} Signifies the digital signature of the Doctor, similarly, H_{PK} is the digital signature of the hospital, P_{PK} is of the pharmacy, and L_{PK} is of the laboratory.

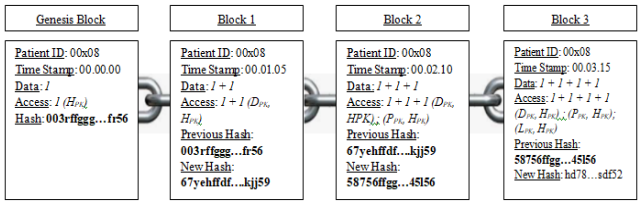

Fig. 8. The Patient's Blockchain.

The patient's Blockchain contains Patient ID, Timestamp of when it is updated, and EHR named as Data. The access permission is updated by the Access option in the block. Every time a person gets access, the access tab is updated. The patient gets alert and the EHR is updated in the frontend. The permission provided by the user is limited by time. It is to be noted that the Genesis Block which has only one hash is the registration block. The block after genesis block contains the previous block hash and generates a new hash making the blocks tamper-proof. Any change in between can be reflected in the hash. The authenticity and non-repudiation are thus maintained throughout the Blockchain. The security is established by this multi-signature methodology.

5.1.2. Data Management: Channel

The channel is linked directly to various parties, and they follow a common rule to preserve the Blockchain history. The connection inside the hospital is managed with one chain but a channel is used to handle connection to other hospitals. In this phase, local ledger, local peer, and global channel come into the picture. If a person in the hospital needs to access their own stored data, they can use the local Blockchain. Local Blockchain holds a particular hospital's medical history. When the same person tries to access data from another hospital, they must communicate via the channel. Only permitted people can access the channel for data management. Figure 9 explains how the hospitals manage EHRs within a given geographical region. This is a feasible solution for data management. The channel helps to maintain a decentralized connection between several hospitals and their databases. Making the consultancy more accurate and precise, the channel is bounded between trusted participants. The concept of channel basically makes the Blockchain private and customized. Hyperledger Fabric helps to maintain this kind of composition of a channel. The channel broadly holds all the ledgers, participants, and smart contracts which is permissioned making it secure.

The channel introduced here contains more than one hospital data and they are connected by a simple consensus of order-execute paradigm. The validation process is very private and limited to trusted participants. As it is a private chain, the identification of every participant is transparent

and connected to their real-world identity. The organizations (Hospitals) within a channel have the peers (participants like patients, doctors, pharmacy, hospital management), the smart contracts (codes to make the Blockchain secure and drive to the conclusion of validation within one Blockchain), and the ledger (contains Blockchain of every patient).

The smart contract used here has several points to describe. The new block is added to the chain after proper validation. For validation, the hash link is used.

$$\textit{Previous Block. Hash} + \textit{New Data} = \textit{New Hash. New Block} \quad (1)$$

If this validation gives success in return, then the timestamp is noted of the communication. The next part of the communication starts when the user provides access to a particular party. This time is given as (X) Time in the pseudo-code. After the diagnosis or action is taken by the parties, there is an alert and update option activated for the hospital and the user both. After that hospital and the patient validate their signatures, the entire block is added to the patient's Blockchain as well as to the channel. The data management is addressed in this method and that has been justified by the channel framework of a private Blockchain. This method can incorporate many hospitals and their databases. This framework might bring a futuristic outcome of EHR management soon.

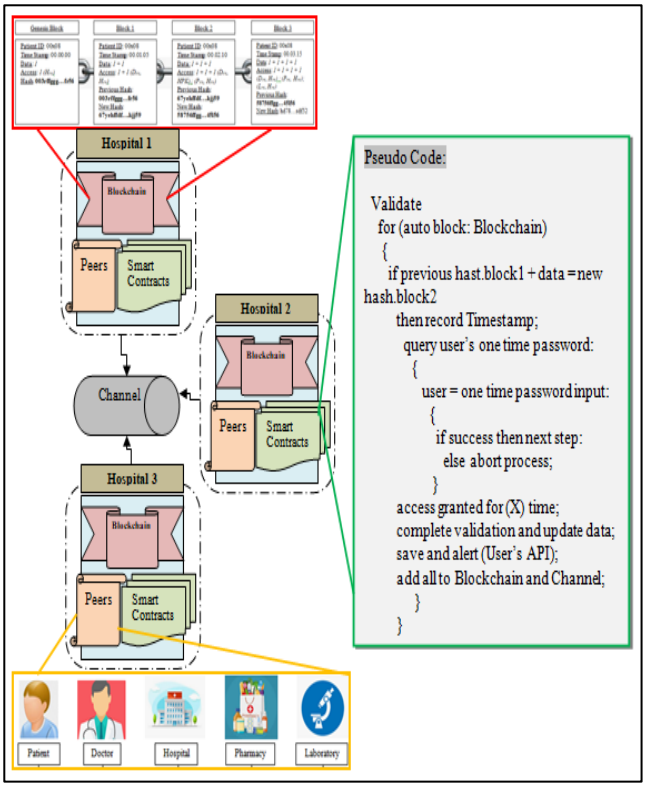

Fig. 9. EHR Management by Channel.

5.1.3. Proposed Algorithms

Algorithm 1: Registration Check

Input: P_{ID}, Pa_{Pk}
Output: Pa_{PK}, Pa_{PuK}, Block
API Registration:
    New Registration:
        Generate Pa_{PK}, Pa_{PuK}, Block;
        Return (Patient API)
    If Existing User:
        P_{ID}, Pa_{PK} matches with Pa_{PuK};
        Enter to the Blockchain
    Else
        Abort

Algorithm 1: Registration Check

In this algorithm new registration of a patient is done followed by patient ID (P_{ID}), and public-private key pair originated by the hospital. The patient can use the private key (Pa_{PK}) and P_{ID} to login and the hospital checks the validity (authentication) of the patient, using public key (Pa_{PuK}). A new patient block should be created in the Blockchain for further query and respond. It is very easy to verify that a patient is not allowed to login using any other credentials. This makes the identity of a patient secure.

Algorithm 2: Multi-Signature and Private Channel

Input: P_{ID}, U_{OTP}, X_{TIME}
Output: Channel, New Block
Validate Success:
    If Genesis Block:
        Genesis Hash + New Data = New Hash;
    Else If Existing Block:
        Previous Block Hash + New Data = New Block Hash;
    Record the Timestamp;
        Query User for U_{OTP}:
            Respond U_{OTP}:
                If Success:
                    Access granted for X_{TIME};
                    Add Signature for Further Verification;
                    Validate Data by Consensus;
                    Save and Update (Notification to User API);
                    Add to Blockchain and Channel;
                    Return Channel and Blockchain Update Number;
                Else:
                    Abort;
    Else:
        Abort;

Algorithm 2: Multi-Signature and Private Channel.

After successful registration the user can be validated, and the access information is provided to them. For any transaction, hash of the new block is generated from the previous block hash and new data. The time stamp is recorded. The doctor, lab, hospital, or medical shop might want to access the user's data, they request for one time passcode (U_{OTP}) and user ID (P_{ID}) for any kind of transaction. The access is given for a certain amount of time (X_{TIME}). After the changes are made the party digitally sign the data for avoiding non-repudiation. Here multiple signatures are added if multiple parties are granting access from the user. The update is validated by selected peers for assurance of correctness. Changes are made permanent, and notification is sent to the user's API. The new block is added to the Blockchain, and the channel is updated. User is given a pointer to their ledger for future use. This step assures a unique solution foe data management. Storage space is saved and yet update data is provided to user's API. If user declines to give access via $U_{OTP,}$ the process is terminated. It is necessary to generate new hash from genesis block by adding new data to it, as genesis block do not have any previous block (Figure: 8).

6. BLOCKCHAIN IN HEALTHCARE SECTOR: MAJOR CHALLENGES AND DISCUSSION

Each new technology has some benefits as well as some drawbacks. Finding out the weaknesses makes it more efficient and user-friendly. Even Blockchain have some issues [36]:

- Blockchain technology undoubtedly has standardization challenges in its practical applications as well as in healthcare.
- It is not easy to adopt and implement a system that is entirely different from conventional methods (cost-wise).
- Blockchain technology is still emerging and thus poses societal problems as well as the technological obstacles, such as cultural change, training to operate, etc.

With Figure 10, an overall wide image of potential data management and medical infrastructure can be portrayed. Blockchain-based EHR management applications involve several members such as patients, doctors, hospitals, laboratories, and pharmacies. There are off-chain as well as on-chain design that Blockchain provides [7]. A smart contract based on Blockchain technology may be built for all the requirements (like specific permissions to data access) depending upon the application [26]. There are several mechanisms in the distributed ledger such as decentralization, hashing, key generation for signature, and data storage (maybe in the cloud). There are layers in which network queries are accomplished such as user interface, Blockchain layer, processing layer and collection of data. Further, Table 4 includes a parallel contrast of the EHR management framework built on Blockchain and the non-Blockchain-based framework focused solely on conventional methods of data storage and connectivity [29].

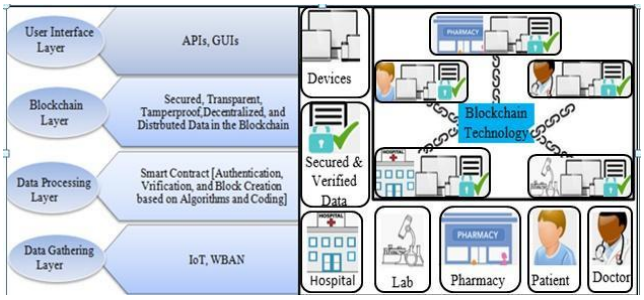

Fig. 10. Infrastructure of Blockchain and EHR Application Programming Interface.

Table 4. Comparison Between Blockchain-based and non-Blockchain-based Technologies

Features	Non-Blockchain based	Blockchain based
Availability	Data should be managed manually.	Algorithms are there to manage data like PBFT.
Confidentiality	Encryption methods are there.	Encryption methods are there.
Immutability	Not possible.	Possible.
Privacy	Encrypted data but can trace back to the user.	Anonymous to protect the identity.
Speed	Dependent upon network.	Dependent upon network as well as verification delay.
Transparency	Not possible as it makes the data vulnerable.	Transparency is there.

MedRec [11] and Dubovitskaya et al. [19] mentioned user-centric APIs for better control and administration. Whereas, with the help of a public key-private key pair, MeDShare [13], SMEAD [16], and Conceicao et al. [18] concentrated on authentication techniques. They suggested a private key public key pair to control the EHR, but the proposed technique suggests a multi-signature system. This scheme also helps in the case of key misplace through multiple checking. Peterson et al. [15] and Dubovitskaya et al. [19] discuss multiple-member community and different database storage. Extending the structure of this specific concept, the proposed model implies a channel for storing and managing multiple community records. Our proposed approach takes into consideration other approaches' limitations to propose a system that might give us a better result soon.

Shi et al. [37] reviews and compares several existing papers on Blockchain technology and EHR as the application in the healthcare domain. Authors introduce sufficient background knowledge needed for understanding the Blockchain technology and then they move to the crux of the application part. Along with the security and privacy aspects of the literature, authors try to incorporate the data storage and data sharing part of a Blockchain. The paper also summarizes the number of potential research works, opportunities, and challenges of some cutting-edge technologies applied with Blockchain in the healthcare sector like Big Data, Machine Learning, IoT (Internet of Things), and Edge computing. There ais no technical methodology proposed by the authors, but they have stated some QoS (Quality of Service) parameters to improve the performance of the existing Blockchain technology. The paper is concluded with the reflections of adopting new technologies and standards. Rashid et al. [38] have tried to manage EHRs stored in the public cloud environment. They used a very novel technique called enhanced role-based access control (ERBAC). The framework does not include Blockchain technology. In contrast, Banotra et al. [39] used Blockchain technology for secure asset management. Banotra et al. [40] used IoT devices with Blockchain technology to enhance data security in healthcare systems. The works mentioned above do not use multi-signature method for security, or private channel for data management. This makes the proposed solution unique among the related works mentioned the paper.

Table 5 describes a comparison between existing technologies and the proposed model. The comparison clearly states that no existing technologies are using the multi-signature stamp and channel method together. There are some existing technologies using Blockchain 3.0, Distributed Ledger Technology (DLT) but no usage the channel as an EHR management system. Shi et al. describe existing technologies but have not proposed any model. The unknown terms are neither marked as Y or as N. It can be concluded that the proposed model which uses a multi-signature stamp and channel to improve the security and management of EHRs does not conflict with other existing technologies.

Table 5. Comparison of proposed model with existing technology

Comparison (Yes/No) / Article and Reference	API	Digital Keys	Consensus	Ethereum	Hyperledger	IoT	Cloud Storage	Multi Signature	Channel
MedRec [11]	Y	Y	Y	Y	-	-	-	N	N
MedBlock [12]	Y	Y	Y	-	-	-	-	N	N
MeDShare [13]	Y	Y	Y	Y	-	-	Y	N	N
ModelChain [14]	-	-	Y	-	Y	-	-	N	N
Peterson et al. [15]	-	Y	Y	-	Y	-	-	N	N
SMEAD [16]	Y	Y	Y	Y	-	Y	Y	N	N
Salahuddin et al. [17]	-	-	Y	-	-	Y	Y	N	N
Conceicao et al. [18]	-	Y	Y	Y	-	-	-	N	N
Dubovitskaya et al. [19]	Y	-	Y	-	Y	-	Y	N	N
Shi et al. [37]	-	-	-	-	-	-	-	N	N
Proposed Model	Y	Y	Y	N	Y	N	N	Y	Y

7. CONCLUSION

This study suggests a scheme in which Blockchain tackles the medical data management solution by incorporating a private channel mechanism. The data security issue is addressed using the multi-signature stamp with the generated EHRs. The study provides an extensive overview of Blockchain possibilities and approaches to healthcare. Evaluating the applications available, we identified the significant design standards and requirements necessary for the healthcare sector. Blockchain has a diverse set of applications creating multiple possibilities in healthcare. Finally, this article examines the effect of Blockchain on healthcare security and suggests a strategy for tackling data ownership, authority, and common channel consensus. This scheme is therefore secure and productive compared with traditional schemes that can help us to change the existing healthcare situation. This is like taking a new step towards e-health applications. The proposed methodology finds performance measurement challenging due to the lack of feasible computational power in regular computers. The future direction of the proposed model is to build the code over the algorithm proposed that can run through many inputs. Moreover, there is an enormous number of

opportunities in the application part of the proposed model. It is necessary to move towards a technological solution that can induce easy access to patient data and reduce medical data fraud. A Blockchain-based healthcare revolution may be challenging now but it is achievable in future.

LIST OF ABBREVIATIONS

EHRs	: Electronic Healthcare Records
P2P	: Peer to Peer
WBAN	: Wireless Body Area Network
IoT	: Internet of Things
APIs	: Application Programming Interface
DNS	: Domain Name System
DPoS	: Delegated Proof of Stake
PBFT	: Practical Byzantine Fault Tolerance
PCOR	: Patient-Centered Outcomes Research
VPN	: Virtual Private Network
FPGA	: Field Programmable Gate Array
SHA	: Secure Hash Algorithm
PoW	: Proof of Work
PoS	: Proof of Stake
HIE	: Health Information Exchange
GUI	: Graphical User Interface
RU	: Registration Unit
PAU	: Private Accessible Unit
GPS	: Global Positioning System
RPM	: Remote Patient Monitoring
PSN	: Pervasive Social Network
PoC	: Proof of Concept
SCs	: Smart Contracts
DLT	: Distributed Ledger Technology
ERBAC	: Enhanced Role-Based Access Control

REFERENCES

[1] Jiang, S., Cao, J., Wu, H., Yang, Y., Ma, M. and He, J. 2018. Blochie: a blockchain-based platform for healthcare information exchange. In *IEEE international conference on smart computing (smartcomp)*, pp. 49-56. IEEE.

[2] Esposito, C., De Santis, A., Tortora, G., Chang, H. and Choo, K.K.R. 2018. Blockchain: A panacea for healthcare cloud-based data security and privacy?. In *IEEE Cloud Computing*, *5*(1), pp.31-37. IEEE.

[3] Wang, J., Han, K., Alexandridis, A., Chen, Z., Zilic, Z., Pang, Y., Jeon, G. and Piccialli, F. 2020. A blockchain-based eHealthcare system interoperating with WBANs. In *Future Generation computer systems*, *110*, pp.675-685.

[4] Uddin, M.A., Stranieri, A., Gondal, I. and Balasubramanian, V. 2019. A decentralized patient agent controlled blockchain for remote patient monitoring. In *International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, pp. 1-8. IEEE.

[5] Rathee, G., Sharma, A., Saini, H., Kumar, R. and Iqbal, R. 2020. A hybrid framework for multimedia data processing in IoT-healthcare using blockchain technology. In *Multimedia Tools and Applications*, *79*(15), pp. 9711-9733.

[6] Jahankhani, H. and Kendzierskyj, S. 2019. Digital transformation of healthcare. In *Blockchain and Clinical Trial*, pp. 31-52. Springer, Cham.

[7] Onik, M.M.H., Aich, S., Yang, J., Kim, C.S. and Kim, H.C. 2019. Privacy protection and management of medical records using blockchain technology. In *Big Data Analytics for Intelligent Healthcare Management*.

[8] Abouelmehdi, K., Beni-Hssane, A., Khaloufi, H. and Saadi, M. 2017. Big data security and privacy in healthcare: a review. In *Procedia Computer Science*, *113*, pp.73-80.

[9] Chakraborty, S., Aich, S. and Kim, H.C. 2019. A secure healthcare system design framework using blockchain technology. In *21st International Conference on Advanced Communication Technology (ICACT)*, pp. 260-264. IEEE.

[10] Pirtle, C. and Ehrenfeld, J. 2018. Blockchain for healthcare: The next generation of medical records?.

[11] Ekblaw, A., Azaria, A., Halamka, J.D. and Lippman, A. 2016, August. A Case Study for Blockchain in Healthcare: "MedRec" prototype for electronic health records and medical research data. In *Proceedings of IEEE open & big data conference* (Vol. 13), pp. 13. IEEE.

[12] Fan, K., Wang, S., Ren, Y., Li, H. and Yang, Y. 2018. Medblock: Efficient and secure medical data sharing via blockchain. In *Journal of medical systems*, *42*(8), pp.1-11.

[13] Xia, Q.I., Sifah, E.B., Asamoah, K.O., Gao, J., Du, X. and Guizani, M. 2017. MeDShare: Trust-less medical data sharing among cloud service providers via blockchain. In *IEEE Access*, *5*, pp.14757-14767. IEEE.

[14] Kuo, T.T. and Ohno-Machado, L. 2018. Modelchain: Decentralized privacy-preserving healthcare predictive modeling framework on private blockchain networks. In *arXiv preprint arXiv:1802.01746*.

[15] Peterson, K., Deeduvanu, R., Kanjamala, P. and Boles, K. 2016. A Blockchain–Based Approach to Health Information Exchange Networks. In *Mayo Clinic, NIST Workshop Blockchain Healthcare*, (Vol. 1), pp. 1–10.

[16] Saravanan, M., Shubha, R., Marks, A.M. and Iyer, V. 2017. SMEAD: A secured mobile enabled assisting device for diabetics monitoring. In *IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, pp. 1-6. IEEE.

[17] Salahuddin, M.A., Al-Fuqaha, A., Guizani, M., Shuaib, K. and Sallabi, F. 2018. Softwarization of internet of things infrastructure for secure and smart healthcare. In *arXiv preprint arXiv:1805.11011*.

[18] da Conceição, A.F., da Silva, F.S.C., Rocha, V., Locoro, A. and Barguil, J.M. 2018. Eletronic health records using blockchain technology. In *arXiv preprint arXiv:1804.10078*.

[19] Dubovitskaya, A., Xu, Z., Ryu, S., Schumacher, M. and Wang, F. 2017. Secure and trustable electronic medical records sharing using blockchain. In *AMIA annual symposium proceedings* (Vol. 2017), pp. 650. American Medical Informatics Association.

[20] Zubaydi, H.D., Chong, Y.W., Ko, K., Hanshi, S.M. and Karuppayah, S. 2019. A review on the role of blockchain technology in the healthcare domain. In *Electronics*, *8*(6), pp.679.

[21] Tanwar, S., Parekh, K. and Evans, R. 2020. Blockchain-based electronic healthcare record system for healthcare 4.0 applications. In *Journal of Information Security and Applications*, *50*, pp.102407.

[22] Zhuang, Y., Sheets, L., Shae, Z., Tsai, J.J. and Shyu, C.R. 2018. Applying blockchain technology for health information exchange and persistent monitoring for clinical trials. In *AMIA Annual Symposium Proceedings* (Vol. 2018), pp. 1167. American Medical Informatics Association.

[23] Kaw, J.A., Loan, N.A., Parah, S.A., Muhammad, K., Sheikh, J.A. and Bhat, G.M. 2019. A reversible and secure patient information hiding system for IoT driven e-health. In *International Journal of Information Management*, *45*, pp.262-275.

[24] Castaneda, C., Nalley, K., Mannion, C., Bhattacharyya, P., Blake, P., Pecora, A., Goy, A. and Suh, K.S. 2015. Clinical decision support systems for improving diagnostic accuracy and achieving precision medicine. In *Journal of clinical bioinformatics*, *5*(1), pp.1-16.

[25] Dimitrov, D.V. 2019. Blockchain applications for healthcare data management. In *Healthcare informatics research*, *25*(1), pp.51-56.

[26] Khatoon, A. 2020. A blockchain-based smart contract system for healthcare management. In *Electronics*, *9*(1), pp.94.

[27] Roehrs, A. 2019. OmniPHR: a Blockchain based interoperable architecture for personal health records.

[28] Al Omar, A., Rahman, M.S., Basu, A. and Kiyomoto, S. 2017. Medibchain: A blockchain based privacy preserving platform for healthcare data. In *International conference on security, privacy and anonymity in computation, communication and storage*, pp. 534-543. Springer, Cham.

[29] Pham, H.L., Tran, T.H. and Nakashima, Y. 2018. A secure remote healthcare system for hospital using blockchain smart contract. In *IEEE Globecom Workshops (GC Wkshps)*, pp. 1-6. IEEE.

[30] Zhang, J., Xue, N. and Huang, X. 2016. A secure system for pervasive social network-based healthcare. In *IEEE Access*, *4*, pp.9239-9250.

[31] Benchoufi, M., Porcher, R. and Ravaud, P. 2017. Blockchain protocols in clinical trials: Transparency and traceability of consent. In *F1000Research*, *6*.

[32] Samaniego, M. and Deters, R. 2016. Hosting virtual IoT resources on edge-hosts with blockchain. In *IEEE International conference on computer and information technology (CIT)*, pp. 116-119. IEEE.

[33] Bocek, T., Rodrigues, B.B., Strasser, T. and Stiller, B. 2017. Blockchains everywhere-a use-case of blockchains in the pharma supply-chain. In *IFIP/IEEE symposium on integrated network and service management (IM)*, pp. 772-777. IEEE.

[34] Zhou, L., Wang, L. and Sun, Y. 2018. MIStore: a blockchain-based medical insurance storage system. In *Journal of medical systems*, *42*(8), pp.1-17.

[35] Mytis-Gkometh, P., Drosatos, G., Efraimidis, P.S. and Kaldoudi, E. 2017. Notarization of knowledge retrieval from biomedical repositories using blockchain technology. In *International Conference on Biomedical and Health Informatics*, pp. 69-73. Springer, Singapore.

[36] Siyal, A.A., Junejo, A.Z., Zawish, M., Ahmed, K., Khalil, A. and Soursou, G. 2019. Applications of blockchain technology in medicine and healthcare: Challenges and future perspectives. In *Cryptography*, *3*(1), pp.3.

[37] Shi, S., He, D., Li, L., Kumar, N., Khan, M.K. and Choo, K.K.R. 2020. Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey. In *Computers & Security*, pp.101966.

[38] Rashid, M., Parah, S.A., Wani, A.R. and Gupta, S.K. 2020. Securing E-Health IoT data on cloud systems using novel extended role based access control model. In *Internet of Things (IoT)*, pp. 473-489). Springer, Cham.

[39] Banotra, A., Gupta, S., Gupta, S.K. and Rashid, M. 2021. Asset Security in Data of Internet of Things Using Blockchain Technology. In *Multimedia Security*, pp. 269-281. Springer, Singapore.

[40] Banotra, A., Sharma, J.S., Gupta, S., Gupta, S.K. and Rashid, M. 2021. Use of blockchain and internet of things for securing data in healthcare systems. In *Multimedia Security*, pp. 255-267. Springer, Singapore.