Article

Secure Data Transmission of Electronic Health Records Using Blockchain Technology

Rahul Ganpatrao Sonkamble [1,2] , Anupkumar M. Bongale [3,*] , Shraddha Phansalkar [1], Abhishek Sharma [4] and Shailendra Rajput [5,*]

1   Computer Engineering, MIT Art, Design and Technology University, Pune 412201, Maharashtra, India
2   Department of Computer Science and Information Technology, Symbiosis Institute of Technology, Symbiosis International (Deemed University), Lavale, Pune 412115, Maharashtra, India
3   Department of Artificial Intelligence and Machine Learning, Symbiosis Institute of Technology, Symbiosis International (Deemed University), Lavale, Pune 412115, Maharashtra, India
4   Department of Computer Science and Engineering, Graphic Era Deemed to be University, Dehradun 248002, Uttarakhand, India
5   Department of Electrical and Electronic Engineering, Ariel University, Ariel 40700, Israel
*   Correspondence: anupkumar.bongale@sitpune.edu.in (A.M.B.); shailendrara@ariel.ac.il (S.R.)

Abstract: Electronic Health Records (EHR) serve as a solid documentation of health transactions and as a vital resource of information for healthcare stakeholders. EHR integrity and security issues, however, continue to be intractable. Blockchain-based EHR architectures, however, address the issues of integrity very effectively. In this work, we suggest a decentralized patient-centered healthcare data management (PCHDM) with a blockchain-based EHR framework to address issues of confidentiality, access control, and privacy of record. This patient-centric architecture keeps the patient at the center of control for secured storage of EHR data. It is effective in the storage environment with the interplanetary file system (IPFS) and blockchain technology. In order to control unauthorized users, the proposed secure password authentication-based key exchange (SPAKE) implements smart contract-based access control to EHR transactions and access policies. The experimental setup comprises four hyperledger fabric nodes with level DB database and IPFS off-chain storage. The framework was evaluated using the public hepatitis dataset, with parameters such as block creation time, transactional computational overhead with encryption key size, and uploading/downloading time with EHR size. The framework enables patient-centric access control of the EHR with the SPAKE encryption algorithm.

Keywords: electronic health records; patient-centric healthcare data management; interplanetary file systems; blockchain; secure password authentication-based key exchange; transaction

1. Introduction

Healthcare and associated health data are critical in daily life. Traditionally, health information was stored in databases, which were prone to alteration and theft [1]. In consequence, healthcare data needed to be stored electronically to eliminate the obstacles to data exchange and data representation among healthcare providers. A large number of electronic health records (EHR) are being created as healthcare digitization progresses. Such rapid EHR adoption necessitates unrivaled data security in the healthcare industry (HI) [1]. Furthermore, because of COVID-19 restrictions on remote working, the consequences of these breaches are far-reaching, including incidents where confidential patient data are traded online for turnover. Furthermore, patients are endangered by threats to publicly divulge their data [2].

The use of the personal data of the patient for a variety of secondary purposes without their agreement would greatly compromise patient privacy. Aside from data security, patients should be permitted to profit financially from sharing health information [3].

Hence, a system for secured storage of EHR and an authorized retrieval mechanism with patient-controlled and incentivized schemes is a solution to these problems.

It has been found that a blockchain-based digital EHR system not only offers secured storage for patient records, but its smart contract-based framework also offers a secured interchange of the records among authenticated identified users. The audit trail on the usage track of transactions on blockchain also offers opportunities for incentivizing data sharing for patients [4,5]. Although blockchain systems offer immutable storage of records, they also offer expensive solutions. Hence, a blockchain-based system is augmented with off-chain storage systems such as the interplanetary file system (IPFS) [6] for the actual storage of records. This offers cost-efficient solutions to the EHR storage needs, but additionally incurs the burden of the mechanism of mapping the off-chain data records to on-chain transactions [7].

The objectives of the presented work are:

(a) Design of a blockchain-based framework with on-chain transactions and off-chain storage.
(b) Design of the SPAKE protocol for password-safe smart contract-based access control to implement patient-centric EHR control.
(c) Implementation of a framework with hyperledger fabric-based on-chain transactions and IPFS-based off-chain EHR storage.
(d) Evaluation of the framework with respect to block creation time, upload and download time, and transaction computational time.

2. Related Work

A chain of informative blocks is called a blockchain. It is a time-stamped and immutable series of records. Blockchain technology is a record-keeping system that holds blocks of data [8,9]. Record keeping system in the blockchain is referred to as a digital ledger. The data in the block are secure and tamper-proof [10–12]. The information in the blockchain is transparent since it may be seen by other members of the network. The blockchain is categorized into public and private blockchains. A permissioned blockchain is denoted as a private blockchain that only registered participants can access, while a public blockchain is a permissionless blockchain that everyone may use. The public blockchain, which has no permissions, fails to protect the integrity of health data and privacy [13,14]. Privacy guidelines such as HIPAA or GDPR will have a significant impact [15] on healthcare frameworks. The details of diseases, treatment histories, prescriptions, personal data of a patient, drug details, electrocardiogram (ECG), scan reports, and microbiological test reports are all necessary to be managed with care in the healthcare systems, as well as should be preserved securely. Despite the preliminary research, two key questions remain unanswered [16]. The first step is to comprehend fast healthcare interoperability resources (FHIR) blockchain on-chain information, which denotes the structure of transactions on FHIR data that will be held within the blockchain. In blocks, on-chain data are theoretically traceable, non-changeable, and transparent because it is part of blockchain networks. Only a few earlier studies briefly state that hashes, FHIR profiles, transaction metadata, and signatures are employed as on-chain data [17].

To address this issue, a blockchain security framework is being developed for securely and efficiently transmitting and storing EHR [18]. Furthermore, the technology keeps audited evidence of all transactions in an immutable distributed ledger (DL), ensuring accountability and transparency in data flow. As a result, patients can save health data and discover them from doctors in their own EHRs, reducing health errors and preserving their privacy [7]. For all the contributors, a number of events can provide speedy authentication and costly data processing. Blockchain has a lot of potential in the HI, such as: (i) protected information is shared and saved with different people [19]; (ii) data interoperability across national borders [20]; (iii) improved access to the information of the patient [21]; (iv) increased traceability and transparency [22]; (v) ensured data privacy and security; and (vi) verified accuracy of billing management [19]. However, there is a lack of scalability in these

decentralized EHR management systems and they provide less protection for critical health information. Therefore, the proposed method puts forth a system that improves on existing blockchain-based EHR solutions in terms of scalability, privacy, and cost.

Medical professionals and healthcare organizations are looking into different processes and techniques for the effective integration of health data into their systems. However, personal and sensitive information of patients is contained in the EHR. Therefore, data-protection, while meeting the need for health data, are an essential issue in this information age. Lee et al. [23] proposed an EHR sharing system based on blockchain to manage and share their EHRs across numerous hospitals. During data sharing and information exchanges, technology secures the patient's data from security threats, including simulated and privacy assaults. It also offers scalability by allowing the users to instantly share an EHR, regardless of its type or size. Due to the time limits, they are unable to review health histories as well as a broad range of prescriptions and past reports. Hence, Vinay Chamola et al. [24] developed an artificial intelligence (AI)-assisted blockchain-based architecture in which health records are saved and processed using multiple AI schemes, such as the recognition of optical characters, to create a report for a single patient. For the ease of use and reading, the report displays only the most significant information and is safely saved on a network called a decentralized blockchain for further use.

The blockchain concept was utilized by Megha Jain et al. [25]. The authors examined the architecture of blockchain-based systems for adaptability, safety, and other important system components that must be secured against manipulation and misuse. To avoid changes in EHR, Junaid et al. [12] have proposed a model with cloud and fog integrated with blockchain. Healthcare devices are widely used in the health sector. However, privacy and security are major concerns to the sensitive health data of a patient. To address these challenges, Verma et al. [26] developed a hybrid system with a combination of decentralized and centralized blockchains for sharing secured health data among hospitals and health devices. To increase the security of health data and access control (AC), an ethereum-based blockchain was utilized to create a healthy environment. The deployment cost of the proposed model could be a stumbling block. Due to a new wave of verifiable credentials and decentralized identifiers data modeled by blockchain, decentralized entity authentication is now possible. Manoj et al. [27] introduced a blockchain-based architecture for consent management and patient identification for EHR access, utilizing proven authorizations leveraging decentralized identifiers. The findings of this work can be used to implement decentralized identity authentication and management in EHR structures. Zhe Peng et al. [28] proposed a secured privacy-preserving approach using blockchain for sectors such as EHR, financial records, social records, and geospatial records. The authors have used solidity smart contracts for implementation. They have evaluated their performance using parameters such as gas consumption, proof generation time, verification time, etc.

A privacy-preserving smart city-based healthcare business model is proposed in [29]. The proposed model comprises the internet of medical things (IoMT) with fog, clouds, and blockchain. EHR accessibility and privacy preservation are achieved by smart contracts. A blockchain-based privacy-preserving method is suggested by Boumezbeur et al. [30,31], and a secure EHR-sharing architecture and AC are implemented. The proposed system aims to adopt an EHR blockchain scheme and ensure proper preservation of the certified electronic records by defining user access permissions. This work uses ethereum blockchain platform which replicates the cryptographic primitives and utilize smooth deals to represent the connections between the user and the owner of EHR. Accordingly, the experimental and security analysis demonstrates that it is safe to use in real-time applications. However, it involves a single entity that cannot successfully safeguard files from unwanted attacks or access. Thus, the central management of electronic health systems is a huge difficulty. In central electronic health schemes, some services such as verification and file search are difficult to deliver due to this problem. Therefore, Alrebdi et al. [32] presented a system that comprises a framework with decentralized user requests to interact with the structure. The system stores patient data and related files using cloud storage and IPFS. The experiment

evaluation and security assessment of the system show that precise verification and search activities are conducted rapidly and securely across the network.

Mondal et al. [33] suggested a blockchain multi-signature stamp based on the private channel infrastructure to create an EHR administration structure. Data authority and ownership are addressed through multi-signature stamps. This method aids in the proper procedure development for reviewing the database of the user, which ensures that all participants follow a set of rules to keep the blockchain ledger safe. Le et al. [34] proposed an EHR-based blockchain model in which data sharing strategy is controlled. The address of the EHR file was created by preserving and encrypting the IPFS-based EHR file system (IEFS) in EHR abstracts for privacy and security. As EHR synopses are encrypted with their public keys, the patients have control over EHR file sharing. Cerchione et al. [35] proposed a distributed EHR ecosystem which incorporates electronic health information into a permissioned and private blockchain. In this case, a blockchain-based EHR structure building and evaluation is enabled by information processing theory. It improves data interchange and health record storage across healthcare suppliers while diminishing environmental hesitation.

The rest of the work is laid out as follows. The proposed research methodology is presented in Section 3. Section 4 illustrates the experimentation. Section 5 contains details about the results and discussion, and the conclusion of the research is presented in Section 6.

3. Materials and Methods

The speedy change in healthcare is due to enhanced patient care services. EHRs are digitally stored records of health-related information. Health data may be easily shared across various healthcare providers due to the EHR. EHR improves healthcare by providing accurate and precise health records in situations. However, system security and privacy preservation are difficult to maintain.

Blockchain has recently established itself as a practical technology that has spread to numerous industries. Because of the requirement for patient-centric systems and the need to integrate various systems, blockchain has a lot of potential in the HI. Blockchain holds great promise for the security and privacy protection of the HI. As a result, the research work provided perspectives on blockchain-based healthcare data management, mainly the exchange of EHR data between research studies and healthcare providers. The system architecture of the suggested work is portrayed in Figure 1.
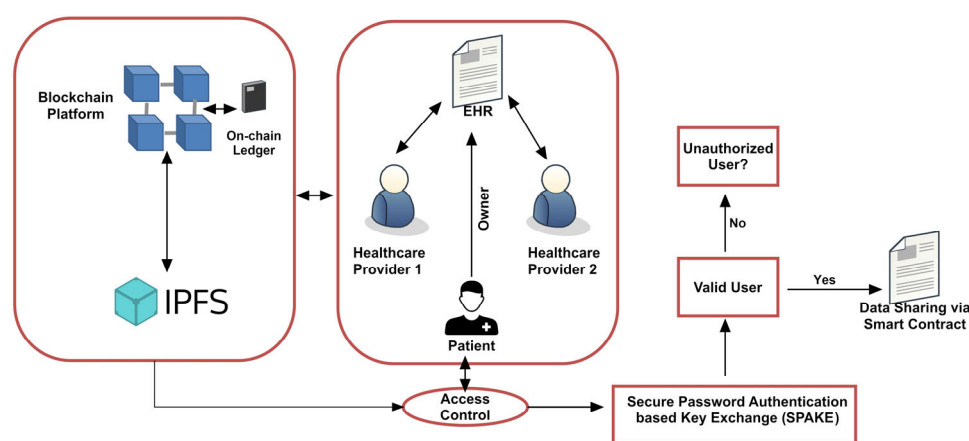

Figure 1. System architecture.

The owner of the data is the patient, and they should have ownership over their health information. They should be able to share it, if needed. Authorization of the patient could be done with a secure password authentication-based key exchange (SPAKE) access control mechanism using smart contracts. If the patient is authorized, then they can give EHR access to healthcare providers. With the patient's permission, healthcare providers may

share EHR. EHR hashes and primary attributes will be stored on the blockchain, and actual records in the form of any type of document will be stored on IPFS. Consequently, the research is intended to establish a patient-centric EHR system. The most difficult issue here is ensuring the access control and privacy of the data that is accessed and shared.

The proposed solution protects patient privacy in EHRs through a health information sharing procedure that includes access restriction and data encryption. Moreover, the study looks deeper for privacy, data security, and access control requirements for blockchain-enabled security, using real test case scenarios to do so.

3.1. EHR Data Storage

The overall objective is to create an architectural model for storing a portion of an EHR on the blockchain. There are certain specific intentions for this, such as leveraging the health level seven (HL7) [36] FHIR data standard for blockchain-based data stores. It enables you to keep track of the information about a patient on an EHR that follows the HL7 FHIR standard. Consequently, HL7 provides a thorough examination of the proper handling of EHRs. Patient-centered healthcare data management (PCHDM) is suggested as a solution to the problem in this study. It is built with IPFS, a permissioned decentralized storage system based on hyperledger fabric that stores health information with the owner's permission [37]. A unique cryptographic public-key encryption technique is utilized to encrypt the IPFS data to establish an EHR blockchain system. In the health chain architecture model, Byzantine fault tolerance [38] is utilized to select and identify the blocks for inclusion in the blockchain.

3.1.1. Blockchain-Based System Model

A unique application model called blockchain incorporates encryption algorithms, decentralized data storage, consensus mechanisms, peer-to-peer transmission, and other technologies for the health data search process and to record the storage, leveraging the blockchain. The blockchain-based data storage cannot be randomly changed due to the immutability of the blockchain. It can be used as evidence for verifying the fluidity and originality of the data. In this system, four types of entities are presented. They are data users, Blockchain, EHR, and IPFS [39]. The IPFS will be used to store the data produced by the medical system while ensuring its privacy, verifiability, and searchability.

An ordered list of records is linked together through a chain of blocks. It is based on the blockchain, which is a distributed database. Some transaction information is held in the individual entities and the blocks are described as sets. An increasing list of records is maintained by the blockchain, which is immutable and distributed. The secure distribution of the assets is achieved among the untrusted clients by the numerous systems built on blockchain technology.

Based on this work, the individual blocks are formed in the blockchain network, which is formed by chaining together events from the genesis (first block) to the broadcasted current block [40]. The blocks, which contain information of an entire event, are broadcasted into the network. From the moment the user initiates a request to the moment he receives the data, a chain is formed that cannot be updated, changed, or removed. When a malicious threat is detected in the system or when a user violates the group's data handling policies, it performs data forensics and improves data traceability in events. Until the block is published into the blockchain, a single event is composed in a block, and from the moment a request is generated, the event lasts. When an authorized entity wants to look into systemic irregularities, a request is made and permission is given to look into the irregularities. The responsibility of the consensus node is to investigate and report on the outcomes of such abnormalities. This is simply because the blocks are associated with the appealing aspect of blockchain immutability.

3.1.2. Hyperledger Fabric Blockchain

Hyperledger fabric [37] is being used in various real time applications [41–43]. In the proposed system, users must register themselves to use the permission-based hyperledger blockchain network. The access control mechanism and modeling of hyperledger are used to manage permissions on the network. Hyperledger fabric, a distributed ledger solution platform, provides high levels of confidentiality, robustness, scalability, and adaptability. It is supported by a modular architecture. Medical information is frequently extremely both socially and legally sensitive. As a result, a closed blockchain for such an application is required, which aids in maintaining the required privacy. Since hyperledger fabric supports several layers of authorization, the data owners can decide which portions of their data are accessed, making it a better choice for controlling access to health records. The smart contract negotiations follow the rules of smart contract (SC) stores. The PCHDMAC-SC is the name of the framework created for the chain code of the role-based access control (RBAC) mechanism.

Based on pre-specified parties, a permissioned blockchain employs the hyperledger fabric to share health information reliably and effectively without relying on a single source of authority. The benefit of using a byzantine fault tolerance consensus protocol is offered by hyperledger fabric, which may be used to reach consensus without requiring mining or a separate currency. The IPFS objects are used for replication by a graph tree structure known as merkle directed acyclic, which serves as the state database for the hyperledger blockchain. An off-chain and an on-chain blockchain are modeled for the storage of health records and utilize IPFS [44]. A clear, fine-grained access control system is developed that utilizes a hyperledger blockchain and the PCHDMAC-SC protocol to avoid hacking without patient consent.

3.1.3. Background of the PCHDM System

The suggested system architecture uses three peer nodes to create web apps for a single organization, using a hyperledger composer user permissioned blockchain based on hyperledger fabric. The organization uses three peer nodes, one of which serves as a validating peer node, and the other two serve as an ordering node for registering stakeholders. Multiple peers can access the same database in this system, which is realized by IPFS for distributed data storage, a data certificate authority, smart contracts, a membership service provider, and a solo order node for blockchain connectivity. Multiple peers can be merged at various places on diverse machines to test the scalability of the system. Ledger access is available to smart contracts through this structure. Peer nodes are linked to the application, which then uses smart contracts to update the ledger. Peernode0 (PE0), Peernode1 (PE1), and Peernode2 (PE2) are the three peer nodes in the system, and they each have copies of the smart contracts and ledger.

A single channel (CH) in hyperledger composer makes peer communication easy. This network creates a transaction T and sends it to peer nodes 0, 1, and 2 for our application. The peers install the chain codes based on the execution of a transaction. To communicate with peers, the application employs chain codes when requesting or changing the ledger. The framework of the Health Record (HR) chain network enables the blocks in the blockchain to display hash values as changes in the histories that were made to the framework.

A block in a ledger record that pertains to a patient's health record is mostly made up of the workload for that transaction $WL_{tr(n)}$, the current transaction $WL_{h(n)}$, and the hash of previous transactions, $WL_{ph(n)}$. Utilizing $WL_{Tot(n)}$, the workload of the block may be determined.

$$WL_{Tot(n)} = WL_{tr(n)} + WL_{ph(n)} + WL_{h(n)} \tag{1}$$

The diseases diagnosed, doctor suggestion, address, location, hospital ID, profile of patient, next review notes, name of doctor, medicine, and scan and test image reports are presented in the HR.

The PCHDM takes the following stakeholders into account:

(i)   Owner of record

HR belongs to the patients. A PCHDMAC-SC agreement must be signed by a patient and stored on the hyperledger blockchain. Patients can choose access permissions to view their health reports through health record chain networks. This is defined by each PCHDMAC-SC in its specific context.

(ii)   Data uploader

For data uploaders, the health information of the patient may be uploaded. The high responsibilities of data uploader include adding encrypted clinical data of the affected person to the IPFS community. The initial transaction is validated on the blockchain.

(iii)   Data users

Parties who are interested in receiving health or clinical data about patients, including hospitals, physicians, insurance companies, and researchers, are referred to as "data customers" in this data user. According to the role, the access control model is provided to the patient to grant access rights to the data users in PCHDMAC-SC.

3.2. Data Encryption

Cryptographic methods such as public key cryptography [45], paring-based cryptography [46], and secure cryptographic techniques (proxy re-encryption) [47] guarantee the integrity and confidentiality of the blockchain data. The doctors and patients can have mutual interaction while accessing their HRs. The doctors bring up the IPFS HRs. Then, they appeal to access the records. It builds a request-based patient-centric view of the records instead of disclosing all of the data of the patient. The session key S_k, is encrypted and stored, facilitating the patient-centric view in IPFS. It is required to retrieve records in a certain session. The encryption session key S_k and the encrypted patient-centric views are received by doctors and patients. The patient-centric perspectives and S_k is decrypted by the doctors for the updating of the HR of a patient.

The patient is informed following the IPFS record update. The patient-centric view and the S_k will be automatically erased when a HR is committed by the patient. The access to HRs is prohibited to the stakeholders until consent of the patient is given. This framework protects the privacy of the patient. The hash value of the data is then safely stored in the hyperledger blockchain by utilizing the smart chain code that runs on the back end of the system. As a result, the ledger will inform the patient after the successful addition or updating of the records.

3.3. Interplanetary File System (IPFS)

IPFS is a decentralized storage protocol [48]. It assigns each one a distinct hash value, based on the file content, and it can share and permanently store a variety of file types by using the hash value. This makes it easy for users to find the files. Additionally, the data are efficiently prevented from being stored twice, and it conserves storage space by using the deduplication technique of IPFS. In this paper, an IPFS is used to store our EHR. The use of content-based addressing makes HRs possible. It is the main advantage of IPFS for accessing it rather than relying on location-based addressing. IPFS allows for the distribution of a huge amount of data without duplication, which can reduce storage requirements and bandwidth costs. It also improves record download rates. IPFS is an immutable storage mechanism and the hash value of an IPFS file cannot be altered.

3.4. PCHDMAC-SC

The doctor requests permission from the patient to access the IPFS HR of the patient. The RBAC permissions either deny or grant requests to authorized users. After obtaining the patient's permission, the doctor can create, write, and read the patient's records. The patient can commit his record after the write operation in order to have permanent storage. The HRs with a patient-centric view can be accessed by the other stakeholders such as pharmacists, insurance agents, and researchers in this health chain framework for a specific

session if their object ID as well as the ownership ID match the patient. The patient's HR may be updated by the laboratory technician with the patient's and the doctor's consent. The hyperledger fabric blockchain controls the access control, policies, and privacy agreement provided by the certificate authority. There are certain conditions that are followed by this approach, as follows:

(1) The specific identity of each stakeholder to whom access is granted must be stated by the policy of access control.
(2) The authorized value is assigned by the system to resources, action types, stakeholders, and environmental attributes after allowing the patients to access their records.

There are three layers of privacy in this system:

Level 1: Only the patients can see their HR.
Level 2: Authorized stakeholders have access to the HR.
Level 3: An authorized patient caretaker can access HR in an emergency.

The patients can manage their data privacy by adjusting their privacy level. The authorizations are transferred before their submission to the HR chain network or to other authorized users. The tiers in this model are configured to change conditions or are flexible.

3.5. PCHDM Algorithm

The patient (P), the doctor (D), the pharmacist (P), and the lab technician (LT) are the four stakeholders used in this work, where, $n = 1, 2, \ldots . N$, which represents the number of patients, doctors, pharmacists, health records, and lab technicians. Among the n stakeholders, hyperledger certificate authority issues public key certificates, which include doctors, pharmacists, lab technicians, and patients and for each stakeholder, a pair of the key is created. The patient's and the doctor's private keys and public are $Paprk_n$, $Papk_n$, $Dprk_n$, and Dpk_n, respectively. Based on PCHDMAC-SC, the authorized doctor D_n, the patient Pa_n, and HR access (HR_n) is presented in algorithm 1 [44]. As a result, the system creates a health record HR_n with a patient-centric view Pa_{cvn}. Instead of sharing complete patient health information, the doctor D_n requested that the attribute-based data be recovered from the Pa_{cvn}. The users can access and modify the necessary record data, which offers a patient-centric perspective Pa_{cvn} of a patient's particular health.

Otherwise, HR is a patient-centric view subset. Additionally, during a certain session, the system produces a session key S_k that is shared by the patient and the doctor. The public keys of doctors and patients are used and an encrypted session key, such as encrypted $(Papk_n (S_k))$ or encrypted $(Dpk_n (S_k))$, is constructed for the patient and the doctor. Doctors can obtain the session key S_k, which is encrypted with Pa_{cvn}. Algorithm 1 uses the create update () function of Algorithm 2 to update the health record HR_n.

PCHDM Algorithm 2 of HR form a patient-centric view after the patient-centric view session key and doctor session key have been decrypted. Then, the updates are uploaded into the updated patient-centric view UPa_{cvn}. The encrypted private keys are decrypted by employing the patient's password and adding the encrypted UPa_{cvn}, the patient private key that is obtained, which is used to update the patient system. Once it is updated the encrypted health record HR_n is decrypted. The patient then saves the changes to the IPFS and commits them to the health record (HR_n). The health record HR_n is instantly committed by the patient and the session key and Pa_{cvn} become invalid. A health record hash value $HR_{n\_}$ hash is generated by IPFS and saved in hyperledger blockchain blocks.

Algorithm 1 System Function (Creating and Updating Health Records in Hyperledger Blockchain), PCHDM Algorithm for Health Record Creation and Updating

---

Input: A Doctor D_n, with their Dpk_n, and $Dprk_n$, **with session key S_k,** of Health Record HR_n, A Patient Pa_n, with their $Papk_n$, **and** $Paprk_n$, with session key S_k, of Health Record HR_n,
Output: Boolean (Success or Failure)
    The procedure of storing and updating health records
    Each user u having access permission to Health Record
    Check PCHDMAC-SC
    If (permission =="GRANT" && role == "DOCTOR") then
    Create patient-centric view Pa_{cvn} of HR_n in IPFS
    $Pa_{cvn} \rightarrow$ Decryption (Encryption (HR_n))
    Create S_k
    send Encrypted ($Papk_n$, (S_k), Dpk_n,(S_k), Pa_{cvn}(S_k)) to Pa_n, D_n, and Pa_{cvn}
    Create Update ()
    $HR_n \rightarrow$ [(Decryption $Paprk_n$, (Encrypted $Papk_n$, (HR_n))+ Encryption (UPa_{cvn})]
    $Pa_n \rightarrow$ Commit (IPFS (HR_n))
    IPFS $\rightarrow HR_n$_hash
    HR_n_hash $\rightarrow$ Hyperleger Fabric Blocks
    Return True
Else
    Permission = Deny
    Return False
Endif
End For ()
End procedure

Algorithm 2 Create Update 0Create and Update the Patient centric view of the Health Record, PCHDM Algorithm for Patient-centric view of the HR

    Input: A Doctor D_n, with their Dpk_n, with session key S_k,
    Output: Storage of health record
    Procedure Doctor Dpk_n,
    For each Doctor having Dpk_n, with session key S_k
    $D_n \leftarrow$ Decrypt (Dpk_n (S_k))
    $D_n \leftarrow$ Decrypt (Pa_{cvn} (S_k))
    $Pa_{cvn} \rightarrow UPa_{cvn}$
    IPFS Storage Encrypt (UPa_{cvn}(S_k))
    End For
    End procedure

3.5.1. Access Control and Secure Data Sharing

AC is a crucial tool in managing EHR data and protecting their security and privacy. The identifiers and rules of AC are controlled by a blockchain-based controller which ensures pseudo-anonymity inside the architecture. Ethereum has more features, such as the ability to utilize SC [49]. The SC of the blockchain can help a user to utilize their access privileges. As a result of this, the risk of revealing confidential medical data might be considerably decreased. The block chain indices ensure that EHRs cannot be changed arbitrarily.

The secured data transfer may be carried out automatically by the specified access permissions of the patients using blockchain SCs. Apart from content extraction, the signature technique ensures the secured transfer of the data. These decentralized systems provide patient-centric privacy protection with EHR data segmentation and leveraged access constraints. Accordingly, these systems produce key-based access control for safe EHR transactions, utilizing the SPAKE with access restrictions set in the SC. Meanwhile, EHR summaries are encrypted using the public keys of patients and EHR file sharing is controlled by the patients. The healthcare providers can reliably access EHRs from the

remote providers on demand using cloud computing, regardless of the time difference, their working hours, or their location. The secured medical resource sharing that includes message authentication systems is made possible by private cloud environments.

Secure Password Authentication Based Key Exchange (SPAKE)

An additional realistic scenario is assumed by the protocol called password-based authenticated key exchange, where secret keys are selected from a restricted range of potential values (for example, a four-digit pin) rather than being randomly dispersed over a broad area. Human-memorable passwords are also easier to utilize. For instance, new cryptographic devices that can store high-entropy secret keys make them seem more practical. However, the great protocols that are employed do not consider such situations and are frequently vulnerable to "dictionary attacks." A predetermined narrow value set (i.e., the dictionary) might have the chance to compromise a scheme's security by trying every combination of secret keys. The dictionary attacks are attempts by an adversary to use the brute-force method. Dictionary attacks of this type can typically be classified into two categories: offline and online.

The information about patient HR stored in the EHR is a real-time record system. These HRs are allergies, health histories, images from x-ray scans, blood reports, a list of previous operations and surgeries undergone, etc. Insurance agencies, patients, doctors, test laboratories, etc., are the various entities who are stakeholders in an EHR access. A doctor can retrieve a patient's information via an EHR system and treat or operate on him accordingly. This EHR system is very helpful in emergencies when time is of the essence. There is no need to perform another allergy test. It can save someone's life while also saving time, money, and effort. Because these systems hold sensitive information, security will be a crucial concern. A significant issue is caused by any unauthorized data transfer. Therefore, for creating EHR systems, security and authentication are still crucial components.

When the password is a secret key, several protocols that have been created to solve this issue are secured. These methods are designed to limit the success of an adversary's online-guessing attack. The system must be engaged and present to check the accuracy of the adversary's guess in these attacks. After a given number of unsuccessful attempts, the security of this system often relies on a rule that invalidates or blocks the use of a password.

Accordingly, unwelcome or unsafe EHR system communication may result in legal issues or problematic situations. It could generate issues with the insured amount. A scenario where a doctor refuses to disclose the details of the patient throughout a communication procedure can be taken into consideration. Common authentication and an agreed-upon key are thus required in this setting during the doctor's communication. The doctors desire patient interaction before submitting their reports to the EHR system which may employ a client-server architecture. This creates false health information; an altered data and device-to-device wireless communication system can cause a variety of legal problems and may endanger the life of a patient during an emergency or operation. Then there must be genuine communication between the doctor and the patient.

As a result, a SPAKE protocol is utilized, which is the safest password authentication-based key exchange, to create secure channels. The password is used by the parties for an obtained standard session key S_k. The advantage of an attacker in distinguishing a real session key from a random key is less than $O(n/D)\,\epsilon\,(k)$, where, n is the number of active sessions, $|D|$ is the dictionary size D, and based on the security parameter k, $\epsilon\,(k)$ is a negligible function. The protocols are said to be secured against the dictionary attacks.

Protocol Participants: Either a client $C \in C$ or a server $S \in S$ participates in the password-based key exchange. The union $C\ U\ S$ is all the participants or users U set.

Long-Lived Keys: Each client $C \in C$ holds a password $pw_S\,[C]$. Every server $S \in S$ keeps a vector called $pw_S = \langle pw_S\,[C]\rangle\,_{C \in C}$, where $pw_s\,[C]$ is the transformed password, with an entry for each client, although in some systems they might not be the same in a symmetric model $pw_S\,[C] = pw_C$. For server S and client C, the terms pw_C and pw_S also refer to the long-lived keys, respectively.

Protocol Execution: Only oracle inquiries, in a real attack, the capabilities of an attack are simulated, and the contact between protocol participants and adversary A occurs. The adversary may construct several concurrent instances of the participants during the execution. The following queries, where U^i stands for the participant U's i instance:

Execute (C^i, S^j): The executions between a server and a user instance, S^j and C^i, respectively, are intercepted by the attacker using this query, which simulates passive attacks. The exchanged messages are the result of this query throughout the honest execution of the protocol.

Send (U^i, m): Simulation of an active attack by this query in which the adversary intercepts a communication and either modifies it by creating a new message, or simply forwards the original to the planned recipient. The message that the participant instance U^i would produce as a result of receiving message m is the result of this query.

4. Experimentation Section

4.1. Dataset

The characteristics of the hepatitis dataset [50] for our proposed framework are multivariate, and the characteristic features are integer, categorical, and real. The number of instances is 155, with 20 attributes. Class, age, sex, steroids, fatigue, bilirubin, antivirals, malaise, liver firmness, ascites, protime, and other characteristics are included.

4.2. Experimental Setup

Hyperledger fabric chooses level DB to be the world state database. Docker is used to run the individual nodes in the fabric. We set up each hyperledger fabric with four peers (commitment nodes) and one ordering node. The nodes were running on 64-bit Linux, version 5.4.0-90-generic. The server contained 32 CPUs, each of which was an Intel (R) Xeon (R) Silver 4110 with the architecture x86_64. Each CPU ran at 2.1 GHz with 32 K of L1d cache, 32 K of L1i cache, 1024 K of L2 cache, and 11,264 K of L3 cache. The memory was DDR4 with a capacity of 32 GB. The fabric block size was set to 256. We have evaluated the results, taking 200 s of simulation time into consideration.

5. Results and Discussion

The results of the performance graphs for the research work are portrayed in the following figures.

The uploading time refers to the time required to upload data of a fixed size and its encryption time. The downloading time includes the cumulative time to download the fixed data and the time it takes to decrypt it. Uploading time and downloading time are given in the below Figure 2. It indicates that the data size varies from 0.003 MB to 100 MB. That is, when the data size increases, it results in an increase in the uploading and downloading time. However, the rate of rise in the downloading time is found to be higher than the uploading time with the increase in block size.

Figure 3 illustrates the probability of creating a block within k seconds. In this figure, the probability of block creation varies between 17 and 600 s. The 17-s and 600 s blocks produce probabilities of 1 and 0.65, respectively. The 17-s blocks produce the constant value of 1. The blockchain with the fastest block creation speed is defined as a faster blockchain. The faster blockchain results in a probability of 0.629 at 600 s, which is approximately equal to the predicted 0.632 ($1 - 1/e \sim= 0.632$, where e is Euler's constant). The probability of two blocks being generated simultaneously is very small due to the rise in time between two successive block creations.
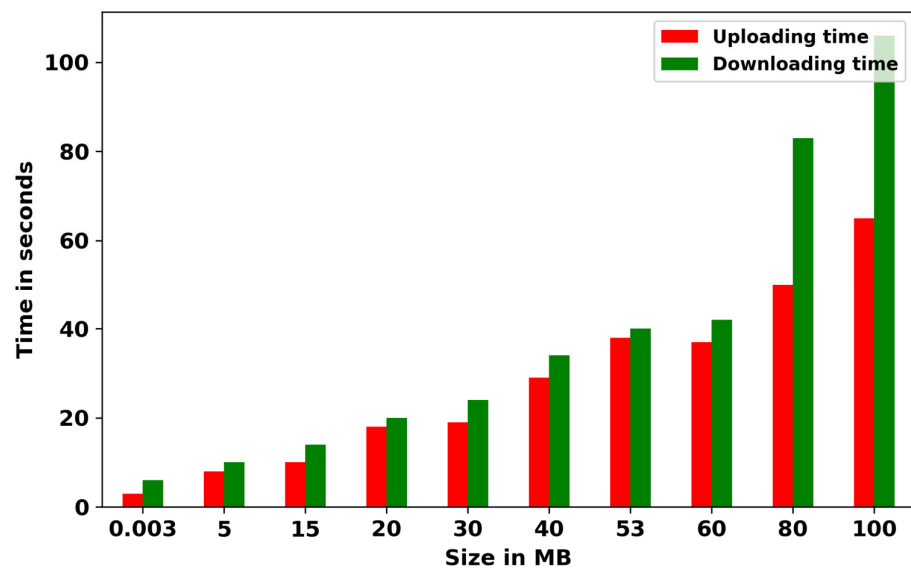
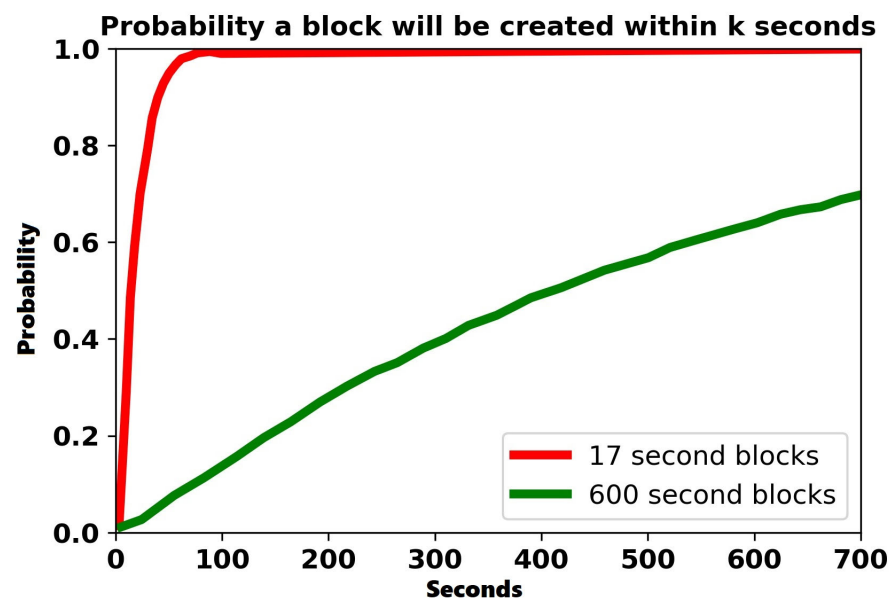**Figure 2.** Uploading and downloading Time.

Figure 3. Probability of creating a block within k-seconds.

Figure 4 displays the computational time in milliseconds with different key sizes. Record size was kept at 100 MB, which is the maximum record size for this experiment. As there is a change in the key size from 16, 64, 128, 256, or 512 bits, we trace the time it takes to encrypt the record and upload it to the blockchain. We run the experiment five times for each key size, and then the average of the results is taken into consideration. It is inferred that the computational time increases with the increasing length of the key. Although it requires additional computation time, a key with a higher length gives higher security from attacks.
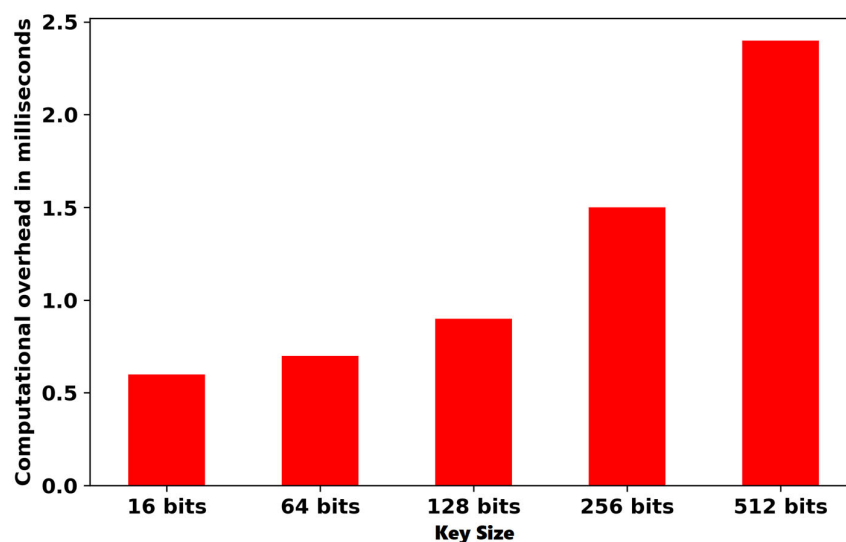
Figure 4. Transactional computational time in milliseconds with key size.

Figure 5, shows detailed information about the transaction sets and the time in seconds. Here, a set is represented as a transaction set, on which we have applied an access control policy. It represents the number of groups of access control policies and the EHR transferred per second (throughput). The comparative analysis of this proposed framework and benchmark model, MedChain [51], is based on a number of transactions for the same access policies. In this work, an attribute-based access control policy framework is used with multiple certificate authorities, which provide more security and fine-grained access control. In Figure 5, the x-axis symbolizes the access policies on transaction sets, while the y-axis represents throughput.
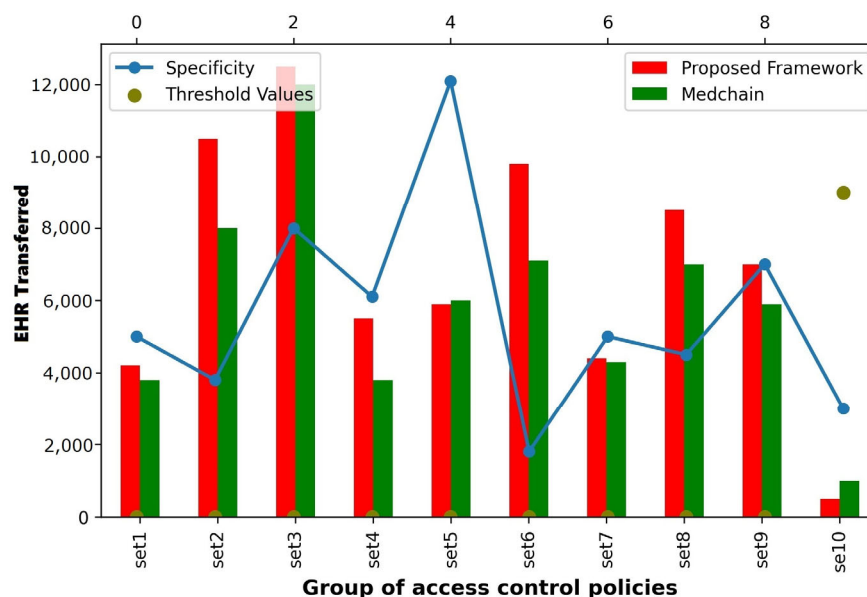

Figure 5. EHR transaction set for time in seconds.

IPFS EHR data uploading and downloading are depicted in Figure 6. It consists of the data size and the duration of uploading and downloading EHR data. Figure 6 shows that the EHR size ranges from 1.1 MB to 100 MB. Figure 6 shows that as the EHR data size increases, the uploading and downloading time for the data also increases.
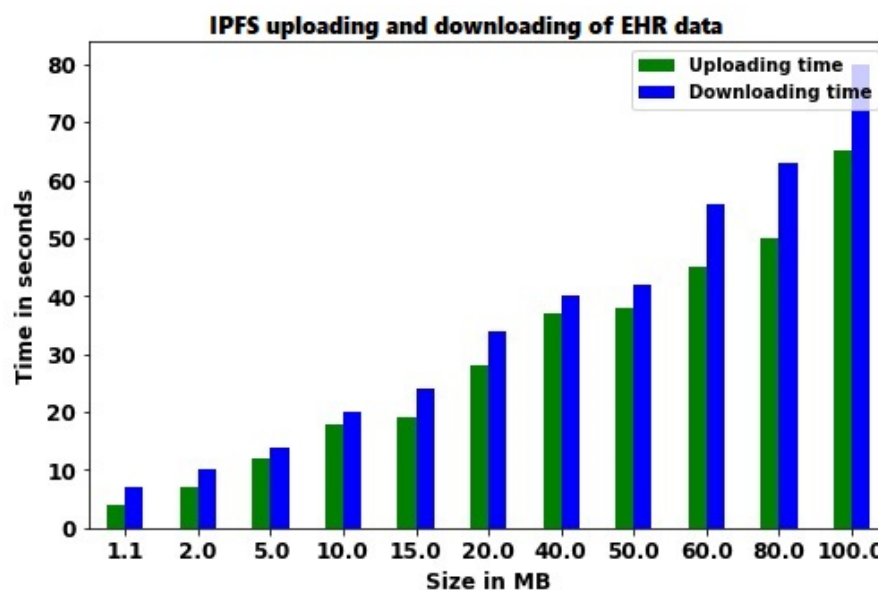
Figure 6. IPFS uploading and downloading of EHR data.

6. Conclusions

Blockchain is a promising technology for deploying digital healthcare systems. However, there are problems with access control for electronic health records (EHR). Due to their massive volume, EHR transactions must be stored on distributed storage on the blockchain. There are some specific goals for this, such as utilizing the health level 7 fast healthcare interoperability resources (HL7 FHIR) as the data standard for storing information on the blockchain platform. Accordingly, using IPFS, this study presents a patient-centered healthcare data management (PCHDM), a permissioned distributed ledger (DL) system that controls access to the EHR. EHR transactions are private health records, and distributed storage compromises their confidentiality. Access control is thus a crucial management tool for EHR data to protect its security and privacy. The smart contracts of the blockchain can assist users in using their access rights. Accordingly, a secure password authentication-based key exchange (SPAKE) method is proposed for secured EHR transactions. The experimental setup in the work comprises four hyperledger fabric nodes with level DB database as an on-chain storage and IPFS as off-chain storage. The proposed framework is evaluated using the public hepatitis dataset. The framework enables patient-centric access control of the EHR with the SPAKE encryption algorithm. The framework is evaluated with parameters such as block creation time, transactional computational overhead with encryption key size, and uploading/downloading time with EHR size. The proposed model results in secure EHR transactions which are controlled by role-based access control mechanism to data owners, i.e., patients. The proposed framework is an experimental prototype in the permissioned blockchain ecosystem with hyperledger fabric. It is additionally compared with existing framework, i.e., MedChain for performance metrics such as throughput, upload-download time and block creation time. Evaluation reveals that our proposed framework outperforms MedChain with respect to throughput. Additionally, the IPFS based off-chain storage makes this solution scalable for larger data sizes.

Moreover, in the future, the system should trace the EHR for users requesting personal behavior. This will help user classification based on their behavior and interactions. The presented work works on homogenous and single blockchain. Cross-chain EHR transactions which are transmitted with privacy should be the future of the proposed work.

Abbreviations

AC	Access Control
AI	Artificial Intelligence
DL	Distributed Ledger
EHR	Electronic Health Records
FHIR	Fast Healthcare Interoperability Resources
HI	Healthcare Industry
HL7	Health Level Seven
HR	Health Record
IEFS	IPFS-based EHR File System
IoMT	Internet of Medical Things
IPFS	InterPlanetary File System
PCHDM	Patient-Centered Healthcare Data Management
RBAC	Role Based Access Control
SC	Smart Contract
SPAKE	Secure Password Authentication-based Key Exchange

References

1. Raghav, N.; Bhola, A. Blockchain Based Privacy Preservation in Healthcare: A Recent Trends and Challenges. *Psychol. Educ.* **2021**, *58*, 5315–5324.
2. Fatokun, T.; Nag, A.; Sharma, S. Towards a Blockchain Assisted Patient Owned System for Electronic Health Records. *Electronics* **2021**, *10*, 580. [CrossRef]
3. Chelladurai, U.; Pandian, S.; Ramasamy, K. A blockchain based patient centric electronic health record storage and integrity management for e-Health systems. *Health Policy Technol.* **2021**, *10*, 100513. [CrossRef]
4. Ali, A.; Rahim, H.A.; Ali, J.; Pasha, M.F.; Masud, M.; Rehman, A.U.; Chen, C.; Baz, M. A Novel Secure Blockchain Framework for Accessing Electronic Health Records Using Multiple Certificate Authority. *Appl. Sci.* **2021**, *11*, 9999. [CrossRef]
5. William, A.D.J.; Rajendran, S.; Pranam, P.; Berry, Y.; Sreedharan, A.; Gul, J.; Paul, A. Blockchain Technologies: Smart Contracts for Consumer Electronics Data Sharing and Secure Payment. *Electronics* **2022**, *12*, 208. [CrossRef]
6. IPFS. Available online: https://ipfs.tech/ (accessed on 10 October 2022).
7. Sonkamble, R.G.; Phansalkar, S.P.; Potdar, V.M.; Bongale, A.M. Survey of Interoperability in Electronic Health Records Management and Proposed Blockchain Based Framework: MyBlockEHR. *IEEE Access* **2021**, *9*, 158367–158401. [CrossRef]
8. Ruan, P.; Chen, G.; Dinh, T.T.A.; Lin, Q.; Ooi, B.C.; Zhang, M. Fine-grained, secure and efficient data provenance on blockchain systems. *Proc. VLDB Endow.* **2019**, *12*, 975–988. [CrossRef]
9. Wang, H.; Xu, C.; Zhang, C.; Xu, J.; Peng, Z.; Pei, J. May. vChain+: Optimizing Verifiable Blockchain Boolean Range Queries. In Proceedings of the 2022 IEEE 38th International Conference on Data Engineering (ICDE), Kuala Lumpur, Malaysia, 9–12 May 2022; pp. 1927–1940.
10. Kaur, J.; Rani, R.; Kalra, N. Blockchain-based framework for secured storage, sharing, and querying of electronic healthcare records. *Concurr. Comput. Pract. Exp.* **2021**, *33*, e6369. [CrossRef]
11. Bharimalla, P.K.; Choudhury, H.; Parida, S.; Mallick, D.K.; Dash, S.R. A Blockchain and NLP Based Electronic Health Record System: Indian Subcontinent Context. *Informatica* **2021**, *45*, 605–616. [CrossRef]
12. Gul, M.J.; Rehman, A.; Paul, A.; Rho, S.; Riaz, R.; Kim, J. Blockchain Expansion to secure Assets with Fog Node on special Duty. *Soft Comput.* **2020**, *24*, 15209–15221. [CrossRef]
13. Loh, C.M.; Chuah, C.W. Electronic Medical Record System Using Ethereum Blockchain and Role-Based Access Control. *Appl. Inf. Technol. Comput. Sci.* **2021**, *2*, 53–72.
14. Lee, J.; Park, Y.R.; Beck, S.S. Deriving Key Architectural Features of FHIR-BlockChain Integration through the Qualitative Content Analysis. 2021. Available online: https://assets.researchsquare.com/files/rs-936437/v1/010fb5c7-7010-4133-9617-986510b70abe.pdf?c=1647432873: (accessed on 15 December 2022).
15. Shuaib, M.; Alam, S.; Alam, M.S.; Nasir, M.S. Compliance with HIPAA and GDPR in blockchain-based electronic health record. *Mater. Today Proc.* **2021**. [CrossRef]

16. Pineda Rincón, E.A.; Moreno-Sandoval, L.G. Design of an Architecture Contributing to the Protection and Privacy of the Data Associated with the Electronic Health Record. *Information* **2021**, *12*, 313. [CrossRef]

17. Abunadi, I.; Kumar, R.L. BSF-EHR: Blockchain Security Framework for Electronic Health Records of Patients. *Sensors* **2021**, *21*, 2865. [CrossRef] [PubMed]

18. Jain, N.; Gupta, V.; Dass, P. Blockchain: A Novel Paradigm for Secured Data Transmission in Telemedicine. In *Wearable Telemedicine Technology for the Healthcare Industry*; Academic Press: Cambridge, MA, USA, 2022; pp. 33–52. [CrossRef]

19. Boumezbeur, I.; Zarour, K. Blockchain-Based Electronic Health Records Sharing Scheme with Data Privacy Verifiable. *Appl. Med. Inform.* **2021**, *43*, 124–135.

20. Jabbar, R.; Fetais, N.; Krichen, M.; Barkaoui, K. Blockchain Technology for Healthcare: Enhancing Shared Electronic Health Record Interoperability and Integrity. In Proceedings of the 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT), Doha, Qatar, 2–5 February 2020; pp. 310–317.

21. Bazel, M.A.; Mohammed, F.; Ahmed, M. Blockchain Technology in Healthcare Big Data Management: Benefits, Applications and Challenges. In Proceedings of the 2021 1st International Conference on Emerging Smart Technologies and Applications (eSmarTA), Sana'a, Yemen, 10–12 August 2021; pp. 1–8.

22. Rodríguez-Espíndola, O.; Chowdhury, S.; Beltagui, A.; Albores, P. The potential of emergent disruptive technologies for humanitarian supply chains: The integration of blockchain, Artificial Intelligence and 3D printing. *Int. J. Prod. Res.* **2020**, *58*, 4610–4630. [CrossRef]

23. Lee, S.; Kim, J.; Kwon, Y.; Kim, T.; Cho, S. Privacy Preservation in Patient Information Exchange Systems Based on Blockchain: System Design Study. *J. Med. Internet Res.* **2022**, *24*, e29108. [CrossRef]

24. Chamola, V.; Goyal, A.; Sharma, P.; Hassija, V.; Binh, H.T.T.; Saxena, V. Artificial intelligence-assisted blockchain-based framework for smart and secure EMR management. *Neural Comput. Appl.* **2022**, *41*, 1–11. [CrossRef]

25. Jain, M.; Pandey, D.; Sharma, K.K. A Granular Access-Based Blockchain System to Prevent Fraudulent Activities in Medical Health Records. In *Advances in Data Computing, Communication and Security*; Springer: Singapore, 2022; pp. 635–645.

26. Verma, D.K.; Tyagi, R.K.; Chakraverti, A.K. Secure Data Sharing of Electronic Health Record (EHR) on the Cloud Using Blockchain in Covid-19 Scenario. In *Proceedings of Trends in Electronics and Health Informatics*; Springer: Singapore, 2022; pp. 165–175.

27. Manoj, T.; Makkithaya, K.; Narendra, V.G. A Blockchain Based Decentralized Identifiers for Entity Authentication in Electronic Health Records. 2022. Available online: https://www.tandfonline.com/doi/full/10.1080/23311916.2022.2035134 (accessed on 15 December 2022).

28. Peng, Z.; Xu, J.; Hu, H.; Chen, L.; Kong, H. BlockShare: A Blockchain empowered system for privacy-preserving verifiable data sharing. *Bull. IEEE Comput. Soc. Tech. Comm. Data Eng.* **2022**, *1*, 14–24.

29. Gul, M.J.; Subramanian, B.; Paul, A.; Kim, J. Blockchain for public health care in smart society. *Microprocess. Microsyst.* **2020**, *80*, 103524. [CrossRef]

30. Boumezbeur, I.; Zarour, K. Privacy Preservation and Access Control for Sharing Electronic Health Records Using Blockchain Technology. *Acta Inform. Pragensia* **2022**, *11*, 105–122. [CrossRef]

31. Peng, Z.; Xu, C.; Wang, H.; Huang, J.; Xu, J.; Chu, X. P2b-trace: Privacy-Preserving Blockchain-Based Contact Tracing to Combat Pandemics. In Proceedings of the 2021 International Conference on Management of Data, Xi'an, China, 20–25 June 2021; pp. 2389–2393.

32. Alrebdi, N.; Alabdulatif, A.; Iwendi, C.; Lian, Z. SVBE: Searchable and verifiable blockchain-based electronic health records system. *Sci. Rep.* **2022**, *12*, 266. [CrossRef] [PubMed]

33. Mondal, S.; Shafi, M.; Gupta, S.; Gupta, S.K. Blockchain Based Secure Architecture for Electronic Healthcare Record Management. *GMSARN Int. J.* **2022**, *16*, 413–426.

34. Li, H.; Yang, X.; Wang, H.; Wei, W.; Xue, W. A Controllable Secure Blockchain-Based Electronic Healthcare Records Sharing Scheme. *J. Health Eng.* **2022**, *2022*, 2058497. [CrossRef]

35. Cerchione, R.; Centobelli, P.; Riccio, E.; Abbate, S.; Oropallo, E. Blockchain's coming to hospital to digitalize healthcare services: Designing a distributed electronic health record ecosystem. *Technovation* **2023**, *120*, 798–805. [CrossRef]

36. Chatterjee, A.; Pahari, N.; Prinz, A. HL7 FHIR with SNOMED-CT to Achieve Semantic and Structural Interoperability in Personal Health Data: A Proof-of-Concept Study. *Sensors* **2022**, *22*, 3756. [CrossRef] [PubMed]

37. HyperLedger FOUNDATION. Available online: https://www.hyperledger.org/use/fabric (accessed on 12 February 2021).

38. Adlam, R.; Haskins, B. A Permissioned Blockchain Approach to the Authorization Process in Electronic Health Records. In Proceedings of the 2019 International Multidisciplinary Information Technology and Engineering Conference (IMITEC), Vanderbijlpark, South Africa, 21–22 November 2019; pp. 1–8.

39. Jayabalan, J.; Jeyanthi, N. Scalable blockchain model using off-chain IPFS storage for healthcare data security and privacy. *J. Parallel Distrib. Comput.* **2022**, *164*, 152–167. [CrossRef]

40. Xia, Q.; Sifah, E.B.; Smahi, A.; Amofa, S.; Zhang, X. BBDS: Blockchain-based data sharing for electronic health records in cloud environments. *Information* **2017**, *8*, 44. [CrossRef]

41. Peng, Z.; Zhang, Y.; Xu, Q.; Liu, H.; Gao, Y.; Li, X.; Yu, G. NeuChain: A fast permissioned blockchain system with deterministic ordering. *Proc. VLDB Endow.* **2022**, *15*, 2585–2598. [CrossRef]

42. Ruan, P.; Dinh, T.T.A.; Lin, Q.; Zhang, M.; Chen, G.; Ooi, B.C. Revealing Every Story of Data in Blockchain Systems. *ACM SIGMOD Rec.* **2020**, *49*, 70–77. [CrossRef]

43. Tith, D.; Lee, J.S.; Suzuki, H.; Wijesundara, W.M.A.B.; Taira, N.; Obi, T.; Ohyama, N. Application of blockchain to maintaining patient records in electronic health record for enhanced privacy, scalability, and availability. *Healthc. Inform. Res.* **2020**, *26*, 3–12. [CrossRef] [PubMed]

44. Mani, V.; Manickam, P.; Alotaibi, Y.; Alghamdi, S.; Khalaf, O.I. Hyperledger Healthchain: Patient-Centric IPFS-Based Storage of Health Records. *Electronics* **2021**, *10*, 3003. [CrossRef]

45. Chenthara, S.; Ahmed, K.; Wang, H.; Whittaker, F.; Chen, Z. Healthchain: A novel framework on privacy preservation of electronic health records using blockchain technology. *PLoS ONE* **2020**, *15*, e0243043. [CrossRef] [PubMed]

46. Sun, J.; Yao, X.; Wang, S.; Wu, Y. Blockchain-based secure storage and access scheme for electronic health records in IPFS. *IEEE Access* **2020**, *8*, 59389–59401. [CrossRef]

47. Thwin, T.T.; Vasupongayya, S. Blockchain Based Secret-Data Sharing Model for Personal Health Record System. In Proceedings of the 2018 5th International Conference on Advanced Informatics: Concept Theory and Applications (ICAICTA), Krabi, Thailand, 14–17 August 2018; pp. 196–201.

48. Verdonck, M.; Poels, G. Decentralized Data Access with IPFS and Smart Contract Permission Management for Electronic Health Records. In *International Conference on Business Process Management*; Springer: Cham, Switzerland, 2020; pp. 5–16.

49. Ashizawa, N.; Yanai, N.; Cruz, J.P.; Okamura, S. Eth2Vec: Learning contract-wide code representations for vulnerability detection on ethereum smart contracts. *Blockchain Res. Appl.* **2022**, *1*, 100101. [CrossRef]

50. Hepatitis Data Set. Available online: https://archive.ics.uci.edu/ml/datasets/hepatitis (accessed on 15 November 2022).

51. Daraghmi, E.-Y.; Daraghmi, Y.-A.; Yuan, S.-M. MedChain: A Design of Blockchain-Based System for Medical Records Access and Permissions Management. *IEEE Access* **2019**, *7*, 164595–164613. [CrossRef]