



# *Article* **Generic Patient-Centered Blockchain-Based EHR Management System**

**Alaa Haddad <sup>1</sup> , Mohamed Hadi Habaebi 1,\* [,](https://orcid.org/0000-0002-2263-0850) Fakher Eldin M. Suliman <sup>2</sup> , Elfatih A. A. Elsheikh <sup>2</sup> [,](https://orcid.org/0000-0001-9556-5861) Md Rafiqul Islam <sup>1</sup> and Suriza Ahmad Zabidi <sup>1</sup>**

- 1 IoT & Wireless Communication Protocols Laboratory, Department of Electrical & Computer Engineering, International Islamic University Malaysia, Kuala Lumpur 53100, Malaysia
	- <sup>2</sup> Department of Electrical Engineering, College of Engineering, King Khalid University, Abha 61421, Saudi Arabia
- **\*** Correspondence: habaebi@iium.edu.my

**Abstract:** Accessing healthcare services by several stakeholders for diagnosis and treatment has become quite prevalent owing to the improvement in the industry and high levels of patient mobility. Due to the confidentiality and high sensitivity of electronic healthcare records (EHR), the majority of EHR data sharing is still conducted via fax or mail because of the lack of systematic infrastructure support for secure and reliable health data transfer, delaying the process of patient care. As a result, it is critically essential to provide a framework that allows for the efficient exchange and storage of large amounts of medical data in a secure setting. The objective of this research is to develop a Patient-Centered Blockchain-Based EHR Management (PCEHRM) system that allows patients to manage their healthcare records across multiple stakeholders and to facilitate patient privacy and control without the need for a centralized infrastructure by means of granting or revoking access or viewing one's records. We used an Ethereum blockchain and IPFS (inter-planetary file system) to store records because of its advantage of being distributed and ensuring the immutability of records and allowing for the decentralized storage of medical metadata, such as medical reports. To achieve secure a distributed, and trustworthy access control policy, we proposed an Ethereum smart contract termed the patient-centric access control protocol. We demonstrate how the PCEHRM system design enables stakeholders such as patients, labs, researchers, etc., to obtain patient-centric data in a distributed and secure manner and integrate utilizing a web-based interface for the patient and all users to initiate the EHR sharing transactions. Finally, we tested the proposed framework in the Windows environment by compiling a smart contract prototype using Truffle and deploy on Ethereum using Web3. The proposed system was evaluated in terms of the projected medical data storage costs for the IPFS on blockchain, and the execution time for a different number of peers and document sizes. The findings of the study indicate that the proposed strategy is both efficient and practicable.

**Keywords:** patient-centered; IPFS; blockchain; privacy; health record

### **1. Introduction**

One of the most important components of healthcare is providing a secure and discreet access control approach. In this age, big data is utilized to maintain and retrieve a significant amount of healthcare records over the Internet. For that purpose, cloud networking is becoming increasingly crucial in this process. Despite their simplicity and efficiency, conventional EHR systems pose a slew of privacy and security issues [\[1\]](#page-17-0). This is because HR are considered the most sensitive data being collected owing to the sensitive information about patients and diagnoses. HR data has, however, become more susceptible to breach due to the advancement of the internet and digital healthcare systems in current times [\[2\]](#page-17-1). As a result, while evaluating a decentralized and trust-based mechanism, the issues of



**Citation:** Haddad, A.; Habaebi, M.H.; Suliman, F.E.M.; Elsheikh, E.A.A.; Islam, M.R.; Zabidi, S.A. Generic Patient-Centered Blockchain-Based EHR Management System. *Appl. Sci.* **2023**, *13*, 1761. [https://doi.org/](https://doi.org/10.3390/app13031761) [10.3390/app13031761](https://doi.org/10.3390/app13031761)

Academic Editor: Gianluca Lax

Received: 21 December 2022 Revised: 20 January 2023 Accepted: 21 January 2023 Published: 30 January 2023



**Copyright:** © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license [\(https://](https://creativecommons.org/licenses/by/4.0/) [creativecommons.org/licenses/by/](https://creativecommons.org/licenses/by/4.0/)  $4.0/$ ).

security and privacy must be considered [\[3\]](#page-17-2). Table [1](#page-1-0) shows the list of abbreviations and acronyms used in the article.  $\blacksquare$ 



<span id="page-1-0"></span>**Table 1.** List of abbreviations and acronyms used in the article.

#### *1.1. Motivation*  $\sum_{i=1}^{n} a_i$  and approach approach, content organizations to  $\sum_{i=1}^{n} a_i$

In the conventional approach, cloud databases are used by content organizations to amalgamate EHRs, EMRs, clinical images, PHRs, and patient information; for example, doctor name, body measurements, and home-checking gadget information. It is worth noting that a centralized database is vulnerable to cyberattacks, jeopardizing the security and privacy of EHR [\[1\]](#page-17-0). Meanwhile, stakeholders and health providers face difficulty in sharing health information attributable to the discordant standards and formats.

The problem is further exacerbated if the EHR of a patient is erased from the hospital's database, resulting in a permanent loss of the record. Thus, it is imperative for the pro-posed system to be tamper-proof by unauthorized parties to avoid that issue occurring [\[4\]](#page-17-3). Another challenge posed by the current healthcare systems is patients do not have total control over their health records since they are maintained by the service providers [\[5\]](#page-17-4). As the healthcare data amount continues to multiply, the security and scalability features have become major concerns. Figure 1 shows the overview of the current system architecture for existing health records.

<span id="page-1-1"></span>

**Figure 1.** Overview of the current system. **Figure 1.** Overview of the current system.

# *1.2. Contribution 1.2. Contribution*

Considering the problems mentioned above, the healthcare industry would require Considering the problems mentioned above, the healthcare industry would require a technology that is able to store data securely and efficiently. The contributions of this article<br>see as fallation are as follows:  $\frac{1}{2}$ 

A proposed PCEHRM system's structure is introduced, and the different system's components interactions are demonstrated.

- The proposal of a patient-centric access control framework is based on a smart contract protocol to grant stakeholders access to the health records. It determines specific functions to be used to send information in and out of the Ethereum blockchain and to provide access privileges between stakeholders.
- The proposed patient-centric distributed architecture focuses on confidentiality, reliability, integrity, portability, and scalability through a blockchain-based approach.
- A novel algorithm is introduced for preserving and securely retrieving healthcare records using blockchains.
- The viability and coherence of the access process and system interaction amongst network participants was tested by putting the suggested framework into practice.
- The average time taken to download and upload health data, the cost of under-taking PCEHRM functions, as well as the efficiency of the transaction were examined and evaluated. Consequently, examining the test network permits us to validate and optimize the prototype prior to publishing it on a public blockchain.

#### **2. Related Work**

This section covers the study related to using blockchain technology in the e-healthcare industry to guarantee safe data storage and effective access management. Blockchain technology offers a cryptographic fix to the security issues that are hindering the growth of electronic health systems. Medical enterprises have encountered taxing challenges over the past 20 years as a result of incidents involving record breaches in major medical data centers [\[6\]](#page-17-5). MedRec became the first organization to suggest a blockchain-based electronic patient record management system in the early days of blockchain technology [\[7\]](#page-17-6). At that time, the Ethereum blockchain and smart contracts preserve detailed accessible healthcare records. However, the medical records are stored in third-party databases operated by healthcare providers, instead on the blockchain network. As a result, the violation or misuse of these records is still a possibility. Healthcare management framework encrypts patient keys during the process of creating or updating data on the blockchain [\[8\]](#page-17-7). To decrypt the record, healthcare personnel and lab technician would have to request authorization from a patient's public key. This is starkly in contrast to our approach, as patients are the sole party with access to and control over their data. Any node can connect to the network and conduct transactions on the public blockchain [\[9\]](#page-17-8). A blockchain-based application called Medchain allows patients, pharmacists, and hospitals to exchange healthcare data [\[10\]](#page-17-9). This architecture stores data on-chain, and thus, presents scalability and privacy issues. A blockchain-based IoT solution may utilize smart contracts to track patients' health [\[11\]](#page-17-10). The authors in [\[12\]](#page-17-11) proposed a blockchain-driven system for maintaining electronic medical records, while [\[13\]](#page-17-12) presented a blockchain-based architecture that incorporates distributed health records with node models to optimize the replication of healthcare records. The researchers in [\[14\]](#page-17-13) used blockchain smart technology, a decentralized network with smart contracts, to save and transfer data in a secure manner. In a study by [\[15\]](#page-17-14), a privacy-preserving system was developed for remote patient surveillance. A permissioned blockchain with an access control audit log was also developed to store health records, but it raises privacy concerns owing to the distribution of the audit log with all interested parties [\[16\]](#page-17-15). The authors of [\[17\]](#page-17-16) argued about the robustness of blockchain technology in storing medical records and raised concerns about the scalability and privacy issues concerning the framework. In another study by [\[18\]](#page-17-17), they proposed a ring structure-based access control that ensures privacy, but inadvertently leads to an unstable system as the data is maintained in an on-chain database. Ref. [\[19\]](#page-17-18) also proposed an intelligent data management framework for the cyber system. The decentralized storage and access of records, as described in [\[20\]](#page-17-19), effectively utilize the network's power and resources. In another study by [\[21\]](#page-17-20), they employed high-end privacy-enhancing technologies such as homomorphic encryption, which permits data processing while maintaining complete encryption to avoid vulnerability problems. Meanwhile, the researchers in [\[22\]](#page-17-21) adopted the zero-knowledge proofs approach, along with proof authority consensus for

mutual authentication to enhance privacy by ensuring that nodes were not engaging in a malicious manner. Using blockchain technology, several cryptographic mechanisms for preventing tampering and becoming an effective data storage and sharing solution are shown in Table [2.](#page-3-0)

<span id="page-3-0"></span>Table 2. Several solutions of the existing techniques EHR systems currently lack adequate interoperability to provide private, effective, and secure access control.



### **3. Framework Components 3. Framework Components**

<span id="page-3-1"></span>In this study, as shown in Figure [2,](#page-3-1) we established a permissioned infrastructure in In this study, as shown in Figure 2, we established a permissioned infrastructure in an Ethereum Blockchain framework that allows complete control of records by patients an Ethereum Blockchain framework that allows complete control of records by patients while ensuring privacy, durability, and security. This is carried out by maintaining health while ensuring privacy, durability, and security. This is carried out by maintaining health information primarily on the blockchain as hashes, whereas the original bulk quantities of information primarily on the blockchain as hashes, whereas the original bulk quantities data are stored off-chain in IPFS to guarantee effectiveness and scalability.



**Figure 2.** Framework of the proposed system. **Figure 2.** Framework of the proposed system.

The smart contract chain code protocol in this paper is termed a Patient-Centric The smart contract chain code protocol in this paper is termed a Patient-Centric Healthcare Data Management Access Control-Smart Contract, in which this SC is used to Healthcare Data Management Access Control-Smart Contract, in which this SC is used to write the role-based access control chain code for recognized stakeholders involved and write the role-based access control chain code for recognized stakeholders involved and does not employ any incentive mining beyond ensuring that every party has equal access does not employ any incentive mining beyond ensuring that every party has equal access to the system. The role-based unique ID is initiated after the registration of stakeholders. Following this process, public and private key pairs are provided to each stakeholder for the storage and transfer of health information. In this architecture, a patient's health record is created by doctors. Subsequently, the patient would commit the encrypted health

record to be stored in IPFS indelibly while the record hash from IPFS is conserved via the Ethereum blockchain.

In the event that the doctors need to update the patient's health record, one can allow or block the process by granting or revoking access, respectively. The temporary view, or patient-centric view, of the health record, is constructed from IPFS. In this view, the doctor is allowed to update the documentation before the patient commits to the update using their key pairs to save the updated files in IPFS. In this way, this framework would ensure the interoperability of the mechanism.

Additionally, patients have the right to grant access to share the records with only the relevant stakeholders in a patient-centric view of the record from the IPFS system. A doctor's session also would expire before the hash value is committed to the ledger so that non-concerned personnel would have gained access to a record without the patient's permission, hence, safeguarding the data privacy in the system. At the back end, smart contracts are generated for several healthcare procedures.

Hence, role-based access control employed in this framework protects the privacy of the patient. Moreover, our proposed system also has improved scalability and interoperability features as compared to the current system.

#### *3.1. Ethereum Blockchain*

Ethereum is designed based on the Bitcoin architecture and features a framework for programmable smart contracts (SC) [\[23](#page-18-0)[,24\]](#page-18-1). Simply put, SC is a software program that holds guidelines for negotiating contract conditions. The cost of building and maintaining a centralized database can be minimized by allowing programs to autonomously validate and implement contract-related agreements. SC utilizes the Ethereum virtual machine to enable users to operate SC well within the blockchain network. The value of gas generally determines how the Ethereum system calculates fees [\[5,](#page-17-4)[23\]](#page-18-0). A certain amount of gas, which in turn is purchased using digital currency, is required to perform SC and handles a transaction. Hence, the actual transaction cost can be defined as in the equation below:

$$
Ether = gas price \times gas used
$$

The Ethereum platform predominantly consists of two types of accounts: contract accounts commanded by the contract code, and externally owned accounts (EOAs) controlled by private keys. EOAs are used to undertake ether-sending transactions or to initiate SC execution. Account nonce, sender signature, recipient address, gas limit, ether values, gas price, and the endpoint of the medical data are just a few of the factors that are included in an Ethereum transaction. An affiliated state database for the Ethereum blockchain is built on an IPFS-like Merkle-Patricia tree structure [\[25\]](#page-18-2). Essentially, we can design a blockchain framework using IPFS for a more robust and secure off-chain and on-chain storage of medical records. We implemented the proposed system using the Ethereum blockchain's smart contract architecture, resulting in an unambiguous, fine-grained access control mechanism that prohibits hacking and unauthorized access without the patient's consent.

#### *3.2. Distributed InterPlanFile System (IPFS)*

Within the P2P IPFS system, a cryptographic hash serves as a distinct fingerprint for each file. In this regard, the hash address is employed to make the contents immutable [\[11](#page-17-10)[,26\]](#page-18-3). In the IPFS file storage structure, Merkle DAGs combined Merkle trees with DAGs. The fundamental functionality of IPFS to access health information may be achieved by contentbased addressing rather than location-based addressing. By harnessing the IPFS structure, lowered bandwidth costs can be achieved, file download speeds can be improved, and a substantial amount of data may be transmitted without duplication, which can free up storage space. Additionally, IPFS is an immutable storage solution since the hash value of an IPFS file cannot be modified.

<span id="page-5-0"></span>Our system structure, as displayed in Figure 3, has the organization use three peer Our system structure, as displayed in Figure [3,](#page-5-0) has the organization use three peer nodes, with one acting as a validating peer node and the others as an ordering node for registering stakeholders. Multiple peers can access the same database in this system, which also uses IPFS for distributed data storage [\[27\]](#page-18-4). Multiple peers can be added to which also uses IPFS for distributed data storage [27]. Multiple peers can be added to various locations on different machines to test the system's scalability. This framework, various locations on different machines to test the system's scalability. This framework, which contains its own ledger and smart contract copies, provides access to ledgers for which contains its own ledger and smart contract copies, provides access to ledgers for smart contracts. smart contracts.



**Figure 3.** PCEHRM structure. **Figure 3.** PCEHRM structure.

Peer nodes are linked to the application, which then uses smart to update the ledger. Peer nodes are linked to the application, which then uses smart to update the ledger. Figure [4](#page-6-0) shows the data structure of the blockchain ledger after the integration of Figure 4 shows the data structure of the blockchain ledger after the integration of PCEHRM data fields, as it is intended to record only the information that patients wish to provide in a transaction. Peernode1, Peernode2, and Peernode3 are the three peer nodes in the in the organization, and each one has a copy of the ledger and a smart contract. organization, and each one has a copy of the ledger and a smart contract.

In this sense, the patient's profile, address and location, diagnoses, doctor recommendations, next review notes, physician's names, medication, scan and test reports, and hospital ID are all included in the healthcare records.

The following stakeholders make up the PCEHRM:

<span id="page-6-0"></span>

**Figure 4.** The data structure of the blockchain ledger of PCEHRM. **Figure 4.** The data structure of the blockchain ledger of PCEHRM.

#### **4. Record Owner**

In this sense, the patient's profile, address and location, diagnoses, doctor recommen-Patients retain their medical data, making them the owner of the record. To store the data, patients are required to acknowledge and sign an agreement on PCEHRM-SC in the healthcare required to acknowledge and sign an agreement on PCEHRM-SC in the Eutereum bioexenam. The entity networks permit patients to speeny access rights to their<br>healthcare information, defined by each PCEHRM-SC within its context. Table [3](#page-6-1) further **4. Record Owner**  describes the patient roles in detail. Ethereum blockchain. The chain networks permit patients to specify access rights to their

<span id="page-6-1"></span>Table 3. Patient roles.



### **5. Data Uploader**

ers. The primary responsibilities of the data uploaders include submitting the concerned The doctors/lab technicians may upload their patients' medical data to Data Uploadindividual's encrypted clinical data to the IPFS community and validating the preliminary transaction at the blockchain. This is further illustrated in T[ab](#page-6-2)le 4.

<span id="page-6-2"></span>**Table 4.** Doctors/lab roles.



# **Table 4.** Doctors/lab roles. **6. Data Users**

for further action, namely, hospitals, researchers, insurance companies, and doctors. In this Data users are defined as the parties that require patients' medical or clinical records context, the role-based access control approach in PCEHRM-SC specifies the mechanism for patients to grant access rights to data users.

#### *6.1. Data Encryption*

Cryptographic methods guarantee the privacy and integrity of blockchain data. Figure [5](#page-7-0) depicts the interaction between patients and their doctors while examining health records. The doctor initiates the process by requesting access permission to retrieve the information stored in the IPFS. Depending on the data fields requested, this generates a patient-centric view of the records rather than disclosing all the patient's information. The session key, Sk, is used to store the encrypted patient-centric view in IPFS and to retrieve records in

a finite period. After doctors and patients have received encrypted patient-centric views and Sk, doctors may decrypt the Sk and patient-centric views for the process of updating the record.

patient-centric view of the records rather than disclosing all the patient's information. The

<span id="page-7-0"></span>

**Figure 5.** Collaboration diagram between patient and doctor in PCEHRM. **Figure 5.** Collaboration diagram between patient and doctor in PCEHRM.

patient-centric view are automatically erased when a patient commits to his health record. By prohibiting complete access to health records without the patient's consent, this framework is advantageous in terms of protecting patients' privacy. Then, utilizing smart chain code operating on the system's back end, the hash value of the data is safely preserved on the Ethereum blockchain. The ledger will then notify the patient after the records were successfully created or updated. successfully created or updated. The patient would be notified after the revision of the record in IPFS. The Sk and

#### *6.2. PCEHRM-SC*

The process of role-based access is initiated once doctors request permission to the IPFS health record of patients, in which patients are in control to allow or revoke access for authorized users as shown in Figure 6. With the patient's consent, the doctor may create, view, and modify medical records before the patient commits the update to permanent storage. The patient-centric view of the health information can only be accessed by other participants in this health chain architecture for a given session, provided their ownership and object ID match the patients' [\[27\]](#page-18-4). These stakeholders include insurance agents, pharmacists, and researchers. As for laboratory technicians, they can only modify or update patients' medical records after the approval of the patient and the doctor. The regulations, access control, and privacy agreement are provided by authorization of smart contracts and are governed by the Ethereum blockchain. This methodology adheres to certain situations:

- 1. An access control regulation specifies the stakeholders' distinct profiles and defines their access rights.
- 2. After the patient allows access, the system defines the approved value to stakeholders, resources, action types, and environmental attributes.

In addition, the proposed solution segregates privacy attributes into three levels below:

Level 1: Patients are the sole party to access the health record.

Level 2: Approved stakeholders may be made available to the medical record.

Level 3: The permitted patient's caregiver has access to the health record in an emergency.



receive a key pair consisting of public and private keys. On that note, *Papubkn*, *Paprkn*,

By setting their privacy level, patients may manage the confidentiality of their data. our proposed framework consists of the construction of the construction of the ph, and model are calibrated to alter the terms during the transfer of authorizations to other stations in the number of doctors,  $\frac{1}{n}$ Prior to submitting a modified medical record to the chain network, the levels in our authorized participants. *r* data. *Appl. Sci.* **2023**, *13*, x FOR PEER REVIEW 10 of 20

# **6.3. PCEHRM Algorithm**

<span id="page-8-0"></span>thorized participants.

Our proposed framework consists of four stakeholders: Pa, D, Ph, and LT, which represent patients, doctors, pharmacists, and lab technicians, respectively. Table 5 shows [the](#page-9-0)se symbols in the algorithm functions. The n is the number of doctors, patients, health records, pharmacists, and lab technicians where  $n = 1, 2 ... N$ . Patients, medical professionals, and pharmacists are among the n stakeholders provides public key. All stakeholders will each receive a key pair consisting of public and private keys. On that note,  $\mathcal{P}apubk_n$ ,  $\mathcal{P}aprk_n$ ,  $\mathcal{D}pubk_{n}$  and  $\mathcal{D}prk_{n}$  are the public and private keys of the patient and doctor, respectively. rh rep-*Phone* is these *<u>l</u>* necords, *i*onals, *Payu* is will  $Papr \hat{R}_{n'}$ *Ply.* 

In Algorithm 1, the patient allows the doctor access to their health record based on<br> $CCTID$   $CCTID$ In Algorithm 1, the patient allows the doctor access to their health record based on<br>PCEHRM-SC. Hence, a patient-centric view of the health record is generated by the system. *P*<br>British Doctor Private Key<br>British Doctor Private Key *Phropa is generated by the system.*<br>Pharmachine Pharmachine Pharmachine Pharmachine Pharmachine Pharmachine Pharmachine Pharmachine Pharmachine Ph

nt-vaseu uata<br>pri contric can *Pacenta Centric Cent*<br>Pating whole *Pacence Patient* ystem.<br><sup>1</sup> data *p* data<br>Pacens whole enside of granting uncestived access to the patient's nearly record, as patient-centric can<br>enable users to view and update only the specific fields of HR instead of sharing whole<br>patient health records. *\_hsh* nth Health Record Hash Value Based on the doctor request, the patient-centric is queried for attribute-based data<br>instead of continuous properties of a case to the national health massed as nation contributed instead of granting unrestricted access to the patient's health record, as patient-centric can<br>anable users to view and undate only the specific fields of HP instead of sharing whole *HRn* patient health records. *Dpubkn* nth Doctor Public key **Philadelphia**  $\frac{1}{2}$ *HRn* nth Health Record *L*<sub>n</sub> negative *Laborator* negative *and*  $\alpha$  negative *continue con*tinues *Papuak of the Public Key Willie Key Williams & Williams & Williams & Williams & Williams* 

Essentially, the patient-centric view is a subset of the medical record. In accordance, the session. An encrypted session key for  $\mathcal{P}apubk_n$  and  $\mathcal{D}pubk_n$  is derived using the public key for patients and doctors, respectively. The session key  $s_k^*$  which can be sent to doctors is  $\mathbf{r}$  and  $\mathbf{r}$ ic key system creates a session key ( $S_k$ ) used by both patients and physicians within a particular also encrypted with a patient-centric view. instead of granting unrestricted access to the patient's health record, as patient-centric can enable users to view and update only the specific fields of HR instead of sharing whole *httic* view. **Department** networks network  $\mathbf{P}$ 

 $$^{10\, of\, 19}$$  Algorithm 1 calls the  $create\_Update\_HR()$  function of Algorithm 2 to start updating the  $\mathcal{H}_{R_n}$ . After the doctor's and  $\mathcal{P}_{\text{acenv}}$ 's session key have been decrypted, the modifications are uploaded into the updated patient-centric view  $(\mathcal{UP}_{\perp}$ *Pacenv<sub>n</sub>*).  $\frac{1}{2}$  in  $\alpha$  the ng uit<br>rations *Papubkn* nth Patient Public Key

**Symbols Definition**

key for patients and doctors, respectively. The session key *Sk* which can be sent to doctors

*Dpubkn* nth Doctor Public key

the IPFS and saved in blocks.

*Papubkn* nth Patient Public Key *Paprkn* nth Patient Private Key

**Symbols Definition** *Pan* nth Patient

enable users to view and update only the specific fields of HR instead of sharing whole

*HRn*

Based on the doctor request, the patient-centric is queried for attribute-based data

*\_hsh* nth Health Record Hash Value

Based on the doctor request, the patient-centric is queried for attribute-based data

*Dpubkn*, and *Dprkn* are the public and private keys of the patient and doctor, respectively.

*LTn* nth Lab Technician

receive a key pair consisting of public and private keys. On that note, *Papubkn*, *Paprkn*,

The encrypted *HRn* is decoded once the system is updated, acquired by decryption of

instead of granting unrestricted access to the patient's health record, as patient-centric can

enable users to view and update only the specific fields of HR instead of sharing whole

Algorithm 1 calls the *create\_Update\_HR()* function of Algorithm 2 to start updating

In Algorithm 1, the patient allows the doctor access to their health record based on

*\_hsh* nth Health Record Hash Value

The encrypted  $\mathcal{H}R_n$  is decoded once the system is updated, acquired by decryption of The encrypted  $\mathcal{H}_{\mathcal{R}_n}$  is decoded once the system is updated, acquired by decryption of<br>the encrypted private key using the patient's password, and appended to the encrypted<br> $\mathcal{H}_{\mathcal{R}}$ .  $D_1$  *Du* and  $n_a$ . Then also step, the  $M_n$  is saved in it to after the patient committed by the step of  $S$  and  $\mathcal{L}_{\text{C}}$  of the Session Centric Lemma Contribution Communical, it intinctuately clases the  $\mathcal{L}_{k}$  and  $\mathcal{L}_{\text{C}}$  and  $\mathcal{L}_{\text{C}}$ the IPFS and saved in blocks.  $\alpha$  and  $\alpha$  is commuted, it in the case are  $\epsilon_k$  and  $\alpha$  are  $\epsilon_k$  and  $\alpha$  are  $\alpha_k$ . In the Ethereum blockchain, the health record hash value  $\beta R_{\mu}$  fash is generated by  $v_{\text{P}\_\text{Pacenv}}$ . For the last step, the  $H_{\text{R}}$  is saved in IPFS after the patient commits to the updates. Then, once the health record  $\mathcal{H}_{R_n}$  is committed, it immediately ceases the  $S_k$  and  $\mathcal{H}_{R_n}$ . Then, once the health record  $\mathcal{H}_{R_n}$  is committed, it immediately ceases the  $S_k$  and  $\overline{\text{S}}$  nth Session Key *Paper 100* nth Patient Private Reset *Pr*ypted to the *Pacerby* nted by *acv<sub>n</sub>*. In the Ethereum blockchain, the health record hash value  $\mathcal{HR}_{n}\_hash$  is generated by<br>health record hash value  $\mathcal{HR}_{n}\_hash$  is generated by plates. Then, once the health record  $\mathcal{H}_{n}$  is saved in 11.5 and the patient commits to the plates. Then, once the health record  $\mathcal{H}_{n}$  is committed, it immediately ceases the  $S_{\ell}$  and the IFF<sub>3</sub> and saved in Diocks.  $p$ uates. Then, once the health record  $\pi x_n$  is commuted, it immediately ceases the  $\sigma_k$  and

<span id="page-9-0"></span>Table 5. Symbols in the algorithm functions. Table 5. Symbols in the algorithm functions. **Definitions Definition Definition** *Dpubkn* nth Doctor Public key **Symbols in the algorithm functions.** 

*Dn* nth Doctor

*HRn* nth Health Record



#### *Mearithm 1. System\_Function()*. The *HRn* is saved in IPFS and *HRn* is saved in IPFS and patient commitment commits to the patient commitment commits to the patient commitment commitment commitment commitment commitment  $\frac{1}{\epsilon}$ algorithm 1 calls the *created* function of Algorithm 2 to start update  $\mathcal{L}$ updates. Then, once the health record *HRn* is committed, it immediately ceases the *Sk* and *Aloorithm 1. System Function() \_hsh* nth Health Record Hash Value  $\sum_{i=1}^n$  and  $\sum_{i=1}^n$  and  $\sum_{i=1}^n$  and  $\sum_{i=1}^n$  access to the doctor access to the doctor based on  $\sum_{i=1}^n$  and  $\sum_{i=1}^n$  and  $\sum_{i=1}^n$  and  $\sum_{i=1}^n$  and  $\sum_{i=1}^n$  and  $\sum_{i=1}^n$  and  $\sum_{i=1}^n$  an Algorithm 1. System\_Function() **Symbols Definition** *Phn* nth Pharma *LT* nth Lab Technician *L* nth Lab Technician **Lab Technician Lab Technician Control** <u>Dan Doctor Doctor De Barbara (Barbara de Barbara de Doctor Doctor De Barbara de Doctor Doctor De Doctor De Do</u><br>De Doctor Doctor De receive a key pair consisting of public and private keys. On that note, *Papubkn*, *Paprkn*, where  $P$  $\mathbf{A}$ *Appl. Sci.* **2023**, *13*, x FOR PEER REVIEW 10 of 20 *Dpubkn*, and *Dprkn* are the public and private keys of the patient and doctor, respectively.

**Input:** Doctor  $\omega_{n'}$  with their Public key  $\Omega_{n'}$  with their Private key  $\Omega_{n'}$  with session key  $S_{\ell}$  of  $HR_n$  Health\_Record. Patient  $Pa_n$  with their Public  $Papubk_{n'}$  and Private key  $Paprk_n$ . *R* proton, Health Internet step, the last step and the patient computer the patient of  $\mathbb{Z}_{q}^{H}$ . The encrypted once the system is decoded on  $\mathbb{R}^n$  is decoded on  $\mathbb{R}^n$  is updated, and decryption of  $\mathbb{R}^n$  $\frac{1}{\sqrt{2}}$   $\frac{n}{\sqrt{2}}$  **and**  $\frac{n}{\sqrt{2}}$   $\frac{n}{\sqrt{2}}$  **and**  $\frac{n}{\sqrt{2}}$   $\frac{n}{\sqrt{2}}$  **and**  $\frac{n}{\sqrt{2}}$  **and \frac{n}{**  $\frac{1}{\mu}$  calls the *coreated*  $\frac{1}{\mu}$ on key using the patient  $\mu$ **Constant Control**<br> **Constant Constant Public Key**  $\mathcal{D}pubk_n$ **, with their Private key**  $\mathcal{D}prk_n$ **, with session key<br>
also Health Becord, Bationt**  $\mathcal{D}a$ **, with their Public**  $\mathcal{D}awbb$ **, and Private key**  $\mathcal{D}awb_n$  $S_k$  of  $HR_n$  Health\_Record. Patient  $Pa_n$  with their Public  $Papubk_{n'}$  and Private key  $Paprk_n$ .<br>Output: Boolean (True or False) **Input:** Doctor  $\mathcal{D}_{n'}$  with their Public key  $\mathcal{D}pubk_n$ , with their Private key  $\mathcal{D}prk_n$ , with session key  $S_k$  of  $HR_n$  Health\_Record. Patient  $Pa_n$  with their Public  $Papubk_n$ , and Private key  $Paprk_n$ . **Output:** Boolean (True or False) *Sk* nth Session Key  $Paprk_n$ . **Input:** Doctor  $\mathcal{D}_{n'}$  with their Public key  $\mathcal{D}pubk_{n'}$  with their Private key  $\mathcal{D}prk_{n'}$ , with session key  $S_k$  of HR, Health Record. Patient 4 and Rey  $2F^{\mu\nu}$  with their Public Papubk<sub>n</sub>, and Private key Paprk<sub>n</sub>.<br>Output: Realth Record. Patient  $a_n$  with their Public Papubk<sub>n</sub>, and Private key Paprk<sub>n</sub>. **Symbols Definition Talse Symbols** in the algorithm functions. receive a key pair consisting of public and private keys. On that note, *Papubkn*, *Paprkn*, pharmacists are among the n state public key. All states  $p$ *Paprk*.  $\frac{1}{n}$ **Panned Line Collection Collection**  $\mathcal{L}_{n}^{w}$  with their Collection  $\mathcal{L}_{n}^{w}$  and Collection City is **Boolean** (True or False)

**Symbols Definition**

- 1. Function for storing and updating health records. the *HR* and <sup>Pacen</sup> the doctor's and **Pacenter** session key have been decrypted, the model of model is model to modificate the model of model in the model 1. **Surput: Boolean** (True or False)<br>1. Function for storing and updating health records.<br>2. **For** user  $U$  have Access permission to HR  $\frac{1}{2}$ . Function for storing and updating health records. *Pacence Pacence Pacence*<br>Centric View Pacence 1. Function for storing and updating health records.<br>2. For user  $I$  have Access permission to HR n records.<br><sub>I</sub>D **L** nth L<sub>ab</sub> Technician is the Lab Technician in the Lab Technician ds. *Dpubkn*, and *Dprkn* are the public and private keys of the patient and doctor, respectively.
- 2. For user  $\nu$  have Access permission to HR The encary product on contract  $\theta$  is decoded on  $\theta$  is decryption of  $\theta$  is updated, and acquired by decryption of  $\theta$ are uploaded into the updated patient-centric view (*UP\_ Pacenvn*). 1. Function for storing and updating nearth records.<br>
2. **For** user  $U$  have Access permission to HR<br>
3. Check PCEHRM-SC<br>
4. **If** (permission = "Crant" *k*-*k*- rele--"Dector") then 1. Function for storing and updating nearly records.<br>2. **For** user  $U$  have Access permission to HR<br>2. Check PCEHPM CC *Pape Access permission to TIR*<br>RM-SC **UPDATE Pacent intervalse Patient-Centric View Patient** mission to HK *Philadelphia Philadelphia Philadelphia* **Division in the Doctor Doctor Doctor** Doctor D 2. For user  $U$  have Access permission to HR<br>2. For user  $U$  have Access permission to HR **HR** nth HR *Phine Phine Pharmaceutical* Pharmaceutical Pharmaceutica
	- 2. To user C have Access permission to The updates. Then, once the health record *HRn* is committed, it immediately ceases the *Sk* and 2. 3. *Department Control of the Control of the Department Control of th* 3. Check PCEHRM-SC<br>4. **If** (parmission-"Crapt" *P-P* relative "Dector") than **LTERM-SC**
	- 4. If (permission=="Grant" & & role=="Doctor") then 3. Check Technon = "Grant" & & role== "Doctor") then *b*  $\ln$  nth Health Record Hash Value Hash Val *Sk* nth Session Key 3. Check PCEHKM-SC<br>4. If (permission=="Grant" && role=="Doctor") then *PPFS HRn* nth Health Record *Papubkan* nth Papuakan nth Public Key American Public Key Ame *Paper Parkin* nth Patient Private Key *Paper and Paper and Private Keyer* Assembly Private Keyer As )) formulation **System**  $\frac{1}{2}$ *(permission=="Grant" && role=="Doctor")* then
	- 5. Create  $Pacenv_n$  for  $HR_n$  in IPFS updates. Then, once the health record *HRn* is committed, it immediately ceases the *Sk* and Create Pacent, for  $\mathcal{H}R_n$  in IPFS 5. Create Pacent, for  $HR_n$  in IPFS **Papuak nth Papuak nth Patient Public Key Additional Public Key Additional Public Key Addition**
	- Pacent  $\psi_n$  of  $\mathcal{F}(\mathcal{X}_n)$  in T<sub>1</sub> 3<br>
	Pacent  $\psi_n \to \text{Decryption}$  (Encryption ( $\mathcal{H}\mathcal{R}_n$ ))  $\text{ion } (\mathcal{H}R_n)$ ) 6.  $\qquad \qquad \mathcal{C}$  *Create*  $\mathcal{C}$  *at the*  $\eta_n$  of  $\mathcal{F}(\mathcal{X}_n)$  if  $n \to 0$  *Cacenv*<sub>n</sub>  $\to$  Decryption (Encryption ( $\mathcal{H}(\mathcal{X}_n)$ ) 6.  $P_{\text{accept}} \rightarrow \text{Decryption}(\text{Encryption}(\mathcal{H}^{\mathcal{R}}_{n}))$  $\binom{1}{n}$ 6.  $H_{\mathcal{R}_n}$ ) *Dpubkn* nth Doctor Public key 6.  $P_{\text{accept}} \to \text{Decryption}$  (Encryption ( $\mathcal{H}R_n$ ))<br>*7* Create S<sub>c</sub>  $\mathbf{S}$  becomes  $\mathbf{S}$ 
		- the system create  $S_k$  (*Sk)* used by both patients and physicians with a particle- $\frac{1}{\alpha}$  create  $\frac{1}{\alpha}$  used by both patients and physicians with patients and physicians with a particle- $\frac{m}{2}$  create  $S$ .  $\mathcal{T}$ . Secretar session. An encrypted session key for  $P_k$  is derived using the public the public the public the public the public term is derived using the public term is derived using the public term in the public ter **ultar session. An encrypted sets** session and  $P_k$  is derived using the public of public  $P_k$  is derived using the public the public the public of public the public the public the public term of public the public term of  $\overline{z}$  session. An encrypted session is derived using the public of public  $\overline{z}$  is derived using the public the public the public the public the public the public term is derived using the public term is derived usi key for patients and doctors, respectively. The session  $S_k$  which can be sent to doctors,  $S_k$ 7. **Create**  $S_k$  $\frac{1}{2}S_{\xi}$  $S_k$  $S_k$

of *HRn*

8. Send Encrypted (Papubk<sub>n</sub> (S<sub>k</sub>), Dpubk<sub>n</sub>(S<sub>k</sub>), Pacenv<sub>n</sub>(S<sub>k</sub>)) to Pa<sub>n</sub>,  $k = \frac{1}{\sqrt{N}} \sum_{n=1}^{\infty} \sum_{n$ ular session. An encrypted session. An encrypted session and *Papuakan is derived* using the public of public the public the public of public the public of public the public term is derived using the public term in the pub 8. Send Encrypted ( $\mathcal{P}$ apub $k_n(S_k)$ ,  $\mathcal{P}$ pub $k_n(S_k)$ ,  $\mathcal{P}$ acen $v_n(S_k)$ ) to  $\mathcal{P}$ a<sub>n</sub>,  $\mathcal{D}_n$  and  $\mathcal{P}$ acen $v_n$ .  $\nu$ , session. An encrypted session and  $P_k$  for  $P_k$  for  $P_k$  is derived using the public term of  $P_k$  is defined using the public term of  $P_k$  is defined  $\sum_{n=0}^{\infty}$  and  $\sum_{n=0}^{\infty}$  patients  $\sum_{n=0}^{\infty}$  and  $\sum_{n=0$  $k_{\text{c}}$  for patients and doctors, respectively. The sent to do to do to do to do to do can be sent to do can be 7. Create  $S_k$ <br>
8. send Encrypted (*Papubk<sub>n</sub>* ( $S_k$ ), *Opubk<sub>n</sub>*( $S_k$ ), *Pacenv<sub>n</sub>*( $S_k$ )) to *Pa<sub>n</sub>*, *Sk* nth Session Key 6. *Pacenvn HRn* 7. Create **Symbols Definition** *\_hsh* nth Health Record Hash Value *Paprkn* nth Patient Private Key 2. Create  $S_k$ <br>
8. send Encrypted (Papubk<sub>n</sub> (S<sub>k</sub>), Dpubk<sub>n</sub>(S<sub>k</sub>), Pacenv<sub>n</sub>(S<sub>k</sub>)) to Pa<sub>n</sub>,  $\text{Create } S_k$  and UP data Patient-Centric View Patient-Ce *Papubkn* nth Patient Public Key  $Pa_{n'}$ *LT<sub>n</sub>* intervals and Lab Technician and Lab Techni *Ph<sub>n</sub>* nth Ph<sub>n</sub>  $\eta \wedge \eta'$ ,  $\eta \wedge \eta''$ ,  $\eta \wedge \eta''$ ,  $\eta \wedge \eta''$  $\mathcal{L}_{\ell}$ <br>Encrypted (Panubb (S.) Omubb (S.) Paceng (S.)) to Pa  $\frac{d}{dx} \left( \frac{d}{dx} \left( \frac{d}{dx} \left( \frac{d}{dx} \right) - \frac{d}{dx} \right) - \frac{d}{dx} \left( \frac{d}{dx} \left( \frac{d}{dx} \right) \right) + \frac{d}{dx} \left( \frac{d}{dx} \left( \frac{d}{dx} \right) \right)$ **Create**  $o_k$ <br>**Paper Programed** *(Danubb*  $(S)$ ) Drubb $(S)$ ) Dreams  $(S)$ ) to  $p_2$ Send Encrypted  $\langle u \psi u v_{n} \rangle_{n}$  ( $\langle v_{k} \rangle_{n}$ ,  $\psi$ *publ<sub>n</sub>* $\langle v_{k} \rangle_{n}$ ,  $\psi$ *uthln<sub>n</sub>* $\langle v_{k} \rangle_{n}$ ) to  $\psi$ *u<sub>n</sub>*,

is also encrypted with a patient-centric view.

*HRn*

- 9.  $\mathcal{D}_n$  and  $Pacenv_n$ .  $\mathcal{D}_n$  and *Pacenc<sub>n</sub>*. racenv<sub>n</sub>.<br><u>Internatient-Centric View</u> Pacenv<sub>n</sub>. 9.  $\mathit{Pacenv}_n$ . 9. *Dn*  $\mathcal{L}_n$  and  $\mathcal{L}_n$  in  $\mathcal{L}_n$
- $\mathcal{D}_n$  and *Tatent<sub>n</sub>*.<br>10. create\_Update\_HR() de algorithm 1 calls the *create\_Update\_HR()* function of Algorithm 2 to start updating the Algorithm 2 to start updatin  $\mathcal{L}_n$  and  $\mathcal{L}_m$  function  $\mathcal{L}_n$ .  $\begin{array}{c}\n \nu_n, \\
 n\n\end{array}$ eate\_Update\_HR()<br> **Philadelecture** Pharmaceutic Company Phone Containers
- $H\mathbb{R}_n \to \left[\text{(Decryption } \text{Papubr}\right]$  (Encrypted  $\text{Papub}\left(\mathcal{H}\mathbb{R}_n\right)$ ) + Encryption ( $\mathcal{UP}\_\text{Pacenv}_n$ )] the *HRn*. After the doctor's and *Pacenvn's* session key have been decrypted, the modifications Algorithm 1 calls the *create\_Update\_HR()* function of Algorithm 2 to start updating  $\lim_{n \to \infty} \frac{H(x)}{n}$  ( $\lim_{n \to \infty} \frac{H(x)}{n}$  ( $\lim_{n \to \infty} \frac{H(x)}{n}$   $\lim_{n \to \infty} \frac{H(x)}{n}$   $\lim_{n \to \infty} \frac{H(x)}{n}$   $\lim_{n \to \infty} \frac{H(x)}{n}$ 10. create\_Opdate\_FIK()<br>
11.  $\mathcal{H}R_n \to [$ (Decryption  $\mathcal{P}apubr k_n$  (Encrypted  $\mathcal{P}apubk_n$  ( $\mathcal{H}R_n$ )) + Encryption ( $\mathcal{V}P\_$ Pacen $v_n$ )]<br>
12.  $\mathcal{P}a_n \to$  Commit (IPFS ( $\mathcal{H}R_n$ )) 10. create\_Update\_HK()<br>  $\mathcal{H}R_n \to \text{[(Decryption \textit{Papubrk}_n \text{ (Encrypted \textit{Papubk}_n (\textit{HR}_n)) + Encryption (\textit{VP\_Pacenv}_n)]}$  $\sum_{n=1}^{\infty}$  (Decryption  $\alpha \mu \nu \nu \kappa_n$  (Encryption  $\alpha \mu \nu \kappa_n$  (Fig. ) + Encryption ( $\alpha \nu \nu \nu \nu \kappa_n$ ) *Pacenvn* nth Patient-Centric View  $U_{\mu\nu}$  (Encrypted *Papuor<sub>n</sub>* (*J*<sub>1</sub>x<sub>n</sub>)) + Encryption (*Cv*\_*Pacenv*<sub>n</sub>)]  $\mathcal{P}_{\mathbf{C}}$  and the health record is generated by the system of the system of the system is generated by the system is generated by the system of the system is generated by the system is generated by the system is gene tte\_Update\_HR()<br>*fR\_* → [(Decryption *Papubrk\_* (Encrypted *Papubk\_ (HR\_)*) + Encryption (UP\_*Pacenv*\_)]  $Pacenv_{n}$ )] 9. *Dn* 11.  $B(\mathcal{H}\mathbb{R})$  )  $P(\text{even})^{\text{per}}$  (Figure  $\mathcal{P}(\text{even})^{\text{per}}$ ), and  $\mathcal{P}(\text{even})^{\text{per}}$  and  $\mathcal{P}(\text{even})^{\text{per}}$ ),  $\mathcal{P}(\text{even})^{\text{per}}$  $\Phi$ <sub>D</sub>  $\Phi$ <sup>2</sup>  $\Phi$  (*H* $\Re$  )) + Fncryption (*U* $\Re$  *Pacenu*) I  $\sum_{n=1}^{\infty}$   $\sum_{n=1}^{\infty}$   $\binom{n-1}{n}$ ,  $\sum_{n=1}^{\infty}$   $\sum_{n=1}^{\infty}$   $\sum_{n=1}^{\infty}$ 10. create\_Update\_HR()<br>
10. create\_Update\_HR() *\_hsh* nth Health Record Hash Value *Dpubkn* nth Doctor Public key **DOCT**  $\mathcal{L}_{n}$  (EXCTYPIEG  $\mathcal{L}_{n}$  (*DP*<sub>n</sub><sub>n</sub>) + EXCTYPIION (*OC\_CELENC<sub>n</sub>*)] *UP\_Pacenvn* nth Update Patient-Centric View *HR*<sub>n</sub> (Encrypted *Vapubr*<sub>n</sub> (HR<sub>n</sub>)) + Encryption (UP\_*Pacenv*<sub>n</sub>)]  $F = (10 \frac{(6.66)}{N}) F = (9/2)^{2}$ *Packypied*  $\alpha$  *apubi* $R_n$  (*PP* $R_n$ ) + *Packypiion* (*PP*<sub> $\alpha$ </sub> *Callent*<sub>n</sub>)] *UP\_Pacenvn* nth Update Patient-Centric View *ed Papubr<sub>ri</sub>* (HR<sub>n</sub>)) + Encryption (UP\_*Pacenv<sub>n</sub>)*] *HRn \_hsh* nth Health Record Hash Value *UP\_Pacenvn* nth Update Patient-Centric View  $H(X_n)$ ) + Encryption (UP\_Pacen $v_n$ )] *P<sub>n</sub>*  $\therefore$  (4)  $\text{Lncry}(U \cup T_{\text{L}} \cup \text{Lnciv})$  $\mathcal{L}H_{\mathcal{K}_n} \to$  [(Decryption *Tapuor*<sub>n</sub><sub>,</sub> (Encryption *Tapuor*<sub>n</sub> ( $\mathcal{L}H_{\mathcal{K}_n}$ ) + Encryption *UP\_Pacenvn* nth Update Patient-Centric View 11.  $\mathcal{HR}_n \to \text{[(Decryption \, \, \text{Capubr}k_n \, (\text{Encrypted} \, \, \text{Papub}k_n \, (\text{HR}_n)) + \text{Encryption} \, (\text{VP\_Pacerv}_n)]$

patient health records.

- 12.  $\mathcal{P}a_n \to \text{Commit (IPFS } (\mathcal{H}^n_{\mathcal{R}_n}))$ 12.  $a_n \rightarrow \text{Commit (IPFS } (\mathcal{H}R_n))$ <br>
12.  $a_n \rightarrow \text{Commit (IPFS } (\mathcal{H}R_n))$  $T_{n}$  is decomposited in  $\mathcal{O}(10^{-10})$  is decoded  $\mathcal{O}(n)$ . 12.  $\mathcal{P}a_n \to \text{Commit (IPFS } (\mathcal{H}R_n))$ <br>13. IPES  $\to \mathcal{H}R$  fish  $\tilde{h}$  $\mathcal{L}_{\mathcal{H}}$ *UP\_Pacenvn* nth Update Patient-Centric View  $\frac{1}{\sqrt{1+\epsilon}}$  (i.e.  $\frac{1}{\sqrt{1+\epsilon}}$  ), the patient access to the doctor  $\frac{1}{\sqrt{1+\epsilon}}$  $S(\lambda_1 \lambda_2)$ 12.  $\mathcal{P}a_n \to \text{Commit (IPFS } (\mathcal{H}R_n))$ 12.  $H_{\mathcal{R}_n}$ )
- 13. IPFS  $\rightarrow$   $HR_{\pi}$  lish  $H \to H \Lambda_{n}$  is decoded on concern is updated, and system is updated, and  $\Lambda_{n}$  is updated, and  $\Lambda_{n}$ 15. IFFS  $\rightarrow$   $\pi \frac{m}{n}$  using the particle to the encrypted to the  $PS \to HR_{n-hsh}$ <br> $PS \to FR_{n-hsh}$ *\_hsh* nth Health Record Hash Value Hash Value
- $\frac{H R_{n}}{R_{n}}$  fish  $\rightarrow$  Ethereum Blocks the encrypted private key using the patient's particle particle particle in the encrypted to the encryp 14.  $\mathcal{H}R_{n-k}$  fish  $\rightarrow$  Ethereum Blocks *UP\_ Pacence in IPFS after step*, the last step, the *HR<sub>n</sub>* is saved in IPFS and patient commitment 14.  $\mathcal{H}R_{n}$  fish  $\rightarrow$  Ethereum Blocks<br>15. **Poture True**  $\frac{d}{dt}$  $\sum_{n=1}^{\infty}$   $\sum_{n=1}^{\infty}$   $\sum_{n=1}^{\infty}$  $R_{\mu}$  hsh  $\rightarrow$  Ethereum Blocks enable users to view and update only the specific fields of HR instead of sharing whole **b**cks  $\sum_{k=1}^{\infty}$ *Pacence Pacence Pacen*  $\sum_{i=1}^{n}$ PCEHRM-SC. Hence, a patient-centric view of the health record is generated by the sys-*R<sub>p</sub>\_nsn* → Ethereum Blocks<br>https://www. 14.  $\mathcal{H}R_n$   $\stackrel{\text{def}}{=}$  *HR<sub>n</sub>*  $\stackrel{\text{def}}{=}$  *R<sub>n</sub>*  $\stackrel{\text{def}}{=}$  *Rn*<sub>n</sub>  $\stackrel{\text{def}}{=}$  *F Papubkn* nth Patient Public Key **Papers** nth Papers **P** 14.
- $t_{\text{tot}}$  the encrypted private key using the parameter  $p_{\text{tot}}$  and appendix parameter  $t_{\text{tot}}$ the encrypted private key using the patient's particle parti  $\frac{m}{\hbar}$  Return True  $t_{\text{max}}$  the patient private key using the parameters  $\frac{m}{\sqrt{2}}$ **UP\_Pacencer** Step, the **HR**<sub>n</sub> is saved in IPFS and patient commitment commitm **UP\_PACERS** Step, the *HRn* is saved in IPFS and the patient commitment commitm **UP\_NEXTERS after steps, the IPFS after the patient commitment commitment committee in IPFS after the patient commitment commitment committed, it is consi UP\_COPACERS**<br>15. **Else**<br>16. **Else** *u*<br>15 **Beturn** True updates. Then, once the health record *HRn* is committed, it immediately ceases the *Sk* and updates. Then, once the health record *HRn* is committed, it immediately ceases the *Sk* and ence the users to view and update only the specific fields of  $H_0$  instead of sharing whole sha  $\frac{d\tau}{dt}$ **Paper 1996**<br>Prima True *Department* Department Doctor Private Key Association Private Key Associati *LTD*  $\alpha$  is the Lab Technician of  $\alpha$  Technician of  $\alpha$  Technician of  $\alpha$  Technician of  $\alpha$  Technician of  $\alpha$
- *UP\_ Pacenca* step, the *HR*<sub>n</sub> is saved in IPFS and patient commitment commitm **UP\_C\_Pacencers**. For the last step, the last step, the *HRn* is saved in IPFS after the patient commitment comm **UP\_Pacencers**. For the *HRn* is saved in IPFS after the patient commits to the patient commitment commitment commits to the patient commitment commitment commitment commitment commitment commitment commitment commitment c **UP\_Pacenvil. For the last step, the interval.** For the *HRn* is saved in IPFS after the patient commitment comm **UP\_Pacenvil. For the last step, the last step, the initial step, the patient commitment c** *UP\_ Pacenvn*. For the last step, the *HRn* is saved in IPFS after the patient commits to the updates. Then, once the health record *HRn* is committed, it immediately ceases the *Sk* and updates. Then, once the health record *HRn* is committed, it immediately ceases the *Sk* and  $i$ s also encrypted with a patient-centric view. The patient-centric view  $i$ 16. **Else** 16. **Else**
- updates. The health record record recording the health record-<br>19 is committed, it is committed, it is considered the *Sk and Sk and Sk and Sk and Sk and Sk* and Sk and Sk and 17. Permission=Deny updates. Then, once the health record *HRn* is committed, it immediately ceases the *Sk* and *Packy* **Packain, the HRN**<br>10 **D** otherm blockchain, the health record has health record has health in the health is generated by the health is generated by the health is generated by the health in the health is generated *Pacvn*. In the Ethereum blockchain, the health record hash value *HRn\_hash* is generated by  $\mathsf{n}$ =Deny  $P_{\rm env}$  $\sum_{i=1}^{\infty}$  $\mathbf{B}$ ased on the doctor request, the patient-centric is  $\mathbf{B}$ 17.<br>
18  $\mathbb{R}^n$  $\blacksquare$  $\Gamma$ CEHRM-SC. Hence, a patient-centric view of the system of the system  $\Gamma$
- **Pacific Ethereum blockchain, the health record has health record has health record has had if generated by Find if**  $\mathbf{F}$  **is generated by**  $\mathbf{F}$  **is generated by**  $\mathbf{F}$  **is generated by**  $\mathbf{F}$  **is generated by \mathbf{F Packain, the example of the health record has health record has health record has health record has health is generated by the health is gen Packain, the Ethereum blockchain, the health record has hea Packwain, the Ethereum blockchain, the health record has health record has health record has have** *HRn***<sub>ha</sub>sh is generated by the health record has have** *HRn***hamsh in the health record has health record has have been also** 17. Termission-Beny<br>18. **Return** False **Packurn. Ealth record has health record h** *Permission=Deny*<br>18. **Return** False<br>19. **F** *Packground has health record by the IPFS and saved in blocks.* enable users to view and update only the specific fields of  $\mathbb{R}$  is specific fields of sharing whole shar the **Hernandie** and **Pacence** in a session key have been decrypted, the modifications in the model of modifications of modifications in the model of modifications of model of model of model of model of model of model of mo esturn-Falsentially, the patient-centric view is a subset of the medical records of the system creates a session key (*Sk)* used by both patients and physicians with a particle and physicians within a particle and physicians within a particle and physicians with a particle and physicians with a particle a Essentially, the patient-centric view is a subset of the medical records of the medi  $\mathbf{e}_i$  and update only the specific fields of  $\mathbf{e}_i$  fields of sharing whole specific fields of sharing whole specific fields of sharing whole sharing whole specific fields of sharing whole specific fields of sharin instead of granting unrestricted access to the patient of granting unrestricted access to the patient-centric can patient-centric can be patient-centric can be patient-centric can be patient-centric can be patient-centric
- the IPF and in blocks. **Electrical in blocks.** The IPF and save in blocks. The IPF and save in blocks. The IPF and September 2016. In the IPF and September 2016. In the IPF and September 2016. In the IPF and September 2016 19. **End if** are uploaded into the updated patient-centric view (*UP\_ Pacenvn*). the system creates a session key (*Sk)* used by both patients and physicians and physicians with a particle and physicians with a the system creates a session key (*Sk*) used by both patients and physicians within a partic-*Pacence Pacence Patient-Centric View Pacence Pacence* **UPDATE Package Patient-Centric View Patient-Centric V** *Paper Reserves* **Paper Private Key Priv**
- **End For** *Papubkan session.* ular session. An encrypted session key for *Papubkn* and *Dpubkn* is derived using the public *HRn* 18. **Return** False 20. **End For Department**  $\overline{D}$  **D**  $\overline{D}$  **D**
- the system creates a session key (*Sk*) used by both patients and physicians within a partic-The encrypted *HRn* is decoded once the system is updated, acquired by decryption of the encrypted private key using the patient's password, and appended to the encrypted 21. End Function 18. **Return** False  $\mathop{\rm on}\nolimits$ key for patients and doctors, respectively. The session key sent to doctors, respectively. The sent to doctors, respe the system creates a session key (*Sk*) used by both patients and physicians within a partic-**UPDATE** Parameters **D**<br>**E**unction *HRn \_hsh* nth Health Record Hash Value *\_hsh* nth Health Record Hash Value 20. **End For** *Dependent Department D*  $\sum_{i=1}^{\infty}$ patient health records. enable users to view and update only the specific fields of HR instead of sharing whole

are uploaded into the updated patient-centric view (*UP\_ Pacenvn*).

the encrypted private key using the patient's password, and appended to the encrypted

the *HRn*. After the doctor's and *Pacenvn's* session key have been decrypted, the modifications

patient health records. Essentially, the patient-centric view is a subset of the medical record. In accordance,

*Paprkn* nth Patient Private Key *Dpubkn* nth Doctor Public key

**Table 5.** Symbols in the algorithm functions.

*HRn* nth Health Record

The encrypted *HRn* is decoded once the system is updated, acquired by decryption of

*Dpubkn* nth Doctor Public key

Based on the doctor request, the patient-centric is queried for attribute-based data

In Algorithm 1, the patient allows the doctor access to their health record based on



**Table 5.** Symbols in the algorithm functions.

*Dn* nth Doctor

#### *UPDATE Protocol Operation*  $\Omega$  Operation  $\Omega$  instead of granting unrestricted access to the patient  $\Omega$  $\mathbf{r}$ patient health records.  $P<sub>peration</sub>$ In Algorithm 1, the patient allows the patient allows the doctor access to  $\mathcal{P}_{\mathcal{A}}$  , a patient-centric view of the health record is generated by the system of the system is generated by the system of the system is generated by the system of the system is generated by the system is generat natio:<br>. *Paprkn* nth Patient Private Key  $\mathbf{P}(\mathbf{c}) = \mathbf{p}(\mathbf{c})$ tem. PCEHRM-SC. Hence, a patient-centric view of the health record is generated by the sys-tem. **7. PCEHRM Protocol Operation**  $P$ CEE HRM-SC. Hence, a patient-centric view of the health record is generated by the system of the system  $\sim$  $I_n$  and patient allows the doctor access the doctor access to the doctor  $P(\mathcal{P}_\text{C})$  is generated by the health record is generated by the system of the system is generated by the system In Algorithm 1, the patient allows the doctor access to their health record based on PCCI UP EXTENDERMENT - A patient-centric view of the health record is generated by the system of the system is generated by the system of the system is generated by the system of the system is generated by the system of th

tem.

**FRAPT PERTIME CORDING TO A 2019 VALUE 2019**<br>Interest architecture consists of two parts of development environments, back-In Algorithm 1, the patient allows the doctor and the doctor and the doctor access to the doctor and the doctor access to the doctor and the doctor and the doctor access to the doctor and the doctor and the doctor and the on a intel $^{\circ}$ Core<sup>TM</sup>i7  $^{\circ}$  3.38 GHz processor and 16 GB of RAM. For the back-end the state state and system creates a session with the session with the state of the place of the place of the p<br>ht, we used the Ethereum Platform and a Windows Foundation project, while velopment was implemented using JavaScript, CSS3, HTML5, and ReactJS. example. The subset of the same state of the second terms of the second teams of the second the second term of<br>expansion of the second terms of the second terms of the second terms of the second teams of the second terms o enable users the specific specific fields of  $\frac{1}{2}$  and  $\frac{1}{2}$  secondary to construct the sharing patient and sharing whole sharing whole sharing whole sharing whole sharing whole sharing whole sharing a more user-fr then in a libre discrimination of Algorithm 2 to 2 to 1 the *Servers* were<br>cute back-end programming while a database was employed for Front-end of the programming while a database was employed for from end.<br>On top of that, Truffle Framework, Ganache (Ethereum Blockchain), NodeJS ries, as well as Metamask Browser extension (to connect Browser to Blockchain) lopted for this experiment. Solidity programming language was adopted for the the matter and on permanent century programming anguage was and presented and the stabilished ransmitted an encrypted medical record to the network, returning a distinct hash value associated with the uploaded record. Then, by specifying the IPFS hash, the ial medical record attributes, and the patient Ethereum public key, we modified the medical record difficults, and the patient Entered in paths key, we medined<br>tions on the blockchain. HTTP methods, for instance, POST, GET, PUT, and DELETE ggered once clients consume web applications to call out actions. These methods, in turn, invoke HTTP responses by the web service based on the request by the client. The CEHRM-SC prototype code is available in our GitHub repository.  $\frac{1}{2}$  and update  $\frac{1}{2}$  is the specific field of  $\frac{1}{2}$  instead of  $\frac{1}{2}$  instead of sharing whole we used the Ethereum Platform and a Windows Foundation project, while<br>exclorment was implemented using IsyaSeript, CCC2, HTMLE, and ReadIS enable users to view and update only the specific fields of the specific fields of HR instead of Sharing whole hitecture consists of two parts of development environments, back-<br>. ne proposed architecture consists of two parts of development environments, back-<br>and front-end. It is also developed upon network entities and smart contracts to n by utilizing an IPFS storage solution. Performance evaluation was<br>Contri<sup>cted</sup> session. An encrypted the public the public the public the public to public the public to public the ular session. And the processor and *D* GD of KAM. For the pack-end using the session key *SSS* GHz processor and D GD of KAM. For the pack-end rty frameworks such as jQuery and bootstrap to construct the<br>the doctor's and *effective* feebies. BECT A BL corrected, the model asei-inentify and enective iashion. KE51 AF1 servers were  $m$ niumig while a database was employed for From-end the entries entries parameter  $\mu$  using the patient  $\mu$  and  $\mu$  and  $\mu$ *UP\_N* Provided Step, the *HRn* is said the *HRn* is saved in IPFS and the patient committee the patient commitment commitm updates. Then, once the health record *HRn* is committed, it immediately ceases the *Sk* and *Packa Pacifical Blockchain, the health record hash valued* by the health record has health recorded by the *HRN*  $\frac{1}{1+t}$  $B$ ased on the doctor requester requester is queried for attributenestricted access to the patient records the matrices and sinustriculates to on by unnearty un in it o storage solution. I enformance evaluation was<br>ConsTN:7 @ 2.20 CH= association of 1 CCD of DAM For the book on d patient in the specific structure under the specific fields of the specific fields of HR instead of the specific fields of the spe essentially, the patient-centric view is a subset of the medical records. The medical records with records. The medical records of the medical records. In an according to the medical records. The medical records of the med then the impremented asing fattocrips, essert interest and protection. the party trainer critic calent as  $\chi$  and  $\sigma$  colorates are public the public property is derived using the public system of  $\sigma$ and programming while a database was employed for Front and  $\alpha$ is and programming with a manual with carp to for the session and to do to do to the session of the set of the<br>And the set of the session and to do t all as Metamask Browser extension (to connect Browser to Blockchain) this experiment, Solidity programming language was adopted for the  $\Gamma$ FHRM in the remix IDF [28] LIsing Kubo (go-infs), we established PCEHRM-SC. Hence, a patient-centric view of the health record is generated by the syschitecture consists of two parts of development environments, back-<br>In the patient record, and the patients of the end and front-end. It is also developed upon network entities and smart contracts to<br>handle each transaction by utilizing an IPFS storage solution. Performance evaluation was Leath dansaction by unitality and *F<sub>D</sub>* storage solution. In accordance evaluation was<br>d out on a intel®Core<sup>TM</sup>i7 @ 3.38 GHz processor and 16 GB of RAM. For the back-end of the first cold the Ethereum Platform and a Windows Foundation project, while the front-end development was implemented using JavaScript, CSS3, HTML5, and ReactJS. Respected third-party frameworks such as jQuery and Bootstrap to construct the egrated third-party frameworks such as jQuery and Bootstrap to construct the web application in a more user-friendly and effective fashion. REST API servers were the *calls the algorithm is a detailed the start update. The system with the system of the system of the system of*  $\alpha$  *and*  $\beta$  *used by*  $\alpha$  *and*  $\beta$  *used by*  $\alpha$  *and*  $\beta$  *used by*  $\alpha$  *and*  $\beta$  *is and physician and physic* ng. On top of that, Truffle Framework, Ganache (Ethereum Blockchain), NodeJS Bibraries, as well as Metamask Browser extension (to connect Browser to Blockchain) lso adopted for this experiment. Solidity programming language was adopted for the the encryption of PCEHRM in the remix IDE [28]. Using Kubo (go-ipfs), we established **Disk of Doctor Private Key Algorithm 1, the patient allows the patient and the patient access to the doctor access the doctor access to t** architecture consists of two parts of development environments, back-<br>Based on the patient-centric is queried for attribute-based data for attribute-based on the patient-centric is end and front-end. It is also developed upon network entities and smart contracts to<br> development, we used the Ethereum Platform and a Windows Foundation project, while<br>the frant and development was involvemented using Jacob Critich CSS2. UTM E and Boart IS We also integrated third-party frameworks such as jQuery and Bootstrap to construct the<br>ush application in a more user friendly and effective faction. BEST API convers users  $\alpha$  and the case in an addition by unified and  $\alpha$  is storage solution. Tenderated evaluation was web application in a more user-mendly and effective rashion. REST API servers were<br>used to execute back-end programming while a database was employed for Front-end programming. On top of that, Truffle Framework, Ganache (Ethereum Blockchain), NodeJS and its libraries, as well as Metamask Browser extension (to connect Browser to Blockchain) were also adopted for this experiment. Solidity programming language was adopted for the and its libraries, as well as Metamask Browser extension (to connect Browser to Blockchain)<br>were also adopted for this experiment. Solidity programming language was adopted for the<br>implementation of PCEHRM in the remix IDE IPFS and transmitted an encrypted medical record to the network, returning a distinct<br>had relax associated with the value deductor of Them has a sifrice the IPFS hade the **Dependient of the Department of the Depar** The proposed architecture consists of two parts of development environments, back-<br>and frant and . It is also developed surem naturally artities and amout earliests to the IPFS and saved in the IPFS and saved in the form of the chemical committees. It is the form of the Sk and S<br>IPHDM CC protetype code is excelled in our CitLub repository. essential medical record attributes, and the patient Ethereum public key, we modified transactions on the blockchain. HTTP methods, for instance, POST, GET, PUT, and DELETE reconductive and saved in the Ethereum block and the ethereum block in the health record has health record has h<br>T<sup>h</sup>n anisations on the blockmant. 11111 includes, for instance, 1 CO1, CE1, 1 C1, and DEEETE<br>are triggered once clients consume web applications to call out actions. These methods, in full PCEHRM-SC prototype code is available in our GitHub repository. programming. On top or that, frame framework, canadic (Bandr  $\mathbb{R}^n$  and  $\mathbb{R}^n$  as  $\mathbb{R}^n$  as  $\mathbb{R}^n$  as  $\mathbb{R}^n$  to connect Browser t  $\text{I}$ al isactions on the plockchally. The file mediods, for filstance, F $\text{C51}$ full I CEHRM-SC prototype code is available in our GitHub repository.

*Pacenvn* nth Patient-Centric View

*LTn* nth Lab Technician

*Dn* nth Doctor

*Phn* nth Pharma

*Pan* nth Patient

*Phn* nth Pharma

*Dn* nth Doctor

*HRn* nth Health Record

*Phn* nth Pharma

*Dn* nth Doctor

*LTn* nth Lab Technician

**Symbols Definition**

#### updates. Then, once the health record *HRn* is committed, it immediately ceases the *Sk* and are uploaded into the updated patient-centric view (*UP\_ Pacenvn*). the *HRn*. After the doctor's and *Pacenvn's* session key have been decrypted, the modifications *7.1. Add Users 7.1. Add Users*

*Pacvn*. In the Ethereum blockchain, the health record hash value *HRn\_hash* is generated by Figure 7 details the successive steps to add users to the network. The smart contract The encrypted *HRn* is decoded once the system is updated, acquired by decryption of Figure 7 details the successive steps to add users to the network. [Th](#page-10-0)e smart contract<br>may now create a role-based unique ID for the enrolled stakeholders upon their registration. are uploaded into the updated patient-centric view (*UP\_ Pacenvn*). tion.

<span id="page-10-0"></span>

**Figure 7.** Add user in PCEHRM. **Figure 7.** Add user in PCEHRM.

#### *7.2. Add Records and Update Records*

After the patient has been allowed access, the doctor may create a record before it is encrypted and stored in IPFS using the hash value that is maintained via the Ethereum blockchain. A temporary, patient-centric view of the medical record is supplied so that the physician may update the view and subsequently, the existing record incessantly in both IPFS and health record chains following the patient's authorization. Consecutively, the session key would lapse, denying doctors access to patient-sensitive information. Figure [8](#page-11-0) specifies the step-by-step operation of appending and modifying health records in the network.

<span id="page-11-0"></span>

Figure 8. Add records and update records.

#### *7.3. Assuring Authorized Users Have Access*  Patients maintain restrictive access control to grant or deny access permissions to *7.3. Assuring Authorized Users Have Access*

Patients maintain restrictive access control to grant or deny access permissions to providing patients full authority and control over their health records. This is carried out stakeholders within a restricted setting to allow them to view, modify, or create records, providing patients full authority and control over their health records. This is carried out by authorizing consent to medical records based on the role and permission type for authenticated users approved by consensus. In the event that healthcare personnel  $\frac{1}{2}$  requests, perform data updating, and provide actions the actions of  $\frac{1}{2}$ are denied access, the records would not be made available to them or other attending physicians. Upon interaction of users with the system, smart contracts identify and validate the requests, perform data updating, and provide access rights. Figure [9](#page-11-1) describes the actions sequentially for the role-based access rights and permission. Patients maintain restrictive access control to grant or deny access permissions to physicians. Opon interaction or users whill the system, smart contrat

<span id="page-11-1"></span>

Figure 9. Assuring authorized users have access.

# *7.4. Records Retrieval 7.4. Records Retrieval*

Patients must allow access for the retrieval of partial attribute-based data from IPFS Patients must allow access for the retrieval of partial attribute-based data from IPFS using the hash value in the chain network, so that all stakeholders may access their records. Figure [10](#page-12-0) delineates the view record step-by-step implementation.

<span id="page-12-0"></span>

### **Figure 10.** Records retrieval. **Figure 10.** Records retrieval.

# *7.5. Framework Implementation 7.5. Framework Implementation*

Chain codes, smart contracts, network entities, and IPFS storage are all components Chain codes, smart contracts, network entities, and IPFS storage are all components of the Health Chain Network Transaction Framework [\[26\]](#page-18-3). In the user sign-up module of the Health Chain Network Transaction Framework [26]. In the user sign-up module of the network, receptionists, pharmacists, physicians, and other medical personnel can enroll using their respective roles, upon which the certificate of authority is produced after the registration. Users can sign in using their email address credentials and password after enrolment. In this case, receptionists may approve or decline appointments made by the stakeholders using patient IDs and update them based on the patient's data. If the pointment proceeds, doctors may create or update the patient's medical record via notes appointment proceeds, doctors may create or update the patient's medical record via notes or diagnosis results before being uploaded to IPFS. or diagnosis results before being uploaded to IPFS.

Our recommended business ecosystem contains elements such as assets, stakeholders, and transactions, as depicted in Figure [11.](#page-13-0) Several tests were carried out for the health chain framework prototype to evaluate its performance and functionality through four chain framework prototype to evaluate its performance and functionality through four case studies that describe its storage, scalability, efficiency, and security.

#### 7.5.1. Storage Efficiency

To assess if the interplanetary database can sufficiently hold and retain health records, a few cases were performed in the following ways:

- 1. Doctors were able to upload health records.
- 2. With the patient's permission, a doctor could view the medical records.
- 3. Patients were capable to view their health data.
- 4. Patients and doctors were permitted to retrieve health records based on their credentials.
- 5. Encrypted health records were generated proficiently.

<span id="page-13-0"></span>

Subsequently, encryption and decryption of the modified records in IPFS could be accomplished by doctors and patients, respectively, using their corresponding session keys.

**Figure 11.** Proposed business ecosystem. **Figure 11.** Proposed business ecosystem.

## 7.5.2. Security

Before the data is saved in IPFS, the following instances were verified to confirm security requirements for the effective implementation of encrypted health records:

- 1. Encryption of the user's password.<br>2. Encryption of the user's password.
- 2. Health records were saved in IPFS with encryption.
- 3. Each record was assigned a distinct hash value.<br>4. Each record was assigned a distinct hash value.
- 4. Public and private keys were assigned to all stakeholders.
- 5. Session keys assignment and expiration.

#### $S<sub>1</sub>$  Privacy 7.5.3. Privacy

The objective of this test is to confirm whether or not stakeholders were granted or keys. denied access to health records depending on their role. The access control was verified using test instances as listed below:

- 1. Depending on their role, stakeholders were able to view their respective home pages.
- Before the data is saved in IPFS, the following instances were verified to confirm se-2. Access rights based on the stakeholders' role.
- 3. Session keys were allocated for viewing medical records.

This was performed to prove that the system is capable of assigning access permissions  $\frac{1}{2}$  based on their levels and roles.

### 4. Public and private keys were assigned to all stakeholders. **8. Evaluation**

In this section, we tested the viability and coherence of the access process and system We investigated the average time taken to download and upload health data, the cost of undertaking PCEHRM functions, as well as the efficiency of the transaction. Consequently, examining the test network permits us to validate and optimize the prototype prior to publishing it on a public blockchain. interaction amongst network participants by putting the suggested framework into practice.

### $1.1 \times 10^{-10}$  role, state the state to view the state  $\sim$ 8.1. Verification of PCEHRM-SC

By testing two key functions for brevity givePermission(), removePermission(), we were able to confirm the access rights and interactions between entities. The results of these  $\,$  test are presented in [Figu](#page-14-0)res [12](#page-14-1) and 13, depicting the summary of the transaction event log maintained in the blockchain once the functions were successfully executed.

By testing two key functions for brevity given  $\mathcal{C}$  , remove  $\mathcal{C}$  , we have  $\mathcal{C}$ 

<span id="page-14-0"></span>{ "event" : "GivePermission" ,<br>"patient\_id" : "0xc87656D593CD4e0178c7dbbE0D982a7d8dDFEA56"<br>"info" : "Approved" }<br>{ "event: "Approved" }<br>"frequester\_id" :" 0x770a246c2CF57D25661Ef48C8D01b14D89264169"

**Figure 12.** Result of give permission function. **Figure 12.** Result of give permission function. **Figure 12.** Result of give permission function.

```
{ "event" : "RemovePermission" ,<br>"patient_id" : "0xc87656D593CD4e0178c7dbbE0D982a7d8dDFEA56" ,<br>"info" : "Failed" }<br>{ "event: "Failed" ,<br>"fequester_id" :" 0x770a246c2CF57D25661Ef48C8D01b14D89264169" ,<br>"finfo" :" Ned more de
event: "Faile"}<br>"requester_id"<br>"Info" :" Need
   "Info" :" Need more details info" }
```
**Figure 13.** Result of revoke permission function. **Figure 13.** Result of revoke permission function. **Figure 13.** Result of revoke permission function.

#### *8.2. Practical Applications and Costs*

*8.2. Practical Applications and Costs 8.2. Practical Applications and Costs* to execute for each transaction. The cost is calculated by ether = gas used  $\times$  gas price; "gas used" means the constant computational cost. The network adjusts the price of gas to compensate for changes in the value of ether [8]. Thus, the total transaction c[os](#page-17-7)ts (ether) for compensate for changes in the value of ether [8]. Thus, the total transaction costs (ether) for<br>the accessibility of health data remain relatively constant. Regarding the paying segment, all participants must pay gas for performing an operation in SC. Therefore, the automated SC process would result in significant cost savings for the patient. In the implemented PCEHRM-SC prototype, we have set a gas limit of 30,000, with each gas unit fixed at  $2 \text{ Gwei.}$  $2$  Gwei.  $\frac{1}{2}$  set a gas limit of 30,000, with each gas unit fixed In the proposed system, we define the cost for the actual transactions and time taken 2 Gwei.

Table [6](#page-14-2) summarizes the time taken and cost of operations performed in SC. The addDoctor() function is implemented once at a cost of 0.00089442 eth with used time 10.316s. The addPatient() function costs around 0.093 eth, which is higher than other functions due to the additional input bytes that are included during function execution, such as the patient's blockchain address and usage notes. However, the used time for execute this function is not high compared to executing the getpatient<br>details() function was 0.213s which requires fetch the EHR's data of the patient.



<span id="page-14-2"></span>requires fetch the EHR's data of the patient. **Table 6.** PCEHRM time and cost analysis (database).

In general, the overall costs can be further reduced by keeping the size of the input data to a minimum. However, these costs are still lower than those associated with purchasing storage space from a third party or maintaining a database through a centralized system such as ISN [\[29\]](#page-18-6), MedBlock [\[30\]](#page-18-7), MeDShare [\[31\]](#page-18-8), and MedChain [\[11\]](#page-17-10).

#### *8.3. Performance Evaluation*

Storing large amounts of data on the blockchain is costly, so to minimize costs, IPFS hashes are stored on the blockchain. Figure [14](#page-15-0) shows the predicted difference in cost events as the number of transactions on the blockchain increases. Primarily foresee the cost of writing data to the blockchain, as it is a more expensive transaction than reading data from

<sup>&</sup>quot;Info" :" Authorised access to HR" }

<span id="page-15-0"></span>

the blockchain. As shown in Figure [14,](#page-15-0) storing his IPFS hash rather than the entire image significantly reduces storage costs.

events as the number of transactions on the blockchain increases. Primarily foresee the

**Figure 14.** Medical data storage costs projected vs. IPFS on blockchain. **Figure 14.** Medical data storage costs projected vs. IPFS on blockchain.

Our proposed system stores the media in IPFS, and IPFS stores media with the help Our proposed system stores the media in IPFS, and IPFS stores media with the help of peers. Figure [15](#page-15-1) shows that as the number of peers accessing the transaction or contributing to image storage increases, the execution time, or the time required to retrieve the media, increases. Depending on the previous section, the larger the image or report size, the longer it takes to access the same.

<span id="page-15-1"></span>

**Figure 15.** Execution time based on the number of peers and document size. **Figure 15.** Execution time based on the number of peers and document size.

## **9. Discussion 9. Discussion**

To ensure the best possible health care experience for the patient, the patient should To ensure the best possible health care experience for the patient, the patient should be able to access or grant access to his or her medical information as needed. This is currently not possible when the data is stored in a hospital's proprietary Electronic Health Record Record (EHR). As a result, there is a requirement for patient operated where the details of (EHR). As a result, there is a requirement for patient operated where the details of the patient's treatment are with the patient. This paper proposes a secure, interoperable patientcentric data access management system based on blockchain. In our proposed system, the patient has complete control over his or her health record-related data, which is stored

PCEHRMAN

[17]

 $t_{\text{acces}}$  control strategies for  $\alpha$ 

 $t_{\text{t}}$  and its effects. The existing architectures in  $[10,18,32]$ 

 $t_{\rm{reco}}$ 

securely using IPFS. Using a token, patients can grant controlled access to their medical securely using IPFS. Using a token, patients can grant controlled acc[es](#page-16-0)s to their medical<br>data to health care providers for a set period of time. In the following, Table 7 explains the summary of the comparison between the existing and suggested patient-centric health<br>11 February 11 February 12 February 1 the summary or the comparison between the existing and suggested patient-centric health<br>storage models focusing on privacy, scalability, security, and integrity. The authors in [16,17] storage models focusing on privacy, scalability, security, and megrity. The authors in [10,17]<br>reviewed current strategies for healthcare management using blockchain technology and its effects. The existing architectures in  $[10,15,18,32]$  were examined. Each block includes reviewed current strategies for healthcare management using blockchain technology and<br>its effects. The existing architectures in [10,15,18,32] were examined. Each blo[ck](#page-17-9) [inc](#page-17-14)[lud](#page-17-17)es<br>a health record hash value that would transf ensures the records are immutable as it is computationally expensive to manipulate the<br>data of the additional distribution cases to activate's as disclosed in a solid it allows ledger. On top of that, stakeholder access to patients' medical records is prohibited by access control rights and levels. stored securely using  $\mathcal{L}$ medical data to health care providers for a set period of time. In the following, Table 7 and Table 7 and Table explains the summary of the summary of the summary of the existing and support  $\mathbf{c}$ tric health storage models for privacy, security, security, security, and integrity, and integrity. The authors in  $160$  $t$  the effects. The existing architectures in  $[10,15,82]$ block includes a health record has health record that whenever that whenever that we have the record is  $a$  health record is  $a$ updated. This ensures the records are in mutations are in the records are in the records are in the records are in  $\alpha$ manipulate the ledger. On that, stakeholder access to  $\log$ tem, the patient has complete control over his or health record-related data, which is stored securely using I<br>, which is stored access to the intervals can grant controlled access to the intervals can grant controlled ac medical data to health care providers for a set period of time. In the set  $\mathfrak{p}_1$ explains the summary of the summary of the existing and support  $\mathcal{E}$  $t_{\rm F}$ tts en<br>thors in technology and its effects. The existing architectures in the existing architectures in  $\alpha$ block includes a health record hash value that would transform whenever the record is updated. This ensures the records are in mutations are in the records are in  $\mathbb{R}^n$ manipulate the ledger. On the ledger access to patients' medical records in the state of the patients' medical records in the state of the state ss to their medical access to their medical data to health can grant call data to health care providers for a set p ain technology and<br>'ach block includes<br>d is updated. This the patient are with the patients of patients are with the patients. This paper proposes a secure, internal secure, internal secure, in the patients of  $\mathcal{L}$ patient-centric data access management system based on blockchain. In our proposed systhe patient has complete complete control over  $\mathbb{R}^n$  $s_{\text{U}}$ medical data to health care providers for a set period of time. In the following, Table 7  $\frac{1}{18}$  existing comparison between the existing and suggested patient-cen $t_{\rm eff}$  integrity, storage models focusing on privacy, security, and integrity. The au $t_{\rm H}$  reviewed current strategies for  $\frac{1}{2}$ technology and its effects. The existing architectures in  $[10,18]$ block includes a health record has a health record in the record is  $\alpha$ the summary or the complete control over high record-relationships or the complete stored securely using  $\frac{1}{2}$ ledger. On top of that<br>access control rights and ersures the records are infinituable as if<br>ledger. On top of that, stakeholder access control rights and levels.  $teuget.$  On the existing architecture architecture in  $[10,18,18]$ g, Iable 7 explains<br>tient-centric health bo mamputate the<br>ds is prohibited by leads the records are infinitely as it is computationally expensive to manipulate the ledger. On top of that, stakeholder access to patients' medical records is prohibited by access control rights and levels. Record (EHR). As a result, there is a requirement for patient operated where the details of the patient's treatment are with the patient. This paper proposes a secure, interoperable patient-centric data access management system based on blockchain. In our proposed sys- $\frac{\text{t}}{\text{t}}$  $\frac{1}{2}$  is the total using a total using a total controlled access to the controlled access to the controlled access to the interval controlled access to the controlled access to the controlled access to the controlled  $\frac{1}{3}$  data to health care providers for a set period of time. In the following, Table 7. explains the summary of the comparison between the existing and suggested patient-cen $t_{\rm HSR}$  storage models focusing on privacy, security, and integrity. The au- $\frac{1}{16}$  reviewed current strategies for  $\frac{1}{16}$ leager. On top of that, stakeholder access to patients inetical fecolus is prohibited by  $\sum_{i=1}^{\infty}$  and it is computationally expensive to record and  $\sum_{i=1}^{\infty}$  it is computationally expensive to  $\sum_{i=1}^{\infty}$ the increase current strategies for healthcare management is effected as  $\frac{1}{2}$  were examined. Each its effects. The existing architectures in  $\frac{1}{2}$ rently not possible when the data is stored in a hospital's proprietary Electronic Health rently not possible when the data is stored in a hospital's proprietary Electronic Health Record (EHR). As a result, there is a requirement for patient operated where the details of  $\frac{1}{\pi}$  the patient are with the patient. The patient  $\frac{1}{\pi}$  $p_{\text{total}}$ its eff<br>a hea  $\frac{1}{2}$  $\frac{1}{2}$  $\mathbf{b}$ patient-centric data access management system based on blockchain. In our proposed sysstored securely using the traditions of the traditional controlled access to the controlled access to the intermedical data to health care providers for the following for the following. In the following, Table 7, 1992, Table 7, 1993, Table 7,  $\frac{1}{2}$  choices the succession between the existing  $\frac{1}{2}$  $t_{\text{c}}$  is the product strictly on the au-Record (EHR). As a result, there is a requirement for patient operated where the details of access to patients. The exercise is promotived by ss to their medical  $\mathbb{E}\left[\text{a}^{\text{u}}\text{a}^{\text{u}}\text{b}^{\text{u}}\text{b}^{\text{u}}\text{c}^{\text{u}}\text{c}^{\text{u}}\text{c}^{\text{u}}\text{c}^{\text{u}}\text{c}^{\text{u}}\text{c}^{\text{u}}\text{c}^{\text{u}}\text{c}^{\text{u}}\text{c}^{\text{u}}\text{c}^{\text{u}}\text{c}^{\text{u}}\text{c}^{\text{u}}\text{c}^{\text{u}}\text{c}^{\text{u}}\text{c}^{\text{u}}\text{c$  $\frac{1}{2}$  and between the comparison between the existing and suggested patient-cen- $\alpha$  is updated. This to manipulate the  $\frac{1}{1}$  reviewed current using blockchains block healthcare management using blockchains bloc  $\mu$ s is profilonca by be able to access or grant access to his or her medical information as needed. This is cursecurely using IPFS. Using a token, patients can grant controlled access to their medical<br>data to health care providers for a set period of time. In the following, Table 7 explains  $\epsilon$  and summary of the comparison the summary of the existence of the existing and supplies  $\epsilon$  and supplies  $\epsilon$ edger. On top or that, stakeholder access to patients included records is promotica by rently not possible when the data is stored in a hospital's proprietary Electronic Health  $t_{\text{eq}}$  redicare records is profitencare  $t_{\text{eq}}$ ss to their medical<br>g, Table 7 explains the authors in [10,17]<br>ain technology and  $\frac{1}{2}$  denote the following of the following  $\frac{1}{2}$  $\alpha$  is updated. This to manipulate die  $t_{\text{15}}$  is prohibited by rently not possible when the data is stored in a hospital's proprietary Electronic Health  $\mathbf{a}$  requirement for  $\mathbf{b}$  $\frac{1}{1}$  $\frac{m}{2}$  $\frac{1}{1}$  $\mathbf u$  using a token, patients can grant controlled access to the internal controlled  $\mathcal{L}$  data to health care providers for a set  $\mathcal{L}$  $\mathbf{u}$ s the comparison between the existing and suggested patient-cen- $\frac{1}{\sqrt{2}}$  $\mathcal{L}$ 

<span id="page-16-0"></span> $t_{\text{rel}}$  reviewed current strategies for  $\frac{1}{2}$ 

 $t_{\text{min}}$  and  $t_{\text{min}}$ .

[17]



[32]

[17] [18]

Table 7. Comparison between the existing and suggested patient-centric health storage models. **Table 7.** Comparison between the existing and suggested patient-centric health storage models. **Information Data Integrity Data Security Patient-Cen**prohibited by access control rights and levels. Table 7. Comparison between the existing and suggested patient-centric health storage models.  $m_{\rm H}$  is a contop of that, stakeholder access to patients' medical records is patients. manipulate the ledger. On that, stakeholder access to patients' medical records is  $\frac{1}{2}$  medical records in the cords is  $\frac{1}{2}$  medical records in the cords is  $\frac{1}{2}$  medical records in the cords is  $\frac{1}{2}$  me updates tonition rights and levels.<br>This computationally expensive to manipulate the ledger. On top of the ledger. On the ledger. On the computational records is patients in the computation of the computation of the comput updated. This ensures the records are immutable as it is computationally expensive to  $\mathbf{r}_\mathrm{d}$  $m_{\text{N}}$  $T_{\rm eff}$  ensures the records are interesting as it is computationally expensive to the records as it is computationally expensive to  $T_{\rm eff}$ more the companion occurs  $T_{\rm eff}$  is in  $C_{\rm eff}$  are invariant to record are interested. more the comparison section are existing a This ensures the records are increased as it is computational ly expensive to the contribution of  $\mathcal{L}$ more to compute the central and original and ouggested path prohibited by access control rights and levels.  $\mathbf{F}$ updated. This ensures the records are interested as it is contributed as it is computationally expensive to more the comparison between the existing and suggested patient centre nearly storage models. block includes a health record hash value that would transform whenever the record is manipulate the ledger. On top of that, stakeholder access to patients' medical records is permeen are expang and baggebied panem centre. manipulate the ledger. On top of that, stakeholder access to patients' medical records is prohibited by access control rights and levels. prohibited by access control rights and levels. prohibited by access control rights and levels. manipulate the ledger. On top of that, stakeholder access to patients' medical records is manipulate the ledger. On top of that, stakeholder access to patients' medical records is  $b$ technology and its effects. The existing architectures in  $[10,18]$  were examined. Each block includes a health record has  $\frac{1}{2}$  $\text{Table 7}$  Comparison bet  $\frac{1}{\sqrt{2}}$ access control rights and revels.<br>**Table 7.** Comparison between the existing and suggested patient-centric health storage models. atient-centric health storage models. n storage models.

# **10. Conclusions**  $\overline{\phantom{a}}$

[32]

[32]

 $\text{t}_0$  $\frac{1}{\epsilon}$  **records**  $**Model**$ reduced records are the most precious commodity in the measury of nearmedic in-<br>telligence. Often, this information is indeed dispersed across various platforms, posing a completed the international international contracts which as phateting, peaning and challenge in sharing them for an efficient and cohesive healthcare system. Meanwhile, a centralized hosting solution for instance a cloud-Medical records are the most precious commodity in the industry of healthcare inchallenge in sharing them for an efficient and cohesive healthcare system. Meanwhile, a Medical records are the most precious commodity in the industry of healthcare intelligence. Of this indeed dispersed achallenge in sharing platforms, positive in sharing a challenge in sharing <br>
and cohesive healthcare system. Meanwhile, and cohesive healthcare system. Meanwhile, and cohesive healthcare  $\mathbf{u}$  of boothermation is indeed across various platforms, positive across various platforms, positive  $\mathbf{v}$  $\frac{1}{\text{c}}$  challenge in share system. contralized hosting solution, for instance, a cloud-based platform, is vulnerable towards a single point of a cybersecurity attack. Decentralized designs and system interoperability<br>have received more attention as the dispersed nature of healthcare services has come to  $h$ ealthcare in Medical records are the most precious commodity in the industry of healthcare intel- $\sin \theta$ challenge in share them for an effect and cohesive healthcare system. Meanwhile, and cohesive ligue point of a cyber<br>have received more at have received more attention as the dispersed nature of healthcare services has come to<br>light. In this study, we incorporated the PCEHRM system, a decentralized framework for  $\lim_{n \to \infty} \frac{1}{n}$  $\text{sing}$ ligence. Often, this indeed dispersed across various platformation is indeed across various platforms, positiv challenge in sharing them for an effect and cohesive healthcare system. Meanwhile, and cohesi llnerable towards a<br>em interoperability light. In this study, we incorporated the PCEHRM system, a decentralized framework for  $\mathbf{h}$ are the most precise are the industry in the industry intelligence. Often, this information is indeed dispersed across various platforms, posing challenge in sharing them for an efficient and cohesive sharing  $\mathbf{s}_0$ sharing access and storing medical data that is built on the Ethereum blockchain and IPFS rvices has come to<br>zed framework for **10. Conclusions**   $\mathop{\mathrm{to}}$  $\mathbf{r}$  in sharing them for an effect and cohesive healthcare system. Meanwhile, and cohesive  $\mathbf{r}$ architecture. We also introduced a novel access control system termed PCEHRM-SC that provides authorized parties access to the pertinent blockchain data. By giving patients complete management over their healthcare records utilizing smart contract protocol, the PCEHRM system promotes a unique manner to enhance their rights. For example, patients have full control over their medical reports and possess the ability to allow or deny access to the records for use in clinical trials or research. We also analyzed and evaluated the feasibility, effectiveness, and rationality parameters of the proposed framework. As a result of the analysis, the implemented system appears to be efficient and satisfies many security requirements. A high level of privacy, security, confidentiality, and scalability can be achieved.

PCEHRMANISTIC

[17] [18]

By offering higher productivity, data integrity, and efficient audit, while allowing for shared access to medical data, the suggested scheme makes it easier for patients to access an immutable medical database. Since the data storage and exchange model are also decentralized, it is crucial to involve third-party intermediaries and eliminate administrative structures. Our long-term study objective is to implement the suggested system architecture on the public blockchain using real-world examples to establish a worldwide PCEHRM system and to assess associated laws and standards to integrate this cutting-edge technology within the healthcare system. Without a doubt, the artificial intelligence component would aid clinicians in the analysis of diagnostic medical data and communicate more effectively with patients.

**Author Contributions:** Conceptualization, methodology, and writing, A.H. and M.H.H.; software, A.H.; validation, supervision and revision: M.H.H., M.R.I., S.A.Z., E.A.A.E. and F.E.M.S.; funding: M.H.H., M.R.I., E.A.A.E. and F.E.M.S. All authors have read and agreed to the published version of the manuscript.

**Funding:** The authors extend their appreciation to the Deanship of scientific research at King Khalid University for funding this work through Research Group Program under grant number (RGP.1/147/43).

**Institutional Review Board Statement:** Not applicable.

**Informed Consent Statement:** Not applicable.

**Data Availability Statement:** Not applicable.

**Acknowledgments:** This work was conducted at the IoT and Wireless Communication Protocols Laboratory at the ECE department, International Islamic University Malaysia (IIUM).

**Conflicts of Interest:** The authors declare that they have no conflicts of interest.

#### **References**

- <span id="page-17-0"></span>1. Madine, M.M.; Battah, A.A.; Yaqoob, I.; Salah, K.; Jayaraman, R.; Al-Hammadi, Y.; Pesic, S.; Ellahham, S. Blockchain for giving patients control over their medical records. *IEEE Access* **2020**, *8*, 193102–193115. [\[CrossRef\]](http://doi.org/10.1109/ACCESS.2020.3032553)
- <span id="page-17-1"></span>2. Idrees, S.; Nowostawski, M.; Jameel, R.; Mourya, A. Security Aspects of Blockchain Technology Intended for Industrial Applications. *Electronics* **2021**, *10*, 951. [\[CrossRef\]](http://doi.org/10.3390/electronics10080951)
- <span id="page-17-2"></span>3. Sharma, A.; Tomar, R.S.; Chilamkurti, N.; Kim, B.G. Blockchain Based Smart Con- tracts for Internet of Medical Things in e-Healthcare. *Electronics* **2020**, *9*, 1609. [\[CrossRef\]](http://doi.org/10.3390/electronics9101609)
- <span id="page-17-3"></span>4. Saidi, H.; Labraoui, N.; Ari, A.A.; Maglaras, L.A.; Emati, J.H. DSMAC: Privacy-aware Decentralized Self-Management of data Access Control based on blockchain for health data. *IEEE Access* **2022**, *10*, 101011–101028. [\[CrossRef\]](http://doi.org/10.1109/ACCESS.2022.3207803)
- <span id="page-17-4"></span>5. Makridakis, S.; Christodoulou, K. Blockchain: Current challenges and future pro-spects/applications. *Future Internet* **2019**, *11*, 258. [\[CrossRef\]](http://doi.org/10.3390/fi11120258)
- <span id="page-17-5"></span>6. Seh, A.H.; Zarour, M.; Alenezi, M.; Sarkar, A.K.; Agrawal, A.; Khan, A.R. Healthcare Data Breaches: Insights and Implications. *Healthcare* **2020**, *8*, 133. [\[CrossRef\]](http://doi.org/10.3390/healthcare8020133)
- <span id="page-17-6"></span>7. Azaria, A.; Ekblaw, A.; Vieira, T.; Lippman, A. Medrec: Using blockchain for medical data access and permission management. In Proceedings of the 2016 2nd International Conference on Open and Big Data (OBD), IEEE, Vienna, Austria, 22–24 August 2016; pp. 25–30.
- <span id="page-17-7"></span>8. Ivan, D. Moving toward a blockchain-based method for the secure storage of patient records. In Proceedings of the ONC/NIST Use of Blockchain for Healthcare and Research Workshop, ONC/NIST, Gaithersburg, MD, USA, 4 August 2016.
- <span id="page-17-8"></span>9. Dannen, C. *Introducing Ethereum and Solidity*; Springer: Berlin/Heidelberg, Germany, 2017.
- <span id="page-17-9"></span>10. Shen, B.; Guo, J.; Yang, Y. Medchain: Efficient healthcare data sharing via blockchain. *Appl. Sci.* **2019**, *9*, 1207. [\[CrossRef\]](http://doi.org/10.3390/app9061207)
- <span id="page-17-10"></span>11. Jamil, F.; Ahmad, S.; Iqbal, N.; Kim, D.-H. Towards a remote monitoring of patient vital signs based on iot-based blockchain integrity management platforms in smart hospitals. *Sensors* **2020**, *20*, 2195. [\[CrossRef\]](http://doi.org/10.3390/s20082195)
- <span id="page-17-11"></span>12. Margheri, A.; Masi, M.; Miladi, A.; Sassone, V.; Rosenzweig, J. Decentralised provenance for healthcare data. *Int. J. Med. Inform.* **2020**, *141*, 104197. [\[CrossRef\]](http://doi.org/10.1016/j.ijmedinf.2020.104197)
- <span id="page-17-12"></span>13. Roehrs, A.; da Costa, C.A.; da Rosa Righi, R.; da Silva, V.F.; Goldim, J.R.; Schmidt, D.C. Analyzing the performance of a blockchain-based personal health record implementation. *J. Biomed. Inform.* **2019**, *92*, 103140. [\[CrossRef\]](http://doi.org/10.1016/j.jbi.2019.103140)
- <span id="page-17-13"></span>14. Jha, N.; Prashar, D.; Khalaf, O.I.; Alotaibi, Y.; Alsufyani, A.; Alghamdi, S. Blockchain Based Crop Insurance: A Decentralized Insurance System for Modernization of Indian Farmers. *Sustainability* **2021**, *13*, 8921. [\[CrossRef\]](http://doi.org/10.3390/su13168921)
- <span id="page-17-14"></span>15. Dwivedi, A.D.; Srivastava, G.; Dhar, S.; Singh, R. A decentralized privacy- preserving healthcare blockchain for iot. *Sensors* **2019**, *19*, 326. [\[CrossRef\]](http://doi.org/10.3390/s19020326) [\[PubMed\]](http://www.ncbi.nlm.nih.gov/pubmed/30650612)
- <span id="page-17-15"></span>16. Rajput, A.; Li, Q.; Ahvanooey, M. A blockchain-based secret-data sharing framework for personal health records (2021) in emergency condition. *Healthcare* **2021**, *9*, 206. [\[CrossRef\]](http://doi.org/10.3390/healthcare9020206) [\[PubMed\]](http://www.ncbi.nlm.nih.gov/pubmed/33672991)
- <span id="page-17-16"></span>17. Jagadeesh, R.; Mahantesh, K. Blockchain-based knapsack system for security and privacy preserving to medical data (2021) in SN COMPUT. *Scientifur* **2021**, *2*, 245.
- <span id="page-17-17"></span>18. Egala, B.S.; Pradhan, A.K.; Badarla, V.; Mohanty, S.P. Fortified-chain: A blockchain- based framework for security and privacyassured internet of medical things with effective access control. *IEEE Internet Things J.* **2021**, *8*, 11717–11731. [\[CrossRef\]](http://doi.org/10.1109/JIOT.2021.3058946)
- <span id="page-17-18"></span>19. Alsufyani, A.; Alotaibi, Y.; Almagrabi, A.O.; Alghamdi, S.A.; Alsufyani, N. Optimized intelligent data management framework for a cyber-physical system for computational applications. *Complex. Intell. Syst.* **2021**, 1–13. [\[CrossRef\]](http://doi.org/10.1007/s40747-021-00511-w)
- <span id="page-17-19"></span>20. Singh, P.; Masud, M.; Hossain, M.S.; Kaur, A. Blockchain and homomorphic encryption- based privacy-preserving data aggregation model in smart grid. *Comput. Electr. Eng.* **2021**, *93*, 107209. [\[CrossRef\]](http://doi.org/10.1016/j.compeleceng.2021.107209)
- <span id="page-17-20"></span>21. Peng, C.; He, D.; Chen, J.; Kumar, N.; Khan, M.K. EPRT: An Efficient Privacy-Preserving Medical Service Recommendation and Trust Discovery Scheme for eHealth System. ACM Trans. *Internet Technol.* **2021**, *21*, 1–24. [\[CrossRef\]](http://doi.org/10.1145/3397678)
- <span id="page-17-21"></span>22. Piao, Y.; Ye, K.; Cui, X. A Data Sharing Scheme for GDPR-Compliance Based on Consortium Blockchain. *Future Internet* **2021**, *13*, 217. [\[CrossRef\]](http://doi.org/10.3390/fi13080217)
- <span id="page-18-0"></span>23. Wood, G. Ethereum: A Secure Decentralised Generalised Transaction Ledger. Available online: <https://gavwood.com/paper.pdf> (accessed on 23 November 2022).
- <span id="page-18-1"></span>24. Buterin, V. Ethereum White Paper. Available online: <https://github.com/ethereum/wiki/wiki/White-Paper> (accessed on 25 November 2022).
- <span id="page-18-2"></span>25. Dhillon, V.; Metcalf, D.; Hooper, M. *Blockchain Enabled Applications*; Apress: Berkeley, CA, USA, 2017.
- <span id="page-18-3"></span>26. Foschini, L.; Gavagna, A.; Martuscelli, G.; Montanari, R. Hyperledger Fabric Blockchain: Chaincode Performance Analysis. In Proceedings of the ICC 2020—2020 IEEE International Conference on Communications (ICC), Dublin, Ireland, 7–11 June 2020; pp. 1–6.
- <span id="page-18-4"></span>27. 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. [\[CrossRef\]](http://doi.org/10.3390/electronics10233003)
- <span id="page-18-5"></span>28. Kumar, S.; Bharti, A.K.; Amin, R. Decentralized secure storage of medical records using Blockchain and IPFS: A comparative analysis with future directions. *Secur. Privacy* **2021**, *4*, e162. [\[CrossRef\]](http://doi.org/10.1002/spy2.162)
- <span id="page-18-6"></span>29. Langer, S.G.; Tellis, W.; Carr, C.; Daly, M.; Erickson, B.J.; Mendelson, D.; Moore, S.; Perry, J.; Shastri, K.; Warnock, M.; et al. TheRSNA Image Sharing Network. *J. Digit. Imaging* **2014**, *28*, 53–61. [\[CrossRef\]](http://doi.org/10.1007/s10278-014-9714-z) [\[PubMed\]](http://www.ncbi.nlm.nih.gov/pubmed/25037586)
- <span id="page-18-7"></span>30. Fan, K.; Wang, S.; Ren, Y.; Li, H.; Yang, Y. MedBlock: Efficient and Secure Medical DataSharing Via Blockchain. *J. Med. Syst.* **2018**, *42*, 136. [\[CrossRef\]](http://doi.org/10.1007/s10916-018-0993-7) [\[PubMed\]](http://www.ncbi.nlm.nih.gov/pubmed/29931655)
- <span id="page-18-8"></span>31. Xia, Q.; Sifah, E.B.; Asamoah, K.O.; Gao, J.; Du, X.; Guizani, M. MeDShare: Trust-Less Medical Data Sharing among Cloud ServiceProviders via Blockchain. *IEEE Access* **2017**, *5*, 14757–14767. [\[CrossRef\]](http://doi.org/10.1109/ACCESS.2017.2730843)
- <span id="page-18-9"></span>32. Lee, W. Getting Started with Smart Contract and using the MetaMask Chrome Extension. In *Beginning Ethereum Smart Contracts Programming*; Apress: Berkeley, CA, USA, 2019; ISBN 978-1-4842-5086-0.

**Disclaimer/Publisher's Note:** The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.