electronics

MDPI

Article

GDPR Compliant Data Storage and Sharing in Smart Healthcare System: A Blockchain-Based Solution

Pinky Bai [1], Sushil Kumar [1], Kirshna Kumar [1], Omprakash Kaiwartya [2,*], Mufti Mahmud [2] and Jaime Lloret [3]

[1] School of Computer & Systems Sciences, Jawaharlal Nehru University, New Delhi 110067, India
[2] Department of Computer Science, Nottingham Trent University, Clifton Lane, Nottingham NG11 8NS, UK
[3] Instituto de Investigación para la Gestión Integrada de Zonas Costeras, Universitat Politécnica de Valencia, Camino Vera s/n, 46022 Valencia, Spain
* Correspondence: omprakash.kaiwartya@ntu.ac.uk

Abstract: Smart healthcare systems provide user-centric medical services to patients based on collected information of patients inducing personal health information (PHI) and personal identifiable information (PII). The information (PII and PHI) flows into the smart healthcare system with or without any regulation and patient concern with the help of new information and communication technologies (ICT). The use of ICT comes with the security and privacy issues of collected PII and PHI data. The Europe Union has published the General Data Protection Regulation (GDPR) to regulate the flow of personal information. Towards this end, this paper proposes a blockchain-based data storage and sharing framework for a smart healthcare system that complies with the "Privacy by Design" rule of the GDPR. The personal information collected from patients is stored on off-chain storage (IPFS), and other information is stored on the blockchain ledger, which is visible to all participants. The smart contracts are designed to share the PII data with another participant based on prior permission of the data owner. The proposed framework also includes the deletion of PII and PHI in the system as per the "Right to be Forgotten" GDPR rule. Security and privacy analyses are performed for the framework to demonstrate the security and privacy of data while sharing and at rest. The comparative performance analysis demonstrates the benefit of the proposed GDPR-compliant data storage and sharing framework using blockchain. It is evident from the reported results that the proposed framework outperforms the state-of-the-art techniques in terms of performance metrics in a smart healthcare system.

Keywords: smart healthcare system; GDPR; data sharing; data storage; right to be forgotten

Citation: Bai, P.; Kumar, S.; Kumar, K.; Kaiwartya, O.; Mahmud, M.; Lloret, J. GDPR Compliant Data Storage and Sharing in Smart Healthcare System: A Blockchain-Based Solution. *Electronics* **2022**, *11*, 3311. https://doi.org/10.3390/electronics11203311

Academic Editors: Sabrine Kheriji, Olfa Kanoun and Faouzi Derbel

Received: 19 September 2022
Accepted: 8 October 2022
Published: 14 October 2022

1. Introduction

Recent developments in information and communication technology (ICT) have revolutionised the whole healthcare system. The main aim of smart healthcare systems is to enhance the quality of healthcare and reduce related costs. The introduction of IoT in the healthcare system significantly increased the processing of large data for targeted services on a daily basis [1]. The smart healthcare system collects the patient's health information (PHI), including personal identifiable information (PII), and shares that information with relevant stakeholders to provide medical services to the patient [2]. The idea of smart healthcare has been researched in many directions to provide healthcare services over a connected network. The smart ambulance, patient monitoring, nurse reservation, smart hospital, and blockchain-enabled security system are proposed to support the smart healthcare system in smart cities. The smart healthcare system architecture involves all the important stakeholders, including government, hospitals, medical research institutes, pharmaceuticals, clinics, and transport systems, to ensure timely services to citizens. Figure 1 describes the information flow among the components/stakeholders in a smart healthcare ecosystem.

A smart healthcare system includes the Internet of Medical Things (IoMT) as a non-separable part of the healthcare system to provide data for better diagnosis. The IoMT is a connected infrastructure of smart medical devices that connect with smart healthcare via the internet. IoMT with mobile application enables the data collection and sharing of patient information to doctors or hospitals for the prevention of chronic issues, and the tracking, monitoring, and better control of diseases [3]. The mismanagement of patient data resulted in many kinds of data breaches. The Health Insurance Portability and Accountability Act (HIPAA) stated that 13,236,569 medical records were breached in 2018, double the record breaches in 2017. The data breaches expose economic threats, possible social stigma, and mental anguish (Health privacy project, 2007) [4]. As the usage of technology increases in the healthcare system, various information about patients' health also flows in the system with or without necessary regulations. The service providers collect a good amount of PII information to provide user-centric services. In addition, the gathered information is shared with other stakeholders without the necessary consent of the patient. In response to increasing threats to the privacy of PII, the EU published the General Data Protection Regulation (GDPR) in 2016. In particular, Art. 25 of the GDPR, "Data Protection by Design and by Default", is the most interesting and controversial article since it addresses the anonymisation mechanisms [5]. Healthcare is one of the domains where a large amount of data are being managed on a daily basis [6]. Blockchain is able to maintain a large distributed database [7]. Blockchain plays a crucial role in healthcare applications for improving medical record management, insurance claim processes, accelerating clinical/biomedical research, and advancing the healthcare data ledger [8].

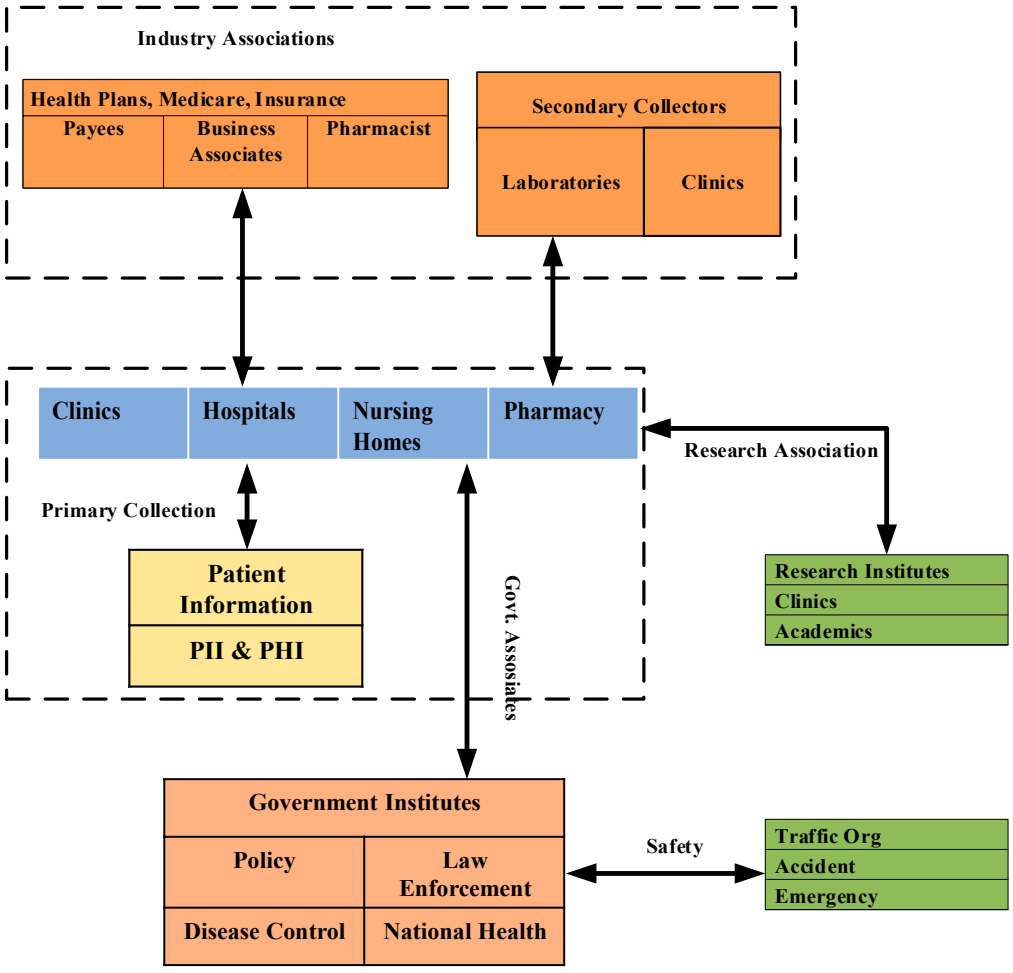

Figure 1. Smart healthcare system architecture.

A smart healthcare system includes multiple stakeholders, as presented in Figure 1, and has multiple communications among these stakeholders. The most commonly used truncations involve patients, such as hospitals, clinics, nursing homes, and pharmacies collecting patients' health data to provide medical services. Government institutes use patients' information for health policy making, disease control (such as COVID-19), law enforcement, and national health guidelines. The transpiration system is also an active participant in a smart healthcare system to handle accidents and emergency services. Research institutes and industry associations also play important roles in a smart healthcare system to provide quality health services to patients.

In this context, this paper proposes a framework that is GDPR "privacy by design" and "Right to be Forgotten" compliant for data storage and sharing in the smart healthcare system using blockchain. It is highlighted that the GDPR is considered in this research as the regulation covers all personal information protection in any area of usage, while HIPAA covers information protection in the health insurance area only. Moreover, the limit on data access time for requesters is provided in the GDPR only.

Blockchain technology is a distributed security solution for healthcare applications. The main characteristics of the blockchain include decentralised data management, immutable audit trails, data provenance, robustness, availability, security, and privacy. The distributed data-centric security characteristics increase the suitability of blockchain for healthcare applications compared to traditional databases. The proposed framework uses blockchain in a smart healthcare system to store non-personal information. Smart contracts are designed to share health data. Based on prior permission, the requestor can access information for a period. Moreover, information sharing is auditable because the transactions are stored on a blockchain. Despite the advantages mentioned above, blockchain has two major issues. First, data cannot be deleted after uploading on blockchain because blockchain provides immutability. Second, when a large volume of data are saved on the blockchain, retrieval and search of information are inefficient. To deal with these issues, an Inter-Planetary File System (IPFS) is used in the proposed framework. The framework separates the PII and PHI with the public information and stores the private information offline, separated with other public information. The framework uses IPFS to store critical information, including PII and PHI, off-chain. IPFS is a distributed data storage file system. Other members cannot access this personal information, except the owner/creator. Further, a protocol is embedded to delete the information on IPFS to make the framework comply with the GDPR's "Right to be Forgotten" rule. The key contribution of the paper can be summarised in the direction of GDPR "Privacy by Design" as follows:

- Firstly, a GDPR-compliant data storage and sharing framework using blockchain is proposed for smart healthcare systems while storing public information on blockchain and private information (such as PII, PHI, etc.) off-chain.
- Secondly, IPFS is used to store private data in an encrypted form. Users and IoMT devices can upload data on IPFS, and only owners can access the data.
- Thirdly, smart contracts are designed to share the off-chain data. Further, a proxy re-encryption network is used to share the encrypted data.
- Finally, the proposed blockchain-based framework is implemented using permissioned blockchain along with IPFS and an oracle proxy re-encryption network, and evaluated in comparison with the state-of-the-art protocols, considering several metrics for blockchain-based healthcare systems.

The remainder of this paper is organised as follows: Section 2 elaborates on related studies on GDPR and smart healthcare, and reviews the literature on data storage and sharing techniques using blockchain. The proposed blockchain framework to store and share PII and an elaboration and detailed description with scenarios are presented in Section 3. Experimental results and their analyses are discussed in Section 4. Finally, the conclusion and future works are presented in Section 5.

2. Literature Review

This section reviews related literature on the GDPR, healthcare data storage, and sharing using blockchain technology in smart healthcare systems. Further, healthcare data storage and sharing using blockchain technology in a smart healthcare system is described while focusing on on-chain healthcare data storage and sharing using blockchain and off-chain healthcare data storage and sharing using blockchain.

2.1. General Data Protection Regulation (GDPR)

The first draft of the GDPR came in 2012 in place of the data protection framework. The European Union adopted the GDPR in 2016 and enforced it in May 2018 [9]. Though data protection is present in other countries as well, such as HIPAA in the USA, the IT Act in India, the Privacy Protection Act in Australia, Canada's Personal Information Protection act, etc., the scope of the GDPR is broader and more comprehensive to protect the PII [9,10]. While HIPAA focuses on health insurance-related data, there is no clause in HIPAA on the collection of PII by the agencies. The GDPR covers a total of 99 Articles under 11 Chapters. It defines the following roles in protecting the personal data of users:

- The data subject is an individual living whose data are collected, held, or processed.
- The data processor defines why and how the personal data should be processed
- The data controller analyses or processes the data on behalf of the data processor
- Data protection officers monitor the data protection strategy and its implementation.
- The supervisory authority audits GDPR compliance.

The GDPR defines six data processing principles. These principles should be followed by a controller at the time of collecting, storing, and processing personal data. Personal data must be:

1. Managed fairly, lawfully, and transparently
2. Relevant, adequate, and limited to what is necessary
3. Updated and accurate
4. Stored for a fixed time period
5. Processed with integrity
6. Collected for a reasonable purpose.

GDPR, Chapter 1, Article 4 "Definition" includes the definition of personal data as "'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person". The GDPR introduced stronger controls on personal and special categories of data. The definitions can be decoded in Table 1 [1].

Table 1. Personal data category.

Personal Data	Special Category of Personal Data
Name	Race
Address	Religion
Email address	Sexual orientation
Photo	Health information
IP address	Biometric data
Location data, etc.	Genetic data, etc.

Chapter 3 and Articles 12–23 explain the rights of data subjects. The data subjects possess the following rights: right to inform, right to access, right to rectifications, right

to erasure, right to restrict processing, right to data portability, right to object, and rights that concern on automated decision making and profiling [11]. Personal data are processed only if data subjects have given their consent. The consent should be given freely, specific and unambiguous (GDPR, Article 6). The meaning of consent at the technical level can be defined as the data processor who wants to access or process the data subject's personal information and shall ask for consent approval from the data subject. The data subject shall have the right to withdraw the consent approved for a specific party (Art. 7, Chapter. 3 GDPR).

Data processors and controllers must ensure the organisational and technical measures necessary to implement data processing principles effectively (Art. 25 GDPR). Article 25 should be followed by the IT system when handling personal data. The user's privacy should be promoted as the default setting in an IT system and implemented during the design stage [5]. The privacy by design principle enforces organisations to consider privacy from the start of the project to throughout all the phases of the design and development of products or services rather than after the development of products or services. However, this is the major widespread gap observed in adopting a privacy by design principle in engineering practice because of different mindsets between technical and legal teams [11]. Privacy by design: GDPR, Article 25, defines privacy as being incorporated in the system from the design time. Privacy must be part of every protocol, standard, and process that builds the system. Privacy by design has the following seven principles [11,12]:

- Privacy as the default
- Proactive rather than reactive
- Respect for user privacy
- Privacy embedded into designs
- Full functionality
- Transparency and visibility
- end-to-end security

GDPR's right to be forgotten, Article 17, defines that the data subject has the right to erase the personal information in the system. It means that individuals have the right to define the time limit to access their personal data, and controllers or requestors must erase the personal information concerning them without undue delay [12]. In other words, personal data must be erased from the system after fulfilling the desired data collection purpose. The proposed system refers to the GDPR (Article 25, privacy by design and Article 17, right to be forgotten) to propose a secure framework to store and share personal data in smart health systems. A detailed description of the framework is provided in Section 4. We completely understand the significance of this critical situation of consent processing. Towards this, it is clarified that the patient's signatory consent is necessary to receive any medical treatment, test, or laboratory examination. However, a close relative's consent is also admissible in the case of medically incapable patients. The consent must be voluntary, informed, and with capacity. Voluntary means the consent decision should be of their own, not influenced by others. Informed means all related information must be available before the consent processing.

2.2. On-Chain Healthcare Data Storage and Sharing Using Blockchain

MedShare enables the sharing of medical records to third parties, such as research institutions, using cloud services. A smart contract-based data access auditing and access control of health records stored on the cloud has been proposed [13]. A patient-centric health data access model has been suggested while utilising MPC (multi-party computing) for data sharing computations on behalf of the patient [14]. In this model, blockchain has been utilised as a database for storing health records. Blockchain usage in medical image sharing has been proposed while storing medical files on the healthcare service provider and then sharing a link of files on blockchain [15]. This technique is not scalable; as the amount of data increases, the performance degrades. Blockchain-based solutions for access control and privacy preservation for EHR sharing have been proposed [16,17]. However,

both research works face interoperability issues. In these techniques, the system is less efficient because of manual interference.

Some researchers also proposed a framework for sharing medical data on the cloud or mobile applications. A technique for sharing data on mobile applications with Amazon cloud computing using the Ethereum Blockchain platform has been suggested [18]. A blockchain-based architecture for managing personal identifiable information (BcPIIMS) has been proposed while separating PII and non-PII and storing the PII off-chain [16,19]. On the same theme, a GDPR-compliant personal data management platform using a blockchain and smart contracts has been suggested [20]. This platform provides a decentralised mechanism to process service providers' and owners' personal data. In addition, blockchain technology empowers data transparency and data provenance to the platform. These solutions focused on access control and data integrity for health records. In these solutions, the actual data shall be transferred on a blockchain, and this causes communication and computation overheads in data transmission. However, data sharing is not sufficiently discussed. Further, the proposed solutions did not include IoMT data, which are an important part of the healthcare system [13–20].

2.3. Off-Chain Healthcare Data Storage and Sharing Using Blockchain

A detailed survey on IPFS and blockchain storage solutions for healthcare is presented [21]. Some practical approaches have been proposed, which should be implemented, from the design to the development of IoT applications for data collection and sharing in the healthcare system [22]. A blockchain-based patient health record system has been proposed while implementing multi-party authorisation (MPA) using a smart contract [23]. The proposed system utilises an Inter-Planetary File system to store the patient health record and a trusted oracle re-encryption network in the architecture for sharing among other parties. The architecture has been analysed in terms of security, confidentiality, and integrity. However, the researchers do not include medical device data control. A private blockchain-based health information exchange information (HEI) system has been suggested while using permissioned blockchain to limit the participants and smart contracts that implement the access control list to access the patient health in the health record exchange system [24]. The system contains two-levels, a smart contract level and an application level of data security for patient information. A health chain scheme has been suggested to preserve large health data privacy based on blockchain [25]. The scheme has two different chains to separate the patient and doctor data. Health data are stored in encrypted form and have an access control list. Further, the patient has control over permitting data access to a specific doctor or revoking the data access permission.

A blockchain-based, fully decentralised multi-party authorisation solution has been proposed to provide a source of access or permission logs while maintaining immutability, auditability, and security [26]. This solution uses IPFS to store the data off-chain, and logs are maintained on a blockchain. In the system, the data owner uploads the encrypted file with a symmetric key on IPFS and its encrypted keys. The keys are encrypted with the wallet's public key shared between the owner and MPA. Further, smart contracts, which have a hash of all data, are deployed to provide access to other parties. The major shortcoming is the high cost of operation due to the requirement of multiple encryptions and decryptions for sharing the data with others. A blockchain solution has been proposed to provide remote users with online doctor consolations and prescriptions. Telemedicine technology provides high-quality health servicing to remote area patients with the help of advanced technology such as mobile, IoT, blockchain, etc. As the involvement of ICT has increased in healthcare, data breaches, fraud, incorrect diagnosis and prescription, and other security risks have also increased. So, an Ethereum blockchain-based and smart contract-assisted framework have been suggested for solving these issues and transparency achieved by storing the logs of the healthcare system on blockchain [27]. They stored doctor prescriptions and other data on IPFS to save the cost of the system. However, sharing the

patient record with other doctors or institutions was not discussed. Further, they proposed a solution for a single organisation, so scalability was also not considered.

Blockchain and IPFS have also been presented as storage layers in the healthcare system [28]. Blockchain is used to store all the transactions generated on data storage, and IPFS is used to store the actual data. For fast search and retrieval of data on IPFS, the IPFS hash of data, including the database index, is also stored on blockchain. On the storage of data on IPFS, the data are divided into 250 bits each, and SHA-256 is used to produce the hashes. Further, base58 encoding is used to encode the generated hash, and these encoded data are used to retrieve the data from the IPFS network. The system provides a robust and secure infrastructure to the participants; only the registered participants can get the data. The system places mechanisms to stop data theft and unauthorised access. The system faces some shortcomings in that the system does not support scalability, as this is proposed for a single hospital only. Further, the emergency cases have also not been managed by the system.

3. The Proposed Blockchain-Based Data Storage and Sharing Framework

This section describes the detailed design of the proposed blockchain-based data storage and sharing of IoMT data in smart healthcare. Figure 2 shows the main component of the proposed blockchain-based system along with its workflow in Box 1. In the system design, IoMT device interaction is different to other stakeholders' (doctors, patients, hospitals, etc.) interaction with the system. The participants of the blockchain network, except for the constrained IoMT device, directly interact with the blockchain through a smart contract to read and write the content on the blockchain. The IoMT devices do not interact directly with the blockchain. These devices interact via owners such as patients, doctors, hospitals, and other owners. Further, PII and PHI are stored off-chain on IPFS, and the hash of data are stored on the blockchain to maintain immutability and transparency. The rest of the section will explain each component of the system.

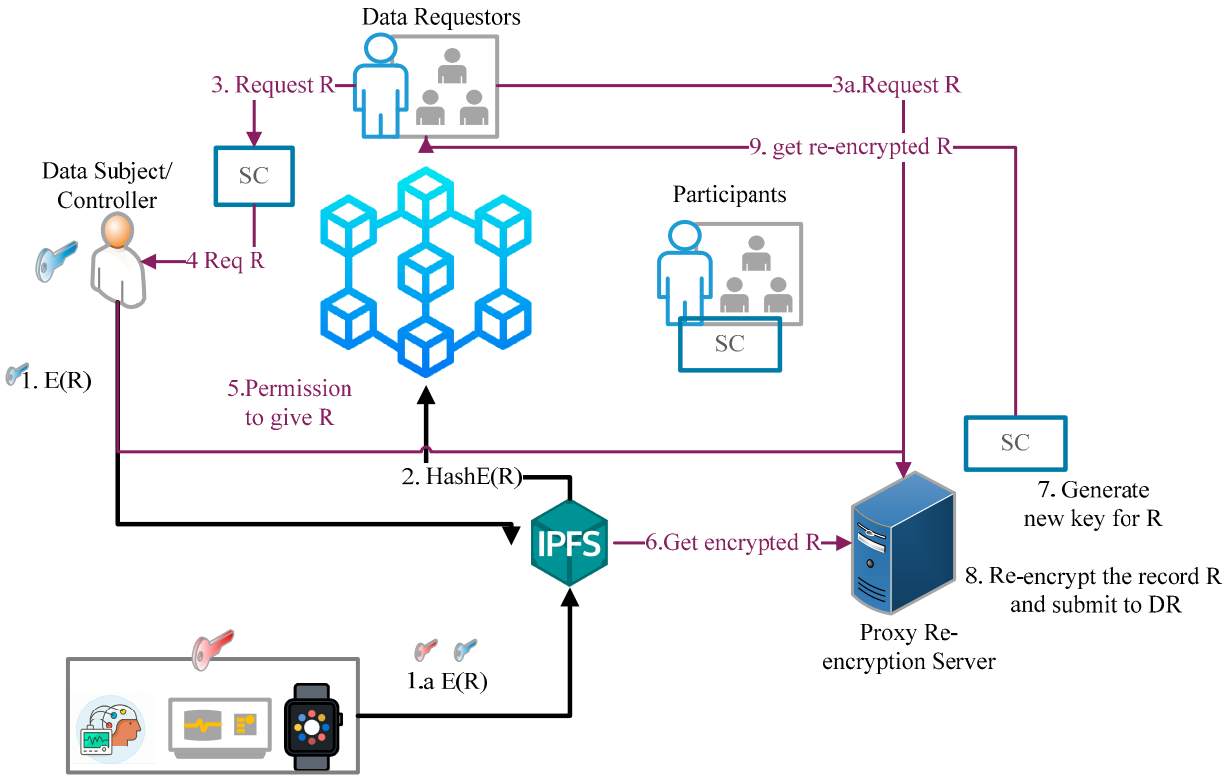

Figure 2. Architecture of a blockchain-based data storage and sharing.

Box 1. Workflow of the proposed blockchain based data storage and sharing architecture

1. Data subject (DS) of data uploads the encrypted record with her symmetric key on IPFS.
   - 1a. IoMT devices upload the record encrypted with its symmetric key, and after that it is encrypted with the owner's key on IPFS.
2. Hash of record is pushed on a blockchain.
3. The data requestor (DR) requests the record to data subjects with a smart contract.
4. DS gets the request to access the record from DR.
5. DS grant permission to access the hash of record R at IPFS to proxy the re-encryption server.
6. Proxy re-encryption server gets the encrypted R with the help of the received hash of R.
7. Proxy re-encryption server generates a new key.
8. IPFS re-encrypts the encrypted record R and sends it to DR with a smart contract.
9. DR decrypt the record with their own symmetric key, and the record R.

3.1. IoMT Devices

The IoMT devices are implanted with patients to monitor the activity and health status of the patients. These IoMT devices have limited computing, network, and storage power. Due to limited capabilities, the IoMT devices need a gateway to interact with the blockchain and IPFS. In the system design, the owner of the devices acts like a gateway, and devices interact with blockchain and IPFS with the help of owner nodes. The data are collected or sensed by the IoMT devices, stored off-chain, and their hash is logged on chain with the timestamp. When a participating node downloads data from the off-chain store, it can cross-verify the data with the hash of data downloaded from the blockchain. This enforces transparency, integrity, and trust in the system.

3.2. Participants

The proposed system is designed for a private blockchain network, so all the participants must register in the system. Each participant is treated like a blockchain node. Participants are all important stakeholders of smart healthcare such as hospitals, doctors, patients, drugs and medical device manufacturers, medical centres, and many others who connect with healthcare to get or provide services. The GDPR terminology is used to explain patient data storage and sharing scenario. The patient is a data subject and willingly provides his information to data collectors and the data analyser. Table 2 shows the mapping of terminologies between the healthcare system and GDPR roles.

Table 2. Healthcare system and GDPR roles.

Healthcare System Stakeholder	GDPR Terminology
Patients	Data subjects (DS)
Doctors, hospitals, clinic centres	Data collectors (DCs)/Data analyser (DA)
Medical device and drug manufacturers, pharmaceutical department, nurses	Data analyser/data collectors
Lower-level professionals such as nurses	Data leakage identifiers

3.3. Off-Chain Data Storage (IPFS)

IPFS stores the IoMT stream data and other health data such as health reports, prescriptions from doctors, critical diseases history, etc. The critical information that can be used to harm the subject or PII is stored off-chain, and other information can be stored on the blockchain directly. The information of IoMT devices and other information is stored on IFPS, encrypted to provide secrecy. The data are distributed, and at the same time, are secure, and only the data subject can access the data. There are two motivations behind off-chain storage. The first one is to comply with the system against the "Right to be Forgotten" rule under the GDPR to protect the privacy of the data owner. Further,

the owner of data has full control over their data. The second one is to reduce the cost of storing data on-chain. The IoMT devices first encrypt the data with their symmetric key and encrypt the symmetric key with the owner's public key. Then, the encrypted key is stored on IPFS along with the encrypted data. Only the hashes of off-chain data without the actual data are stored on the blockchain. The deletion of data on IPFS to practice the "Right to be Forgotten" right will be discussed in the implementation section. Further, the implementation section also discusses the communication between blockchain and IPFS and the communication of nodes/participants with blockchain and IPFS. Figure 3 illustrates the sequence flow of uploading the data on blockchain and IPFS.

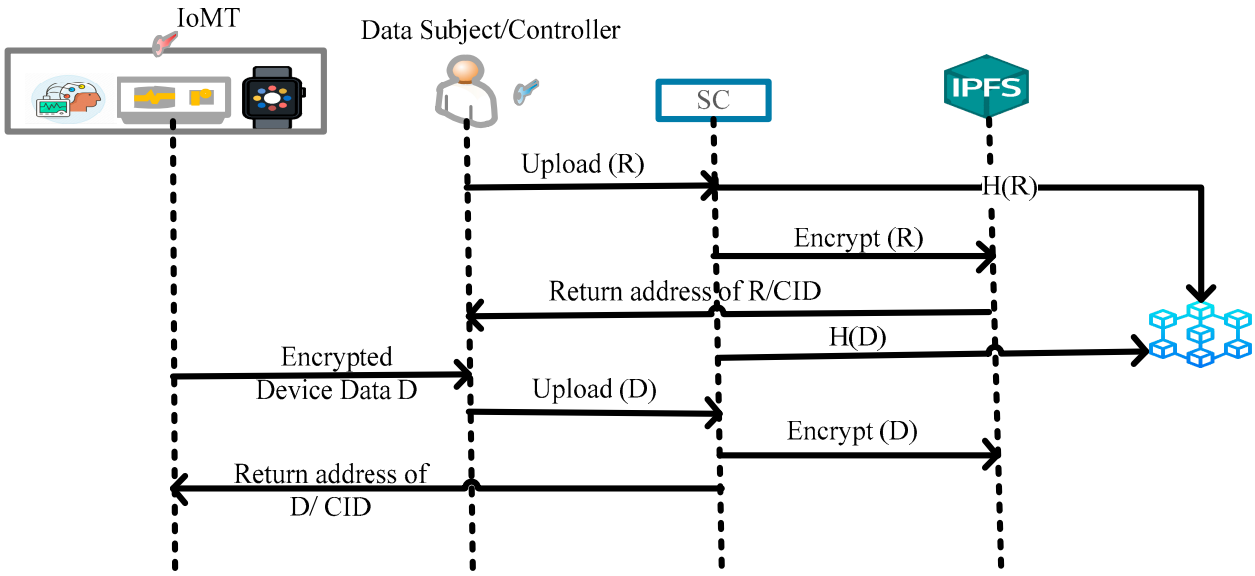

Figure 3. Sequence flow for uploading data.

The device with a symmetric key K_{device} encrypts sensed data D before storing it on IPFS. Further, the owner of the device encrypts the symmetric key of the device K_{device} with the owner's public key (E_k) and stores both data E_D and E_k on IPFS and returns the address to the device. Algorithm 1 defines the data upload of device D.

Algorithm 1: Record upload on IPFS by IoMT

1. **Start**
2. Device with data D and symmetric key K_{device}
3. Device encrypts D with symmetric key:
$$E_D \leftarrow encrypt_{K_{device}}(D)$$
4. Encrypt the device key with the owner's public key:
$$E_k \leftarrow encrypt_{\mathbf{PBown}}(K_{device})$$
5. Store (E_D, E_k)
6. Return CID
7. **Exit**

Doctors, lab technician, and other stakeholders also store their report R on IPFS in encrypted form, as described in Algorithm 2. Here, in the Algorithm 2, node means all stakeholders of smart healthcare systems who participated and registered in the blockchain network.

Algorithm 2: Record upload on IPFS by Node

1. Start
2. Node with record R and symmetric key K_{node}
3. Node encrypts R with symmetric key:
   $E_R \leftarrow encrypt_{K_{node}}(R)$
4. Encrypt the node key with the public key:
   $E_k \leftarrow encrypt_{\mathbf{PBnode}}(K_{node})$
5. Store (E_R, E_k)
6. Return CID
7. Exit

3.4. Blockchain

Blockchain is the core component of the proposed system. All stakeholders of smart healthcare register themselves in the smart healthcare blockchain network to get the services. According to the access control list, the participants, nodes, or stakeholders have access privileges on the blockchain. The access control list is also saved on the blockchain, and smart contracts are designed to implement the access control list. The blockchain provides data provenance, data tracking, logging of transactions, and accountability of actions performed by the participants.

3.5. Smart Contract

The smart contracts are deployed on the blockchain, and participants of the blockchain run the smart contract to perform a specific task. The smart contracts are designed to provide authentication, authorisation, access control, and logging of the transactions on the blockchain. The smart contract offers three main functionalities. First, the owner of the IoMT device controls the device's data and streaming using a smart contract. Second, the participants use a smart contract to share the data among the network. Third, the owner shares data access control of devices with authorised nodes. For example, a patient gives access to the thermostat to the doctor to check the temperature. The doctor provides the prescription or treatment to the patient based on IoMT device data.

3.6. Data Sharing

The streamed data from the IoMT devices and uploaded by the participants is stored on IPFS in encrypted form. Only users authorised by the owner of the data can access the encrypted data, which preserves the privacy and confidentiality of data. The next step is how the requester gets the decrypted data and conducts the analysis to provide some health service. The smart contracts are designed and deployed on blockchain to share the data with other participants. Further, the proxy re-encryption server is also deployed to ensure the confidentiality and privacy of data. The re-encryption server also maintains a copy of the symmetric key of all stakeholders and IoMT devices.

Whenever a participant wants to access the encrypted data, she sends a request to the owner of the data or device (data subject). If the data subject wants to share the data, then they send the address of the IPFS tuple and simultaneously send consent to the re-encryption server to generate the new re-encryption key along with an encrypted symmetric key. There-encryption server then generates a new key with the private key of DS and the public key of the requester. The re-encryption server encrypts the encrypted key with a new generated key and sends the re-encrypted key to the requestor. The re-encrypted key is with a timestamp, which means the key will be invalid after a specified time. The requestor decrypts the re-encrypted key with her private key to obtain the symmetric key. After getting the encrypted key, the requestor decrypts the data and analyses it on the basis of the desired service. Figure 4 describes the sequence flow for sharing the data in the system.

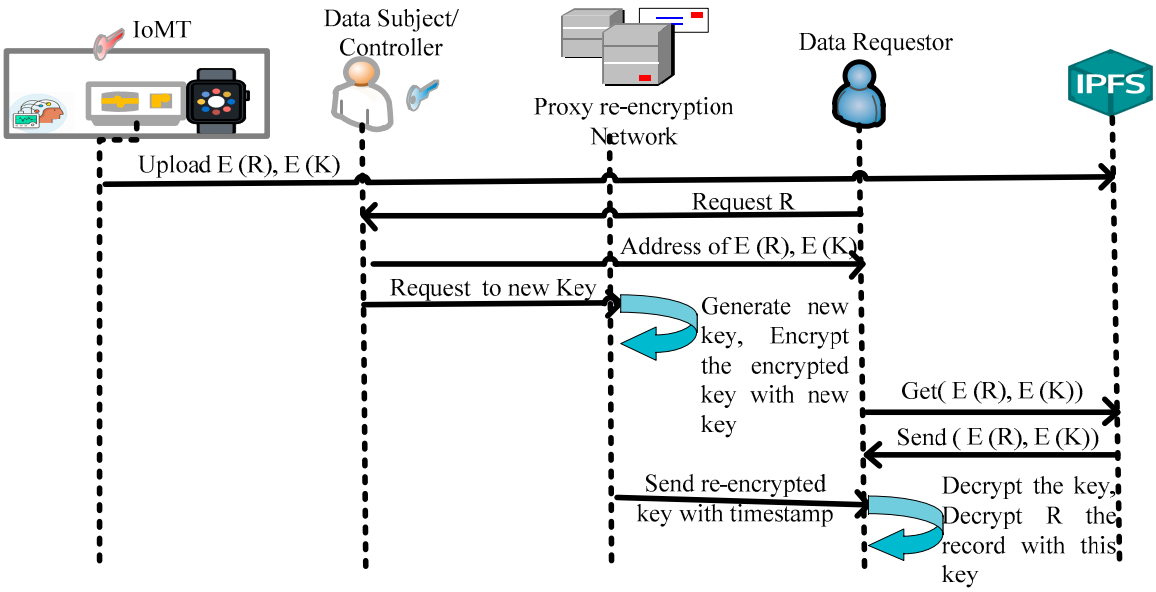

Figure 4. Sequence flow for sharing data.

After uploading the record, only the owner who uploaded the record controls the data and can share it with other participants. For example, a patient consults a doctor regarding a specific disease and needs access to a patient's health record. The doctor requests the patient to share the specific record. Algorithm 3 describes the sharing process of the record.

Algorithm 3: Record R sharing on IPFS by Node

1. **Start**
2. Participant *P* request for R record tuple: E_R, E_k to DS
3. If DS accepts sharing request
4. Then generate re-encryption key N with public key of participant P and private key of DS for the time T
5. DS send N to the proxy re-encryption server
6. Re-encryption proxy network encrypts E_K with N
$$E_{N_{EK}} \leftarrow encrypt_N\ (E_K)$$
7. Send re-encrypted $E_{N_{EK}}$ to Participant P
8. Participant P decrypts $E_{N_{EK}}$ with her private key P_R
$$K_{node} \leftarrow decrypt_{PR}\ (E_{N_{EK}})$$
9. Decrypt the record R with K_{node}
$$R \leftarrow decrypt_K\ (E_R)$$
10. End If
11. Else denied
12. **Exit**

3.7. Deletion at IPFS

For the compilation of deletion of content in GDPR, the framework follows the "Proof of ownership" concept proposed in Politou et al. [2]. The proposed model saves the PII and PHI on IPFS (offline), as discussed earlier. The ownership of the file is added with the file while uploading it to IPFS. When the owner of content wants to delete content permanently, she sends an erasure request on IPFS. The requester sends a hashed version of the file along with the content-dependent key d. The key d is derived from the master key that each user owns. This extension is only for PII and PHI, and other information can be shared without proof of ownership. The user appends the proof when she wants to delete specific information and preserve the right to be forgotten rule of GDPR.

The protocol is described in three phases: initialisation, record distribution, and record deletion, and five functions: *KeyGen*, *RecKeyGen*, *ProofGen*, *GenDelRequest*, and *CheckProof*.

The protocol runs these functions:

KeyGen $(1)^m \rightarrow mKey$: A random generation function which generates the master key $mKey \in \{0,1\}^m$ for each user. The user keeps this key secret.

RecKeyGen ($mKey$, R) $\rightarrow$ *rKey*: A function that generates the record *key rKey* for the master key *mKey* and record $R \varepsilon \{0,1\}^*$. In the proposed work,

$$RecKeyGen\ (mKey,\ R)\ \in\ K_{mKey}\ (h(R)) \tag{1}$$

ProofGen ($rKey$, R) $\rightarrow$ P: This function generates the proof of ownership for the record R using the record *key rKey*.

$$ProofGen\ (rKey,\ R)\ \in\ k_R\ (h(R)) \tag{2}$$

GenDelRequest (R, *rKey*) $\rightarrow$ (h, *rKey*): This function generates the delete request for record R and record *key rKey*. This function results in a delete request with the hash of record S and record *key rKey* as proof of ownership.

$$GendelRequest\ (R,\ rKey)\ \in\ (h(R), rKey) \tag{3}$$

CheckProof (h, *rKey*) $\rightarrow$ (*Pass*, *Fails*): This function checks that the owner pushed the record R with hash S. This function gives a pass only if the owner pushed the record.

In the initialisation phase, each user runs *KeyGen*(), generates the master *key mKey,* and keeps the *key* secret. The master *key* is different to the private *key*.

In the record distribution phase, the user stores a record on IPFS using the record *key*. The functions *RecKeyGen* () and *ProofGen* ($rKey$, R) are used to generate the record *key rKey* for the record R and its ownership proof P.

To distribute the record, the user commits a tuple (R, P) that distributes the record on the IPFS network. The IPFS network uses distributed sloppy hash table (DSHT) and BitSwap protocol to distribute the record over the network [4]. To delete a record R that was uploaded earlier, the user uses *GenDelRequest* () to delete the record on the IPFS. The user sends the request as tuple d = (*h(R), rKey*) to the network. After receiving the request, the node in the network runs *CheckProof* () to locate the *h(R)* and verify the ownership. If the request is valid, the node forwards the request to the neighbouring node to delete the record R by sending the *h(R)*. Algorithm 4 describes the same process. It is highlighted that the proposed *GDPR* compliant framework can also be utilised in other domains such as a connected vehicle traffic environment [29–31] or electric vehicle charging network environment [32–34] for driver and vehicle data protection. In the next section, experimental implementation and analysis of results are presented.

Algorithm 4: Record delete by the owner

1. Start
2. Node receives delete request d = ($h(R)$, *rKey*)
3. If the $h(R)$ = h stored with the node then
4. If CheckProof (h, *rKey*) = = true then
5. Delete R from the local store
6. Forward d to neighbour nodes using DSHT
7. End if
8. End if
9. Exit

4. Experimental Results and Discussion

In this section, simulation experiments are performed to carry out a performance analysis of the proposed blockchain-based privacy-preserving framework in a smart healthcare system. Simulation setting, parameters, and performance analysis of results are discussed for a smart healthcare environment. The discussion is divided into three steps: the first

is GDPR compliance, the second is security and privacy analysis, and the third is performance evaluation. The system uses the Hyperledger fabric blockchain platform to make a distributed network, and smart contracts (called chain code in the Hyperledger fabric) are implemented in GO language and deployed on the blockchain. Further, the IPFS is used to store the IoMT data and other data, as specified in the architecture. The first step in implantation is creating the distributed network and the ledger. The network is built using five nodes, i.e., patient along with two IoMT devices, doctor, hospital, laboratory, and government.

The prototype was implemented to analyse the performance of the system. Many obstacles were faced during the implementation of a prototype. The major obstacles were low-performance matrix such as time to verify the transactions, high query time, high search time due to system configuration such as random access memory (RAM) and read-only memory (ROM) size and processor capacity, etc. So, the implementation was moved to a larger RAM and ROM with a higher capacity processor system to get the desired result. Further, the complexity of programs (smart contract and network design) was also very crucial. The programs were also improved many times to get lower complexity, directly impacting the performance. So, we can conclude that the performance depends on the system components such as central processing unit (CPU), RAM and ROM size, the complexity of smart contract programs, and other algorithms.

4.1. GDPR-Compliance

As discussed in Section 4, the data owner can perform CRUD operations on their data, and others are not able to modify these rights. This defines the "Right to access" and "Right to rectification". Smart contracts support the "Right to be informed" by implementing the request and access policy before sharing health data with other parties (who are not owners). The owner has full access of their own data and can manage data usage. This is how data owners exercise the "Right to restricted processing" and "Right to data portability". The deletion of data on IPFS is defined to comply with the "Right to be Forgotten". The owner can delete their own data at any time on IPFS, and the blockchain does not have any personal data. The deletion of PII or PHI on a blockchain is proposed to comply with the "Right to be Forgotten" rule of the GDPR. The PII and other critical information, including PHI, is stored on the IPFS database off-chain. The data owner can delete the off-chain data via smart contract using a proxy re-encryption network. The transactions of uploading data, deleting data, or any modification of data are present on the blockchain and these transactions do not include the actual data.

4.2. Security and Privacy Analysis

Further, the proposed framework is analysed for security and privacy using the following parameters:

- Authentication: The proposed solution is based on a private blockchain that implies a secure identity-based solution. Participants must register on the network before uploading, accessing, or sharing the health data. All participants/stakeholders of the healthcare system are verifiable through the standard identity management system, i.e., identities managed by a trusted CA. It is noted that all the transactions are digitally signed at the proposal time. So, all the identities in the private network of the healthcare system are authenticated. In the prototype implementation, Hyperledger fabric service MSP is used for identity management.
- Privacy by design: GDPR, Article 25, defines that privacy must be incorporated into the system from the design time itself. In the proposed framework, privacy from the design is incorporated. The PII and other critical data are stored off-chain at the peer level on IPFS. The private data could share the private data with other participants on the chain with the help of smart contracts. The proposed framework enables confidentiality through off-chain data storage and sharing through smart contracts.

Only network participants have access to smart contracts and data transactions; this preserves confidentiality and privacy within the permissioned network.

- Visibility and transparency: The proposed framework ensures data transparency. All the transactions related to the private data are visible to the data controller, and the data controller is responsible for informing the data subject about their private data.
- Traceability: The proposed framework enforces trust in the system, as the data logs are stored on the blockchain ledger, and the blockchain provides immutability. The changes in data, data requests, data sharing, and other transactions related to data are stored on the blockchain and cannot be modified at any point. These logs can be used to track the data for forensics or other purposes.

4.3. Performance and Scalability

The proposed framework is applicable to serve many participants accessing data simultaneously. Therefore, the performance and scalability should be evaluated. The performance of a blockchain platform can be affected by many variables such as transaction size, block size, network size, as well as limits of the hardware, etc. In this subsection, the effectiveness and efficiency of the proposed framework are evaluated. To evaluate the proposed framework, Hyperledger tool Caliper is used, which is also utilised to evaluate the performance of various private blockchain frameworks such as Hyperledger Fabric, Sawtooth, etc.

Figures 5 and 6 present the latency and throughput of the READ WRITE operation on the blockchain. As presented in Figure 5, the WRITE operation takes more time than the READ operation. In READ operation, users throw a query via smart contract or other user interaction method and get the results. Whereas in WRITE operation, the user updates some data on a ledger or off-chain storage. The consensus algorithm also runs to sync up all nodes' data after a defined time. So, the whole process takes time greater than the READ operation. Further, the READ and WRITE operation time also increases with the increment in the number of nodes. As the number of nodes increases, the search time also increases in the case of the READ operation and WRITE time also increases accordingly. The throughput of the network is calculated on 200 TPS and 500 TPS workloads on READ and WRITE operations, respectively. As the number of nodes increases, the throughput for READ and WRITE operations decreases. Because, as the number of transactions per second increases, the database also increases, so the system takes more time to process the operations.

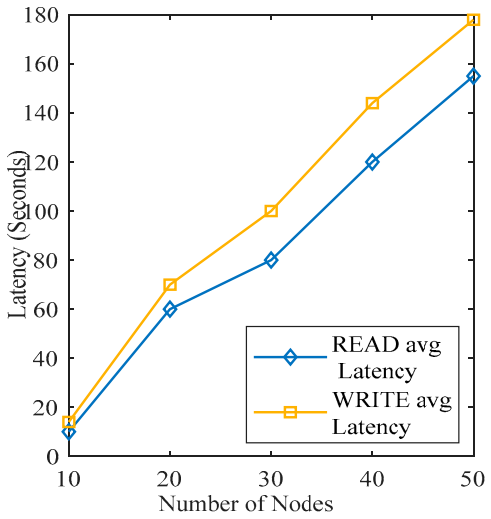

Figure 5. READ WRITE latency.

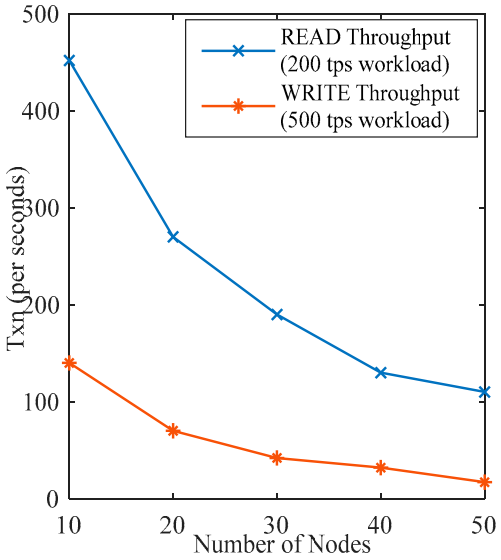

Figure 6. READ WRITE throughput.

The performance of READ and WRITE operations in the system is described in Figure 7. The throughputs of READ and WRITE operations on different workloads of 100 TPS, 200 TPS, 300 TPS, 400 TPS, and 500 TPS were collected to calculate the performance. As shown in Figure 7, the WRITE operation got the highest performance on a 200 TPS workload, and it was 157 TPS. Then, the performance started degrading as workload increased. In contrast, the READ operation performed best on 500 TPS as 498 TPS. After that, the performance started to degrade.

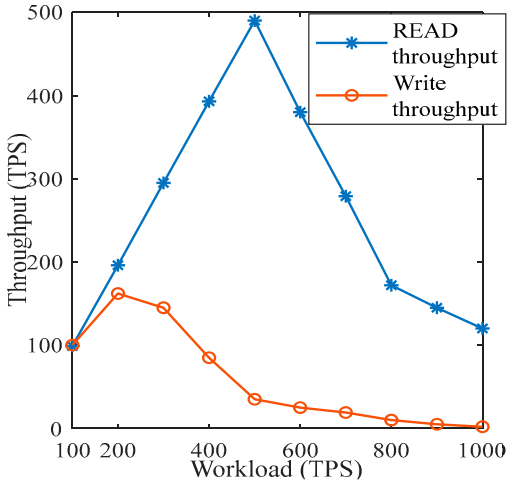

Figure 7. READ and WRITE performance.

The smart contract is deployed on the blockchain, and nodes trigger queries through a smart contract for different functionality such as storing the IoMT data, deleting the record on IPFS, requesting to share the record, etc. An increment in the number of nodes increases the number of smart contract queries, leading to a slowing down of the execution process of queries with the existing computation resources. As shown in Figure 8, the execution time of a smart contract increases with the increment in the number of nodes participating in the network.

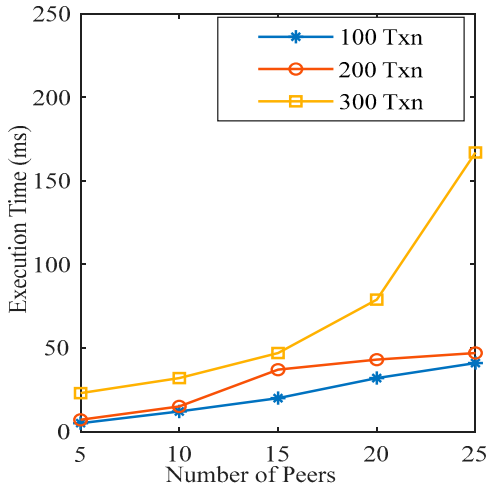

Figure 8. Smart contract deployment.

4.4. Comparative Results Analysis

The first comparison is between the computation and storage throughput with Healthchain [22] and the traditional system. The Healthchain takes 8.565 ms to generate the user transactions, and the traditional system takes about 130 ms. We analysed our system and found that it takes only 6.098 ms to generate the user transaction when only ten nodes are present in the network. Figure 9 represents the same. As the number of nodes increases in the network, the time to generate the transactions also increases. When the number of participants increases in the system, the number of transaction requests per second also increases. The increased transactions take time to compute with the existing computation resources. It complies that computation time and storage of the system increase with the extra number of participants. The computation time and storage were measured when the number of transactions was 50, 100, 150, 200, and 250 in the network. Figure 9 represents storage overhead as the number of transactions varies. The figure illustrates that as the number of transactions increases, storage overhead also increases.

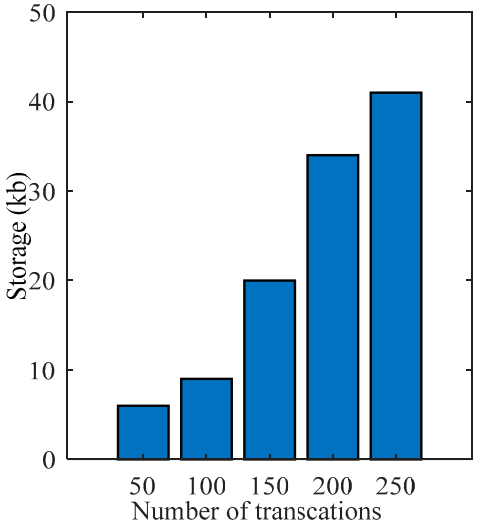

Figure 9. Storage overhead performance.

Figures 10–12 depict that the proposed framework ensures high accuracy in terms of security, privacy, and authorisation. These parameters are observed and compared with the previous work. Figure 10 presents the accuracy of security of the proposed framework along with the security accuracy of the FHIR Chain (FHIRC) [35], Attribute-Based Encryption (ABE) [36], and the Decentralised Telemedicine Framework (DTF) [27]. The results show that the proposed framework possesses high security accuracy (99.6 per cent) when the number of nodes is 600. At the same time and with the same number of records, DTF has 99.5 per cent, ABE has 98.5, and FHIRC only has 97.3 per cent security accuracy. Maximum authentication privacy is observed at 99.5 per cent when the number of records is 400, as presented in Figure 12. Maximum privacy accuracy is 99.6 per cent when the number of records is 600, as presented in Figure 11. The privacy and authentication accuracy are compared with FHIRC, ABE, and DTF. The results show that the proposed system has high accuracy compared to the state-of-the-art techniques.

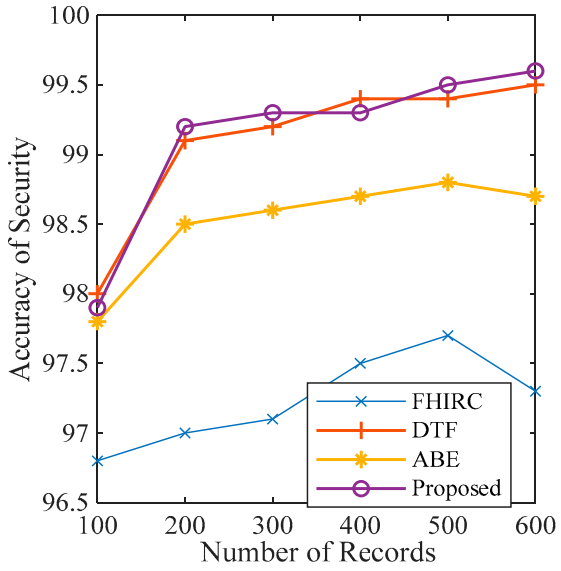

Figure 10. Comparison of security accuracy.

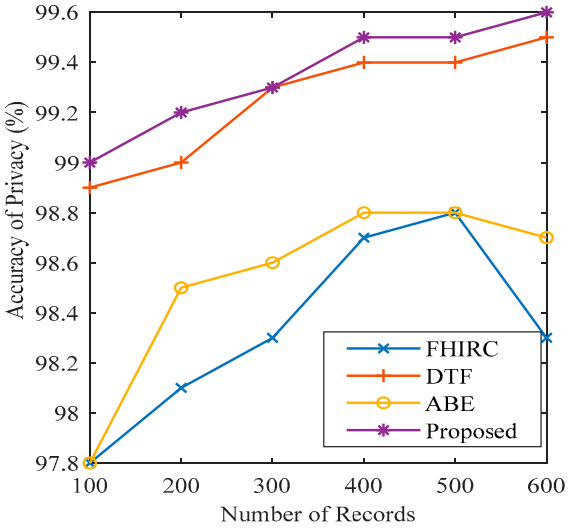

Figure 11. Comparison of privacy accuracy.

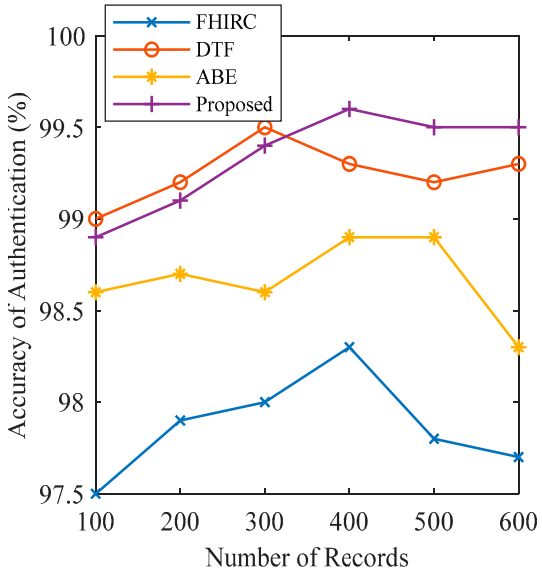

Figure 12. Comparison of authentication accuracy.

5. Conclusions and Future Work

This paper presents a GDPR-compliant data storage and sharing framework using blockchain for the smart healthcare system while storing public information on blockchain and private information (such as PII, PHI, etc.) off-chain. In the proposed framework, data control is given to the data owner. The medical data, including data from the IoMT devices, is managed (e.g., storage, option, sharing, and deletion) only by the data owner. IPFS stores the data offline to improve privacy and provide deletion control to the user. The data are stored in encrypted form on-chain and off-chain. The system uses a proxy re-encryption network to share the encrypted data. The result shows that the framework provides security and privacy to health data and gives control to the owner rather than the service provider. In addition, simulation results show that the proposed framework outperforms the state-of-the-art protocols. For the future perspective, the proposed framework can introduce the patient to the blockchain network to take a trace of their own data at any time. This can be performed using the integration of mobile API with the framework. Further, this paper does not include an emergency service scenario, and this can be considered in future research propositions.

Author Contributions: Conceptualisation, P.B.; Formal analysis K.K.; Investigation, P.B.; Methodology, P.B.; Resources, M.M. and O.K.; Supervision, S.K., O.K., M.M. and J.L.; Validation, K.K.; Writing, P.B.; Review and Editing, S.K., O.K. and M.M. All authors have read and agreed to the published version of the manuscript.

Funding: The research is funded by the School of Computer and Systems Science, Jawaharlal Nehru University, India.

Data Availability Statement: Research data will be available on individual requests to the corresponding author considering collaboration possibilities with the researcher or research team and with restrictions that the data will be used only for further research in the related literature progress.

Acknowledgments: The research is supported by the Department of Computer Science, Nottingham Trent University, UK.

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

Abbreviations

Parameter Definitions

K_{device}	Symmetric key of device D
K_{node}	Symmetric key of device node
E_D	Encrypted data D
E_R	Encrypted record R
E_k	Encrypted symmetric key of device
E_k	Encrypted symmetric key of node
PB_{OWN}	Public key of owner of device
E_R	Encrypted record R;
E_K	Encrypted symmetric key
$E_{N_{EK}}$	Re-encrypted key
K_{node}	Symmetric key of node

h: $\{0,1\}^* \rightarrow \{0,1\}^n$ is a secure hash function
$K_x : \{0,1\}^n \rightarrow \{0,1\}^a$ and $K_y : \{0,1\}^n \rightarrow \{0,1\}^b$ are key permutations where key $x \in \{0,1\}^m$ and key $y \varepsilon \{0,1\}^n$
$n, a, b, m \in N$

References

1. Kumar, K.; Kumar, S.; Kaiwartya, O.; Cao, Y.; Lloret, J.; Aslam, N. Cross-Layer Energy Optimization for IoT Environments: Technical Advances and Opportunities. *Energies* **2017**, *10*, 2073. [CrossRef]
2. Verma, G.K.; Singh, B.B.; Kumar, N.; Kaiwartya, O.; Obaidat, M.S. PFCBAS: Pairing free and provable certificate-based aggregate signature scheme for the e-healthcare monitoring system. *IEEE Syst. J.* **2019**, *14*, 1704–1715. [CrossRef]
3. Rahman, A.U.M.; Afsana, F.; Mahmud, M.; Kaiser, M.S.; Ahmed, M.R.; Kaiwartya, O.; James-Taylor, A. Toward a heterogeneous mist, fog, and cloud-based framework for the internet of healthcare things. *IEEE Internet Things J.* **2018**, *6*, 4049–4062. [CrossRef]
4. Yaraghi, N.; Gopal, R.D. The role of HIPAA omnibus rules in reducing the frequency of medical data breaches: Insights from an empirical study. *Milbank Q.* **2018**, *96*, 144–166. [CrossRef] [PubMed]
5. Schwerin, S. Blockchain and privacy protection in the case of the european general data protection regulation (GDPR): A delphi study. *J. Br. Blockchain Assoc.* **2018**, *1*, 3554. [CrossRef]
6. Chukwu, E.; Garg, L. A systematic review of blockchain in healthcare: Frameworks, prototypes, and implementations. *IEEE Access* **2020**, *8*, 21196–21214. [CrossRef]
7. Esposito, C.; De Santis, A.; Tortora, G.; Chang, H.; Choo, K.-K.R. Blockchain: A panacea for healthcare cloud-based data security and privacy? *IEEE Cloud Comput.* **2018**, *5*, 31–37. [CrossRef]
8. Kumar, S.; Dohare, U.; Kumar, K.; Dora, D.P.; Qureshi, K.N.; Kharel, R. Cybersecurity Measures for Geocasting in Vehicular Cyber Physical System Environments. *IEEE Internet Things J.* **2019**, *6*, 5916–5926. [CrossRef]
9. EUGDPR. EUGDPR—Information Portal. Available online: https://eugdpr.org/ (accessed on 4 July 2022).
10. Koops, B.J.; Leenes, R. Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by design' provision in data-protection law. *Int. Rev. Law Comput. Technol.* **2014**, *28*, 159–171. [CrossRef]
11. EU Data Protection Regulation. Available online: https://www.itgovernance.co.uk/data-protection-dpa-and-eu-data-protection-regulation (accessed on 7 August 2022).
12. Voigt, P.; Von dem Bussche, A. The EU general data protection regulation (GDPR). In *A Practical Guide*, 1st ed.; Springer International Publishing: Cham, Switzerland, 2017.
13. Xia, Q.; Sifah, E.B.; Asamoah, K.O.; Gao, J.; Du, X.; Guizani, M. MeDShare: Trust-less medical data sharing among cloud service providers via blockchain. *IEEE Access* **2017**, *5*, 14757–14767. [CrossRef]
14. Yue, X.; Wang, H.; Jin, D.; Li, M.; Jiang, W. Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control. *J. Med. Syst.* **2016**, *40*, 218. [CrossRef]
15. Patel, V. A framework for secure and decentralized sharing of medical imaging data via blockchain consensus. *Health Inform. J.* **2019**, *25*, 1398–1411. [CrossRef]
16. Shen, B.; Guo, J.; Yang, Y. MedChain: Efficient healthcare data sharing via blockchain. *Appl. Sci.* **2019**, *9*, 1207. [CrossRef]
17. Tanwar, S.; Parekh, K.; Evans, R. Blockchain-based electronic healthcare record system for healthcare 4.0 applications. *J. Inf. Secur. Appl.* **2020**, *50*, 1024–1046. [CrossRef]
18. Nguyen, D.C.; Pathirana, P.N.; Ding, M.; Seneviratne, A. Blockchain for secure EHRs sharing of mobile cloud based e-health systems. *IEEE Access* **2019**, *7*, 66792–66806. [CrossRef]
19. Al-Zaben, N.; Onik, M.M.H.; Yang, J.; Lee, N.Y.; Kim, C.S. General Data Protection Regulation Complied Blockchain Architecture for Personally Identifiable Information Management. In Proceedings of the 2018 International Conference on Computing, Electronics & Communications Engineering (iCCECE), Southland, UK, 16–17 August 2018; pp. 77–82.
20. Truong, N.B.; Sun, K.; Lee, G.M.; Guo, Y. Gdpr-compliant personal data management: A blockchain-based solution. *IEEE Trans. Inf. Forensics Secur.* **2020**, *15*, 1746–1761. [CrossRef]

21. Madine, M.M.; Salah, K.; Jayaraman, R.; Yaqoob, I.; Al-Hammadi, Y.; Ellahham, S.; Calyam, P. Fully decentralized multi-party consent management for secure sharing of patient health records. *IEEE Access* **2020**, *8*, 225777–225791. [CrossRef]
22. O'Connor, Y.; Rowan, W.; Lynch, L.; Heavin, C. Privacy by design: Informed consent and internet of things for smart health. *Procedia Comput. Sci.* **2017**, *113*, 653–658. [CrossRef]
23. Battah, A.A.; Madine, M.M.; Alzaabi, H.; Yaqoob, I.; Salah, K.; Jayaraman, R. Blockchain-based multi-party authorization for accessing IPFS encrypted data. *IEEE Access* **2020**, *8*, 196813–196825. [CrossRef]
24. Zhuang, Y.; Sheets, L.R.; Chen, Y.-W.; Shae, Z.-Y.; Tsai, J.J.P.; Shyu, C.-R. A patient-centric health information exchange framework using blockchain technology. *IEEE J. Biomed. Health Inform.* **2020**, *24*, 2169–2176. [CrossRef]
25. Xu, J.; Xue, K.; Li, S.; Tian, H.; Hong, J.; Hong, P.; Yu, N. Healthchain: A blockchain-based privacy preserving scheme for large-scale health data. *IEEE Internet Things J.* **2019**, *6*, 8770–8781. [CrossRef]
26. Kumar, S.; Bharti, A.K.; Amin, R. Decentralized secure storage of medical records using Blockchain and IPFS: A comparative analysis with future directions. *Secur. Priv.* **2021**, *4*, e162–e184. [CrossRef]
27. Abugabah, A.; Nizamuddin, N.; Alzubi, A.A. Decentralized telemedicine framework for a smart healthcare ecosystem. *IEEE Access* **2020**, *8*, 166575–166588. [CrossRef]
28. Marangappanavar, R.K.; Kiran, M. Inter-Planetary File System Enabled Blockchain Solution For Securing Healthcare Records. In Proceedings of the 2020 Third ISEA Conference on Security and Privacy (ISEA-ISAP), Guwahati, India, 27 February–1 March 2020; pp. 171–178. [CrossRef]
29. Cao, Y.; Kaiwartya, O.; Aslam, N.; Han, C.; Zhang, X.; Zhuang, Y.; Dianati, M. A trajectory-driven opportunistic routing protocol for VCPS. *IEEE Trans. Aerosp. Electron. Syst.* **2018**, *54*, 2628–2642. [CrossRef]
30. Sheet, D.K.; Kaiwartya, O.; Abdullah, A.H.; Cao, Y.; Hassan, A.N.; Kumar, S. Location information verification using transferable belief model for geographic routing in vehicular ad hoc networks. *IET Intell. Transp. Syst.* **2017**, *11*, 53–60. [CrossRef]
31. Kaiwartya, O.; Kumar, S. Guaranteed geocast routing protocol for vehicular adhoc networks in highway traffic environment. *Wirel. Pers. Commun.* **2015**, *83*, 2657–2682. [CrossRef]
32. Cao, Y.; Kaiwartya, O.; Zhuang, Y.; Ahmad, N.; Sun, Y.; Lloret, J. A decentralized deadline-driven electric vehicle charging recommendation. *IEEE Syst. J.* **2018**, *13*, 3410–3421. [CrossRef]
33. Kaiwartya, O.; Kumar, S. Cache agent-based geocasting in VANETs. *Int. J. Inf. Commun. Technol.* **2015**, *7*, 562–584. [CrossRef]
34. Prasad, M.; Liu, Y.-T.; Li, D.-L.; Lin, C.-T.; Shah, R.R.; Kaiwartya, O.P. A new mechanism for data visualization with TSK-type preprocessed collaborative fuzzy rule based system. *J. Artif. Intell. Soft Comput. Res.* **2017**, *7*, 33–46. [CrossRef]
35. Zhang, P.; White, J.; Schmidt, D.C.; Lenz, G.; Rosenbloom, S.T. FHIRChain: Applying blockchain to securely and scalably share clinical data. *Comput. Struct. Biotechnol. J.* **2018**, *16*, 267–278. [CrossRef] [PubMed]
36. Ji, Y.; Zhang, J.; Ma, J.; Yang, C.; Yao, X. BMPLS: Blockchain-based multi-level privacy-preserving location sharing scheme for telecare medical information systems. *J. Med. Syst.* **2018**, *42*, 147. [CrossRef]