Research Article

Privacy-preserved Secure Medical Data Sharing Using Hierarchical Blockchain in Edge Computing

Rasel Iqbal Emon[1], Md. Mehedi Hassan Onik[1], Abdullah Al Hussain[1], Toufiq Ahmed Tanna[1], Md. Akhtaruzzaman Emon[1], Muhammad Al Amin Rifat[1] and Mahdi H. Miraz[2,3,*]

[1]American International University-Bangladesh (AIUB), Dhaka, Bangladesh
ras.iqbal.97@gmail.com; mehedi.onik@aiub.edu; abdullahalhussainf11@gmail.com; toufiqtanna@gmail.com; azaman.emon@gmail.com; alaminrifat.aiub@gmail.com
[2]Xiamen University Malaysia, Sepang, Selangor, Malaysia
m.miraz@ieee.org
[3]Wrexham Glyndŵr University, Wrexham, UK
m.miraz@ieee.org
*Correspondence: m.miraz@ieee.org

Received: 8th August 2022; Accepted: 17th September 2022; Published: 1st October 2022

Abstract: A distributed ledger technology, embedded with privacy and security by architecture, provides a transparent application developing platform. Additionally, edge technology is trending rapidly which brings the computing and data storing facility closer to the user end (device), in order to overcome network bottlenecks. This study, therefore, utilises the transparency, security, efficiency of blockchain technology along with the computing and storing facility at the edge level to establish privacy preserved storing and tracking schemes for electronic health records (EHRs). Since the EHR stored in a block is accessible by the peer-to-peer (P2P) nodes, privacy has always been a matter of great concern for any blockchain-based activities. Therefore, to address this privacy issue, multilevel blockchain, which can enforce and preserve complete privacy and security of any blockchain-based application or environment, has become one of the recent blockchain research trends. In this article, we propose an EHR sharing architecture consisting of three different interrelated multilevel or hierarchical chains confined within three different network layers using edge computing. Furthermore, since EHRs are sensitive, a specific data de-identification or anonymisation strategy is also applied to further strengthen the privacy and security of the data shared.

Keywords: ***Blockchain; De-identification; Edge Computing; Health Level Seven (HL7); Medical Data; Privacy; Security***

1. Introduction

Although Blockchain was first introduced by Satoshi Nakamoto as an enabler for Bitcoin crypto currency, it is now a widely adopted technology for various non-monetary transactions including data sharing and storage [1]. In fact, the fusion of Blockchain with the smart-contracts as well as the Internet of Things (IoT) has helped in re-structuring many existing and commencing new innovative business models in various sectors, including healthcare [2]. Despite the fact that Blockchain provides a secure decentralised distributed Peer-to-Peer (p2p) architecture for data sharing, trading and integrating data across all users and third parties, implementation of Blockchain based applications requires careful consideration due to privacy concerns [3]. Since all the peers participate in the consensus process, particularly the validation and verification of any transactions (i.e., messages) and the data is stored in a distributed ledger granting wide

Rasel Iqbal Emon, Md. Mehedi Hassan Onik, Abdullah Al Hussain, Toufiq Ahmed Tanna, Md. Akhtaruzzaman Emon, Muhammad Al Amin Rifat and Mahdi H. Miraz, "Privacy-preserved Secure Medical Data Sharing Using Hierarchical Blockchain at the Edge", *Annals of Emerging Technologies in Computing (AETiC)*, Print ISSN: 2516-0281, Online ISSN: 2516-029X, pp. 38-48, Vol. 6, No. 4, 1st October 2022, Published by International Association for Educators and Researchers (IAER), DOI: 10.33166/AETiC.2022.04.005, Available: http://aetic.theiaer.org/archive/v6/v6n4/p5.html.

access to the participating peer nodes, privacy of the users have always been a matter of great concerns, in blockchain environment. Although such privacy concern is less severe in private Blockchain ecosystems, however, for healthcare sectors private Blockchain is not a good fit for several reasons, one of which being the need to share the data amongst multiple parties [4].

In healthcare system, the patients rather retain the ownership of their respective Electronic Health Records (EHRs), which they may need to securely access and share with other connected healthcare providers [5]. The most significant barrier for adapting a shared EHR system through Blockchain is that; data on the Blockchain is usually totally accessible to all the parties, making user privacy almost impossible to protect [5]. Another emerging technology, which can maximise operational efficiency as well as on demand availability, is edge computing [6]. Besides that, by keeping and preparing information at the edge, it is conceivable to extend protection by minimising the transmission of delicate data to the cloud. Besides, the proprietorship of collected information shifts from the benefit suppliers to the end-users. Therefore, this study blend edge computing with blockchain technology, in order to increase privacy of EHR.

To address the privacy concerns of any Blockchain ecosystems, with particular application in the healthcare systems, a blockchain-based privacy-preserved secure Electronic Health Record (EHR) solution has been advocated in this research. We proposed the implementation of three different distributed ledgers (i.e. multilevel blockchain) for three different layers of storage.

2. Background Study and Literature Review

2.1. Background Study

Blockchain is a distributed ledger that securely carries data within some mathematically interconnected blocks. Blockchain not only provides extra layer of security over other traditional systems, but also offers trust, transparency, immutability, decentralisation and support for smart-contracts et cetera [7]. Medical IoT devices' processing and storage capacities are lower to those of a typical Computer. By transferring difficult operations to its embedded Edge devices, medical IoT devices can tremendously reduce their energy consumption and speed up the processing [8]. Blockchain can provide enhanced EHR sharing system combined with the IoT, artificial intelligence, edge and cloud computing as well as smart-contracts. Some of the terms associated with these technologies are briefly elucidated here:

Distributed Ledger Technology (DLT) or Blockchain Technology: DLT is a shared database system, similar to accounting ledger, organised chronologically with timestamped and spanned over multiple sites/peers across the globe [9]. Each node usually has a copy of the most up-to-date ledger and have access to the data [10]. Entry to the ledger is validated and verified by the participating nodes and subject to reaching a consensus. Therefore, efforts to any unauthorised changes, additions or modifications are propagated to the network within a very shorter time-span and rejected by the participating peers. In a study, researchers examined the security and privacy issues in big data by outlining some of the current methods and strategies for ensuring security and privacy [11].

Multilevel or Hierarchical Blockchain: It is a multi-layer blockchain-based arrangement for ensuring the privacy and security of IoT frameworks and upgrading framework adaptability [12]. The arrangement accomplishes a lightweight security instrument by embracing a neighbourhood private blockchain to meet the IoT necessities.

Privacy of Personally Identifiable Information (PII): PII [13-14] are those items of information which when used alone or with other relevant data can be applied to infer the identity of an individual, such as date of birth (DoB), credit card numbers, phone number, passport number, etc.

Cloud or Cloud Computing: Cloud computing is a portage of service computations including servers, storage, databases, networking, software, analytics and intelligence over the internet, which offers speedier alterations, flexible resources and emphatic economies of scale.

Edge Computing: "Edge computing is a unique system that aids or assists users to be location-aware, maintain low latency, support heterogeneity, and improve the quality of service (QoS) of applications by providing computing power, storage of data and application services, especially computation-intensive and delay-sensitive", as defined in [15].

Data De-identification Method: The main principle of De-identification lies over the data hiding phenomenon where any particular data is secured through the use of some special symbols such as !@#$%

and mostly *. For example: if a name is 'DROGBA', applying de-identification, it can be represented as either 'D@og*!' or simply 'D*og**'.

2.1. Literature Review

Chen *et al.* [16], advocates the use of blockchain technologies for sharing EHR of each patient while storing the respective data in a certain storage. They opine that the blockchain possesses the potentials to topple the existing healthcare hierarchy as well as create novel systems through which the patients can manage their own care. Additionally, Malamas *et al.* [17] presented a typical hierarchical multi-expressive blockchain architecture to preserve healthcare ecosystem privacy. In this architecture, the fine-grained access to EHR was focused through an effective mechanism applying the hierarchical blockchain as the main component. While the proposed solution is generally convincing to some extent, the use of the same type of Proof-of-Stake (POS) consensus mechanism for both the blockchains, may cause a bit of imbalance between the security and the scalability of the proposed system.

While [16] proposed a method of Ethereum-based implementation of blockchain ecosystem, along with a limited number of remote machines, for the sharing process of medical data access [17], it provided a standard description of multi-expressive architecture along with significant execution of hierarchical chain in the medical domain. However, neither of the previous articles considered any sort of data masking or de-identification strategy [18].

Another specific architecture was presented by Zarour *et al.* [19] to create an Electronic Health Record (EHR) that involves a Patient Agent and coordinates with the insertion of continuous data streams into blockchains. They also included an evaluation of some existing blockchain technology models for secure EHRs. Instead of implementing the blockchain architecture by using any programming languages, the authors established a different kind of data analysis using mathematical logics, to evaluate the outcomes of securing the specific electronic medical information for any individuals.

With paces of time the research of data sharing, securing data or storing the data appropriately in the medical world has also gone through some revolutions. Another research by Liaw *et al.* [20] visualises the use case of EHR data for main and secondary perspectives, to protect the security of each of the records and identify the relevant issues, to evaluate the possible solutions and eventually the consideration of future directions.

None of the above articles used both edge computing architecture along with data de-identification mechanisms in their applications of varied blockchain ecosystems. In our work, a special data de-identification strategy has been executed along with the multilevel blockchain and edge computing, which not only ensures the novelty of our work, but also helps securing the privacy of any individual while sharing EHRs amongst the stakeholders.

3. Proposed Method

3.1. Overview

A novel multi-level Blockchain architecture, with data de-identification mechanism, has been proposed for a privacy-preserved secure medical data sharing platform using hierarchical blockchain in edge computing. Figure 1 demonstrates the proposed multilevel architecture with three different layers (cloud, edge and user device) having three different chains of ledgers, for storing different type of data ensuring enhanced PII privacy and security.

Firstly, the doctor generates an EHR and sends it to a patient by digitally signing it. After receiving the EHR, the patient fills it in and then sends it to the multilevel blockchains to store the relevant data.

Before storing the data in the blockchain, a data de-identification method is applied to ensure the complete privacy of each and every user (patients). The de-identification technique is randomly selected and applied to the EHR. In the blockchain, each block storing the records consists of a hash of each previous block, time-stamp and de-identified data. Since our system is a multi-level blockchain, there are obviously three different ledgers and all the data of each patient is always categorised into three portions, such as medication data, medical test data and physiological data.

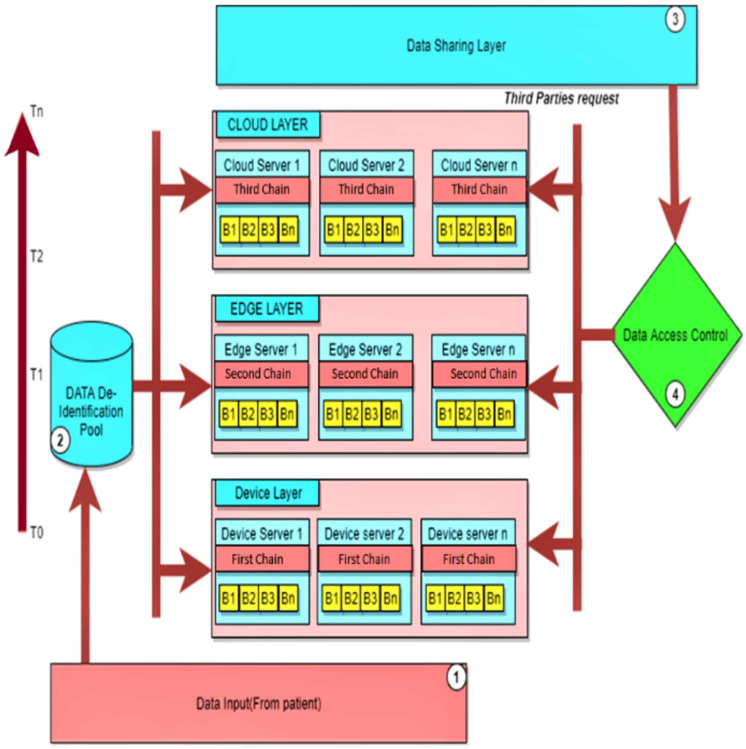


Figure 1. Hierarchical blockchain architecture associated with three ledgers

Finally, once the data is stored in the appropriate ledger(s), any third-party (doctor, government, healthcare or insurance companies, researchers, etc.) can request the patient for granting access to the respective EHR based on the national identification (NID) or by the patients' unique ID (PID) number, using the proposed blockchain platform.

Only if the patient's permission is granted, the access is given. To facilitate these features, smart-contacts are utilised, so that permissions can be automatically granted to access the respective data, only if some pre-defined conditions (set by the patients or any other legal representatives) are met.

3.2. Three-layered Architecture

As shown in Figure 1, our system is designed based on the three-layered architecture. These three layers consist of: 1) local device, 2) edge server and 3) cloud storage. Each layer has its own isolated blockchains, also known as the distributed ledgers.

Local Device: The first blockchain is implemented in the local device. This ledger records the data provided by the patient through completing the EHR form. To mask the personally identifiable data of the patents, a de-identification method is applied, before the data is stored on the ledger. This ensures that if any third party get access to the first chain, only the de-identified EHR can be read, not the original record. However, this is to note that the data stored in this chain will be subject to encryption mechanisms (i.e. they will be in the form of cypher texts), keys of which will be maintained and managed through smart-contracts.

Edge Server Layer: The second blockchain is implemented in the edge layer, which stores the relevant data portion, i.e. the medical test data, from the user input. Similar to layer one, data de-identification method is applied and smart-contact were utilised to access control mechanisms.

Cloud Layer: The third blockchain is implemented in the cloud layer, which stores the patient's physiological data. Along with data de-identification mechanism, access to the data is controlled using smart-contacts so that only legitimate users can read the data, considering the individual patient's preference.

3.3. Data Classification

Any new data input goes through the data classification phase. Based on the type of the information, the user input is classified into three different categories: medication data, medical test data and lastly the physiological data. Refer to Figure 2, after the classification of the data, each identified categories of information then goes through the de-identification process, before they are stored in the respective chain, as stated in the previous sections.

Medication Data: Medication data is stored in the first chain within the local device layer, as shown in Figure 2. When the patient receives the data, it is sent to the data de-identification pool for the random de-identification procedure and then stored in the associated (first) chain.

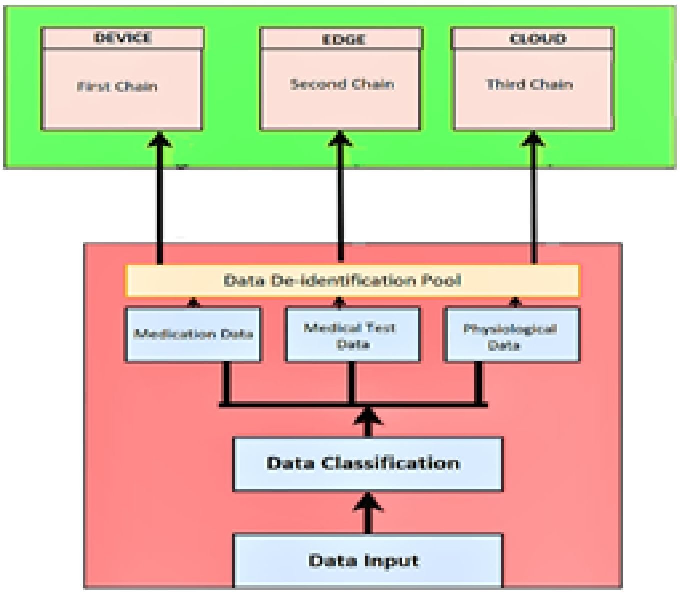


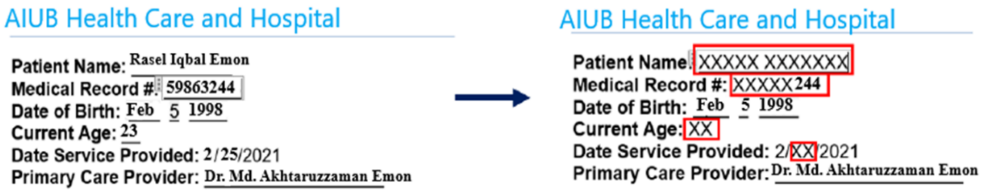
Figure 2. Classified data and a demonstration of all the associated ledgers.

Medical Test Data: Medical test data is stored in the second chain located within the edge server layer, as outlined in Figure 2. When data is classified, the medical test data is sent to the data de-identification pool for processing through the de-identification method. The de-identified data is then stored in the specified second chain.

Physiological Data: After classification physiological data is sent to the similar kind of data de-identification pool. In this pool, physiological data has been de-identified and then sent to the third chain which is installed in the cloud layer.

3.4. Data De-identification Method

Before storing all the data in each chain, a unique kind of de-identification procedure is executed. Sensitive information or personally identifiable information (PII) is concealed with the aid of the data de-identification method. As a result, when any patient shares his/her respective de-identified electronic health records (EHR) or data of any ledger with a third party, the patient's identity is obscured, as shown in Figure 3.



AIUB Health Care and Hospital

Patient Name: Rasel Iqbal Emon
Medical Record #: 59863244
Date of Birth: Feb 5 1998
Current Age: 23
Date Service Provided: 2/25/2021
Primary Care Provider: Dr. Md. Akhtaruzzaman Emon

AIUB Health Care and Hospital

Patient Name: XXXXX XXXXXXX
Medical Record #: XXXXX244
Date of Birth: Feb 5 1998
Current Age: XX
Date Service Provided: 2/XX/2021
Primary Care Provider: Dr. Md. Akhtaruzzaman Emon

Figure 3. Example of a random data de-identification process

3.5. Leading Chain Architecture

The suggested architecture is built on the foundation of three different layered blockchains. Furthermore, the blockchains are private and completely separated from each other. Only the patients have exclusive control of their own data stored on the blockchains. The perspective of the blockchain includes the reflection of all its volatile contents. A brief explanation of such blockchain architecture is presented in the following section.

First Chain: The first chain is located in the local device server. It is the nearest blockchain of the data input portion in the executive architecture, refer to Figure 4. The specified chain is used for storing the medication data. The advantage of this chain is that it is secure and takes less time to access the data, because of its location.

Second Chain: The edge server accommodates the specified second chain, as demonstrated in Figure 4. This particular chain mainly stores the medical test data. Because of its location, response time is very fast within the entire layered architecture. It is the fastest processing layer for our system. Storing any new data and retrieving any data already stored in the second chain is very fast and efficient than the other two chains.

Third Chain: The location of third chain is in the cloud server layer. The third chain is the most distant from data input portion of the executive architecture, as outlined Figure 4. Physiological data is stored in this chain. Fundamentally, because of its location, it takes a longer response time to access the data in comparison with the rest of two servers.

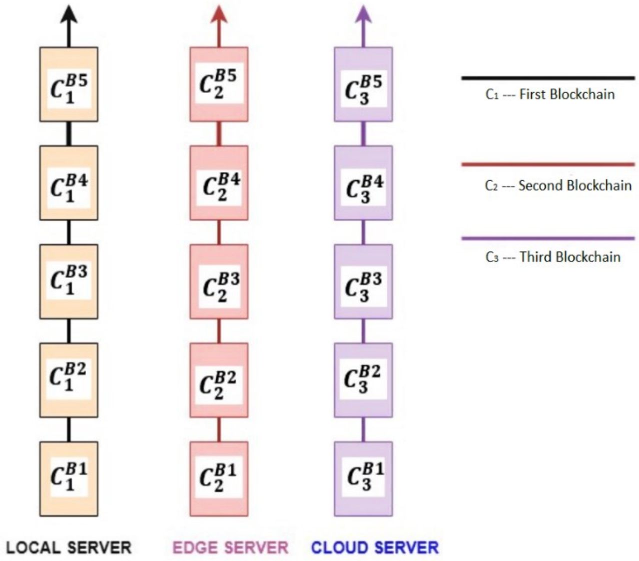


Figure 4. Three isolated chains in three different ledgers of the proposed blockchain architecture. BN indicates the associated block numbers in each layer.

3.6. Functional Properties

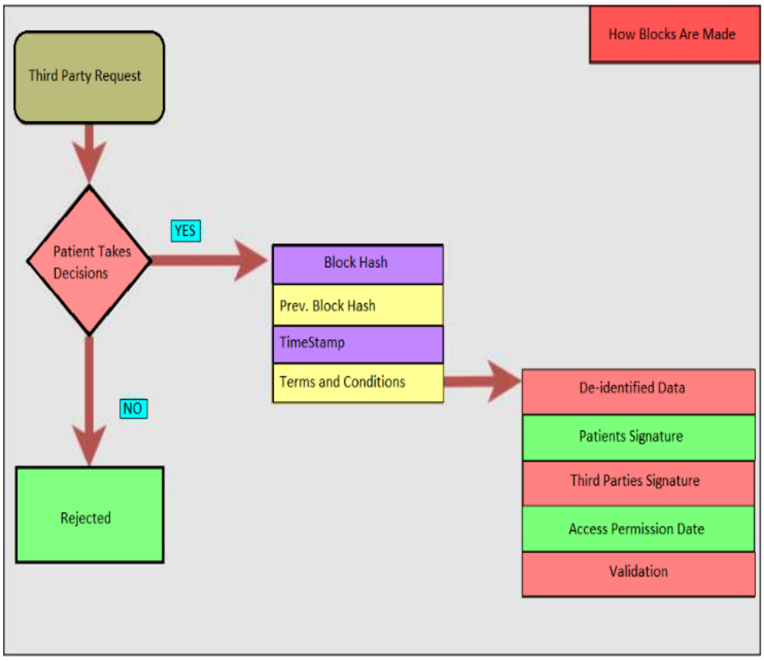


Figure 5. Functional properties of the Blockchain architecture.

Scheme of Block Generation: A block is similar to an accounting ledger or record book page. Blocks are files in which network-related data is permanently stored. A block keeps track of some or all of the most recent transactions that have not been recorded in any of the previous blocks, as shown in Figure 5.

Scheme of Third-parties Access: Through this particular segment, the sequential process of gaining the access for any sort of data that is controlled by the respective patients and received by any certain third party is notable. Firstly, a third-party needs patients' identification number to request the data. After patient gets the request, he/she takes the decision. If it is a 'NO', as shown in Figure 5, then the request is straightway rejected. Otherwise, the patient sets some conditions, to contribute to the creation of the smart-contract for controlling the access. The data are then de-identified through the data de-identification pool, as demonstrated in Figure 5. Finally, the third-parties eventually get the de-identified data to access from the respective blockchains and thus the access request process is completed.

4. Discussion and Implementation

4.1. Threat Analysis of the Proposed System

The major motivation behind using three isolated blockchains in this entire system is that, if any of them is compromised by any hackers, they will not be able to find complete data. Thus, higher level of privacy and security is ensured. Multilevel blockchain, also increases the performance and response time in this system.

Edge computing, is a distributed computing paradigm that puts data processing and data storage closer to the point of use in order to enhance reaction times (latency) and reduce bandwidth usage. We have used edge server to reduce our transaction time and to speed up the entire system. By using edge, we also can ensure better data management, lower cost of connectivity and uninterrupted connection. Moreover, the extra layer of security and reliability can be achieved through the use of edge server in any system, particularly in comparison to any traditional cloud server.

De-identification is a method of hiding patient identities from electronic health record information. Using data de-identification technique, we can share patients' data to any third parties while protecting the privacy.

4.2. Implementation

In this paper, we have represented pseudocodes and deployment guidelines for the overall implementation of the process. The executable system architecture components are stated in Figure 6.

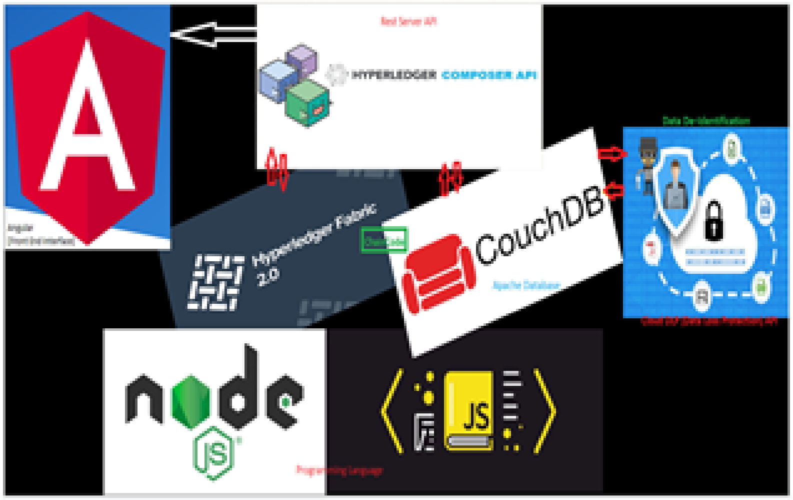


Figure 6. Executable Components to implement the overall architecture.

Throughout the system, JavaScript is selected to be used as the programming language, NodeJS as the framework tool, Hyperledger Composer as the rest server API, Hyperledger Fabric as the main blockchain platform of the entire decentralised application (DApps), CouchDB as the on-chain database. A very renowned front-end interface recognised as Angular is also used for the Application Programming Interface (API) of certain third-parties in this DApps. For executing the special method of data de-identification, the cloud data loss prevention (Cloud DLP) API is used in this implementation process, as shown in Figure 6.

4.3. Pseudocodes

In order to help the implementation, few algorithms (pseudocodes) have been executed for all the three-layer architecture. For these following pseudocodes, Table I depicts some special notations indicating each and every work attribute associated with all the three available collaborators (i.e. patients, primary care provider or doctor and third parties).

Table 1. Notations for pseudocodes

Explanations	Notations
Patients	P_N
Primary Care Provider [Doctor]	D_N
Third Parties	TP_N
Data De-identification Pool	DDP
Local Device Layer	$LD_{C_1}^{B_N}$
Edge Server Layer	$ED_{C_2}^{B_N}$
Cloud Server Layer	$CL_{C_3}^{B_N}$
Rest Server API	API_{RS}
Cloud DLP API	API_{CD}
Data Access Control	DAC
Medication Data	$MD_{C_1}^{B_N}$
Medical Test Data	$MTD_{C_2}^{B_N}$
Physiological Data	$PHY_{C_3}^{B_N}$
De-identified Medication Data	$d\ MD_{C_1}^{B_N}$
De-identified Medical Test Data	$d\ MTD_{C_2}^{B_N}$
De-identified Physiological Data	$d\ PHY_{C_3}^{B_N}$
Hyperledger Composer	H_{COM}
Terms and Conditions	TC
Patients Primary Key [Local Device Layer]	$PLD_{PRK}^{B_N}$
Patients Primary Key [Edge Server Layer]	$PED_{PRK}^{B_N}$
Patients Primary Key [Cloud Server Layer]	$PCL_{PRK}^{B_N}$
Patients Public Key [Local Device Layer]	$PLD_{PK}^{B_N}$
Patients Public Key [Edge Server Layer]	$PED_{PK}^{B_N}$
Patients Public Key [Cloud Server Layer]	$PCL_{PK}^{B_N}$
Doctors Public Key [Local Device Layer]	$DLD_{PK}^{B_N}$
Doctors Public Key [Edge Server Layer]	$DED_{PK}^{B_N}$
Doctors Public Key [Cloud Server Layer]	$DCL_{PK}^{B_N}$
Doctors Primary Key [Local Device Layer]	$DLD_{PRK}^{B_N}$
Doctors Primary Key [Edge Server Layer]	$DED_{PRK}^{B_N}$
Doctors Primary Key [Cloud Server Layer]	$DCL_{PRK}^{B_N}$
Third Parties Public Key [Local Device Layer]	$tpLD_{PK}^{B_N}$
Third Parties Public Key [Edge Server Layer]	$tpED_{PK}^{B_N}$
Third Parties Public Key [Cloud Server Layer]	$tpCL_{PK}^{B_N}$

Pseudocode 1. System (): Create and Send Preliminary EHR Form to Patients

- **Input:** A Particular Patient P_N having public key P_{PK} for each of the three layers and a Data De-identification Pool DDP receives an EHR form from a Primary Care Provider or Doctor D_N.
- **Output:** Creation and transferring the EHR Form from D_N to P_N.

```
for each Patient $P_N$ with the digital signature of $D_N$ to EHR Form
if (EHR Form == “Signed” && User == “Primary Care Provider”)
CREATE $DDP$ for each $P_N$ to de-identify the attributes of the EHR form
GENERATE $API_{RS}$ view of EHR form for $P_N$ in $H_{COM}$
$API_{RS} \subseteq$ EHR $(P_N) \Leftrightarrow API_{RS} \supseteq H_{COM}$
EHR $(P_N) \leftarrow API_{RS}$
End
```

Pseudocode 2. Request (): Medication Data Sharing Process in Local Device Layer [First Chain]

- **Input:** Any specific Third Party TP_N having the public key for Local Device Layer $tpLD_{PK}^{B_N}$ request to gain access to the First Chain Medication data from a Patient P_N.
- **Output:** De-identify Medication Data $MD_{C_1}^{B_N}$ for Local Device Layer and share with TP_N with some specific Terms and Conditions (TC) of the access.

```
for each request from $TP_N$ with Public Key $tpLD_{PK}^{B_N}$ to $P_N$
```

```
[2]  if ( Patient Decision == "YES" && $tpLD_{PK}^{B_N}$ == "Accessible" )
[3]  $TP_N$ ← $P_N$ ( EHR ( $MD_{C_1}^{B_N}$ ))
[4]  If (Third Party Signature == "TRUE" && Patient Signature == "TRUE")
[5]  DDP ⊇ $P_N$ ( $PLD_{PRK}^{B_N}$ ( $MD_{C_1}^{B_N}$ ))
[6]  $API_{CD}$ ⊇ DDP
[7]  DDP ( $PLD_{PRK}^{B_N}$ ( $MD_{C_1}^{B_N}$ )) → $P_N$ ($PLD_{PK}^{B_N}$ ( $dMD_{C_1}^{B_N}$ ))
[8]  $TP_N$ ← $P_N$ ( $dMD_{C_1}^{B_N}$ )
[9]  $API_{RS}$ ← $TP_N$( $dMD_{C_1}^{B_N}$ )
[10] else
[11] Go back to line no. [3]
[12] else
[13] rejected ← Request
[14] return Request ( $TP_N$ )
[15] end
```

Pseudocode 3. Request (): Medical Test Data Sharing Process in Edge Server Layer [Second Chain]

- **Input:** Any specific Third Party TP_N having the public key for Edge Server Layer $tpED_{PK}^{B_N}$ request to gain access to the Second Chain Medical Test data from a Patient, P_N.
- **Output:** De-identify Medical Test Data $MTD_{C_2}^{B_N}$ for Edge Server Layer and share with TP_N with some specific Terms and Conditions (TC) of the access.

```
[1]  for each request from $TP_N$ with Public Key $tpED_{PK}^{B_N}$ to $P_N$
[2]  if ( Patient Decision == "YES" && $tpED_{PK}^{B_N}$ == "Accessible" )
[3]  $TP_N$ ← $P_N$ ( EHR ( $MTD_{C_2}^{B_N}$ ))
[4]  If (Third Party Signature == "TRUE" && Patient Signature == "TRUE")
[5]  DDP ⊇ $P_N$ ( $PED_{PRK}^{B_N}$ ( $MTD_{C_2}^{B_N}$ ))
[6]  $API_{CD}$ ⊇ DDP
[7]  DDP ( $PED_{PRK}^{B_N}$ ( $MTD_{C_2}^{B_N}$ )) → $P_N$ ($PED_{PK}^{B_N}$ ( $dMTD_{C_2}^{B_N}$ ))
[8]  $TP_N$ ← $P_N$ ( $dMTD_{C_2}^{B_N}$ )
[9]  $API_{RS}$ ← $TP_N$ ( $dMTD_{C_2}^{B_N}$ )
[10] else
[11] Go back to line no. [3]
[12] else
[13] rejected ← Request
[14] return Request ( $TP_N$ )
[15] end
```

Pseudocode 4. Request (): Physiological Data Sharing Process in Cloud Layer [Third Chain]

- **Input:** Any specific Third Party TP_N having the public key for Cloud Layer $tpCL_{PK}^{B_N}$ request to gain access to the Third Chain Physiological data from a Patient P_N.
- **Output:** De-identify Physiological Data $PHY_{C_3}^{B_N}$ for Cloud Layer and share with TP_N with some specific Terms and Conditions (TC) of the access.

```
[1]  for each request from $TP_N$ with Public Key $tpCL_{PK}^{B_N}$ to $P_N$
[2]  if ( Patient Decision == "YES" && $tpCL_{PK}^{B_N}$ == "Accessible" )
[3]  $TP_N$ ← $P_N$ ( EHR ( $PHY_{C_3}^{B_N}$ ))
[4]  If (Third Party Signature == "TRUE" && Patient Signature == "TRUE")
[5]  DDP ⊇ $P_N$ ( $PCL_{PRK}^{B_N}$ ( $PHY_{C_3}^{B_N}$ ))
[6]  $API_{CD}$ ⊇ DDP
[7]  DDP ( $PCL_{PRK}^{B_N}$ ( $PHY_{C_3}^{B_N}$ )) → $P_N$ ($PCL_{PK}^{B_N}$ ( $dPHY_{C_3}^{B_N}$ ))
```

```
[8] $TP_N \leftarrow P_N\,(\,dPHY_{C_3}^{B_N}\,)$
[9] $API_{RS} \leftarrow TP_N\,(\,dPHY_{C_3}^{B_N}\,)$
[10] else
[11] Go back to line no. [3]
[12] else
[13] rejected ← Request
[14] return Request $(\,TP_N\,)$
[15] end
```

5. Conclusion

In this paper, we have proposed a novel privacy-preserved secure medical data sharing using hierarchical blockchain in edge computing. We have demonstrated how privacy of the patients personally identifiable information can be masked from the EHR, using data de-identification and security can be ensured by a multi-level blockchain application, utilising edge computing model. We have advocated the use of three different distributed ledgers at three different layers of the network, with complete access control using smart-contacts. We have also presented the architecture with respective pseudocodes. The overall architecture is designed to be highly secure, with the privacy concerns addressed.

Acknowledgement

This research was funded by the Xiamen University Malaysia Research Fund (XMUMRF), grant numbers XMUMRF/2022-C10/IECE/0043 and XMUMRF/2021-C8/IECE/0025. Support from the Ministry of Higher Education Malaysia through the Fundamental Research Grant Scheme (FRGS), project number FRGS/1/2021/ICT08/XMU/02/1, is also gratefully acknowledged.

References

[1] Garrick Hileman and Michel Rauchs, "Global cryptocurrency benchmarking study", in *Cambridge Centre for Alternative Finance Reports*, vol. 33, pp. 33–113, 2017, Available: https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2017-04-20-global-cryptocurrency-benchmarking-study.pdf.

[2] Amir Faraji, Maria Rashidi, Srinath Perera and Bijan Samali, "Applicability-Compatibility Analysis of PMBOK Seventh Edition from the Perspective of the Construction Industry Distinctive Peculiarities", *Buildings*, vol. 12, no. 2, p. 210, 2022, DOI: 10.3390/buildings12020210, Available: https://www.mdpi.com/2075-5309/12/2/210.

[3] Zhi Li, Ali Vatankhah Barenji and George Q. Huang, "Toward a blockchain cloud manufacturing system as a peer-to-peer distributed network platform", In *Robotics and Computer-Integrated Manufacturing*, vol. 54, pp. 133–144, December 2018, Published by Elsevier B. V., DOI: 10.1016/j.rcim.2018.05.011, Available: https://www.sciencedirect.com/science/article/abs/pii/S073658451830022X.

[4] Saurabh Singh, Pradip Kumar Sharma, Byungun Yoon, Mohammad Shojafar, Gi Hwan Cho *et al.*, "Convergence of blockchain and artificial intelligence in IoT network for the sustainable smart city", In *Sustainable Cities and Society*, vol. 63, p. 102364, December 2020, Published by Elsevier B. V., DOI: 10.1016/j.scs.2020.102364, Available: https://www.sciencedirect.com/science/article/abs/pii/S2210670720305850.

[5] Tsung-Ting Kuo, Hyeon-Eui Kim and Lucila Ohno-Machado, "Blockchain distributed ledger technologies for biomedical and health care applications", In *Journal of the American Medical Informatics Association*, vol. 24, no. 6, pp. 1211–1220, 2017, DOI: 10.1093/jamia/ocx068, Availavle: https://pubmed.ncbi.nlm.nih.gov/29016974/.

[6] Wei Yu, Fan Liang, Xiaofei He, Wiiliam Grant Hatcher, Chao Lu *et al.*, "A survey on the edge computing for the Internet of Things", In *IEEE Access,* vol. 6, pp. 6900–6919, 2017, DOI: 10.1109/ACCESS.2017.2778504, Available: https://ieeexplore.ieee.org/document/8123913.

[7] Khaled Salah, M. Habib Ur Rehman, Nishara Nizamuddin and Ala Al-Fuqaha, "Blockchain for AI: Review and open research challenges", In *IEEE Access,* vol. 7, pp. 10127–10149, 2019, DOI: 10.1109/ACCESS.2018.2890507, Available: https://ieeexplore.ieee.org/document/8598784.

[8] Md. Mehedi Hassan Onik, Satyabrata Aich, Jinhong Yang, Chul-Soo Kim and Hee-Cheol Kim, "Blockchain in Healthcare: Challenges and Solutions", In Big Data Analytics for Intelligent Healthcare Management, Massachusetts, USA: Academic Press, pp. 197-226, ch. 8, 2019, DOI: 10.1016/b978-0-12-818146-1.00008-8, Available: https://www.sciencedirect.com/science/article/pii/B9780128181461000088.

[9] David C. Donald and Mahdi H. Miraz, "Multilateral Transparency for Securities Markets through DLT", In *Fordham Law Review*, Vol. XXV, Issue 1, January 2020, pp. 97-153, Available: https://ir.lawnet.fordham.edu/jcfl/vol25/iss1/2/.

[10] D. Sivaganesan, "Smart contract based industrial data preservation on blockchain", In *Journal of Ubiquitous Computing and Communication Technologies*, vol. 2, no. 01, pp. 39–47, 2020, DOI: 10.36548/jucct.2020.1.005, Available: https://www.irojournals.com/jucct/V2/I1/05.pdf.

[11] Karim Abouelmehdi, Abederrahim Beni-Hessane and Hayat Khaloufi, "Big healthcare data: preserving security and privacy", In *Journal of Big Data*, vol. 5, no. 1, 2018. DOI: 10.1186/s40537-017-0110-7, Available: https://journalofbigdata.springeropen.com/articles/10.1186/s40537-017-0110-7.

[12] Swagatika Sahoo, Akshay M. Fajge, Raju Halder, and Agostino Cortesi, "A hierarchical and abstraction-based blockchain model", In *Applied Sciences*, vol. 9, no. 11, p. 2343, 2019, DOI: 10.3390/app9112343, Available: https://www.mdpi.com/2076-3417/9/11/2343.

[13] Md Mehedi Hasan Onik, Chul-Soo Kim, Nam-Yong Lee, and Jinhong Yang, "Privacy-aware blockchain for personal data sharing and tracking", In *Open Computer Science*, vol. 9, no. 1, pp. 80–91, 2019, DOI: 10.1515/comp-2019-0005, Available: https://www.degruyter.com/document/doi/10.1515/comp-2019-0005/html.

[14] Bacem Mbarek, Nafaa Jabeur, Tomas Pitner, and Ansar-Ul-Haque Yasar, "MBS: Multilevel Blockchain System for IoT", In *Personal and Ubiquitous Computing*, vol. 25, no. 1, pp. 247–254, Feb. 2021, DOI: 10.1007/s00779-019-01339-5, Available: https://link.springer.com/article/10.1007/s00779-019-01339-5.

[15] Wazir Zada Khan, Ejaz Ahmed, Saqib Hakak, Ibrar Yaqoob, and A. Ahmed, "Edge computing: A survey", In *Future Generation Computer Systems,* vol. 97, pp. 219–235, 2019, DOI: 10.1016/j.future.2019.02.050, Available: https://www.sciencedirect.com/science/article/abs/pii/S0167739X18319903.

[16] Hannah S Chen, Juliet T Jarrell, Kristy A Carpenter, David S Cohen, and Xudong Huang, "Blockchain in healthcare: a patient-centered model", In *Biomedical Journal of Scientific & Technical Research*, vol. 20, no. 3, p. 15017, 2019, Available: https://pubmed.ncbi.nlm.nih.gov/31565696/.

[17] Vangelis Malamas, Panayiotis Kotzanikolaou, Thomas k. Dasaklis, and Mike Burmester, "A Hierarchical Multi Blockchain for Fine Grained Access to Medical Data", *IEEE Access*, vol. 8, pp. 134393–134412, 2020, DOI: 10.1109/ACCESS.2020.3011201, Available: https://ieeexplore.ieee.org/document/9146294.

[18] Rui Pinto, Bruno M. C. Silva and Pedro R. M. Inacio, "A System for the Promotion of Traceability and Ownership of Health Data Using Blockchain", In *IEEE Access*, vol. 10, pp. 92760-92773, 2022, DOI: 10.1109/access.2022.3203193, Available: https://ieeexplore.ieee.org/document/9870819.

[19] Mohammad Zarour , Md Tarique Jamil Ansari, Mamdouh Alenezi, Amal Krishna Sarkar, and Mohd Faizan "Evaluating the impact of blockchain models for secure and trustworthy electronic healthcare records", In *IEEE Access*, vol. 8, pp. 157959–157973, 27 August 2020, DOI: 10.1109/ACCESS.2020.3019829, Available: https://ieeexplore.ieee.org/document/9178798.

[20] Siaw-Teng Liaw, Gawaine Powell-Davies, Christopher Pearce, Helena Britt, Lisa McGlynn, and Mark F Harris, "Optimising the use of observational electronic health record data: Current issues, evolving opportunities, strategies and scope for collaboration", *Australian Family Physician*, vol. 45, no. 3, pp. 153–156, 2016, Available: https://pubmed.ncbi.nlm.nih.gov/27052055/.