Privacy-preserved Secure Medical Data Sharing Using Hierarchical Blockchain at the Edge

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 bring the computing and data storing facility closer to the user end (device) in order to overcome network bottlenecks. This study, therefore, utilizes the transparency, security, efficiency of blockchain technology along with the computing and storing facility at the edge level to establish privacy preserve EHRs (electronic health records) storing and tracking schemes. 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. Furthermore, since EHRs are sensitive, a specific data de-identification or anonymization strategy is also applied to further strengthen the privacy and security of the data shared.**

Index Terms— **edge; de-identification; multilevel; patients; third-parties, health level seven (HL7), blockchain, privacy, security, medical data.**

I. 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 decentralized 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 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 maximize operational efficiency as well as on demand availability is Edge [6]. Besides that, by keeping and preparing information at the edge, it is conceivable to extend protection by minimizing the transmission of delicate data to the cloud. Besides, the proprietorship of collected information shifts from benefit suppliers to end-users. Therefore, this study blend edge with blockchain technology in order to increase privacy of EHR.

To address the privacy concerns of any the 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 Blockchains for three layers of storage.

II. BACKGROUND STUDY AND LITERATURE REVIEW

A. Background Study

Blockchain is a distributed ledger that securely carries data within some mathematically interconnected blocks. Blockchain not only provides security over other traditional systems, but also offers trust, transparency, immutability, decentralization, and support for smart-contracts etc [7]. Blockchain can provide enhanced EHR sharing system combined with the IoT, artificial intelligence, edge and cloud and smart-contracts. Some of the terms associated with these technologies are briefly elucidated here:

1) Distributed Ledger Technology (DLT) or Blockchain Technology: DLT is a shared database system, similar to accounting ledger, organized chronologically with timestamped and spanned over multiple sites/peers across the globe [8]. Each node usually has a copy of the most up-to-date ledger and have access to the data [9]. Entry to the ledger is validated and verified by the participating nodes and subject to reaching a consensus. Therefore, efforts to any unauthorized changes, additions or modifications are propagated to the network within a very shorter time-span and rejected by the participating peers.

2) Multilevel or Hierarchical Blockchain: A multi-layer blockchain-based arrangement for ensuring the security and security of IoT frameworks and upgrading framework

adaptability [10]. The arrangement accomplishes a lightweight security instrument by embracing a neighborhood private blockchain to meet the IoT necessities.

3) Privacy of Personally Identifiable Information (PII): PII are those 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 [11], [12].
4) 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.
5) Edge and 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" defined by the author Yang, Ruizhe et al. on the content edge computing [13].
6) 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**'.

B. Literature Review

Chen et al. [14], advocates the use of Blockchain technologies for sharing HER 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. [15], 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 [14] proposed a method of an 'Ethereum-based' implementation of a Blockchain ecosystem along with a limited number of remote machines for the sharing process of medical data access [15], provided a standard description of multi-expressive architecture along with significant execution of hierarchical chain in the medical domain. Neither of the previous articles considered any sort of data masking, or De-identification strategy.

Another specific architecture was presented by Zarour et al. [16] 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 been gone through some revolutions. Another research by Liaw et al. [17] visualizes 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 architecture beside data De-identification mechanisms in their applications of varied Blockchain architectures. In our work, a special data de-identification strategy has been executed along with the multilevel blockchain and edge, which not only ensures the novelty of our work, but also helps securing the privacy of any individual while sharing EHR amongst the stakeholders.

III. PROPOSED METHOD

A. Overview

A novel multi-level Blockchain architecture, with Data De-identification mechanism, has been is proposed for a privacy-preserved secure medical data sharing platform using hierarchical Blockchain in Edge Computing. The following figure (Fig. 1) demonstrate 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.

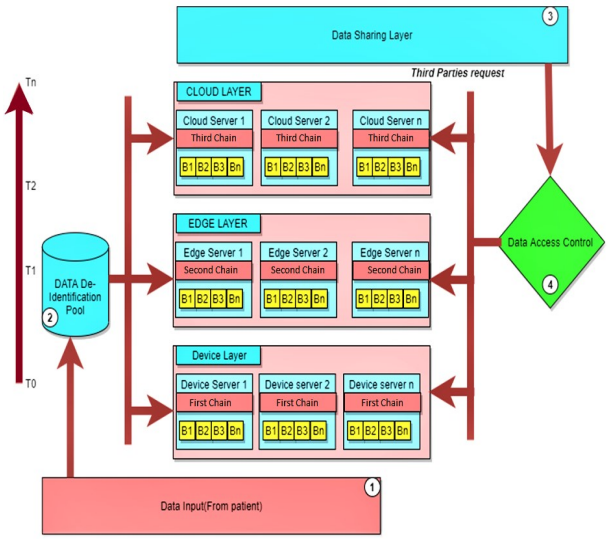

Fig. 1. Hierarchical Blockchain architecture associated with three ledgers.

1) 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.

2) Before storing the data in the Blockchain, a Data De-identification method is applied 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, data is stored as a hash of each previous blocks, time-stamp and De-identified data. Since our system is a multi-level Blockchain, so there are obviously three Blockchains and all the data of each patient is always categorized into three portions, such as medication data, medical test data, and physiological data.

3) Then, any third-party (doctor, government, healthcare or insurance companies, researchers, etc.) can request the patient for access to the respective EHR based on the National Identification (NID) or by the Patients' Unique ID (PID), using the proposed Blockchain platform.

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

B. Three-layered Architecture

As shown in Fig. 1, our system is designed based on the three-layered architecture (Fig. 1). 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 distributed ledger or chains of blocks.

1) 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 here, before the data is stored on the ledger. Which ensures that if any third party get access to the first chain, only the De-identified EHR can be read. However, this is to note that the data stored in this chain will be subject to encryption mechanisms i.e., will be in the form of cypher texts, keys of which will be maintained and managed through smart-contracts.

2) 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 smart-contact based where access control mechanisms are applied.

3) 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 is data is controlled using smart-contacts so that only legitimate users can read the data, considering the individual patient's preference into account.

C. 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. 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 (Fig. 2).

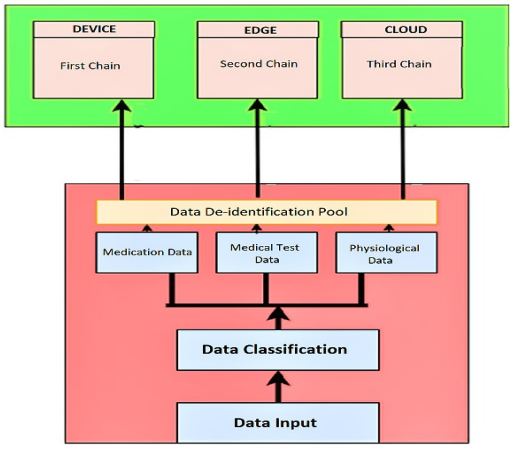

Fig. 2. Classified data and a demonstration of all the associated ledgers.

4) Medication Data

Medication Data is stored in the First Chain within the local device layer (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.

5) Medical Test Data

Medical Test Data is stored in the Second Chain (Figure 2) within the edge server layer. When data is classified, the Medical Test Data is sent to the Data De-identification Pool for processing the De-identification Method and the De-identified data is then stored in the specified Second Chain.

6) 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 remained in the cloud layer.

D. 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 is concealed with the aids of the Data De-identification Method. As a result, when any patient share their respective De-identified Electronic Health Records (EHR) or data of any ledger with a third party, the patient's identity is obscured (Figure 3).

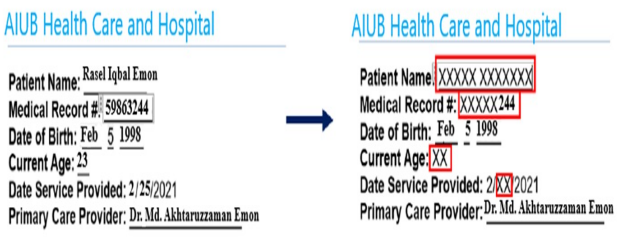

Fig. 3. Example of a random Data de-identification process.

E. *Leading Chain Architecture*

The suggested architecture is built on the foundation of three Blockchains. Furthermore, the Blockchains are private and completely separated from each other. Only the patients have exclusive control of the Blockchain. 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.

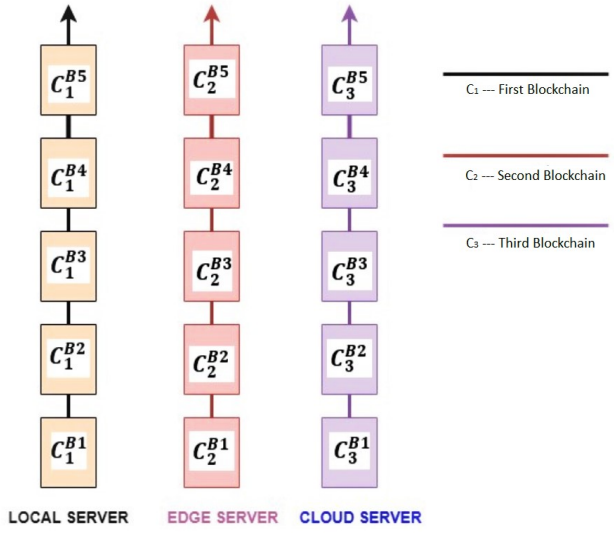

Fig. 4. Three isolated chains in three ledgers of the leading Blockchain architecture. B^N indicates the associated blocks in each of the three layers.

7) *First Chain*

First chain is located in the local device server. It is the nearest blockchain of the data input portion in the executive architecture (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. Although, it has a possibility to be attacked by any professional hacker instantly because of its location.

8) *Second Chain*

Edge server remains in the specified Second Chain (Figure 4). This particular chain stores the medical test data mainly. Second Chain is located in the edge server layer. Because of its location, response time is very fast in the entire architecture. It is the fastest processing layer for our system. Input data and downloading any sort of data from the Second Chain is very fast and efficient than the other two chains.

9) *Third Chain*

The location of Third chain is in the cloud server Layer. Third chain is most distant from data input portion of the executive architecture (Figure 4). Physiological data is stored in this chain. Basically, because of its location, it takes a longer response time to access the data in comparison with the rest of two servers.

F. *Functional Properties*

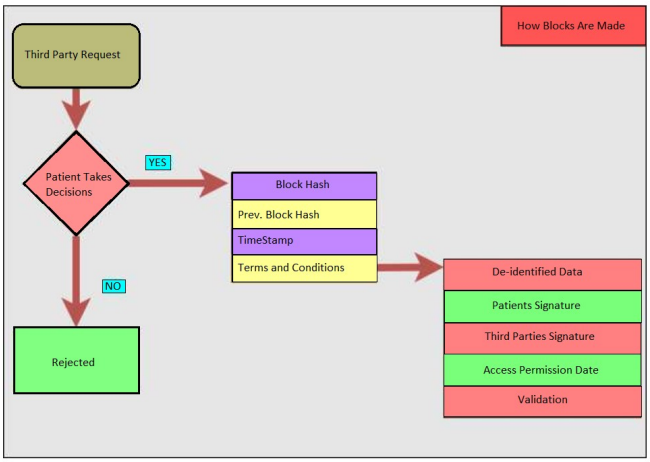

Fig. 5. Functional properties of the Blockchain architecture.

1) *Scheme of Block Generation*

A block is similar to a 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 (Figure 5).

2) *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' then the request is rejected. If it is a 'YES', then patient creates some conditions just like as shown in (Figure 5) and then data are being De-identified within the

"Data De-identification Pool" (Figure 1). After that, third-parties eventually get the De-identified data to access in the respective Blockchains and thus the access request process is completed.

IV. Discussion & Implementation

B. *Threat Analysis of the Proposed System*

1) Motivation behind using specifically three isolated Blockchains in this entire system:

The main reason is that, if any one of the blocks of the Blockchain is corrupted by any hackers, they will not find full data. In this way we can secure our data as well.

2) Advantages of using Hierarchical Blockchain in this architecture:

In our system we have used multilevel Blockchain to store and secure the data more precisely. It cannot be guaranteed that Blockchain cannot be ever compromised or cannot be hacked. That is why multilevel or hierarchical Blockchain has been used in our system so that each of the blocks in the respective Blockchains can contain its own records or details independently and sidewise a dependent link in the collective layer also balances such a duality that helps to create a network regulated by the patients who store and share their information by themselves securely rather than a third party. Multilevel Blockchain, also increase the performance and response time in this system.

3) Effect of executing edge server 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 and reduce bandwidth use. We have used edge server to reduce our transaction time and to speed up the entire system. By using edge, we also can gain better data management, lower cost of connectivity and uninterrupted connection as well. Moreover, the security and reliability can be achieved through the use of edge server in any system.

4) Analysis of the objective and outcome for the De-identification method in the system:

De-identification is a method of hiding patient identities from electronic health record information. Using "Data De-identification", technique, we can give patients data to third parties protecting the privacy. If any Blockchains are somehow hacked, then data privacy will be preserved because of this De-identification method to the process of Blockchain.

5) Elaboration of individuals by whom the full control over Blockchains is subjected:

Actually, the main purpose of our system relies on the security of the data more than the quantity of details we could collect. That means how much this entire system can protect the data of any user is literally a foremost concern for us. For this reason, users themselves (in our case the patients) have the full control over Blockchains.

6) Analysis of the working phenomenon for the request of third parties:

It is indeed much needed to share the respective medical data of each patient for research or other activities of the authority as well. But it is also important to secure the privacy of the patients as well. For achieving the proper access to the patients EHR; third parties like doctors, researchers, government, and companies and so on like them have to fulfill a request procedure to the patients. Patients have the complete rights to accept or refuse the request in case of sharing their own EHR with the external parties. If patients accept the request, then they also have to add some terms and conditions along with the confirmation feedback such as: timestamp, block number or hash of the block. But before sending the ultimate feedback towards the third parties, an EHR must need to be De-identified through the available Data De-identification pool for ensuring the eternal privacy of a patient.

C. *Implementation*

In this paper, we have represented pseudocodes and deployment guidelines which will surely easy the overall implementation of the process.

Fig. 6. Executable Components to implement the overall architecture.

Involving the previous discussions of this paper, one particular phenomenon, "Preserved Privacy or Security" has been focused on repeatedly during any sort of data sharing among the prescribed servers such as local server, edge server and also the cloud server. Along with this motive, in this paper, the executable system architecture components are stated in (Fig. 6).

Throughout the system, JavaScript is selected to use 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 Decentralized Application (DApp), CouchDB as the on-chain database, and a very renowned front end Interface recognized as Angular is also used a bit for only the API (Application Programming Interface) of certain third-parties in this DApp. For executing the special method of Data De-identification, the Cloud DLP (Data Loss Prevention) API is used in this implementation process (Figure 6).

Since the steps or executing sequences have already been described in the previous sections, so it is already known that the security of each piece of medication data, medical test data, physiological data, or even the sensitive protected personal details of respective patients have been ensured genuinely through the method of De-identification.

1) Pseudocodes

In order to help implementation, few algorithms (Pseudocodes) have been executed for all the three-layer architecture briefly to create a plain text-based main logic of the steps in spite of being focused only on the deployment of the Blockchain framework that could be written using the programming languages syntax. Only for the following Pseudocodes, Table I depicts some special Notations indicating each and every work attributes for all three available collaborators (Patients, Primary Care Provider or Doctor, Third Parties).

TABLE I
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	$dMD_{C_1}^{B_N}$
De-identified Medical Test Data	$dMTD_{C_2}^{B_N}$
De-identified Physiological Data	$dPHY_{C_3}^{B_N}$
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 I

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.

[1] **for** each Patient P_N with the digital signature of D_N to EHR Form

[2] if (EHR Form == "Signed" && User == "Primary Care Provider")

[3] CREATE DDP for each P_N to de-identify the attributes of the EHR form

[4] GENERATE API_{RS} view of EHR form for P_N in H_{COM}

[5] $API_{RS} \subseteq$ EHR (P_N) $\Leftrightarrow$ $API_{RS} \supseteq H_{COM}$

[6] EHR (P_N) $\leftarrow$ API_{RS}

[7] **end**

PSEUDOCODE II

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.

[1] **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 $\leftarrow$ P_N (EHR ($MD_{C_1}^{B_N}$))

[4] If (Third Party Signature == "TRUE" && Patient Signature == "TRUE")

[5] DDP $\supseteq$ P_N ($PLD_{PRK}^{B_N}$ ($MD_{C_1}^{B_N}$))

[6] $API_{CD} \supseteq$ DDP

[7] DDP ($PLD_{PRK}^{B_N}$ ($MD_{C_1}^{B_N}$)) $\rightarrow$ P_N ($PLD_{PK}^{B_N}$ ($dMD_{C_1}^{B_N}$))

[8] TP_N $\leftarrow$ P_N ($dMD_{C_1}^{B_N}$)

[9] API_{RS} $\leftarrow$ TP_N($dMD_{C_1}^{B_N}$)

[10] else

[11] Go back to line no. [**3**]

[12] else

[13] rejected $\leftarrow$ Request

[14] **return** Request (TP_N)

[15] **end**

PSEUDOCODE III

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 IV

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 ← P_N ($dPHY_{C_3}^{B_N}$)

[9] API_{RS} ← 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**

V. CONCLUSIONS

In this paper, we have proposed a novel privacy-preserved secure medical data sharing using hierarchical blockchain with edge. 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, with edge computing. 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 presented the architecture with pseudocodes. The overall architecture seems to be highly secure, with privacy concerns addressed.

REFERENCES

[1] G. Hileman and M. Rauchs, "Global cryptocurrency benchmarking study," *Cambridge Cent. Altern. Financ.*, vol. 33, pp. 33–113, 2017.

[2] A. Faraji, M. Rashidi, S. Perera, and B. 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.

[3] Z. Li, A. V. Barenji, and G. Q. Huang, "Toward a blockchain cloud manufacturing system as a peer to peer distributed network platform," *Robot. Comput. Integr. Manuf.*, vol. 54, pp. 133–144, 2018.

[4] S. Singh, P. K. Sharma, B. Yoon, M. Shojafar, G. H. Cho, and I.-H. Ra, "Convergence of blockchain and artificial intelligence in IoT network for the sustainable smart city," *Sustain. Cities Soc.*, vol. 63, p. 102364, 2020.

[5] T.-T. Kuo, H.-E. Kim, and L. Ohno-Machado, "Blockchain distributed ledger technologies for biomedical and health care applications," *J. Am. Med. Informatics Assoc.*, vol. 24, no. 6, pp. 1211–1220, 2017.

[6] W. Yu *et al.*, "A survey on the edge computing for the Internet of Things," *IEEE access*, vol. 6, pp. 6900–6919, 2017.

[7] K. Salah, M. H. U. Rehman, N. Nizamuddin, and A. Al-Fuqaha, "Blockchain for AI: Review and open research challenges," *IEEE Access*, vol. 7, pp. 10127–10149, 2019.

[8] C. Majaski, "Distributed ledgers," *Investopedia. https//www. investopedia. com/terms/d/distributed-ledgers. asp*, 2020.

[9] D. Sivaganesan, "Smart contract based industrial data preservation on block chain," *J. Ubiquitous Comput. Commun. Technol.*, vol. 2, no. 01, pp. 39–47, 2020.

[10] S. Sahoo, A. M. Fajge, R. Halder, and A. Cortesi, "A hierarchical and abstraction-based blockchain model," *Appl. Sci.*, vol. 9, no. 11, p. 2343, 2019.

[11] M. M. H. Onik, C.-S. Kim, N.-Y. Lee, and J. Yang, "Privacy-aware blockchain for personal data sharing and tracking," *Open Comput. Sci.*, vol. 9, no. 1, pp. 80–91, 2019.

[12] B. Mbarek, N. Jabeur, T. Pitner, and A.-U.-H. Yasar,

"MBS: Multilevel Blockchain System for IoT," *Pers. Ubiquitous Comput.*, vol. 25, no. 1, pp. 247–254, Feb. 2021, doi: 10.1007/s00779-019-01339-5.

[13] W. Z. Khan, E. Ahmed, S. Hakak, I. Yaqoob, and A. Ahmed, "Edge computing: A survey," *Futur. Gener. Comput. Syst.*, vol. 97, pp. 219–235, 2019.

[14] H. S. Chen, J. T. Jarrell, K. A. Carpenter, D. S. Cohen, and X. Huang, "Blockchain in healthcare: a patient-centered model," *Biomed. J. Sci. Tech. Res.*, vol. 20, no. 3, p. 15017, 2019.

[15] V. Malamas, P. Kotzanikolaou, T. K. Dasaklis, and M. 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.

[16] M. Zarour *et al.*, "Evaluating the impact of blockchain models for secure and trustworthy electronic healthcare records," *IEEE Access*, vol. 8, pp. 157959–157973, 2020.

[17] S.-T. Liaw, G. Powell-Davies, C. Pearce, H. Britt, L. McGlynn, and M. F. Harris, "Optimising the use of observational electronic health record data: Current issues, evolving opportunities, strategies and scope for collaboration," *Aust. Fam. Physician*, vol. 45, no. 3, pp. 153–156, 2016.