BHEEM: A Blockchain-based Framework for Securing Electronic Health Records

Jayneel Vora*, Anand Nayyar, *Senior Member, IEEE* †, Sudeep Tanwar ‡, Sudhanshu Tyagi, *Member, IEEE*§, Neeraj Kumar, *Senior Member, IEEE* ¶, M. S. Obaidat, *Fellow of IEEE and Fellow of SCS* ‖ & Joel J P C Rodrigues**
*‡ Department of Computer Engineering, Nirma University, Ahmedabad, India, † Graduate School, Duy tan University, Vietnam, ‖ ECE Deptt., Nazarbayev University, Astana, Kazakhstan and King Abdullah II School of IT, University of Jordan, §¶ Thapar Institute of Engg.& Tech., Deemed University, Patiala, India, **National Institute of Telecommunications (Inatel), Santa Rita do Sapucaí-MG, Brazil, **Instituto de Telecomunicações, Portugal, **University of Fortaleza (UNIFOR), Fortaleza-CE, Brazil
Emails: *15bce048@nirmauni.ac.in, †anandnayyar@duytan.edu.in, ‡sudeep.tanwar@nirmauni.ac.in, §s.tyagi@thapar.edu, ¶neeraj.kumar@thapar.edu, ‖m.s.obaidat@ieee.org **joeljr@ieee.org.

***Abstract*—In the present era of smart cities and homes, the private information of the patients such as their names, address, and disease is being breached on a regular basis, which indirectly related to the security of electronic health records (EHRs). The existing state-of-the-art schemes handling the security of EHRs have resulted in data being generally inaccessible to patients. These schemes struggle in providing the efficient balance between the data privacy, need for patients, and providers to regularly interact with data. Blockchain technology resolves the aforementioned issues because it shares the data in a decentralized and transactional fashion. This can be leveraged in the healthcare sector to maintain the balance between privacy and accessibility of EHRs. In this paper, we propose a Blockchain-based framework for efficient storage and maintenance of EHRs. This further provides the secure and efficient access to medical data by patients, providers, and third parties, while preserving the patient private information. The goals of this paper are to analyze how our proposed framework fulfills the needs of patients, providers, and third parties, and to understand how the framework maintains the privacy and security concerns in the healthcare 4.0.**

***Index Terms*—Blockchain, healthcare,electronic health records, contracts, storage, security.**

I. Introduction

In the last decade, large cities across the globe have begun to use technology to secure the patient private information generated from smart healthcare solutions. These patient medical records are ever growing with time. The patient's vitals, physical signs: weight, height, symptoms and signs make up the record. These records are termed to be simple data points, but are complex to handle. Various stakeholders are responsible for generating, storing and manipulating the records for efficient usage and proper care of the patient. Access should be provided to authorized stakeholders as and when required. EHRs consist of various parameters as shown in Fig. 1(b); consisting of clinical notes, patient listings, lab results, imaging results, and screening tests. The medical records are a vital cog in the efficient healthcare providing to the patient. Any change in the staff; doctors, nurses and care providers can create problem in proper accessing of EHRs pertaining to any patient. A survey of healthcare stakeholders have shown that 16% have plans to use a blockchain based solution in the near future, while 56% intend to implement it by 2020 [1]. Various applications, where Blockchain [2][3] can be a viable solution are as briefed below:

- Claims and Billing Management: Intermediateries are unnecessary middlemen in the hospital systems, which could have potential links, where data leaks may occur and also costs of the management systems may rise.
- Medical Research: Current research occurs on localized systems, which is an ineffective manner of sharing the research and taking the field further. A decentralized sharing system for the clinical results of various trials will increase the efficiency of conducting the research.
- Securing Patient's Data: 140 million medical records were sabotaged between the years of 2015-16 [4]. With increasing number of end-devices and data generators, providing security to the data also gets proportionality complicated.
- Drug Supply Chain : Pharmaceuticals companies need to be aware of the mass patient results for efficient drug delivery and avoiding counterfeit products.

A study has shown that by 2020, the amount of medical data will double in 73 days. 80% of the data surrounding the healthcare is in an unstructured format [5]. A staggaring amount of 7 trillion dollars is spent worldwide in various health care programs, out of which 585 billion dollars are wasted on missed opportunities. Healthcare has been heavily influenced by the the advent of newer and newer technology. As described in Fig. 1(c), it started with pen-paper based health records in the 1920's [6], which over a period of time changed into information management systems in the form of registers. The personal computer revolution further keeping on off side record storage and in 2000's the Internet based storage were widely used. 2010's initiated the advent of the cloud computing based solutions and now Blockchain based solutions. The blockchain based solutions are being pursued more and more as described in Fig. 1(a), which predicts an exciting future for the solutions [7]. EHRs [8] have various stakeholders as described in Fig. 1(d). Various implementations [9][10] for patient health records and providing care, which need high amount of data storage and transfers that can be efficiently provided by the Blockchain paradigm. Immense amounts of resources have been pumped into realising the potential of blockchain to further upgrade the delivery of healthcare based products and platforms.

Blockpharma [11] is a blockchain based solution to counter counterfeiting of drugs, where 8,00,000 people die each year due to the consumption. Stakeholders in the supply

978-1-5386-4920-6/18/$31.00 ©2018 IEEE

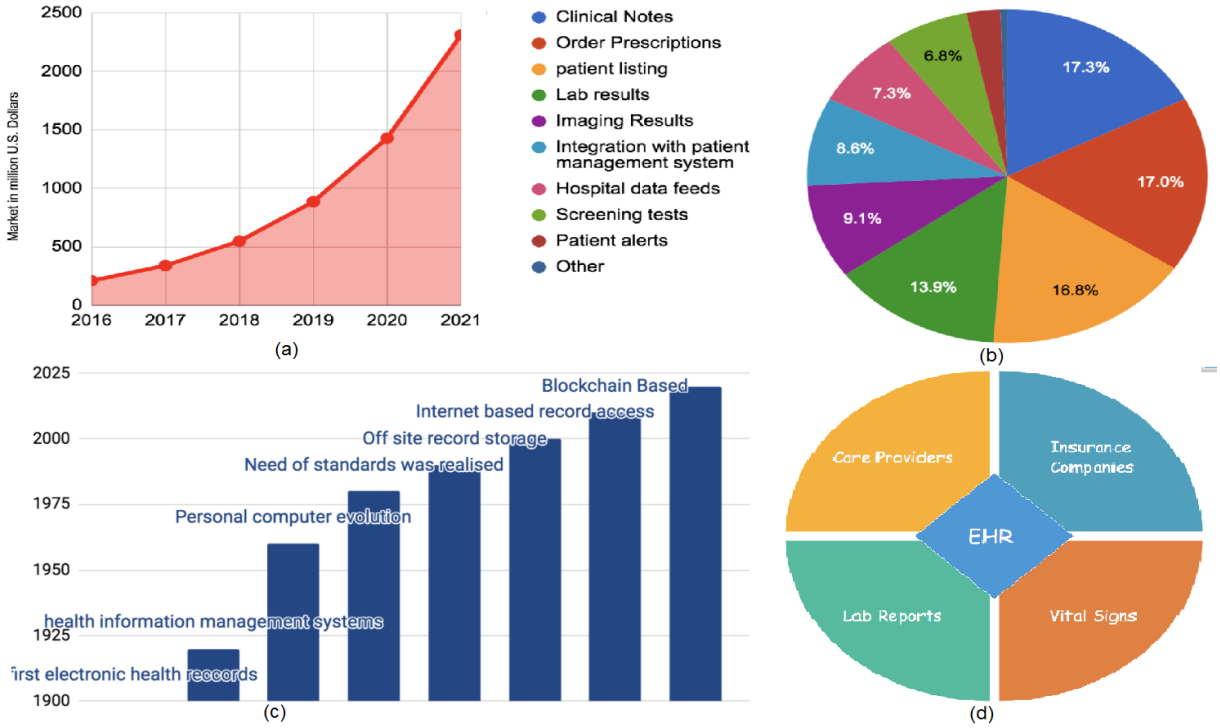

Fig. 1: Revolution in Healthcare sector: (a) Blockchain market over the years and predictions for the future, (b) Different parameters in the EHRs, (c) Evolution of the technologies used in EHR-systems, and (d) Stakeholders in the EHRs.

chain become aware of the position of the drug and any counterfeiting of the drugs may be detected. SimplyVital health [12] emerged as a blockchain-based protocol for the safe adoption by Healthcare [22]. Another product developed by SimplyVital health is connecting care, which is a platorm for sharing of patient data amongst various providers. EncrypGen [13] built a platform for safe sharing of genomic data for enabling the use of cryptocurrency. Medicalchain[14] is a decentralized blockchain platform for secure storage and sharing pre-authorized health records. A telemedicine system is also hosted on the platform. Coral Health [15] utilizes the potential of blockchain for personalized medicine systems. It utilises disparate formats for efficient storage of data related to the patient.

Chronicled [16] is another blockchain based solution combining with various IoT systems on supply chains to increase accountability in fields of pharmacy. The solution speeds up logistics and minimizes discrepancies. Patientory [17] creates users' profiles and tracks their health history, providing patients an ease way of monitoring and listing their bills, information, immunizations and medications. Stacked Denoising Autoencoders (SDA) [18] were implemented to monitor arrhythmia conditions based on a blockchain ledger. Advanced blockchain [19] defines a new norm for social interactive forms of patient and health record management systems [20].

A. Research Contribution

Following are the major research contributions of this paper:

- We propose a Blockchain-based approach for efficient storage and transfer of EHRs.
- Analyze how proposed framework fulfills the needs of patients, providers, and third parties.
- To understand how the framework maintains the privacy and security concerns in the healthcare 4.0.
- Various contracts consisting the blockchain have been discussed in terms of the Healthcare scenario.
- Justify the role of vital functions that make the blockchain effective.

B. Organization

We have organized the paper as follows. Section II describes the proposed Blockchain-based framework for storage and maintenance of EHRs. Section III describes the system architecture. Section IV descibes the contracts consisting the chain and vital functions that are undertaken on the chain. In section IV, we conclude the paper with future scope.

II. Proposed Framework

This section contains a detailed discussion on proposed framework, contracts required in blockchain, and pseudo code of the proposed framework.

1) Execution Modes: Execution takes place as a call or a "sendTransaction" where, a call is worked up on the local machine of the end-user. It is a quick procedure, but works on a read-only paradigm. They are never sent on the network and hence need not be authenticated for intra network communication. Transactions are sent using "sendTrasaction" , which are pursued by verified miners, with a potential of drastically impacting the chain [20].

2) Communication Methods: There are two ways in which Ethereum contracts may pursue intra and inter network communication. First is via Messages, which are between contracts and are not affected by the mining that takes place on the blockchain. Transactions originate from the end-users which initiates various processes. Always

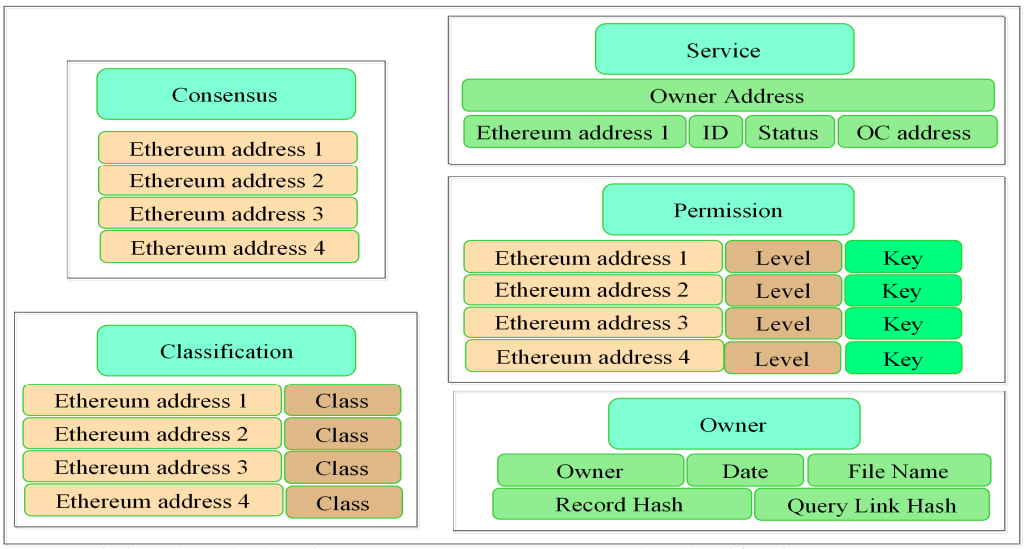

Fig. 2: Contracts consisting the Blockchain: (a) Consensus Contracts, (b) Classification Contracts, (c) Service Contracts, (d) Permissions Contract, and (e) Owner Contracts.

a single transaction is required for the initiation, while multiple messages may be utilized [20].

A. Constituent Nodes

The differentiation not only increases the scalability of the Blockchain such that various stakeholders can interact with the chain to avail of resource in an efficient manner. Nodes constituting the block chain are divided into three categories:

- Full Nodes: Every transaction is stored, with every respective block from the blockchain. A larger storage space and increased computational power is required.
- Light Nodes: Only block headers are stored to verify the change in any block or a transaction that occurred. Specific data can be accessed through the light nodes.
- Archive Nodes: Store every transaction, every block and the receipts of the transactions that take place. This enables the network to retrieve required data.

B. IT Components

1) Database Manager: A manager navigates amongst the databases that save the patient health records and link generation to point to the records. The manager will also create hashes of the records and queries generated for the link. Integrity is preserved using the hashes as they avoid direct access of the database.

2) Cipher Manager: The cryptographic requirements of the paradigm will be handled by the Cipher Manager. Encryption-decryption of the files that are stored/exchanged will be undertaken by the Manager. Keys are used for the purpose; symmetric key style and public key style encryption schema are utilized.

C. Blockchain Contracts

Various blockchain contracts will be a part of the nodes that constitute the chain, as shown in Fig. 2.

1) Classification Contract: defines the various levels and degrees of nodes present in the system and classifies them as:
   - Patients
   - Care Providers
   - External Parties

   Every blockchain has a unique classification contract, which is responsible to maintain the Ethereum addresses and associative relationships of the present nodes. Uniqueness of the entries are thus preserved with an eased complexity of controlling the access of the nodes by functioning as the convergence point for the control [20].
2) Consensus Contract: Consensus is used in the blockchain to keep confirming newer nodes that are added by constant authorization of their safety to the chain. An important use of the contract is the termination of nodes which may cause damage to the chain and hence must be overwritten. The consensus contract is another unique contact for the blockchain, which maintains the registered user lists, mining in the chain. It stores the voting permission and Ethereal address of the registered nodes. The consensus contract is further used to validate nodes, when they are added to the chain.
3) Service Contract: An important feature of the chain is the relationships that are held among the nodes that constitute the chain. Hence, a service contract lists the various relationships that were held and are being held. It further holds the Ethereum address of the nodes and the associated nodes, status of relation; active or inactive. Permission / authorization requests from the patient can be queried using the contract. This contract ensures the patient is aware of the usage of his data access and the transactions that take place.
4) Owner Contract: lists the records that belong to particular patients and tracks the providers that use the records. Owner contracts are created as and when a relationship is defined between nodes. Constituent fields of the contracts are:
   - Owner Field : owner patient
   - Date: time till which the record may be available
   - Hashes (record and query link)
   - Filename of the record

   Links are sent using the *HTTPS* protocol and the

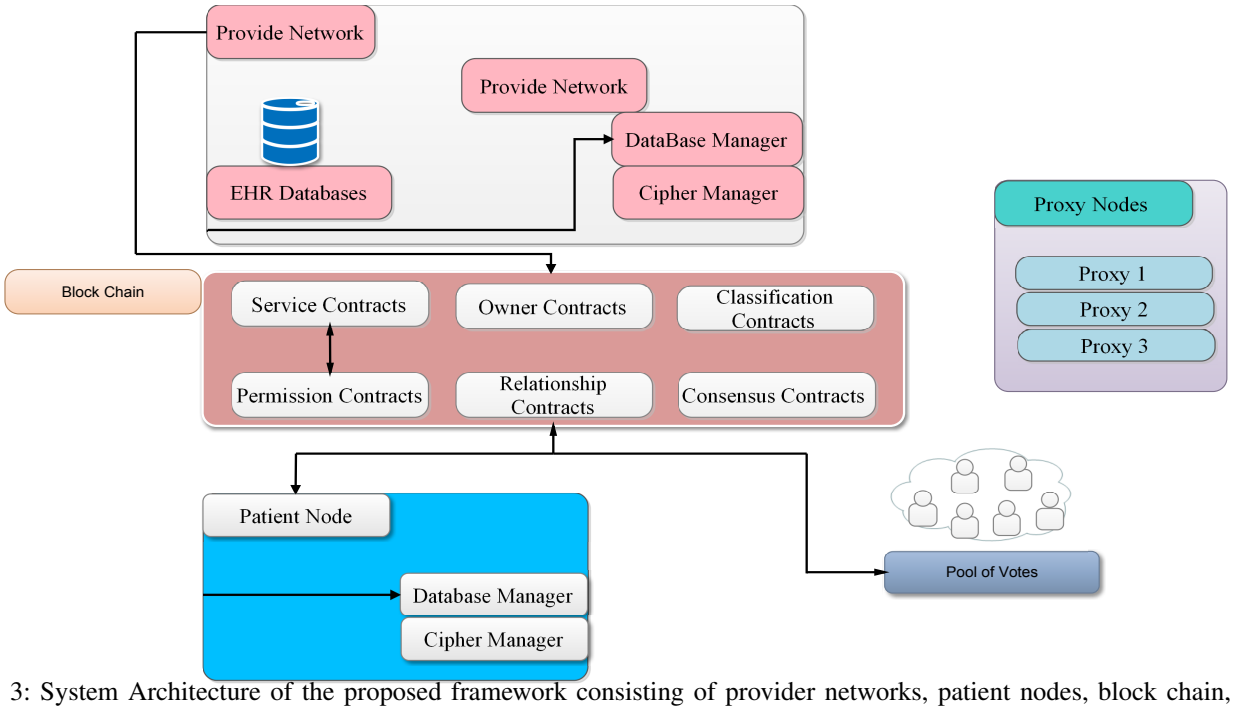

Fig. 3: System Architecture of the proposed framework consisting of provider networks, patient nodes, block chain, pool of voters and the proxy nodes.

alteration of the link can be averted using the hashes in the contract.

5) Permission Contract: It saves the addresses of various nodes, which may interact with the stored records and can be accessible by the chain. It is unique to each record and is built when the record is added. There are various access levels that may be permitted.
   - Read: Retrieve a node and use it as a resource.
   - Write: Retrieve a node, write to the node, use and write to it as a resource.
   - Transfer: Allow exchange of the record with other nodes registered on the chain.
   - Owner: Nodes can be added, removed with the access and a generic access is given to change the whole chain layout.

III. System Architecture

The proposed framework is divided into four major portions on the basis of utility and functions, such as the Blockchain, patient nodes, provider networks and proxy nodes. The complete architecture of the proposed framework is shown in Fig. 3. The Blockchain is a network of nodes that are capable of transferring records, and initiating records. It consists of contracts or service contracts, owner contracts, classification contracts and permission contracts as described in previous sections. Patient nodes are the end-user nodes, where the records are generally created. Provider networks houses the health record database and provider nodes, which consist of a database manager and a cipher manager for the purposes discussed in the previous section. Voter pools help in the validation of the nodes that are added and maintaining integrity of the transactions that take place in the network.

A. Vital Functions performed on the Chain

1) Addition of a Block: Addition of a node takes place after wallet allocation,public identifier and a provision of Ethereum address to the node. Addition is initiated when the public identifiers are validated by the voter nodes for a particular class required.Validation for patient nodes is minimal when compared to the validations performed for health care providers and doctors. The validation requests need to be made from registered nodes. Once validation has been completed, the classification contract generates a new account and service contract for the node. Users receive a notification from the node once the process is completed. A detailed version of the process is described in Algorithm 1. Detailed execution of the proposed framework is given in Algorithms 1 to 6, where CL_C is Classification Contract, CO_C is Consensus Contract, S_C is Service Contract, O_C is Owner Contract, P_C is Permission Contract, R_C is Relationship Contracts, DB_M is Database Manager, D_B is Database, and C_M is Cipher Manager.

Algorithm 1 Addition of a patient node.

Input: Created Nodes (C_N) and provided an E_A.
Output: Addition of node to the chain

1: Provider(New Node E_A and type)-> CL_C
2: CL_C(requested E_A and type)-> CO_C
3: Voter Nodes polled (Type Validation) by CO_C
4: Votes returned to CO_C, compiled and sent to CL_C, and confirmed.
5: CL_C-> request to new node to be added to the chain.
6: Patient Node-> response-> CL_C
7: **if** (affirmative) **then**
8: Update CL_C memory and create S_C
9: S_C sent to patient.
10: **end if**

2) Addition of a Patient: Patient registration is intuitively a relationship creation between two nodes. The Service contracts are used to document the relationships. Each time there is an interaction between the patient and the provider, an updating is required. The detailed process is as defined in Algorithm 2, where a patient is checked for the registration, and data flow takes place towards the service contract, which is updated further. The patient node is requested for appro-

priate validation of the research, and preserving the privacy of patients data. The process can be further terminated or an owner contract can be generated for the same. Service contracts are further updated for future utilization.

Algorithm 2 Addition of a New Record.

Input: Node must be registered, relationships must be defined
Output: New record is added to the block.

Provider (DB_M)-> query->free space (F_S), hash(link), link, record-> C_M
Key Generation : C_M, encrypts new record and link
DB_M : Stores record in D_B
Provider Node(ID)-> S_C
S_C (associated O_C address)-> Provider Node
Provider node(record name, link, hashes, keys)-> O_C
Creation of a new P_C : O_C
Permission creation : P_C
O_C : adds record information
Link-> Patient via HTTPS
Patient Node stores query in C_M.

3) Initiate/Revoke/Change Access Permission: Permissions are required to be changed during the platform run where records are to be transferred from the owner to another party stakeholder. Permissions contract provides read access on the record. Permissions contract checks for the viability of the change in access of the record. The transferee needs to have owner access on the record. The permissions contract is searched initially to request a change in permission and the change is committed. Once the updating is done, a notification is sent to the record owner and the provider.

Algorithm 3 Addition of Provider Patient Relationship.

Input: Patient's E_A and ID.
Output: A new relationship between the provider and the patient.

Verification : Provider node(patient's E_A)-> CL_C
Provider Node (E_A, ID and active status)-> S_C
S_C: confirm new patient
S_C (Asks for authorization)-> Patient
if ($positive$) **then**
    S_C updated, a new O_C created.
    O_C(addresses sent to both S_Cs)
end if

4) Addition of a Record: Provider node is responsible for the encryption of a record when it is to be added to the chain. A relationship and owner contract should be in place between the patient and the provider. The database manager is the next stage from the provider node after the creation of a record, to query the database. Hashes are generated for vital communication with the cipher manager. The owner contract creates a permission contact for the record, and further developing the relationship contract. A quicker transfer is possible with the paradigm. Algorithm 4 details the process behind the addition of the record.

5) Retrieval of a Record: No transaction is needed while retrieving records from the chain. The owner contract is looked up for the provider who keeps the record. A request is issued, and a permission is granted accordingly. The query links are encrypted and stored in the cipher manager to get the records from the database. The records are accessed over the Internet through respective wallets and hence, can be accessed anywhere with secure boundary. The complete process of retrieval of a record is detailed in Algorithm 5.

6) Transfer a Record: An EHR management system requires efficient transfer of records of the patient. The basic pipeline of the process is retrieval of the record, decryption

Algorithm 4 Changing Permissions.

Input: Patient Node with Owner Access.
Output: Permissions added/revoked/initiated.

Provider Node(id)-> Provider S_C
Provider S_C(associated O_C) -> Provider Node
Provider Node(Filename) -> O_C
O_C(File's PC) -> Provider Node
Provider Node(requested permission) -> P_C
Review : current access node by P_C
if ($notlowerlevelaccess$) **then**
    Request to change : P_C
    Authorization by patient
end if
if ($positive$) **then**
    P_C updates file.
    Notify provider and patient
end if

Algorithm 5 Retrieving Record.

Input: Patient Node with Read Access, Access Key.
Output: Patient accesses record.

Patient Node(provider ID)-> S_C
SC(OC address)-> Patient Node
Patient Node(filename, address)-> O_C
Permission check : O_C 5.
if (authorized) **then**
    key -> O_C
    O_C (encrypted key) -> Patient Node
    Decryption of key : Patient Node
    DB_M : link, retrieve encrypted document.
    Decryption of document : C_M
end if

using the cipher manager and sending the record to the receiver. Provider Node locates the permissions contract as required, with a transfer or higher level of access. The permissions are expected to be confirmed by the permission contracts and then they are delivered. The complete process to transfer a record is detailed in Algorithm 6.

Algorithm 6 Transferring a record.

Input: Provider A with Transfer Access, registered Provider B
Output: Record Transferred.

Provider A (patient ID) -> S_C
$S_C(O_C)$ -> Provider A
Provider A (filename) -> O_C
O_C (address of P_C) -> Provider A
Provider A (E_A, request level) -> P_C
Verification : P_C (transaction) -> CL_C
Database updated : read access -> Provider B
P_C (E_A of B, key) -> Proxy Nodes
Re-encrypted : Proxy Nodes
Proxy Nodes(keys) -> P_C
Added to D_B : P_C
P_C (P_C address)-> Provider B
Decryption of link: Provider B

IV. Discussions

By using the cipher manager, and incorporating the use of encryption techniques before sending and receiving the records over the network, the probability of unauthorized use of the records is minimized. Each patient has a unique Ethereum address and identifier, which makes the identification a tedious task for an unauthorized user. The usage of various contracts as described to give a sense of modularity further makes the framework attains a higher level of data security. Using multiple contracts for execution of the full node can in turn lead to more demand on the registration processes and formalities during transactions.

A. Preserving the Privacy

Proposed framework used various privacy-preserving schemes. It is very difficult to identify any specific patient through its existing account number and Ethereum address. In the proposed frameowrk, we have used the encryption schemes on the patient private data stored on the blockchain, which reduces the chances of unauthorized access of the patient private data. Moreover, by using S_C, O_C, and P_C for information separation, data confusion arises. The proposed framework preserve the patient private data, but there are still some gaps, which needs to be filled. These are: (a) to preserve the privacy, the user has to compromise with the ease of use because using blockchain based framework in EHRs requires large computational power and also takes more time to execute each task. Moreover, addition of a new node and adding new patient provider relationship requires large number of steps to verify the genuine user.

It is not easy to hide all the private information of the patient by using the blockchain technology. Use of this technology makes it easier to know which specific node visits a provider and also the frequency of visit, which makes it possible to gather patient private information such as names, disease, and current address. Moreover, it is difficulty to properly arrange this gathered information and find out which person is related with the Ethereum address. To address this issue, our framework used a differential privacy model [21] [23] [24]. It would add noise to the transaction available at blockchain. This model was primarily used to preserve the data privacy and at the same time maintaining the EHRs, which makes the data confidential while any one view this data from outside. In future, we will explore the practicality of using the differential privacy model and try to establish the correlation between the noise and size of blockchain.

B. Scalability

Proposed framework would be used in various ideas to support scalability. To reduce the storage space, only the hashes and small EHRs on the blockchain are needed to be stored. Moreover, when performing the private patient transactions, few nodes require validated transactions having data hashes. This will further reduce the storage and mining cost of the blockchain. On the other side, as more users are added to the system, then the search time of CL_C would definitely increases. Hence, some new alternatives are required to effectively perform the searching of CL_C with large local databases

V. Conclusion

In this paper, we propose a Blockchain-based framework for efficient storage and maintenance of EHRs. We also discuss the management of EHRs using the blockchain paradigm. Here, the patient is given the sole control and ownership over his records and he can monitor the transactions that are undertaken over it. Unauthorized access by various actors is further minimized and a sense of decentralization while consisting certain nodes with an improvised authority is achieved. This study shown that it would be highly unlikely to completely hide all information and maintain an accessible and interoperable system, but by using smart contracts to separate information, proposed framework still offers significant privacy preservation and data integrity. We also conclude that complete encryption of the records and maintaining ease of use cannot go hand in hand and there is a trade-off that needs to be taken care by the network operator. In future, we will explore the practicality of using the differential privacy model and try to establish the correlation between the noise and size of blockchain.

References

[1] Tracy Shumaker, More than 16 million medical records breached in 2016 [Online]. Available: https://www.itgovernanceusa.com/blog/more-than-16-million-medical-records-breached-in-2016/. [Accessed: 12 March, 2018].

[2] K. Clauson, E. Breeden, C. Davidson, and T. Mackey, "Leveraging Blockchain Technology to Enhance Supply Chain Management in Healthcare:", *Blockchain in Healthcare Today*, vol. 1, Mar. 2018.

[3] X. Liang, J. Zhao, S. Shetty, J. Liu and D. Li, "Integrating blockchain for data sharing and collaboration in mobile healthcare applications," *IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, Montreal, QC, 2017, pp. 1-5.

[4] Jennifer Bresnick, 16% of Healthcare Stakeholders Plan to Use Blockchain by 2017 [Online]. Available: https://healthitanalytics.com/news/16-of-healthcare-stakeholders-plan-to-use-blockchain-by-2017. [Accessed: 17 Apr, 2018].

[5] Robmenzies, Healthcare Data Management meet Blockchain [Online]. Available: https://steemit.com/healthcare/@robmenzies/healthcare-data-management-meet-blockchain. [Accessed: 18 Apr, 2018].

[6] [Online]. Available: http://www.acc.org/membership/member-benefits-and-resources/acc-member-publications/cardiosurve/newsletter/archive/2014/07/ehr

[7] Size of the blockchain technology market worldwide from 2016 to 2021. [Online]. Available: https://www.statista.com/statistics/647231/worldwide-blockchain-technology-market-size/. [Accessed: 27 Apr, 2018].

[8] EHR Use Widespread But Challenges Persist. [Online]. Available: http://www.acc.org/membership/member-benefits-and-resources/acc-member-publications/cardiosurve/newsletter/archive/2014/07/ehr

[9] J. Vora, S. Tanwar, S. Tyagi, N. Kumar and J. J. P. C. Rodrigues, "Home-based exercise system for patients using IoT enabled smart speaker," 2017 *IEEE* 19^{th} *International Conference on e-Health Networking, Applications and Services (Healthcom)*, Dalian, 2017, pp. 1-6.

[10] J. Vora, S. Tanwar, S. Tyagi, N. Kumar and J. J. P. C. Rodrigues, "FAAL: Fog computing-based patient monitoring system for ambient assisted living," 2017 *IEEE* 19^{th} *International Conference on e-Health Networking, Applications and Services (Healthcom)*, Dalian, 2017, pp. 1-6.

[11] [Online]. Available: https://www.blockpharma.com/ [Accessed: 24 Apr, 2018].

[12] Simply Vital Health [Online]. Available: https://www.simplyvitalhealth.com/. [Accessed: 20 Apr, 2018].

[13] David Koepsell, The Future of Genomic Data Encryption [Online]. Available: https://encrypgen.com. [Accessed: 28 Apr, 2018].

[14] Medicalchain [Online]. Available : https://medicalchain.com/en/. [Accessed: 27 Apr, 2018].

[15] CoralHealth 2018 [Online]. Available: https://mycoralhealth.com/.

[16] Smart Supply Chain Solutions. [Online]. Available : https://chronicled.com/.

[17] Patientory. [Online]. Available: https://patientory.com/.

[18] A. Juneja and M. Marefat, "Leveraging blockchain for retraining deep learning architecture in patient-specific arrhythmia classification," *IEEE EMBS International Conference on Biomedical & Health Informatics (BHI)*, Las Vegas, NV, USA, 2018, pp. 393-397.

[19] W. Liu, S. S. Zhu, T. Mundie and U. Krieger, "Advanced block-chain architecture for e-health systems," *IEEE 19th International Conference on e-Health Networking, Applications and Services (Healthcom)*, Dalian, 2017, pp. 1-6.

[20] Gaby G. Dagher, Jordan Mohler, Matea Milojkovic, Praneeth Babu Marella, "Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology", *Sustainable Cities and Society*, Volume 39, 2018, Pages 283-297.

[21] Dwork, C., Differential privacy. *Proceedings of the international colloquium on automata, languages, and programming (ICALP)*, 2006, pp. 1–12.

[22] A. Kumari, S. Tanwar, S. Tyagi, N. Kumar, Fog computing for Healthcare 4.0 environment: Opportunities and challenges, *Computers & Electrical Engineering*, Volume 72, 2018, Pages 1-13

[23] J. Vora, P. Dev Murari, S. Tanwar, S. Tyagi, N. Kumar and M. S. Obaidat, "Blind Signatures Based Secured E-Healthcare System," 2*018 International Conference on Computer, Information and Telecommunication Systems (CITS)*, Colmar, 2018, pp. 1-5.

[24] J. Vora, P. Italiya, S. Tanwar, S. Tyagi, N. Kumar and M. S. Obaidat., "Ensuring Privacy and Security in E- Health Records," *2018 International Conference on Computer, Information and Telecommunication Systems (CITS)*, Colmar, 2018, pp. 1-5.