Blockchain based Healthcare System

Priyanka Deshmkuh
Department of Computer Engineering,
Maharashtra Institute of Technology,Pune

Prof. B. S. Tiple
Department of Computer Engineering,
Maharashtra Institute of Technology,Pune

Abstract—Blockchains are distributed ledgers that authorized parties who do not fully believe each other to maintain a set of overall states. The parties approve of the presence, values, and past of the states. As the technology landscape is expanding speedily, however, it is both vital and challenging to have hold of what the core technologies have to propose, In today's life hospital data is deposited more on the cloud. Here data of patient need to store securely. Data and information security are basic for most organizations and even home computer users. Client data, payment data, individual documents, financial account details where the bulk of this data can be difficult to replace and conceivably unsafe that it falls into the wrong hands. Information lost because of disasters, for example, a flood yet losing it to hackers or a malware infection can have significantly more noteworthy results. In block-chain technology, each page in a ledger of transactions forms a block. That block has an effect on the next block or page through cryptographic hashing. Interestingly, when a block is completed, it creates a unique secure hash value, which ties into the next page or block, creating a chain of blocks, or block-chain. In the system, data will be of healthcare data need to secure. This work is designed using blockchain concept and key-based cryptographic technique. Stores the hash tables of raw data on the blockchain, validates other copies by running a hashing technique, and then compares the data stored in the block-chain, any interference with the data will be quickly found because the original hash tables are stored on millions of nodes. System work on storing data from the healthcare system. On the web, more data of the healthcare system is stored and that data needs to stored securely.

***Index Terms*—Block, Blockchain, Ledger, cryptography, hashing, healthcare.**

INTRODUCTION

With the rapid growth of mobile computing, wearable technology, and wireless sensing, people have been using different types of mobile and wearable devices, such as smartphone, smartwatch, smart band, and smart glasses etc., to realize numerous health-related applications, such as remote diagnosis [1], disease monitoring [2] and elderly people caring [3]. The huge amount of personal health data are shaped by these devices and these data are valued resources for healthcare research and marketable applications. Appropriately sharing personal health data will be advantageous to all related stakeholders including the device users, patients, researchers, companies and even the whole public healthcare system. As a personal asset, the health data should be owned and measured by the respective users themselves, while in reality they are usually precise by different service providers, device productions or scattered in different healthcare systems [4], [5]. In general, it brings barriers for the data sharing and puts data security and privacy at risk as these centralized data stores and

The blockchain technology has increased substantial admiration in recent years, primarily in the financial field, due to the cryptocurrencies. For example, Bitcoin was first introduced in 2008 [7] and ever since has attracted the attention of the research community from various academic fields [8], [9], [10] and gained mainstream popularity due to its exclusive characteristics, such as the absence of centralised control, an assumed high degree of anonymity and distributed consensus over decentralised networks. Blockchain solutions could reduce data breach risks by utilizing threshold encryption of data together using public key infrastructure, where cooperation of multiple parties is required to decrypt data and asymmetric cryptography is used to validate communication with system participants [11].

A.Overview

The blockchain based data sharing system could dramatically simplify data acquisition process for research and commercial projects and provide an opportunity for users to gain the ownership and the privileges of their own data and get aids from them. It could also lead to healthier control over their data and assurances fine-grained tracking of all their data practice activities [11]. The aim of this paper is to propose a personal health data sharing system based on the blockchain, to enable users easily and securely share their personal health data and help researchers and commercial data consumers to obtain necessary required data in an effective, transparent way and in compliance with data regulations.

I. REVIEW OF LITERATURE

[12] In this paper purely peer-to-peer version of electronic cash would permit online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main aids are lost if a trusted third party is still essential to prevent double-spending. A solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work.The longest chain not only serves as proof of the order of events witnessed. As long as a majority of CPU power is controlled by nodes, they'll generate the longest chain and outperform attackers.

[13] this paper, Cedpece an innovation, decentralized record management system to handle cats, using blockchain technology. this system gives patients a comprehensive, immutable log and easy access to their medical information across providers and treatment sites. leveraging unique blockchain properties,

MedRec manages authentication, confidentiality, accountability, and data sharing crucial considerations when dealing with sensitive information. A modular design integrates with providers' existing, local data storage solutions, facilitating interoperability and making our system suitable and adaptable. We incentivize medical stakeholders (researchers, public health authorities, etc.) to participate in the network as blockchain â €œminersâ€. This provides them with access to the collective, anonymized data as mining rewards, in return for sustaining and acquiring the network via Proof of Work. [15]This paper depicts Sharing healthcare data between institutions is interesting. Heterogeneous data structures may preclude compatibility, while disparate use of healthcare terminology limits data comprehension. Even if structure and semantics could be agreed upon, both security and data consistency concerns abound. Centralized data stores and authority providers are attractive targets for cyber attack, and establishing a reliable view of the patient record across a data sharing network is problematic. In this paper Blockchain- based approach to sharing patient data is explained. This approach trades a single centralized source of trust in favor of network consensus and predicates consensus on proof of structural and semantic interoperability.[14]This paper illustrates a blockchain platform architecture for clinical trial and precision medicine and discusses numerous design aspects and provides some insights into the technical requirements and challenges. blockchain application data management component for data integrity, big data integration, 3)and integrating disparity of medical related data, verifiable anonymous identity management component for identity privacy for both person and Internet of Things (IoT) devices 4)and secure data access to make possible of the patient centric medicine, and trust data sharing management component to enable a trust medical data ecosystem for collaborative research.

III. System Architecture

A. Overview

Data forms the foundation of the application system, and its integrity is important to the data's value and the aim of data security technology prevention. According to the method of cryptography, digital signature generates a set of data information representing the identity and data integrity of the signer, normally attached to the data file.

Detailed descriptions of the proposed system are as follows:

1) *User*
A user is a patient who is accessing his/her own personal data. Key is provided to encrypt and digitally sign the transaction.

2) *Healthcare data*
Information regarding patients prescriptions, medical record, MRI scan, pathology report. This data is accessed by the patient.

3) *Transaction*
It is a small unit of the task that is stored in blocks. These records consist the healthcare data.

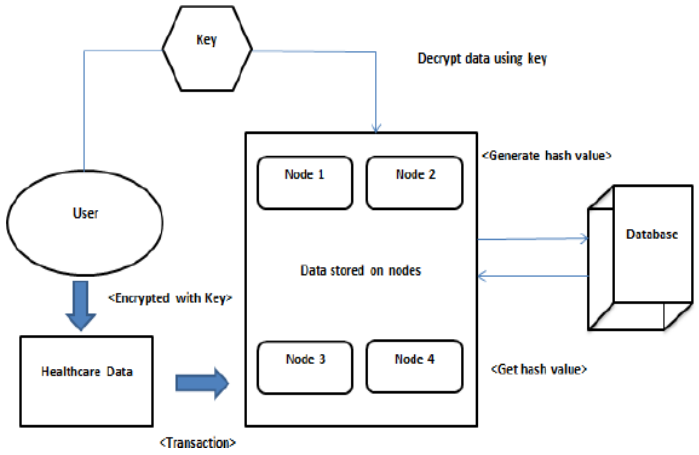

Fig. 1. System Architecture

4) *Nodes*
A node is a device on a blockchain network connected in a peer to peer network.
Blocks
A block represents the 'present' and contains information about its past and future hash value.

5) *Blockchain*
Blocks are linked to each other using the hash value of the previous block. Thus, blockchain is append only KVS database, there is no insert and update. SET, GET query is used. Once the block is attached to the chain.

6) *HealthCare system*
The aim is to secure the healthcare data and its integrity. Digital signature generates a set of data information representing the identity and data integrity of the Patients. Normally appended to the data file. The user validates the digital signature through the user's key to Verify the authenticity and integrity of the data information. Blocks stores the hash tables of raw data and files on the block-chain, Validates other using consensus protocol, then check whether the transaction is valid or not. Patient has a key with which they encrypt and digitally signs the data. Once the transaction is valid block is attached to the chain.
It not then the transaction is discarded. Patient provides key to providers to access the data. A user provides consent to provide patients with data access to providers. This data is accessed by the patient. Data is used by different providers if permission is granted by the patient. These records consist the healthcare data. All nodes use the same consensus protocol to remain compatible with each other. It is the nodes on the network that confirm and validate transactions, putting them into blocks.

IV. ALGORITHM USED

In blockchain based healthcare system, two algorithms have been used, initially, the transaction is hash as a unique value using SHA-256 algorithm, which is encrypted using AES algorithm which makes the transaction more secure.

A. Secure Hashing Algorithm - 256

It works by altering the data using a hash function: an algorithm that consists of bitwise operations, modular additions, and compression functions. The hash function then produces a fixed size string that looks nothing like the original. These algorithms are designed to be one-way functions, meaning that once they are transformed into their respective hash values, it's virtually impossible to transform them back into the original data.
calculate hash code for an input up to 2 to the power (64)-1 bits. output is 256 bit.SHA-256 is a 256 bit (32 bytes) hashing algorithm. It undergoes 64 rounds off hashing. The calculated hash code will be a 64 digit hexadecimal number.

Application:
1.SHA is used to encrypting passwords.
2.Creating unique values.

Advantages:
1.Time efficient.
2.Robustness.

B. Advanced Encryption Standard Algorithm- 256

AES(Advanced Encryption Standard).It is a symmetric algorithm. It used to convert plain text into cipher text.The need for coming with this algorithm is the weakness in DES. The 56 bit key of des is no longer safe against attacks based on exhaustive key searches and 64-bit block also consider as weak. AES was to be used the 256-bit block with 256-bit keys. In this drop, we are using it to encrypt the data owner file. Encryption part converts data into cipher text form while decryption part converts cipher text into text form of data

Input: 256 bit input in terms if 0 and 1
Process: 14,rounds 256 bit input
Hard Disk: 20 GB
State block: Xor (i/p)
Final round: 10,12,14
Each round consists: sub byte, shift byte, mix columns, add round key
Output: cipher text(256 bit)

Advantages:
1.it is most robust security protocol.
2.used for wide various of applications such as wireless communication, financial transactions, e-business, encrypted data storage etc
3.It is one of the most spread commercial and open source solutions used all over the world.
4.For 128 bit, about 2 to the power 128 attempts are needed to break. This makes it very difficult to hack it as a result it is very safe protocol.

Application:
1.Used to secure digital information in various forms data

B. Mathematical Model

In this section, mathematical expression of proposed system is explained.

Let S be a system such that,

S = {I, P, O, Sc, Fc}

where,

I = Inut of the system
P = Processes in the system
O = Output of the system
Sc = Success Case of the output of the system
Fc = Failure Case of the output of the system

I - {T1,T2,T3,T4}

where,

{T1,T2,T3,T4} - Transaction of healthcare data in .text extension file.

Process :

P = {Fc, Hc}

where,

Fc - File is encrypted using Advanced encryption standard Algorithm

Hc - Hash value is created for each transaction in block using Standard Hashing Algorithm

Where

Fc – {Pt, Pk, De}

Where

Pt - Transaction data in terms of plain text
Pk - Private key is generated
De - HealthCare data Encrypted
O - File has been Encrypted and successfully stored.
Sc - It is success case when file of healthcare data stored successfully on network
FC - It is failure case when authentic patient is not able to upload the data

Equation for node N can be given as,

$$N = \sum_{i=1}^{n} Ep(H(Pn))$$

Where

P- Plain text of transaction in form of .text file
Ep- Elliptical curve digital Algorithm
H- Secure hash Algorithm
n- Number of Transaction in each node

O = Healthcare data is accessed by patient and providers securely.

Thus, above mathematical expressions explains the system flow.

V. SYSTEM ANALYSIS

The blockchain is an emerging technology for distributed and transactional data sharing across a large network of un-trusted participants. the patient is able to grant access to different providers using key sharing. thus data oI particular patient is stored on the blockchain. each record is represented as a transaction which is hashed using SHA-256 algorithm and encrypted using AES algorithm-256 is applied to make each transaction more secure. and thus block is created or the number of transaction and those blocks are linked to one another and to form the chain. this the transaction is more secure in case intruder wants to intrude in between. the hash value gets disturbed thus whole chain breaks. which makes the system more robust. thus healthcare data is more secure.

VI. EXPECTED RESULTS

Blockchain-based healthcare system is a data-intensive domain in which a large amount of data in which MySQL is used for data storing purpose. A different table is created to retrieve the information. as shown in below

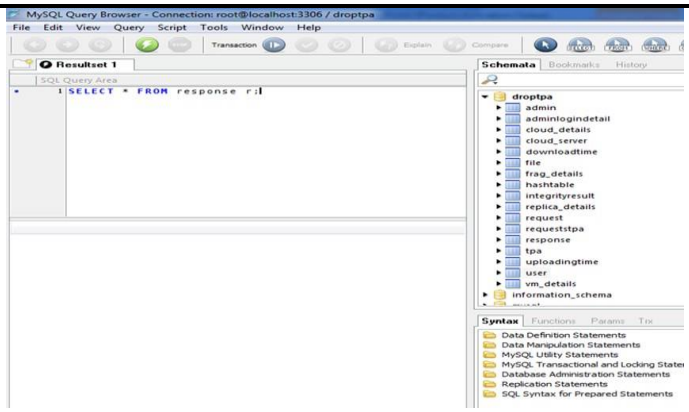

Fig 2. MySQLDatabase

A doctor can review the information by accessing own account which is shown as below The results of the patient s visit is then be stored at the hospital, which will be retrieved at a later time by a physician in another hospital in network.

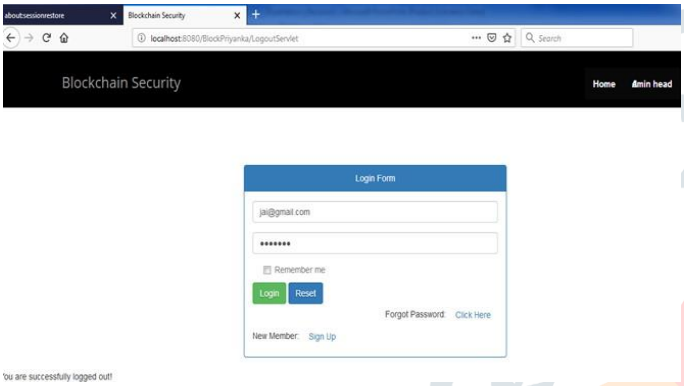

Fig 3. Login page

After logging in patient can access data from different providers

Fig 4. Patient's account

Thus to the nature of the industry, ensuring the security, privacy, and integrity of healthcare data is maintained. Which leads to a sound and secure data management system.

VII. Conclusion

In this work blockchain based concept and key-based cryptographic technique which estimate the security of block-chains specifically using hashing. system work to security on healthcare data. Blockchain technology is not just an application technology for new generation transactions. It creates trust, responsibility, and transparency while simplifying business processes. This approach allows users to authenticate the data access through the public and private key of user sources , while improving network access performance by locally authenticating keys based on blockchain copies and its hash values. This work is designed using blockchain concept and key-based cryptographic technology to offer the security to healthcare data of a patient.

VIII. Future Scope

In the blockchain based healthcare facility, the effective combination of Insurance facility to the patient incorporated in blockchain which gives the invitation to the new domain so as to access medical insurance associated with each patient. Incorporation of medical Insurance data and security to its open door to Insurance domain as a benefit. while making system more secure and data to be more protected future scope could give more benefits to the patient and providers as a whole.

References

[1] D. Son, J. Lee, S. Qiao, R. Ghaffari, J. Kim, J. E. Lee, C. Song, S. J. Kim, D. J. Lee, S. W. Jun et al., "Multifunctional wearable devices for diagnosis and therapy of movement disorders," Nature nanotechnology, vol. 9, no. 5, p. 397, 2014.

[2] X. Zheng, A. Vieira Campos, J. Ordieres-Mere, J. Balseiro, ´ S.Labrador Marcos, and Y. Aladro, "Continuous monitoring of essential tremor using a portable system based on smartwatch," Frontiers in neurology, vol. 8, p. 96,

[6] K. Peterson, R. Deeduvanu, P. Kanjamala, and K. Boles, "A blockchainbased approach to health information exchange networks," in Proc. NIST Workshop Blockchain Healthcare, vol. 1, 2016, pp. 1–10.

[7] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[8] S. T. Ali, D. Clarke, and P. McCorry, "Bitcoin: Perils of an unregulated global p2p currency," in Cambridge International Workshop on Security Protocols. Springer, 2015.

[9] R. Bohme, N. Christin, B. Edelman, and T. Moore, "Bitcoin: Economics, ¨ technology, and governance," The Journal of Economic Perspectives, vol. 29, no. 2, pp. 213–238, 2015.

[10] M. A. Harlev, H. Sun Yin, K. C. Langenheldt, R. R. Mukkamala, and R. Vatrapu, "Breaking bad: De-anonymising entity types on the bitcoin blockchain using supervised machine learning," in Proceedings of the 51st Hawaii International Conference on System Sciences, 01 2018.

[11] P. Mamoshina, L. Ojomoko, Y. Yanovich, A. Ostrovski, A. Botezatu, P. Prikhodko, E. Izumchenko, A. Aliper, K. Romantsov, A. Zhebrak et al., "Converging blockchain and next-generation artificial intelligence technologies to decentralize and accelerate biomedical research and healthcare," Oncotarget, vol. 9, no. 5, p. 5665, 2018.

[12] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." (2008): 28.

[13] Ekblaw, Ariel, et al. "A Case Study for Blockchain in Healthcare:"MedRec" prototype for electronic health records and medical research data." Proceedings of IEEE Open & Big Data Conference. 2016

[14] Shae, Zonyin, and Jeffrey JP Tsai. "On the Design of a Blockchain Platform for Clinical Trial and Precision Medicine." Distributed Computing Systems (ICDCS), 2017 IEEE 37th International Conference on. IEEE, 2017.

[15] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." (2008): 28.

[16] Islam, SM Riazul, et al. "The internet of things for health care: acomprehensive survey." IEEE Access 3 (2015): 678-708.

[17] Ekblaw, Ariel, et al. "A Case Study for Blockchain in Healthcare:"MedRec" prototype for electronic health records and medical research data." Proceedings of IEEE Open & Big Data Conference. 2016

[18] Zhang, Jie, Nian Xue, and Xin Huang. "A Secure System For Pervasive Social Network-Based Healthcare." IEEE Access 4 (2016):9239-9250. R. Nicole, "Title of paper with only first word capitalized," J. Name Stand. Abbrev., in press.

[19] Shae, Zonyin, and Jeffrey JP Tsai. "On the Design of a Blockchain Platform for Clinical Trial and Precision Medicine." Distributed Computing Systems (ICDCS), 2017 IEEE 37th International Conference on. IEEE, 2017.

[20] Zhang, Yin, et al. "Health-CPS: Healthcare cyber-physical system assisted by cloud and big data." IEEE Systems Journal 11.1 (2017):88-95.

[21]Tien Tuan Anh Dinh,"Untangling Blockchain: A Data Processing View of Blockchain Systems" IEEE Transactions on Knowledge and Data Engineering (Volume: 30 , Issue: 7 , July 1 2018)