Blockchain for Healthcare: Privacy Preserving Medical Record

Sarika Kadam
D.Y.P.I.T, Pimpri

Akshata Meshram
Student
D.Y.P.I.T, Pimpri

Sheetal Suryawanshi
Student
D.Y.P.I.T, Pimpri

ABSTRACT
Blockchain technology is considered as a promising in most of the fields like Healthcare, Banking sector, Education industry, digital currency, insurance industry, etc. In today's world it is treated as a most secure and reliable technology to use for the security purpose and eliminate the need for trusted third party. The main focus of this approach is the use of blockchain in managing and securing patient data from malicious activity. The physiological data of a person are sensitive .If the patient have any embarrassing sickness, with the use of private blockchain , aim is to make the patient data secure by applying Secure Hash Algorithm for the generation of hash values and Paillier algorithm for Re-encrypt same information of patient data that is divided in number of different servers. This will increases the difficulty of hacker to hack or access the data. This approach maintains the security parameters i.e. Availability, Integrity and Confidentiality.

Keywords
Healthcare, Privacy, Blockchain, Paillier.

1. INTRODUCTION
Now a days, blockchain has been used in many areas. The application of blockchain in healthcare is rising [10]. Blockchain is used to share health data among pervasive social network nodes, the security of health data is ensured according to[11]. Blockchain is used in electronic health records systems. Blockchain also can be used in remote patient monitoring [12]. A blockchain is a growing list of records, called blocks, which is which are linked using cryptograph where each block contains a cryptographic hash of its previous block, a timestamp, and transaction data (generally represented by hash tree). A blockchain is immune to modification of data.

1.1 Types of Blockchain:
1.1.1 Permission less Blockchain
A public blockchain is a form of peer-to-peer decentralized network that allow multiple nodes to participate in the network transaction without depending on the trusted third party. The transactions are stored on a public ledger and each transaction exchanged between various nodes is verified and added to the blockchain by a set of special nodes called miners. Miners node are required to solve a very difficult mathematical problem known as proof of work, the block is appended to the chain once consensus is achieved through that. In public blockchain, a rewarding mechanism is necessary to incentivize users to join the network and mine blocks of transactions in exchange for the expended rewards such as electricity and CPU time. Once a block is upended then it cannot be delete, modify and any kind of changes is not possible.

1.1.2 Permissioned Blockchain
Sorting and transferring a very large amount of data on blockchain give rise to problem like scalability concern for large-scale and widely used blockchain such as healthcare system. As a result modified version of original technology is introducing known as permission blockchain. It is been said that permissioned blockchain provide better confidentiality, privacy and scalability in addition to basic functionalities supplied by the original blockchain model[3]. There are two sub types of blockchain in permissioned blockchain i.e consortium blockchain and private blockchain. In consortium blockchain the process is controlled by per selected trusted nodes. If there are five nodes for example on the chain a minimum of three entities must sign the transaction to validate the block to be appended to the chain. In private block chain the blockchain write permissions are kept centralized to one organization whereas read permissions may be public a restricted to an arbitrary extent [4]. Private blockchain are also decentralized that can choose participants with there permission rights like who can view blockchain activity, introduce control over which transaction are permitted, enable securely without proof of work and additional associated cost [13].

1.2 Blockchain challenges and opportunities:
Blockchain technologies used to improve the reliability of security infrastructure Blockchain help to improve the security of distributed networks.[15]

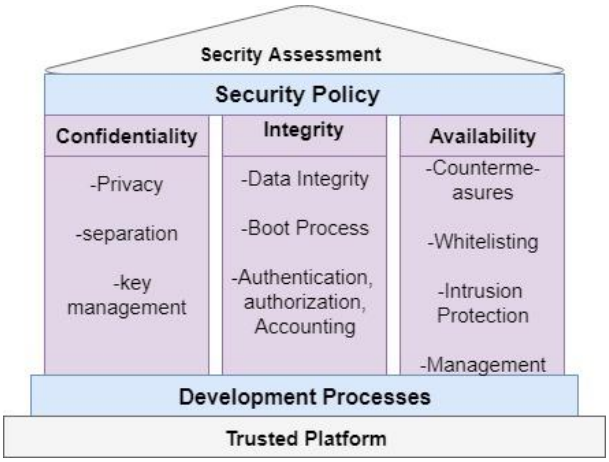

Fig.1: Security Assessment Parameter

Three parameters of security assessment are[16]:

Confidentiality: here confidentiality is refer to protect the data.

Integrity: the overall completeness, accuracy and consistency of data.

Availability: In the context of a computer system, refers to the ability of user to access information in a specified location and in the correct format.

2. ARCHITECTURE

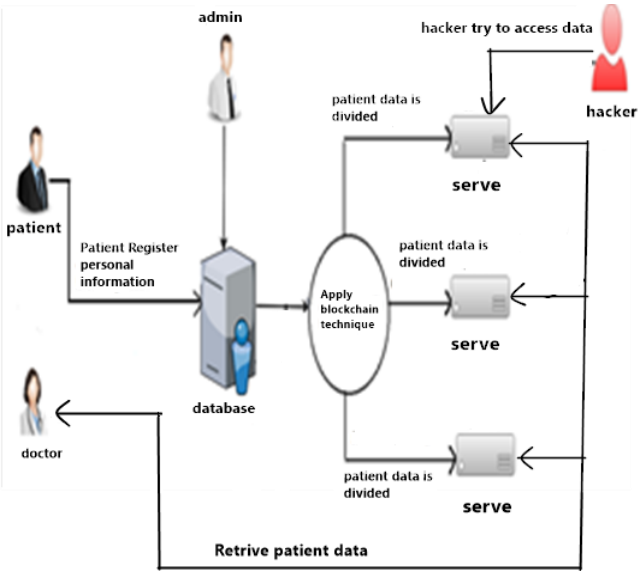

Fig.2: System Architecture

Like most of healthcare applications with blockchain element network, in this design there are three elements the first is patient, the patient first have to do the registration of his personal details. Then his detail will be stored in database server and get divided into three servers. He can login his account whenever he want and can do the check up by filling his symptoms value, as an output he/she will get that his a normal patient, pre-diabetic patient or diabetic patient.

The second element is doctor, he have to do the same registration process like patient and by his login id and password he can get the information of patient check-up history and current stage of patient disease. The doctor will get the patient data directly from the servers where the patient data saved. The doctor can only view the data of the patient but doctor don't access right to do any modification in patient data. based on that history and checkup result doctor will give the prescription to the patient via e-mail.

The third element is administrator, who have access right of all element and he can do all the read and write to the data. The administrators also have to register in the system data to get the access right for do any read and write operation. This will make sure that the administrator is also a trusted entity of that organization. An organization has given right to the administrator to administrate the whole system.

3. PROPOSED SYSTEM

In this approach the main focus is on private blockchain where data is decentralized but the access rights is given by a centralized authorities which give rise to the problems like data privacy, data modification, etc. because it do not use proof of work which are the very hard mathematical problems to solve to get the permission rights to modify in the data. To solve this problem the in private blockchain the rights to access given by centralized authority but read and write rights is also restricted for the users from where the can read the data and where they can write. As the data is divided into different servers the user which have right to access the data can directly get the data from this decentralized servers but he cannot modify that data. The data can be only monitor by the administrator. If in case some third party like hacker try to modify in and particular server the rest of the servers gets disable and the data which the hacker will be in double encrypted form which is very difficult to crack the data as the data is in double encrypted hash value. To generate the hash value AES algorithm is used and pailliers is applied on that AES hash value for re-encryption. The user will get the E-mail that someone have try to change the data with the MAC address and IP address on that device. The main focus is to secure the data of patient from any malfunctioning.

Following Attacks can be possible on this proposed system:

- Denial of Service (DoS)
- Sybil attack
- Eclipse and Routing Attacks.

4. ALGORITHM

The following algorithm is used for achieving the three parameters of security i.e. Integrity, Confidentiality, Availability. The Secure Hash Algorithm is used for achieving Integrity and AES is used for maintaining confidentiality and the paillier is used for key generation and double encryption.

4.1 Secure Hash algorithm

Properties of HASH function H

1) H can be applied to a block of data at any size.

2) H produce fix length output.

3) H(x) is easy to compute for any given X.

4) For any given block x it is computationally infeasible to find x such that H(x)=h

5) For any given block x it is computationally infeasible to find with H(y)= H(x)

6) To computationally infeasible to find any pair (x,y) such that H(x)= H(y)

4.2 AES Encryption Algorithm:

following AES steps of encryption for a 128-bit block:

1) Derive the set of round keys from the cipher key.

2) Initialize the state array with the block data (plaintext).

3)Add the initial round key to the starting state array.

4)Perform nine rounds of state manipulation.

5)Perform the tenth and final round of state manipulation.

6)Copy the final state array out as the encrypted data (ciphertext).

4.3 Paillier Cryptosystem

Key Generation:
Like RSA, pick two primes p, q and let N = p · q — but here we are going to work mod N2.

Note that $\phi(N2) = N \cdot \phi(N) = N \cdot \phi(p) \cdot \phi(q)$ and that all elements have order dividing $\phi(N2)$.

Create PK = (N, g) where g has order a multiple of N and SK = ($\lambda(n)$) where $\lambda(n)$ =lcm(p − 1, q − 1) (where "lcm" denotes lowest common multiple).

5. RESULT AND DISCUSSION

In this proposed system the main focus is on private blockchain where data is decentralized but the access rights is given by a centralized authorities which give rise to the problems like data privacy, data modification, etc. because it do not use proof of work which are the very hard mathematical problems to solve to get the permission rights to modify in the data. To solve this problem in private blockchain the rights to access given by centralized authority but read, write and update rights is also restricted for the users. As the data attribute which are the diabetic symptoms is divided into three different servers. The user which has right to access the data can directly get the data from this decentralized servers but he cannot modify that data. The data can be only monitor by the administrator. If in case some third party like hacker try to modify in a particular server the rest of the servers gets disable and the data which the hacker try to hack will be in double encrypted form which is very difficult to crack the data is in double encrypted hash value. To generate the hash value AES algorithm is used and pailliers is applied on that AES hash value for re-encryption and key generation. The user will get the E-mail when someone tries to change the data with the MAC address and IP address on that device. The main focus is to secure the data of patient from any malfunctioning.

Table.1: Comparison of various features of proposed

Feature	[14]	[15]	[16]	Our system
System Access Control	Y	Y	Y	Y
Integrity	N	Y	Y	Y
Patient/Doctor Authentication	N	N	Y	Y
Confidentiality	N	Y	Y	Y

Table.2: Comparison of access rights

Actors	Read	Write	Update
Patient	Yes	Yes	No
Doctor	Yes	No	No
Admin	Yes	Yes	Yes
Hacker	No	No	No

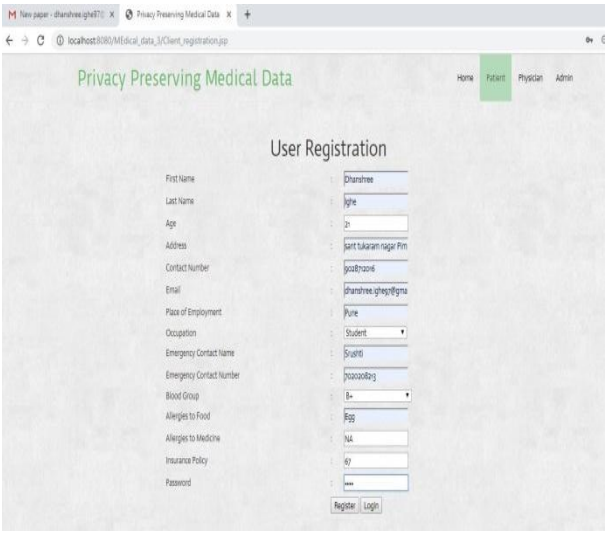

Fig.3 Patient Registration

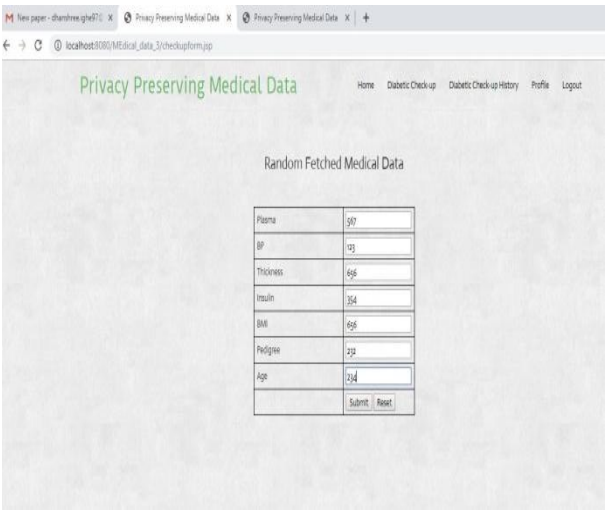

Fig.4 Disease Symptoms of Patient

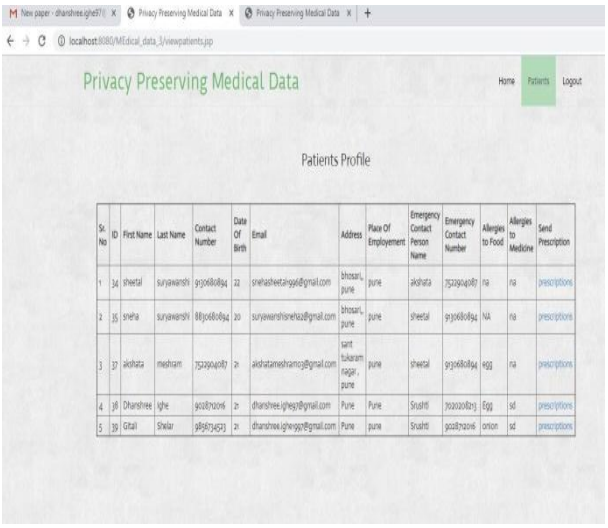

Fig.5 Patient data Profile at Doctor side

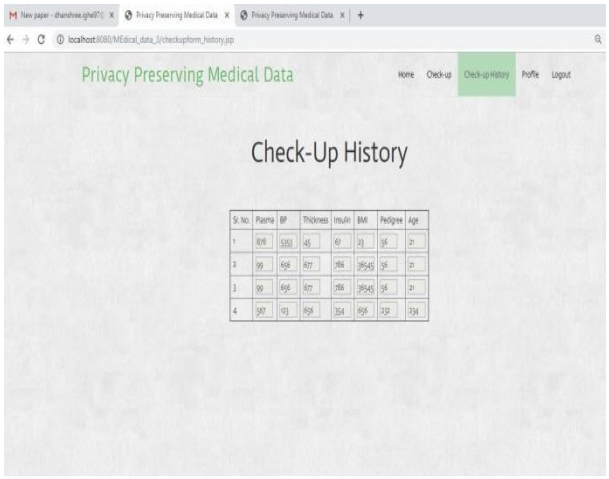

Fig.6 Check-up History of Patient at Doctor Side

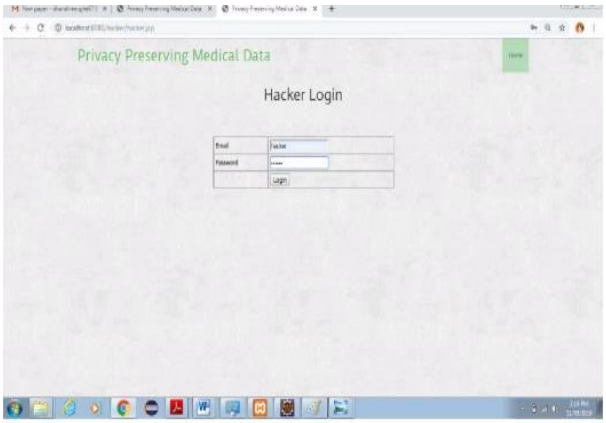

Fig7.Hacker login

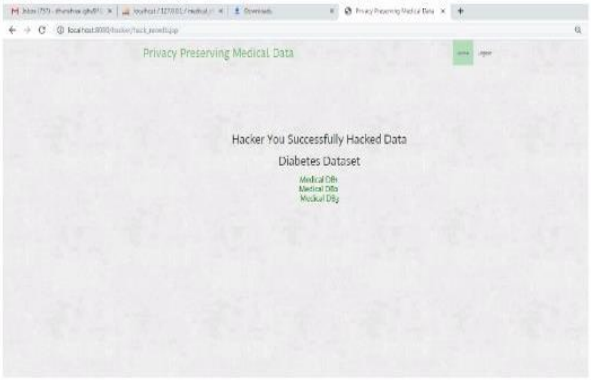

Fig.8 Hacker view diabetic Data

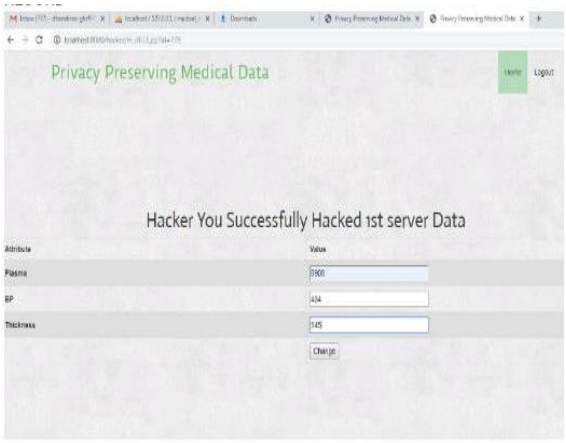

Fig.9 Hacker Try to Hack Database

Fig.10 Hacking Message

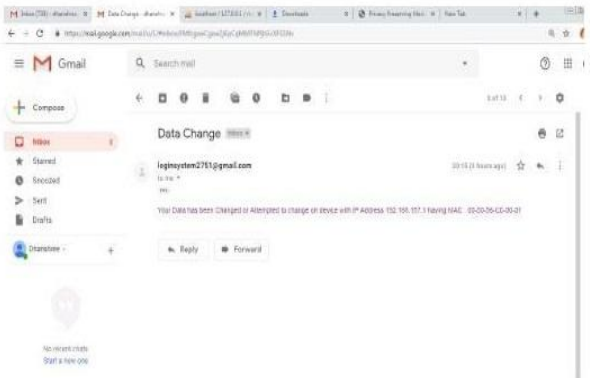

Fig.11 Hack Attempt Alert Message on mail

6. CONCLUSION AND FUTURE WORK

This Approach have focus on the security concerns of the private blockchain by making it more secure for data privacy and by giving access control to the authenticated users only who have permission for rights, i.e. read, write and update as per their role. This approach maintains CAI assessment factors, i.e. the availability, integrity and confidentiality. The use of blockchain can come to an end because of quantum computers. In future the scope of this approach can be enhance by working on the prevention of the attacks like DOS Sybil, etc.

7. REFERENCES

[1] Subhadeep Banik1, Andrey Bogdanov2.A Compact Implementation of the AESEncryption/Decryption Core In Proc.2016,927

[2] Shuai Wang , Jing Wang, Xiao Wang , Member, IEEE, TianyuQiu, Yong Yuan , Senior Member, IEEE,LiweiOuyang, YuanyuanGuo, and Blockchain Powered Parallel Healthcare Systems Based on the ACP Approach2329-924Xc 2018 IEEE..

[3] ZainabAlhadhrami, Salma Alghfeli, Mariam Alghfeli, Introducing Blockchainsfor Healthcare2017 International Conference on Electrical and Computing Technologies and Applications (ICECTA).

[4] K. Malasri, L. Wang. Design and Implementation of Secure Wireless Mote Based Medical Sensor Network. Sensors 9: 6273-6297, 2009A. Azeta, D. O. A. Iboroma, V. I. Azeta, E. O. Igbekele, D. O. Fatinikun, and E. Ekpunobi, "Implementing a medical record system with biometrics authentication in e-health," in 2017 IEEE AFRICON, Sept 2017, pp. 979–983.

[5] P. Belsis and G. Pantziou. A k-anonymity privacy-preserving approach in wireless medical monitoring environments. Journal Personal and Ubiquitous Computing, 18(1): 61-74, 2014.

[6] T. ElGamal. A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Loga-rithms. IEEE Transactions on Information Theory, 31 (4): 469-472, 1985.

[7] P. Paillier. Public-key Cryptosystems Based on Composite Degree Residuosity Classes. In Proc. EUROCRYPT99, pages 223-238, 1999.

[8] "Hyperledger project," 2015. [Online]. Available: https://www. hyperledger.org/

[9] Zhang J, Xue N, Huang X. A Secure System For Pervasive Social Network Based Healthcare[J]. IEEE Access, 2016, 4(99):9239-9250.

[10] Guo R, Shi H, Zhao Q, et al. Secure Attribute-Based Signature Scheme with Multiple Authorities for Blockchain in Electronic Health Records Systems[J]. IEEE Access, 2018, PP(99):1-1.

[11] Alhadhrami Z, Alghfeli S, Alghfeli M, et al. Introducing blockchains for healthcare[C]// International Conference on Electrical and Computing Technologies and Applications. 2017:1-4.

[12] Gideon Greenspan, MultiChain Private Blockchain — White Paper. June 2015 [Online]. Available:http://www.multichain.com/download/MultiChain-White-Paper.pdf [Accessed 4-8-2017].

[13] P. Zhang, M. A. Walker, J. White, D. C. Schmidt, and G. Lenz, "Metrics for assessing blockchain-based healthcare decentralized apps," in 2017 IEEE 19th International Conference on e-Health Networking, Applications and Services (Healthcom),Oct 2017, pp. 1–4. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "Medrec: Using blockchain for medical data access and permission management," in 2016 2nd International Conference on Open and Big Data (OBD), Aug 2016, pp. 25–30.

[14] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, "Medshare: Trust-less medical data sharing among cloud service providers via blockchain," IEEE Access, vol. 5 pp. 14 757–14 767, 2017.

[15] Deepa Mahajan, Sarika Kadam," A Survey Paper on Blockchain Technology" ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177 Volume 7 Issue V, May 2019.

[16] Prof.Sarika Kadam," Symmetric Data encryption using trusted third party Objects in IOT" Asian Journal of Convergence in Technology ISSN No.:2350-1146, I.F-5.11 Volume IV Issue III, 2019