The Ciência & Engenharia -Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 2174-2181

A Systematic Review On Medical Health Data Management Using Blockchain Technology

Prof. A. P. Gaigol[1], Dr. V. S. Wadne[2], Prof. S. R. Bhandari[3], Dr. R. S. Deshpande[4], Dr. T. R. Sangole[5]
[1]Department of Computer Engineering, JSPM's ICOER, Wagholi, Pune, India
ashishgaigol@gmail.com[1]
[2]Department of Computer Engineering, JSPM's ICOER, Wagholi, Pune, India
vinods1111@gmail.com[2]
[3]Department of Computer Engineering, JSPM's ICOER, Wagholi, Pune, India
bhandarishub123@gmail.com3
[4]Dean, Faculty of Science and Technology, JSPM University, Wagholi, Pune, India
raj.deshpande@yahoo.co.in[4]
[5]Department of Computer Engineering, JSPM's ICOER, Wagholi, Pune, India
tusharrsangole@gmail.com[5]

Abstract — "Data" is the trending word since last few decades. When it comes to any type of data its security is important. Relating the same, maintaining the medical health data is also very significant. When the medical health data is stored or retrieved from the internet is called as Electronic Health Record (EHR). Many times an EHR can be accessed in an unethical way when it is maintaining through conventional approach. Misuse of the same data can lead to many unavoidable problems. Use of Blockchain Technology plays pivotal role in dealing with such problems. An already proven and completely functional Blockchain Technology based Crypto-currencies are the best examples of how efficient and capable Blockchain Technology is. Peer to peer network is used in Blockchain Technology to store the data. Key features of Blockchain-based network are Public Distributed Ledger or non-centralization, Hashing Concept, PoW which makes Blockchain Technology one of most robust technology and highly recommended to use to store and retrieve the data safely. Goal of stated work is to study various benefits of Blockchain Technlogy, how an Electronic Health Record (EHR) can be access in a predefined way where the medical health data/an Electronic Health Record (EHR) will remain immutable throughout its existence.

Keywords—Electronic Health Record (EHR), Blockchain Technology, Public Distributed Ledger, Hash Encryption, Consensus Algorithm, SHA-256 Algorithm.

I. INTRODUCTION

Data in all contexts plays crucial role in any type of industry. Almost all companies growth and business is relatively depends on data. With the same consideration, medical health data is significant element in holistic development of hospital system. To deal with such medical health data Blockchain Technology can be exclusively very efficient and capable solution. Medical systems can use Blockchain Technology to store and transmit medical health data. An Electronic Health Record (EHR) can available to hospitals, diagnostic labs, pharmaceutical companies called as Health Information Exchange (HIE) for the intended use. While making its availability, medical health data integrity needs to be maintained thereby an Electronic Health Record (EHR) can be treated in a disciplined manner to avoid it from unauthorized access with the use of Blockchain Technology. As medical health data of a patient saved over a period of time or sometimes even longer and this medical health data needs to be distributed among doctors, hospitals, health insurance providers which leads to use Blockchain Technology as it has capacity to change the conventional approach of handling the medical health data which is prone to unauthorized access and put the medical health data at centre of the health system which will increase the privacy, security, interoperability of the medical health data. To diagnose and provide treatment accordingly to a patient, an Electronic Health Record (EHR) contains extremely private data which needs to be secured in all possible ways. Privacy, Integrity, and all time Availability being minimum criteria for

an (EHR) can be maintained by using Blockchain Technology. Access to this EHR should be limited to concerned and permissioned authorities only.

II. LITERATURE SURVEY

M.Patil,Vinod S.Wadne,"Efficient Cross Media Retrieval Using Mixed Generative based Hashing Method",Vol.7,issue 1.

This paper focuses on how to use hashing. How data is provided as an input and output gets generated by using hashing. Further scope in this paper is advanced functioning can be achieved while dealing with medial health data.

Abdullha Al Mamun, Sami Azam Clementine Gritti, 2022. Blockchain-Based Electronic Health Records Management: A Comprehensive Review and Future Research Direction.

Given comprehensive review concentrates on study of research that has been already carried out regarding dealing with EHR and detailed analysis has been done regarding use of Blockchain Technology to develop a system which will handle EHR very cautiously. Study on regulations, standardization and cross-border accessibility of EHR can be considered as scope to work on.

Andre Henrique Mayer, Cristiano Andre da Costa, Rodrigo da Rosa Righi 2019 Electronic Health Records in a Blochchain: A systematic review

This systematic review gives the information about reveiling the most recent work on using Blockchain in hospital system and exploring the challenges in implementation of the same. Future work like EHR interoperability, making connection on trust basis between all concerns and giving permission to health data by patients.

Ayoub Ghani, Ahmed Zinedine, Mohammed EL Mohajir 2020 A Blockchain Based secure PHR data storage and sharing framework.

This paper focuses on designing framework that allows take benefits of Inter Planetary File System (IPFS).Given framework has a provision of decentralized storage of PHR file. Further scope in this paper is to improve medical health data integrity with the help of steganography.

III. EXISTING SYSTEM

The word "data" has been popular throughout the past few decades. Security is crucial when it comes to any form of data.

Present existing systems have many problems while dealing the medical health data with the help of traditional methodology. As security being one of very important parameter not possible to achieve beyond some extent. At every step, a chance of breaking security of medical health data is there. Full proven system is not available to manage the medical health data. When it comes to medical health data access, non-concern authorities can also access the data. Such crucial data once accessed can be altered very easily. Additionally, no proper way of checking the integrity of the medical health data. Furthermore, medical health data may not be available because of network oriented problems. Facility of granting/denying the permission by patient to medical health data is not available. Conclusion is that for medical health data to be called as Electronic Health Record (EHR), minimum requirements are not followed.

The Ciência & Engenharia -Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 2174-2181

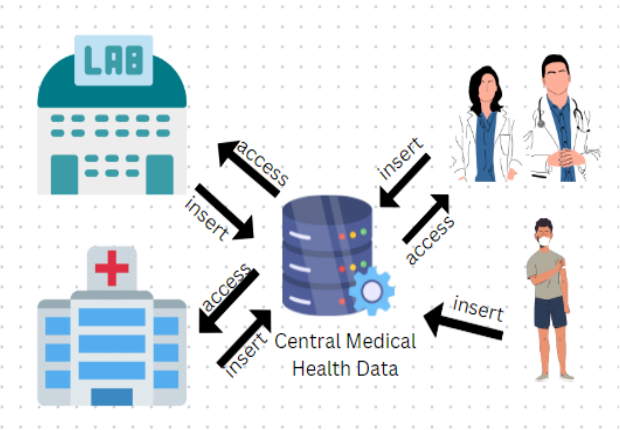

Fig.1 Existing System (General View)

Above figure depicts how existing system works and two major limitations of existing system. First, health data is stored at central place if gets unauthorized access whole system will fail to function in a predefined manner which leads to given medical health data not following minimum criteria to be called as Electronic Health Record (EHR). Additionally, doctors, medical labs, hospitals can insert and access patient's health data means bi-directional functioning is possible where patient is able to only insert the health data. Furthermore, facility of granting/denying the permission by patient to medical health data is not available.

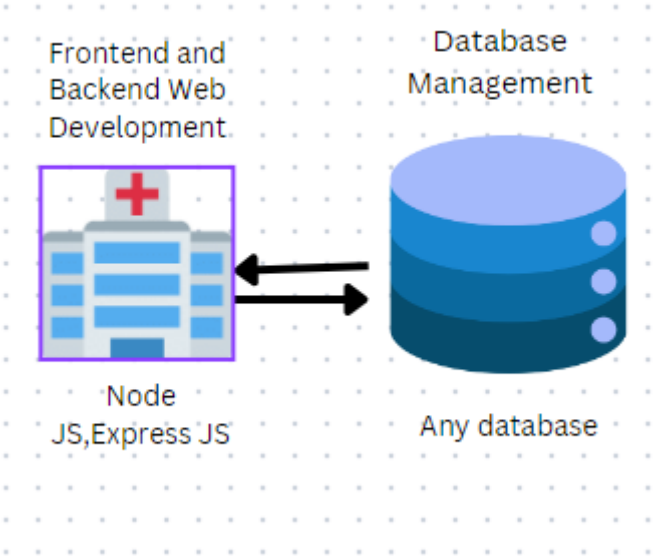

Fig.2 Existing System (Implementation Level View)

Above figure depicts existing system focusing on implementation layout giving front end and back end development through Node JS, Express JS and storing and retrieving the medical health data with the help of database management by using any database like MongoDB, Oracle, MySQL etc. As mentioned above, if designed database which is playing as central component to store and retrieve the data gets fail, complete system will be non-operational.

IV. PROPOSED SYSTEM

1. Blockchain-based network:

Blockchain-based network means use of a peer-to-peer network and cryptographic encryption. A series of blocks connected by cryptographic hashes and each block is time-stamped. Peers, also known as miners, are in responsibility for verifying the transactions in each block. Multiple transactions can be perform in each block, which is why fresh blocks are continuously added to the end of the chain. Every new block uses a cryptographic hash function, such as SHA-256.

Each block is built with the assurance of anonymity, immutability, and transparency. The entire blockchain operation is hosted by a P2P network. To generate hash of the new block, timestamp, total number of

The Ciência & Engenharia -Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 2174-2181

transactions, hash value of the previous block, and nonce value which increases difficulty in mining the block. The hash function do possess one property called as avalanche effect which is very helpful in making proper blockchain functioning.

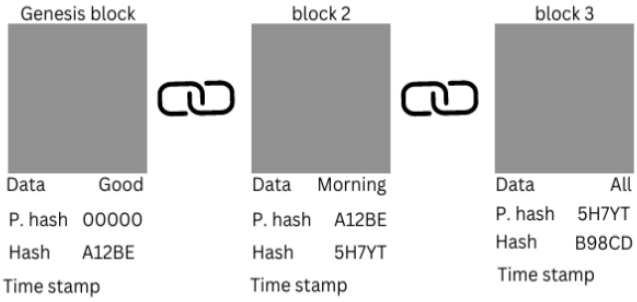

Fig.3 Hash Function In Blockchain Technology Structure

Explanation:

In blockchain technology network, first block called as genesis block. Geneses block will not have any previous has value.

Geneses block and other blocks in network have some important information like data, previous hash value, current hash value and timestamp. Managing the data becomes very efficient in blockchain network as data is saved in decentralized manner which makes high availability of the data. Connecting blocks on after another known as blockchain technology based network.

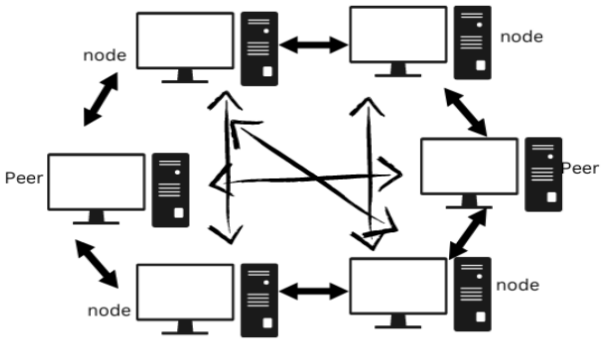

Fig.4 Peer-to-peer model

Explanation:

The decentralisation idea, on which peer-to-peer (P2P) technology is built, enables network users to conduct transactions without the use of a middleman, intermediaries, or central server. Peer-to-peer blockchain networks do not have a central authority. Instead, every node (peer) is interconnected. There is no hierarchy and the network nodes are connected by a mesh network topology. Peer-to-peer networks are open, decentralised, and robust by nature since nodes provide and consume services simultaneously.

2. Implementation roadmap:

As mentioned above once peer-to-peer network with cryptographic hash function is taken into consideration further implementation can be achieved. An application or website can be develop by using Solidity, React, Metamask, Alchemy, Hadrhat and Ethereum Goerli Testnet.

3. Algorithms:

Use of two important algorithms,

1. Consensus Algorithm – Using concepts like peer-to-peer network and encryption using cryptography will form a network called as Blockchain Technology based network. Security, Privacy, Immutability and Transparency being four pillars of Blockchain Technology. Each Blockchain Technology based network must possess above four features.

The Ciência & Engenharia -Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 2174-2181

Such network uses consensus algorithm which leads to
Blockchain Technology based network can consist of no central authority to authenticate transactions still given transactions are considered as safe and verified. It will bring all peers to a common(mutual) understanding. This way in order to make trust between unknown peers, consensus algorithm plays very significant role. Consensus algorithm also confirms that only one version is present in the Blockchain Technology based network of newly added block. For successful consensus process execution, each node should participate and perform agreement, collaboration and cooperation. Several consensus algorithms are.

a. PoW (Proof of Work)

To opt a miner for next block production, corresponding algorithm can be use. This algorithm's main objective is to rapidly and easily offer a solution to a difficult mathematical puzzle. It takes a lot of computational power and thats why the node(miner) who solves the given puzzle will get next block to mine.

b. PoS (Proof of Stake)

It is an alternate to PoW (Proof of Work). Etherium being second well known cryptocurrency has shifted from Proof of work to Proof of stake consensus. In this algorithm, validators reserve some stake rather than investing money in high priced- hardware to find out solution of a difficult task.
All validators will then start validating the blocks after this.
Each validator will validate a block by betting on it if they discover one that they think can be added to the current chain or network. Each validator receives incentives depending on their stakes, and when more blocks are added to the Blockchain network, their stakes grow accordingly. Finally, a validator is chosen to build a new block depending on how much money it has invested in the current network. Since there are incentives involved, PoS encourages validators to concur.

c. PoB (Proof of Burn)

Definitely, this consensus algorithm is also very helpful. Some percentage of the available coins will be burned in order to make sure that the PoW cryptocurrency will be kept protected. This execution is carried out as the miners transfer a bit amount of money to an "Eater Address." To the surprise, these transferred coins(money) cannot be used/spend in any way by the Eater Addresses. Since the burned coins are recorded in a ledger, they are actually unusable as currency. Additionally, the miner (user) who burned the coins(money) will receive a reward too.

d. PoC (Proof of Capacity)

This is one of the important consensus algorithm which helps miner(node) to mine/add new block into existing blockchain network. An important activity is executed which is a node or miner have to prove that they have allocated certain amount of disk to the network. In a proof of capacity consensus algorithm, nodes/miner from existing blockchain based network performs pre-calculation and keeps on their hard drives a set of answers to a challenging mathematical problem. Afterwards nodes can quickly validate their solutions and compete to generate the new block when it is time to add a new block.

e. PoI (Proof of Importance)

Proof of Importance consensus algorithm has gain its significance as it actually consider valid activities by node in Blockchain Technology based network. In this algorithm type, importance score is calculated. By considering activities like total number of transactions it has processed and total number of nodes it has referred, importance score is calculated.

2. SHA-256 Algorithm -

Hash functions can be utilized to create output(of fixed size) by providing data which is input data, such as a text, a number, mixed data (alphabets and numeric data) character, and this hashing function concept is derived from cryptography.

The Ciência & Engenharia -Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 2174-2181

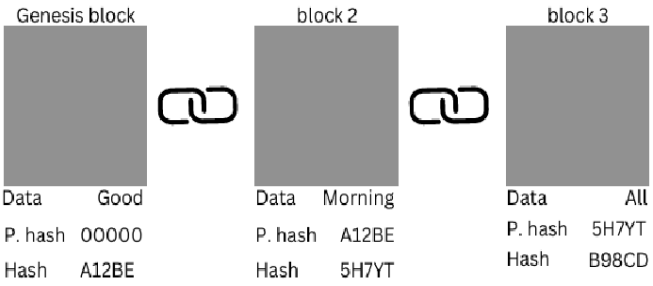

Fig.5 Hash Function in Blockchain Technology

The hash function is used in blockchain technology to create the hash for a certain block, which acts as an unique identifier for identifying the block. The chain is formed by each block storing the hash value of the preceding block. The first block called as genesis block which will have no previous hash to point. The process of generating hash is important for miners.

Hash function in blockchain technology –

1. Pre-image resistance - This means it is impossible to go reverse to get the hash value generated by the hash function to get true input data. Consider given equation, hash fun = m

$$m(a) = b$$

It should never be possible to determine a from b if m is function which is hash fun, a is an input data, and b is the output(hash). This is the one-way or pre-image resistance attribute. Blockchain relies on this to stop unauthorized users for any illegal activity.

2. Post-image resistance - According to this feature, it should be incredibly difficult to develop a separate data which can consider as an input that can generate an output hash data that initially belonged to a different input .Consider given equation to better comprehend this,

$$m(a) = b$$

Given that the hash function m produce hash b for an input a. Since z is no longer equal to a, it should be practically difficult to generate another input z such that h(z) = b.

From the point of view of the blockchain, this is extremely important since, in the absence of this, it would have been possible for unauthorized users to edit contents of the block.

3. Deterministic - This characteristic guarantees that the function which is hash will return the expected (everytime same) output data for every input.

$$m(a) = b$$

It indicates that irrespective how often m(a) is used, it must generate b for the data which is input data of a and no different data which is output data. Due to the deterministic nature of this blockchain network, other miners can examine the value which is generated by hashing of a single block before inserting it to the network as a whole.

4. Fast Calculation - Regardless of the size of the input message, the hashing functions are easy as well as quick to calculate hashing operation output. This is crucial for technology like blockchain as miners makes lot of calculations every second, and a quick function which is hashing function avoids delays in blockchain based-network.

5. Avalanche Effect - The word "avalanche effect" refers to the fact that even a slight change in the input causes avalanche of modifications to hash calculations. Thereby as an output, the new hash is completely

different from the old one rather than varying slightly. This makes difficult for hackers to solve the mathematical puzzle of obtaining the right hash.

4. Advantages:

Once successful implementation is accomplished, confidentiality, availability, integrity, non-repudiation, immutability, privacy, scalability, interoperability these required advantages are possible to achieve.

5. Applications:

Key applications of Blockchain Technology network based Electronic Health Record (EHR) are confidentiality, availability, integrity, privacy which may makes EHR widely acceptable.

V. CONCLUSION

After performing detailed literature review, it has been understood that Blockchain technology is the combination of a peer-to-peer network and cryptographic encryption. Peer-to-peer networks allows to achieve decentralization which can make efficient transaction (transmit or retrieve medical health data) processing. Where cryptographic encryption may play pivotal role in generating hash of the block. Additionally, as hash functions possess key properties like re-image resistance,

second pre-image resistance, deterministic, fast calculation and avalanche effect which may makes blockchain technology based network very robust. It will not allow to have an unauthorized access in the network.

Furthermore, consensus algorithms like Pow, PoS, PoB, PoC, PoI and tools like Solidity, React, Metamask, Alchemy, Hadrhat and Ethereum Goerli Testnet may contribute in development of actual product. Finally it has been concluded that Blockchain Technology based network can transform hospital health data management from centralized and small scale to decentralized and large scale system which will be providing security in all expected contexts.

Future Scope – With the consideration of above development methodology if successful product may gets developed still scope of improvement would be making advancement in various functions execution like transmitting and retrieving an EHR in Blockchain Technology based network.

REFERENCES

[1] Sharma, Y. and Balamurugan, B. “Preserving the privacy of electronic health records using blockchain. Procedia Computer Science”, 173, pp.171-180,2020.

[2] Abdullha Al Mamun, Sami Azam Clementine Gritti, “Blockchain-Based Electronic Health Records Management: A Comprehensive Review and Future Research Direction”,2022.

[3] Andre Henrique Mayer, Cristiano Andre da Costa, Rodrigo da Rosa Righi,“Electronic Health Records in a Blochchain: A systematic review”,2019.

[4] Hao Sen Andrew Fang, Teng Hwee Tan, Yan Fang Cheryll Tan, Chun Jin Marcus Tan,” Blockchain Personal Health Records: Systematic Review”,2021.

[5] J.Vora et al., “BHEEM:A Blockchain Based Framework for Securing Electronic Health Records”,IEEE Globecom,2018.

[6] Ayoub Ghani, Ahmed Zinedine, Mohammed EL Mohajir, “A Blockchain Based secure PHR data storage and sharing framework”,2020.

[7] Shilpa M Walke, Vishal G Puranik, Jaideep G Rana, Rajkumar S Deshpande, “A Novel Technique of Steganography and Watermarking” 2009.

[8] G.Karame and S.Capkun,”Blockchain Security and Privacy”,IEEE Security and Privacy, vol.16, 2018.

[9] W.Wang et al.,”A Survey on Consensus Mechanism and Mining Strategy Management in Blockchain Networks”, IEEE Acess,vol.7,2019.

[10] M.Atzori,”Blockchain Technology and Decentralized Governance: Is the state still necessary?”,SSRN Electronic Journal,2015

[11] V.V.,K.Sabarivelan, J.Tamzhselvan, B.Ranjith and V.B.,”Utilization of BLockchain in Medical Healthcare Record Using Hypdeledger.”

[12] M.Patil,Vinod S.Wadne,”Efficient Cross Media Retrieval Using Mixed Generative based Hashing Method”,Vol.7,issue 1.

[13] M.Holbl,M.Kompara, A.Kamisalic and L.N.Zlatolas,"A Systematic review of the use of blockchain in healthcare",vol.10,2018.

[14] C.C.Agbo,Q.H.Mahmoud and J.M.Eklund,"Blockchain technology in healthcare:A Systematic review",vol.7,2019.

[15] E.Chukwu and L.Garg," A Systematic review of blockchain in healthcare: Frameworks,prototypes, and implementations",IEEE Access, vol.8, 2020.