Warehousing Of Medical Data Using Blockchain

K.KusumaLatha,B.Ram Sai Prakash, P.V.R.D.PRASADA RAO

Abstract: Block chain is one of the genius innovations among all the technologies. It works like a database which stores the data. It changed the traditional method of storing the information and also the transactions that are made between computers virtually and securely throughout the internet. Block chain enables advanced organization of data to traverse the world without being altered, and was initially made for bitcoin exchanges which were virtual currency that was circulated by open source developers. Basically it works as a decentralized (shared) technology. The database updates are shared over the network thus it opposes from single point failure, and the changed will be updated securely with faster settlement. In this procedure no node in the block chain can't able to know what the transaction is. Our aim is to create a secured block chain database system to store and retrieve the Information. This block chain system centralizes the information sharing among all the medicinal hospitals and secures the data without any tampering and retrieves the medical data efficiently.

Index Terms*: *Blockchain, Medical data, Security, SHA256 Algorithm.

I. INTRODUCTION

"Block chain is virtuous digital ledger of economic transactions that can be programmed to record all financial transactions and also virtually everything of value".
It is progressive innovation that is being utilized for bitcoin exchanges from late years.[7] A considerable lot of us believe that block chain is intended for cryptographic forms of currency, for example, bit-coin. It offers security, from multiple points of view. The word block chain has two unique parts as block chain, where the "block" demonstrates a piece of data that is stored and these blocks are associated with one another like a "chain". Block chain is consensus –driven so no one block can take control of the data. For the validation of blockchain and its transactions no other third parties are used because for the security.
[5] This elevated security is the reason, why the blockchain is utilized for digital currency, and it plays a significant role in protecting data such as personal medical information. Blockchain could be utilized to radically improve the worldwide global supply chain, as well as protect assets such as art and real estate.

Revised Manuscript Received on May 10, 2019.

K. KusumaLatha, Department of Computer Science and Engineering, Koneru Lakshmaiah Educational Foundation, Deemed to be University, Vaddeswaram, Guntur, Andhra Pradesh, India-522502.

B.Ram Sai Prakash, Department of Computer Science and Engineering, Koneru Lakshmaiah Educational Foundation, Deemed to be University, Vaddeswaram, Guntur, Andhra Pradesh, India-522502.

P.V.R.D Prasada Rao, Department of Computer Science and Engineering, Koneru Lakshmaiah Educational Foundation, Deemed to be University, Vaddeswaram, Guntur, Andhra Pradesh, India-522502.

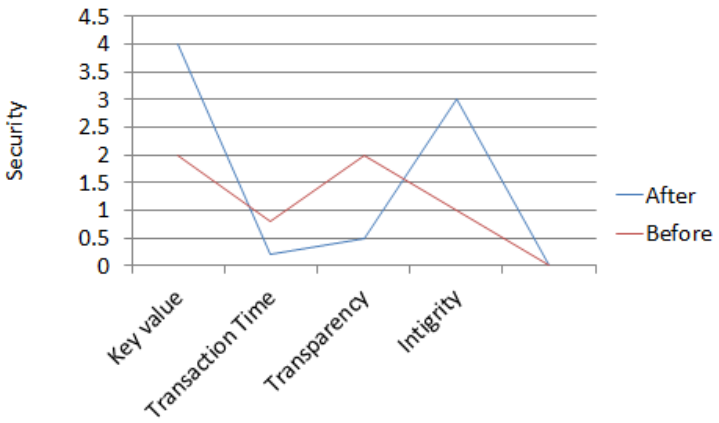

Fig:1 Blockchian network parametes

From the Fig.1.we can able to distinguish the security of data before and after the implementation of the blockchain in medical industry ,there is high secure in key value and the transparency of the transactions can be seen in blockchain.Because of this high security blockchain is used in warehousing of medical data with the special algorithm of SHA-256, here the process of encryption is easy and there is no fear of attacks of the key value,because it cannot be changed.
What's more, as the utilization of blockchain innovation increments, so too does the demand for skilled professionals. In such manner, we are as of now behind. "As indicated by Techcrunch.com, blockchain-related jobs are the second-quickest growing category of jobs", "with 14 employment opportunities for each one blockchain designer". "A blockchain developer specializes in developing and implementing architecture and solutions using blockchain technology". "The average yearly salary of a blockchain developer is $130,000".
The role of the developer is not only one variable in the blockchain space, however. Employers are also looking for software engineers, consultants and project managers. Jobs are available at finance related institutions, but also in retail and healthcare, and soon probably manufacturing as well.

II. BLOCKCHAIN

[4] Block chain is a modern database that uses de-centralized server-architecture, which the data present in the master, will be present in all the child/peer nodes.
It can only perform read and write operations. Once the block is created and the data is saved in the block then there is no other way to manipulate the data
So in block chain , the real preferred standpoint is the hash value that is created for the block can't be decrypted by the user and as well as admin .They can only able to

see the data which is present in the block only when they have the encrypted hash key. Block chain comprises of data, Index, Timestamp, previous hash, hash value.

A user who is authenticated can only able to change the entries that are stored on a centralized server. By evolving the 'master copy', at whatever point a user access a database utilizing their computer, they will get the updated version of the database entry. Control of the database remains with administrators, allowing for access and authorizations to be kept up by the central authority. This is not at all same with a blockchain.

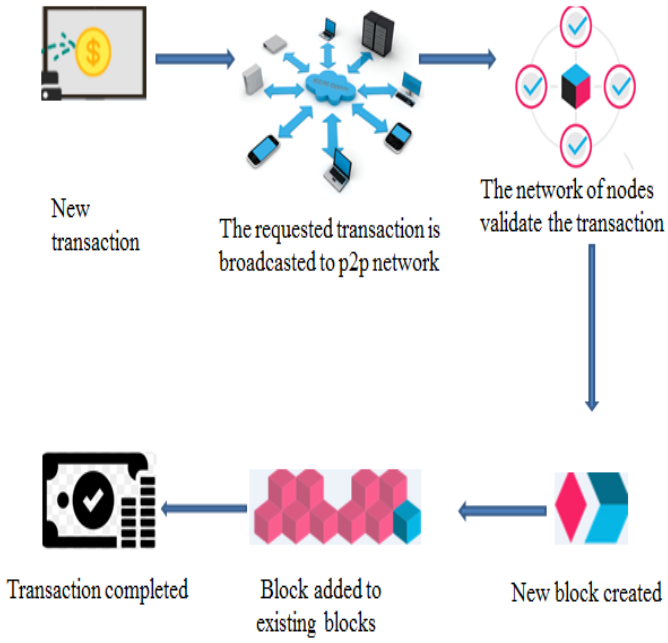

Fig: 2 Blockchain architecture

Fig.2 describes about the construction of the blockchain after the request is generated, how the requested transaction is broadcasted to peer-to-peer network and how the new block is added to the existing blocks with the transmission of hash values of each block with the newly added block.

For a blockchain at each level each participate maintains, calculates and updates new entries into the database. All nodes allied and work in an organization to certify that they are all coming to the like deductions, providing intrinsic security for the network.

Blockchain is used as a platform for the transactions, but the blockchain transactions is treated as slow as database for nowadays because of the technology that we are using for the transactions that done for PayPal and Visa.

Centralized databases on the other hand, which is the first and the most popular database, which is slow in the beginning but as seen in recent years it increases the performance and hence they performed as fast as blockchain but use different technology.

We can also use permissioned blockchain, which is used as a centralized server, where we can grant/control the read and write operations. This means it will only allow the permissions for the admins and for the authorized people who are likely to know the details of the patient. Then only the authorized people can only able to modify the blockchain.

With these features we can able to implement the [2] Electronic health records that which used to store individual patients data. For which the blockchain technology is used in medical industry that which used to store and retrieve the data with high secure and efficient manner by which the unauthorized persons cannot able to access it.

III. METHODOLOGY

Blockchain technology used in the healthcare in various aspects like used to detect the capabilities of prescription medicine, drug monitoring and many more.

[3] As the individual patient's data is increasing more and more we need an analytical tool to sufficient manage of patient's data in the hospitals. Now we are used the blockchain to decentralize the patient's data.Sharing patient data between doctor's offices is sometimes a tricky process as the patient is uneducated or unable to answer the doctor, regarding the disease he is suffering or the medicine he is using — especially if a patient needs to see multiple specialists or is involved with multiple private practices. Using the blockchain, a decentralized system which is centred on the patient instead of the data holder, creates a shared database of patient data.

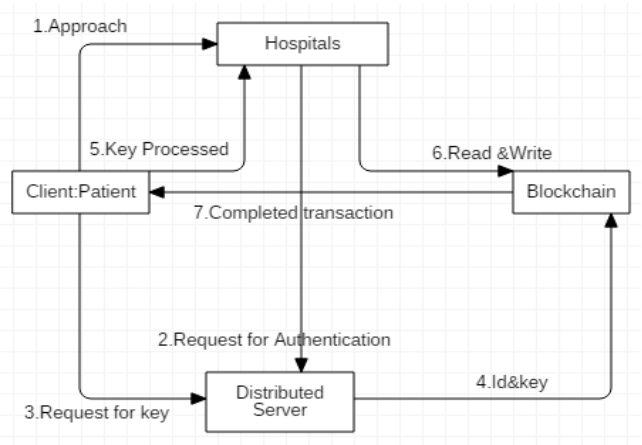

Fig: 3.1 Flowchart of blockchain medical transaction.

Fig.3.1 shows the sequence process of how the doctor can able to retrieve the patient's past data and storage of the present data in the blockchain with the help of patient's unique value. Block chain uses encryption algorithms such as SHA-256(Secure Hash Algorithm [256]), is a secure cryptographic hash function which will take the input data and from that data, this algorithm will undergo encryption to produce a secure hash value which will never be reverted. The security of SHA-256 is, as the algorithm has 16 steps for the encryption of data to produce the hash value/key. The output value of this algorithm will be a hexa- decimal number which is 40-60 digits long. The output produce is 160-bits (20-bytes) hash value which is known as message digest. Once the data is encrypted with this SHA-256 algorithm due to its secure feature which the encrypted hash value will not be able to change and cannot be deleted. The SHA-256

algorithm has the security claim of to 2^{256} which is it is more secure than other hash functions which are MD-5 algorithm has the security claim of to 2^{128} and SHA-1 algorithm has the security claim of to $2^{160.}$ The hash value that generated from this algorithm is 64-bit length; hence due to its size it is more secure. It uses SHA-256 because the main advantage of SHA-256 is once the data is encrypted there is no way to decrypt the encrypted data.We cannot able to broken/decrypted the SHA-256 algorithm because of its process of mathematical calculation. If anyone wants to decrypt the hash value that was produced by this algorithm as mentioned in different sources it will take over a million years. However most of us expect that the SHA-256 can be decrypted by the next hundred years or more.SHA-256 is a asymmetric encryption algorithm which is also known as public cryptographic algorithm. Blockchain mainly uses the [1] merkle chain architecture. This tree has a specialization that which the transactions are done will be stored in the leaf nodes of the tree, and the root, the non-leaf nodes are contained a cryptographic hash value, which is used for security of the block chain transactions. The architecture of the merkle tree is mentioned below.

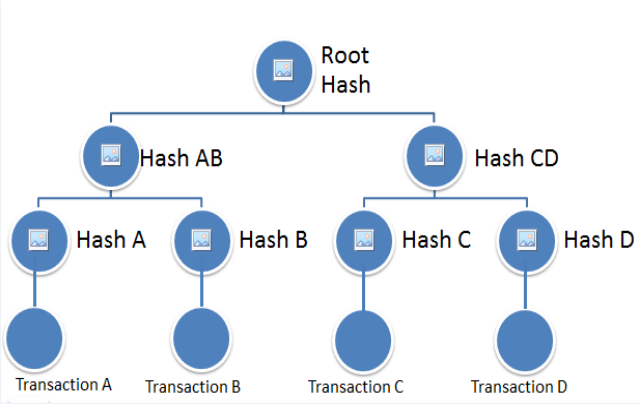

Fig:3.2 Merkle tree for hash values

Fig.3.2 describes how the different hash values are inter-linked to one another in a hierarchal way.

To decentralize the patient's data across all the medical hospitals, a blockchain record is introduced. The blockchain system, which could be easily, shared patient's data across healthcare units.

Here we used to have a unique identification of every patient so that the patient's data cannot be mismatch as well as hacked.

IV. RESULT

Blockchain technology is the efficient solution to secure the patient's information. Blockchain prevents unauthorized individuals from accessing the information.

As we introduced the blockchain technology to retrieve the patient's data, the data stored in the database will be immutable and secure in decentralized and distributed manner.

trans_id	data	time
d055d2174e8481225feb84ee7e47ca24a950f34ced47b30905...	head ache	2018-11-15 13:11:49
025c3b156cdc46ccf9840037eb75a29b6e956210f192dd83871...	heart	2018-11-15 13:12:03
2bd9899c326a1f64e59c780886794 5fb6d192fae95cca94432...	BRAIN	2018-11-15 13:53:54
dd1b7c18f09b87e81fb6feca836b34ab8f67285d0f89e6df89...	fever-dolo	2019-03-01 12:28:51
98afb90a802e5abda1040d0cc912d4ef6455e1b10fe5025f75...	Fever -medicine taken with two dose a day	2019-03-01 12:58:39
2ab88402cdfacd8a204e53ea2dec88db261b8dd770e23849f3...	fever-dolo	2019-03-01 15:58:12

Fig: 4 Medical records with hash values

As we can see from the above fig: 4.There is a different unique hash value for each and every data entry or transaction in the blockchain. With this we can also see the present hash value is dependent on the previous hash value.

With the implementation of the blockchain, we can able to know what the transaction was occur and when it was occur but it cannot able to know by whom the transaction had taken place as each block consists of unique index and timestamp, because of the advantage of the SHA-256 algorithm which is used to hide the data we can able to secure the data without using the third party security.

By this Patient will be able to easily upload and securely store their updated medical information without messing up any previous records.

V. CONCLUSION

In future block chain can revolutionize the healthcare services. It also gives a massive change in the transaction process. While virtually every large bank utilizing the block chain innovation. Block chain is not as much as developed in the healthcare industry till now. According to the survey of IBM healthcare executes it was found that 56% people are except use the block chain by 2020. In the future it can able to store the data on their own by avoiding risking vulnerability.

[11] As the financial organizations are not able to handle the heavy workloads sufficiently and to make the centralized specialist for handing the financial transactions blockchain technology will be used.

[8]In future there are different sectors which use the blockchain. The primary sector that uses the blockchain is digital advertising, because in this sector there may be different news transport through different websites like domain fraud. Another major sector is cyber security because the data that is stored in the blockchain will be less likely to be attacked.

[9]Major advantage of block chain will be that used to remove the requirement of third-party security partners that in any way there may be leakage of data.[10] Block chain is also used in world trade, weather

forecasting and in the Internet of Things [IoT].

Blockchain in future will be used in many of these sectors because the present technology is not as much as efficient as blockchain. And it is less secure when compare to blockchain.

REFERENCES

1. Becker, Georg (2008-07-18). "Merkle Signature Schemes, Merkle Trees and Their Cryptanalysis" (PDF). Ruhr-Universität Bochum. p. 16. Retrieved 2013-11-20.
2. Kemkarl, O. S., and Dahikar, D. P. B., Can electronic medical record systems transform health care? Potential health benefits, savings, and cost using latest advancements in ict for better interactive healthcare learning. International Journal of Computer Science & Communication Networks 2(3/6):453—455, 2012.
3. Bordea, G., Jothi, N., Rashid, N. A., and Husain, W., Data mining in healthcare: a review. Procedia Computer Science 72:306–313, 2015. doi:10.1016/j.procs.2015.12.145.
4. S. Hu, C. Cai, Q. Wang, C. Wang, X. Luo, and Kui Ren, Searching an Encrypted Cloud Meets Blockchain: A Decentralized, Reliable and Fair Realization, in: Proceedings of IEEE INFOCOM, 2018.
5. Qi Zhang, Petr Novotny, Salman Baset, Donna Dillenberger, Artem Barger, Yacov Manevich, LedgerGuard: Improving Blockchain Ledger Dependability, International Conference on Blockchain (ICBC), 2018
6. Ehsani and Farzam, "Blockchain in Finance: From Buzzword to Watchword," CoinDesk (News), 22 December, 2016
7. J. Zhang, N. Xue, and X. Huang, "A Secure System for Pervasive Social Network Based Healthcare," IEEE Access, vol. 4, 2016, pp. 9239–9250.
8. Tao Xie; Fanbao Liu; Dengguo Feng (25 March 2013).
9. Marc Stevens; Elie Bursztein; Pierre Karpman; Ange Albertini; Yarik Markov (2017-02-23).
10. Stevens, Marc (19 June 2012). "Attacks on Hash Functions and Applications" (PDF). *PhD Thesis*.
11. The Future Scope of Blockchain Technology, Blockchain Certification Training ,Oct 10, 2018, Serena Josh

AUTHORS PROFILE

Ms.K.KusumaLatha pursuing B.Tech in Department of Computer Science and Engineering at Koneru Lakshmaiah Education Foundation, Guntur.

Mr.B.RamSai Prakash pursuing B.Tech in Department of Computer Science and Engineering at Koneru Lakshmaiah Education Foundation, Guntur.

Dr.P.V.R.D Prasada Rao, Professor in Department of Computer Science and Engineering .He received B.Tech from Acharya Nagarjuna University, M.Tech (CSE) from AndhraUniversity and Ph.D from Acharya Nagarjuna University in the years 1994, 1999 and 2014 respectively. He published several papers in national & international conferences and journals. His research interests are Datamining, Bigdata and Wireless sensor networks, He is also member of several technical organizations

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication