A Framework to Remove the Stigma of Mental Health and Illness Using Blockchain Technology

Md. Mijanur Rahman, Dept. of CSE, Southeast University, mijanur.rahman@seu.edu.bd
Md. Mamunur Rashid, Dept. of CSE, Southeast University, mamunzaman340@gmail.com
Mahmudul Hassan Rifat, Dept. of CSE, Southeast University, mhrifat007@gmail.com

Abstract-- **Digital Healthcare is struggling with new challenges, especially data sharing and its privacy. Blockchain has become a new weapon to solve different real-world cruxes. Though this technology was introduced to solve the puzzle of cryptocurrency, it has both efficiently and effectively demonstrated new ways in other sectors. The challenges of keeping the records of medical information have become an issue in the digitization of healthcare because data security and continuity as well as data integrity cannot be maintained properly. When it comes to mental healthcare, the challenges have become tougher. Due to stigma in society, mental health is often ignored. In this paper, a blockchain-based framework has been proposed where data of mental health will be cared for with utmost security to minimize the problems of social stigma and the ways to treat them. It will ensure of data integrity, keep the data secured and will bring assurance to the patient as well as ensure that the patient history to the doctors. This paper will be concluded with a framework detail that can be implemented using blockchain technology as well as a few possible research ideas to cope up with the upcoming challenges in the respective fields.**

Index Terms-- Blockchain, Cryptography, Distributed Ledger, Health Information Management, Hashing, Smart Contract.

I. Introduction

In the age of digitalization, analog systems in any platform seem backward. When it comes to the medical sector, this analog system is chaotic and less secured in terms of storing data. So the modern electronic health record system brings more stability and usability in this regard. When we think about the people facing stigma due to mild mental illness, the main issue is lack of data security. Due to the leak of patient information, people often feel negatively in terms of keeping contact with psychiatrists. In any condition whether it is a mild or high mental condition, people in society holding a negative impression on affected people is called stigma [1]. A mild mental patient doesn't show any symptoms visibly so if their problem is not known to the people, stigma can be removed from the society for them. It will create a situation where mild mental patients will not feel hesitant to keep their connection with a specialist doctor in this field. Though due to various verifications from the government or organizations, a patient's data can be asked where he travels. So they may find his mental issues easily though it may not be possible to identify him without that information. Negative news creates a situation where a mild mental patient becomes a victim of stigma for less data security.

Though as of now data security in database systems is not trustworthy due to its security protocols. As blockchain has emerged as a conqueror in many sectors in digitization, the medical system doesn't have many differences. It ensures data security and maintains transparency in data transactions. So those verification policies will not give them any data without the consent and permission from the data owner. Thus blockchain can be a lifesaver for mild mental patients. Blockchain refers to a system that contains records of information which is immune to break, cheat or change. It is based on a modern ledger of transactions which is duplicated and distributed across the nodes of the network. Basically blockchain is a collection of blocks where a block is linked with the previous block. A block is a growing list of recorded information which is linked through cryptography. It contains the location of the previous block, timestamp, data of transactions, nonce etc. [7]. Due to the popularity of bitcoin, blockchain technology has become popular in many industries. Electronic voting, data management, financial services, agriculture and many other industries are trying to implement blockchain for its strong security, transparency, and anonymity. For better security, medical organizations are also trying to implement this technology in place of the existing systems. In this paper section-II talks about the technology which is being used here. Section-III is based on the literature review of some related papers. Section-IV demonstrates the architecture of the proposed system and Section-V discusses the project's success and limitations and ends with a conclusion in section-VI.

II. Blockchain

In the form of bitcoin, blockchain was launch back in 2008 which is known as the first application of blockchain technology [21]. Due to its significant power of keeping secrecy, it has changed the future of cryptocurrency. According to the uses of this technology, it has been classified by different kinds.

Blockchain contains some important properties like distributed data sharing, data persistence, immutability, autonomous code execution, accountability and transparency, and data provenance [9,10].

Distributed data sharing: In the blockchain data is stored in distributed fashion. This redundant fashion of data sharing ensures verification of each transaction which are synced across all the nodes.

Data persistence: This property refers to persistence of data until there are enough nodes to execute the set of institutions. Blockchain cannot be modified even if the cause is removed.

Immutability: Data in blockchain is immune to the attack of other malicious parties. A significant processing power needs to be gained to alter any block which is very unlikely to happen [20].

Autonomous code execution: Once a smart contract is deployed into a blockchain, the contract will be executed by every consensus node in the network. Thus it is eased by smart contract without any failure during the autonomous code execution.

Accountability and transparency: Since blockchain allows permitted entities to verify every transaction, it ensures of accountability as well as transparency.

Data provenance: Blockchain allows only signed transactions which makes sure data provenance [9].

Blockchain is a decentralized data structure which uses pointers and linked lists [12]. When a new block enters a blockchain, pointers store the location of another variable. Using link lists, blocks are kept in the blockchain by linking to the next block.

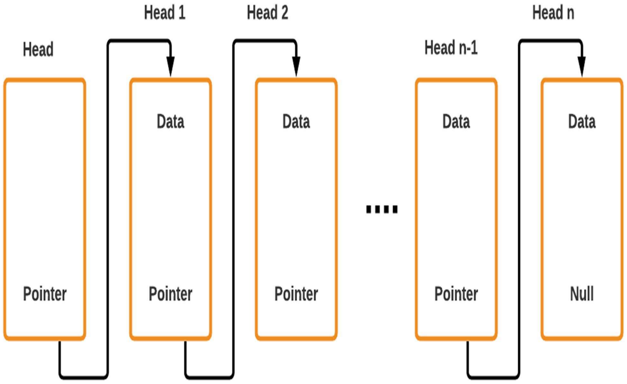

Fig. 1. Architecture of Blockchain

Since we know all the blocks in a blockchain are necessarily linked to the next blocks, we need to understand the concept and uses of a block sincerely.

Initial block which is kept in a block is known as the primary block. It remains as a foundation of the stack. When a new block is added to the stack, it is kept on top of the previous block to form a complete stack which is actually a blockchain [8]. A block consists of transaction details, timestamp, nonce, and previous hash etc. Hash used in the headers identifies the block and it uses the secure hash Algorithms. There are different kinds of hashing algorithms like SHA-128, SHA-256, SHA-512. In this system SHA-512 will be used which generates the idiosyncratic fixed-size 512 bit hash. Though this algorithm is slower than the previous algorithms like SHA-256, it ensures more security since it needs more computational time to crack.
The input values will be in plain text which will be encrypted to a 512-byte binary value. Since it's a one-way function, it ensures that no one can alter the hashing by any means. Figure 2 indicates the hash function.

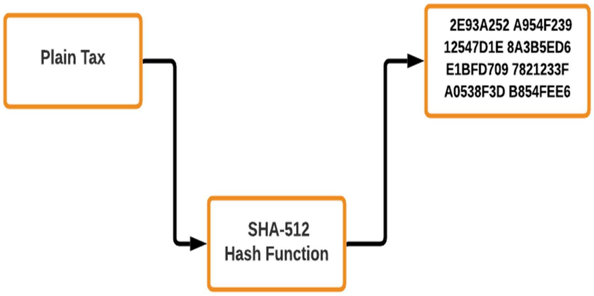

Fig. 2. Representation of SHA-512 algorithm

When a valid transaction occurs a block is created in the blockchain [15]. With each block added to the blockchain, transaction details are updated. It is also linked with the hash value of the previous block. The hash value which is encrypted and kept in the header is known as the primary identifier. After the creation of every new block which is added to the blockchain, the system keeps on tracking. Figure 3 indicates the method of new block creation.

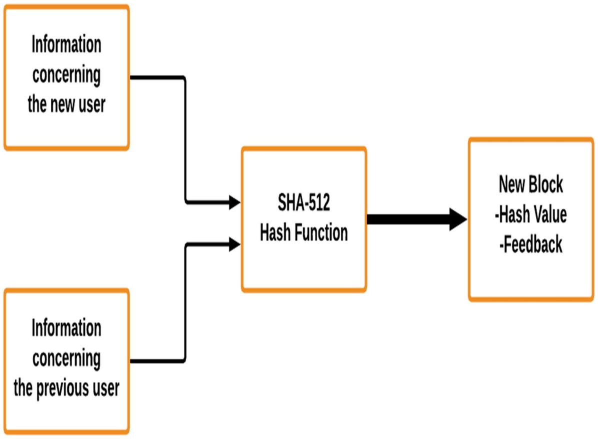
Information concerning the new user
Information concerning the previous user
SHA-512 Hash Function
New Block
-Hash Value
-Feedback

Fig. 3. Method of block creation

The Hashing algorithm is used in this proposed system due to its efficiency in data storing. Since hash functions consist of fixed output but unlimited inputs, the same hash can be found in multiple values [14]. It works like a fingerprint because there are so many possible hash values that can be found and it's highly unlikely that hash values of two concerned plaintext are same. These algorithms ensure collision freeness and it is faster than the others [15]. On the other hand, consensus algorithms are created with common agreements using cryptographic hash functions. These algorithms have differences in terms of usability. Proof of work (POW) acts like hashing algorithms where high electricity of processing power is needed to add the next block to the chain [14]. Proof of stake is similar to the POW but it validates the block using random selection in terms of computational power [16]. It reduces the electricity wastes from POW. Another consensus algorithm is proof of elapsed time (POET) where participating nodes have to wait for randomly chosen time and the winner of the nodes in terms of finishing time is added to the blockchain as a new block [16,20]. Apart from those proof of authority, delegated proof of stake and few other consensus algorithms are used [17]. Since the use of hashing algorithms is easier and wastage of electricity is limited in comparison to the consensus algorithms [18,19], the proposed system used the hashing algorithms.

III. LITERATURE REVIEW

In 2008, a paper was published on Bitcoin written by Satoshi Nakamoto. Blockchain technology was used on cryptocurrency [21]. The basic idea was to secure the transactions and make them safe for the public. This Idea is now integrated in other sectors too.

The infamous problem nowadays is mental health. Even though the treatment gets started, the fear of letting everyone to know about when it comes into play. This incident creates stigma among the community. Stigma refers to the negative thoughts towards certain members of a community who are deeply or mildly affected by some conditions or states of mental health [1]. This stigma creates a big hole of shame carried by a man as a function of being a permanent member of a society [2]. Here blockchain can be a permanent solution for it. The identity of the patients and their families can be secured through this technology.

In 2019, Yon luo, Hao Jin, Peilong Long proposed in a position paper where they identified various challenges when it comes to data sharing and management in the medical sector and they also provided a brief survey on the latest idea of this technology to cope up with the challenges [3]. They also suggested some research ideas and cures of some challenges that can come to the path.

In 2019, Sunil Bakale and Sangamesh K identified the flaws of a patient's data record history where data access is limited to the patient which reduces the availability of data to the healthcare service providers which creates problems in treating the patient [4]. They implemented the idea of storing data of patient history and enabling secure sharing using blockchain technology which may create a revolution in the health industry.

In 2020, Gautami Tripathi, Mohd Abdul Ahad, and Sara Paivab proposed a framework to provide internal security and integrity to the system [5]. This domain is designed to protect the user data and data of various organizations. The use of blockchain technology is essential for the protection and improvement of these data in healthcare. There are many questions about the security and transparency of data in healthcare. We can simplify these through the use of blockchain technology.

In 2018, William J. Gordon, Christian Catalini suggested in their paper that patient-mediated, patient-driven and patient-centered interdependence in health information exchange has become a difficult issue and that the protection and privacy of patient information exchange is a challenge [6]. To solve this problem, they have mentioned five systems of blockchain technology in their research paper which will ease these challenges by sharing patient-centric information.

Related papers of the proposed system have been reviewed here. Since the idea of solving the problem of stigma is new, a lack of collection in terms of papers on this topic has been seen.

IV. METHODOLOGY

System Requirements:

Proposed system ensures the data to be decentralized. For making this system the following features need to be there:

Data Collection: The system will allow its user to keep the patient's data in a blockchain.

Data Integrity: Accuracy of the data and consistency of it will be maintained thoroughly.

Data Allocation: Data will be interoperable so that sharing between entities and different hospitals will be maintained.

Allowable: Patients will use public keys to generate cryptographic signs. Thus doctors will identify their patients.

Anonymity: Since blockchain uses distributed ledger, it keeps all the data and maintains the anonymity of transactions.

System Representation: The system is represented with some common entities like data owner, data provider, cloud server, blockchain, data requester, etc.

Data Storing: This section is solely dependent on the authorization from the data owner. The data provider encrypts the patient's file and uploads it to the cloud server after getting authorization from the data owner. A data transaction will follow afterwards consisting of keyword cipher text for the data owner's address and his records. After that, the data will be sent to the transaction pool which will act as a data translator in the blockchain.

Maintaining the cloud server: Encrypted data has to be stored in the cloud server. It sends the file location to the data owner's account in the blockchain. When the new data arrives it manages to re-encrypt the data and update it into the blockchain.

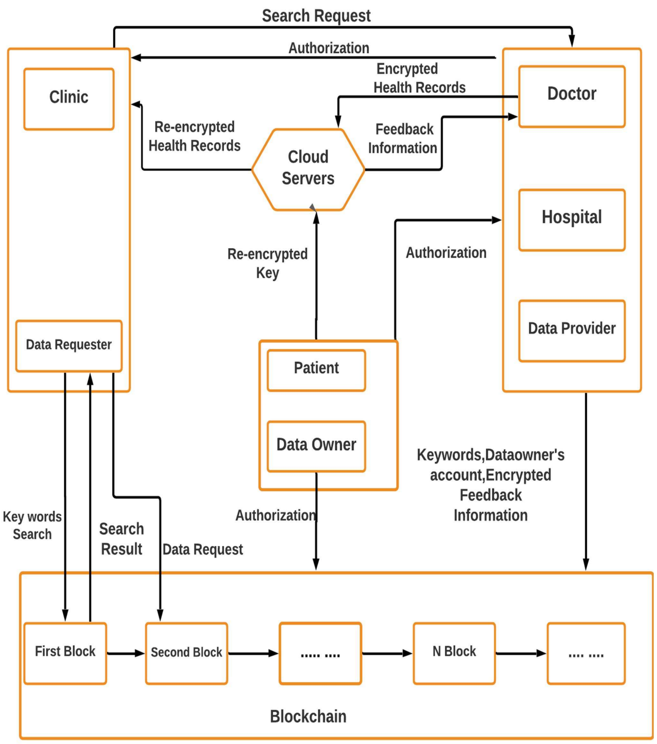

Fig. 4: Architecture of proposed system

Getting the requested data:

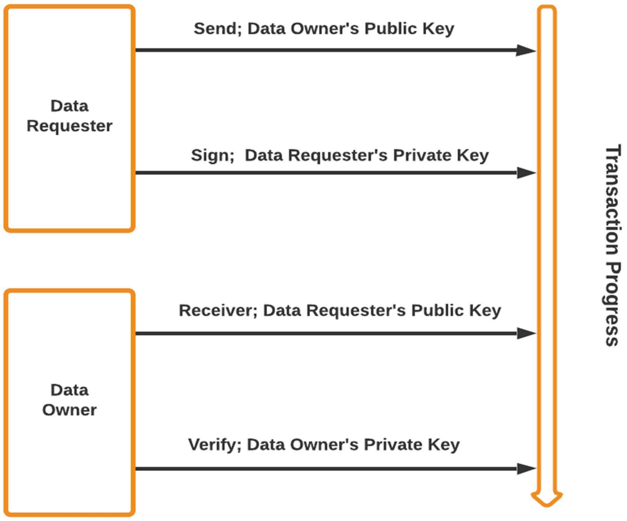
Data Requester
Send; Data Owner's Public Key
Sign; Data Requester's Private Key
Transaction Progress
Data Owner
Receiver; Data Requester's Public Key
Verify; Data Owner's Private Key

Fig. 5: Consortium blockchain network.

Usually, data can be requested by anyone who is connected to the patient. But in this system data requests are limited only to authorized doctors and hospitals who need to access the patient's health records. The data requester has to look for the data in the blockchain and after finding them they will submit a request to the data owner for his approval. After getting the authorization they will be able to collect encrypted files. These transactions are generated by the transaction pool into the blockchain. Since those data requesters are considered ordinary users, they can easily leave the blockchain network when they want.

V. DISCUSSION

In this proposed system data owner's power is maximized. Unlike existing systems using database technology this proposed system will create maximum data security using blockchain technology. Other DLT technology like Hashgraph has similar attributes of distributed ledger systems. But unlike consensus algorithms (for example POW) which are used in blockchain, this technology uses virtual voting to ensure a block [23]. So data transactions are faster in hashgraph than our proposed model. In terms of data availability, we ensure limited data to the end users according to the will of the data owner. In comparison other disturbed ledgers including hashgraph have more data availability for data requesters when they use smart contracts. With the help of interoperability, the data transfer process is user friendly and it maintains a better transfer procedure than existing systems where data needs to be carried out by the data owner. In terms of vulnerability common issues with distributed ledger systems are modeling vulnerability and fraud vulnerability [24]. The proposed system ensures there will be no fraud vulnerability as the data owner directly handles the data. In terms of system vulnerability this system has used consortium blockchain which will make sure that data leak doesn't occur.

VI. CONCLUSION

In the end, the proposed system ensures data security by using hashing algorithms. It will bring a sense of trust among the users. This system will make sure no data leak will create stigma in society and remove an old problem in our society permanently. A smart contract is used to identify, control or execute a system protocol according to the legal agreement. Thus supreme power of the owner in terms of authorization is not fully met here. This proposed system gives the data owner the power of choosing the authorization according to his or her will. This creates a difference between smart contracts and this system. In terms of limitations, this system will not give safety in terms of stigma to the severe mental patients who show their symptoms even though data security will be ensured for all of them. Though this system has a lot of positives, users can use it to their advantage in hiding their medical information to ensure their position in their workplace. In the blockchain, the transfer rate is a lot slower than the database management system. So the proposed system may be slower than usual. In a distributed ledger system if one node is damaged, entire data will be damaged and cannot be retrieved. As blockchain is becoming bigger day by day, so memory storage issues can create a problem. Solving this problem in the future can make blockchain more effective in healthcare and other departments. The proposed system can be implemented anywhere in healthcare management as well as in the business-based organizations.

VII. References

[1] Arboleda-Florez J, Sartorius N, editors "Understanding the Stigma of Mental Illness: *Theory and Interventions. "Chichester: John Wiley*; 2008. pp. 1–17.

[2] Hinshaw SP. "Mark of Shame: Stigma of Mental Illness and an Agenda for Change."*Oxford: Oxford University Press*; 2007.

[3] Yan Luo,Hao Jin,and Peilong Li, "A Blockchain Future for Secure Clinical Data Sharing",*SDN-NFV Sec 19,Richardson,TX,USA* , March 27,2019.

[4] Sunil Bakale1, Sangamesh k2, "Blockchain Technology for Securing Healthcare Records", *International Research Journal of Engineering and Technology (IRJET)*, Mar 2019.

[5] Gautami Tripathia, Mohd Abdul Ahada, Sara Paivab, "S2HS- A blockchain based approach for smart healthcare system",*Healthcare*. Volume 8, Issue 1, March 2020, 100391.

[6] William J. Gordon, Christian Catalini, "*Blockchain technology for Healthcare: Facilitating The Transition to Patient-Driven Interoperability*", *Computational Andstructural Biotechnology Journal 16*, page (224-230), 2018.

[7] "What is blockchain?" 30- Aug 2011. Accessed on January 01, 2021. *[Online]Available:https://www.euromoney.com/learning/blockchain explained/what-is-blockchain*

[8] Nathan Reif, "Blockchain explained" 01-Feb,2020, Accessed on 0-2-Jan,2021.[Online]Available:https://www.investopedia.com/terms/b/blockchain.asp

[9] Daniel Conte de Leon, Antonius Q. Stalick and Ananth A. Jillepalli, Michael A. Haney and Frederick T. Sheldon, "Blockchain: properties and misconceptions" *Asia Pacific Journal of Innovation and Entrepreneurship* Vol. 11 No. 3, 2017, 29 September 2017.

[10] Z. Zheng, S. Xie, H. Dai, X. Chen and H Wang "An overview of blockchain technology: architecture, consensus, and future trends," *in proceedings of 2017 IEEE International Congress on Big Data (Big Data Congress), Honolulu, HI, 2017,* pp 557-564.

[11] ZibinZheng, ShaonXieHongningDai, Xiangping Chen, Huaimin Wang. "An Overview of Blockchain Technology Architecture, Consensus, and Future Trends" *IEEE* 2017.

[12] "Blockchain architecture" on January 31, 2019. Accessed on 2 Feb,2021.[Online] Available: https://mlsdev.com/blog/156-how-to-build-your-own-blockchain architecture?fbclid=IwAR23dKnrfiflM1Nl7di1EwMdpMFSsF19ah8R13sHnoEYOFfX4SsatLwY8FI.

[13] Huaimin wang, zibin zheng,shaoan xie, hong-ning-dai,xianping-chen, "Blockchain challenges and opportunities: a survey", *DOI: 10.1109/BigDataCongress*.2017.85,june 2017.

[14] Mahesh A. Kale, Prof. Shrikanth Dhamdare, "Survey Paper On Different Type of Hashing Algorithms", *International journal of advance scientific research and engineering trends*, vol.3, issue 2, feb-2018.

[15] R.C. Merkle, "One Way Hash Functions and DES", *in CRYPTO*, 1989, pp.428-446.

[16] Du Mingxiao, Ma xiaofeng, Zhang zhe, Wang Xiangwei, Chen Qijun, "A review on consensus algorithm of blockchain", 2017 *IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, Oct. 2017, pp. 2567–2572.

[17] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, in proc. ''An overview of blockchain technology: Architecture, consensus, and future trends,'' *in Proc. Int. Congr. Big Data (BigData Congress)*, Jun. 2017, pp. 557–564.

[18] Niranjan Sapkota and Klaus Grobys, "Blockchain consensus protocols, energy consumption and cryptocurrency prices", (June 13, 2019). *Available at SSRN: https://ssrn.com/abstract=3403983*

[19] Damasevicius, Robertas & Ziberkas, G. & Stuikys, Vytautas & Toldinas, Jevgenijus, "Energy Consumption of Hash Functions", *Elektronika ir Elektrotechnika*, 18. 81-84. 10.5755/j01.eee.18.10.3069, 2012.

[20] M. M. Rahman, M. M. H. Rifat, M. Y. Tanin and N. Hossain, "A feedback system using blockchain technology," 2020 3rd International Conference on Intelligent Sustainable Systems (ICISS), Thoothukudi, India, 2020, pp. 1114-1118, doi: 10.1109/ICISS49785.2020.9315989.

[21] Bitcoin- A peer to Peer Electronic Cash System 2008 by Satoshi Nakamoto.

[22] Yong Wang, Aiqing Zhang, Peiyun Zhang,Huaqun Wang. "Cloud-Assisted EHR Sharing With Security and Privacy Preservation viaConsortium Blockchain", *IEEE Access, 2019.*

[23] Z. Akhtar, "From Blockchain to Hashgraph: Distributed Ledger Technologies in the Wild," 2019 International Conference on Electrical, Electronics and Computer Engineering (UPCON), 2019, pp. 1-6, doi: 10.1109/UPCON47278.2019.8980029.

[24] Bharat k. Vargava, Leszek Lilien, "Vulnerabilities and Threats in Distributed Systems," Distributed Computing and Internet Technology, First International Conference, ICDCIT 2004, Bhubaneswar, India, December 22-24, 2004, Proceedings.