International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-6, March 2020

Patient Health Record Security Based on Blockchain

R. Mythili, Akkudalai Priyanka, Ruchika Prasad, Archit Bhandari

***Abstract*: *It is necessary to keep the patient's health history confidential as it attracts various attackers who can steal the patient's valuable information and can lead to wrong medication which is dangerous for the patients. Healthcare using block chain provides security measures using various algorithms and one of them is consensus algorithm. Block chain is a secure gateway composed of decentralized ledger, when it comes to a specific grant of personalized access. Block chain plays a vital role when it comes to security. In Healthcare Block chain organizes the data so that transactions (i.e. Patient's record) can be verified. Also, Block chain is decentralized ledger which is distributed in nature and has a vital role in securing the data and transactions. Block chain basically contains records in order and is arranged particularly in a block type structure*.

***Keywords:* *Blockchain, Decentralized ledger, Consensus Algorithm, PoW, PoS*.**

I. INTRODUCTION

When it comes to the management of healthcare records or services, we require some applications based on big data. Healthcare data is a confidential and hence it becomes a much prior option to scan for the possible involved risks and threats. A Personal Health Record tool may have an open source access but key lies in the implementation of the security. There are N-number of security options available out there. Out of all the possible considered options, we are counting on Blockchain for the secure part. Blockchain is a secure gateway composed of decentralized ledger, when it comes to a specific grant of personalized access. Blockchain plays a vital role when it comes to security.

Manuscript received on March 15, 2020.
Revised Manuscript received on March 24, 2020.
Manuscript published on March 30, 2020.
* Correspondence Author
R. Mythili*, Assistant professor of Information technology in SRM IST, Chennai, Tamil Nadu, India. Email: mysakavin@gmail.com
Akkudalai Priyanka, Department of Information Technology, SRM IST, Chennai, Tamil Nadu, India. Email: raopriyanka2818@gmail.com
Ruchika Prasad, Department of Information Technology, SRM IST, Chennai, Tamil Nadu, India. Email: ruchika2180@gmail.com
Archit Bhandari, Department of Information Technology, SRM IST, Chennai, Tamil Nadu, India. Email: architbhandari.ab8@gmail.com

In Healthcare Blockchain organizes the data so that transactions (i.e. patient's record) can be verified. Also, Blockchain is decentralized ledger which is distributed in nature and has a vital role in securing the data and transactions.

So, Blockchain being a decentralized ledger is responsible to verify each transaction which includes a financial transfer of a patient, patient's medical research, etc. this makes it secured and trustable. Patients who are the part of this decentralized ledger i.e. Blockchain can be able to change their data this means that the users who are authorized can only get access to the information stored in blockchain and will be responsible to change or upgrade the data. Blockchain basically contains records in order and is arranged particularly in a block type structure.

Every block of data contains a hash which is served as a digital fingerprint or a unique identifier, time stamped batches of the transactions that were recently transacted along with a hash generated for a previous block. In this design, every block is chronologically connected, collectively called blockchain. The Existing System was based on Message Digest Algorithm commonly known as MD5 Algorithm. MD 5 Algorithm uses hash functions that is cryptographic in nature and creates a unique value. Since MD 5 had various drawbacks so to overcome some drawbacks new algorithm was proposed known as Consensus algorithm.

TABLE I. Abbreviations

ABBREVIATION	DESCRIPTION
PHR	Patient Health Record
PoS	Proof of Stake
PoW	Proof of Work
CS	Cloud Storage
GS	Gateway Server
PO	PHR Owner
MD	Message Digest

II. METHODOLOGY

The proposed system is based on consensus algorithm which helps to overcome the drawbacks of message digest algorithm which mainly consists of hash Collision and noises. The Consensus algorithm is explained as a process via which a particular network of blockchain culminates into a unified agreement regarding the decentralized ledger.

A consensus algorithm works at finding a common agreement which is beneficial for the entire network. Blockchain is responsible to maintain the security and integrity for the distributed systems. Consensus algorithm works using several algorithms Distributed systems such as decentralized ledger does not depend on a central authority instead works by the verification of the distributed nodes. Every transaction needs verification in order to proceed with the validity. Here is where the consensus algorithm comes into action. It makes sure that the rules are followed thoroughly and also ensures that the transactions are in a correct order such that each and every transaction is counted as a unique one. This feature of consensus algorithm allows it to remain open and transparent to the client so that the client have the real time idea of what's happening.

The consensus algorithm encrypts the data once and uses the encrypted data for the validation. It also ensures that for every new data that is added to the blockchain is one and only data that is agreed by all the nodes in the blockchain. This algorithm has the main objective that all the data added in it are coming through an agreement and every node of the blockchain have the right participation for validation of each node in the blockchain.

There are many different types of consensus algorithms. The algorithm used in blockchain are PoW (Proof of Work) and PoS (Proof of stake).

1)PoW

The PoW (Proof of Work) mining uses various hashing attempts and therefore more computational power is used which implies that there will be an increased number of trials per second. When we put it other way round then it means that a hash with higher rate has more solution chances than that of before. It works on the principle that a solution is difficult to find than to validate it. The consensus algorithm ensures that the nodes indulge in an agreement and trust each other in a non-trusted environment. Furthermore, the blocks in progress with operate only when a common agreement has been passed down by all other blocks via the valid proof of work. It works on by computing the computation power of a block and mining the solutions in a chronological order so that the time and energy are less used.

2)PoS

Another one the varied option might be the PoS (Proof of Stake), aimed at implementing the consensus algorithm in the blockchain. The Intensive energy is reduced by PoS by reducing the energy consumed by computation resources generated by PoW. Every system implements PoS in various ways ultimately implementing blockchain by using the age coin selection method via the usage of selection of random block.

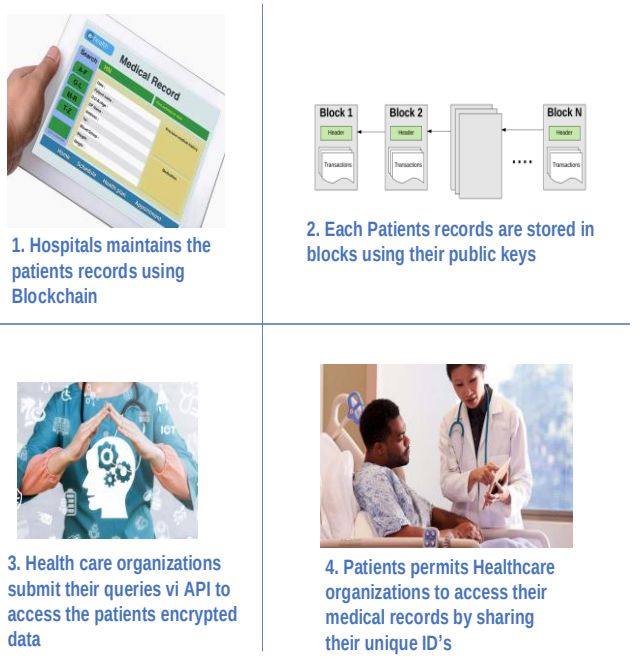

Figure 1: System Layout

III. IMPLEMENTATION

Step 1: To access the details, patients are provided with the login credentials which consists of following details

- At first to access the user- based authorization application the particular address given by the Application Admin (PHR Owner) should be provided in the web address.
- Then the login page will be displayed.
- Add User name and password.
- Following that a Remember Me box will be generated and that should be logged in for minimum 14 days.
- Once successfully logged in patient can access their data.
- The main goal of user -based authorization application is to provide confidentiality, data security and data storage.

Step 2-Information provided by the doctor.

- The main motto of this system is to maximize the ability of the doctors and medical practitioners.
- The automation of the data access is the main feature here.
- The platforms which are instrumental in carrying out this automation are python (IDE).
- Python is an object-oriented programming language which is in features such as having instance attributes and inheritance etc.
- These features eventually culminate into a framework thus providing a robust environment to the above automation.

Step 3: Records of patients and the ehr associated with it

- This module takes care of the demographic details of the patients provided by the doctors or by medical practitioners.
- Patient acts as the main identifier here.

- A registration number allocated will act as a reference number which further will respond to all the queries raised by the authorized party,
- The information which resides in the response to the queries consists of the following content:
  Contact of the patient
  Plan of the patient service
  Day to day report
  Billing details
  Treatment details
  Doctor associated with the particular patient

Electronic health records

An electronic health record is analogous to a record that has a similar role to that of keeping every single and particular detail of the associated person except for the fact, Security. In electronic health records the security is the main issue addressed. Since an Electronic health record everything is done digitally and not only digital but also is pinned on the internet thus making it all the more vulnerable to the attacks such as phishing and scam etc. The trusted source in security proves to be blockchain which has decentralized ledger as the main concept which further ends up in regarding every change

of action as an individual transaction.

TABLE 2. Response Time & Memory Usage

Transactions	Response Time	Memory Usage
Patient Registration	6002 ms	236 B
Doctor Registration	6231 ms	236 B
ED Registration	5963 ms	236 B
Get Patient Data	5683 ms	568 B
Result(Time Consumed)	Time(Consensus)<Time(MD5)	

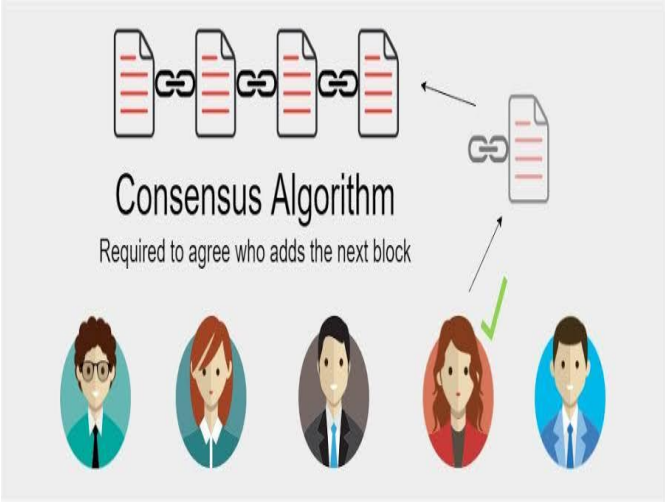

Figure 2: System Architecture

Step 3: file binding and its generation

- Encryption is the most important thing when we address the security concerns. It makes sure that the transactions are quick and are made exclusively private.
- Encrypting data is mostly used to give a better security to the records existing in the electronic health records.

Algorithm for file binding:

- File input is accepted and is encrypted using one of the existing encryption modules.
- The username is taken along with password as the parameter.
- A key will be generated via which the encryption is achieved.
- Each key generated will have a unique reference value, which will help in assisting every transaction as an individual one.
- Hash function is used to maintain all the keys which are generated and another hash function is produced simultaneously to manage the references for those keys generated.
- The unique reference act similar to fingerprint which carries a more secure gateway.

Step 5: Auditing using third party

Verification using third party about the cloud storage and dynamic operations are done in order to increase the efficiency of the transactions known as Auditing. Auditing of various outsourcing data by the third party is accessible by authorized users i.e. Patients and also Patients are allowed to update the data according to their need. Auditor deals with the partial key which is generated by the key generation centre provided by the Gateway server in order to maintain the privacy of the Patient's data. Patients are provided with the private key which is encrypted in nature and can only be accessed by the Patients or the other authorized users such as doctors. This helps to maintain the confidentiality of the Patient's data.

IV. RESULT

i) RESPONSE TIME:

The response time thus generated by the previous transactions in action was reported to have consumed less time than that of the MD5. Earlier in the series of events it was recorded that the response time of the MD5 was far greater than the consensus algorithm. For example taking one of the transactions i.e. patient's registration, the time complexity using MD5 the reported time complexity was 6119 ms as compared to consensus algorithm which only took 6002 ms to retrieve the above stated transaction. Hence using consensus algorithm has greatly aided us in the successful recovery of the existing time lag.

ii) MEMORY USAGE AND ACCESSIBILITY:

The memory usage also proves to an important factor when it comes to the reduction of the time complexity which further results in the time lag between the transactions taking place in the particular system. Consensus algorithm is also effective when it comes to the efficiency of space complexity.

The main factor happens to be the retrieval of the space which further assists the time complexity hence making it user friendly and resulting into better accessibility.

V. CONCLUSION

Blockchain is one of the most important and trusted technologies when it comes to security. The role of blockchain ensures us with the features such as decentralization and its resistance to data hampering. Features such as data integrity and confidentiality are some other features to name. In this project the main focus has been on the confidentiality of the patient's data. Personal health records can be analogues to a ledger. A ledger comprises of records which are arranged in an order to gain access to certain information which can be put to the best of its use. The encryption is another benefitting factor for the blockchain. Blockchain constructively uses end to end encryption to ensure a smooth running. Time complexity is the major issue addressed here in this paper and is effectively solved using the consensus algorithm. If used in an effective way blockchain has the potential to prove itself as trusted source as it keeps the data confidential and secure for any random unknown to access it.

REFERENCES

1. Farahani, B.; Firouzi, F.; Chang, V.; Badaroglu, M.; Constant, N.; Mankodiya, K. Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare. Future Gener. Comput. Syst. 2018, 78, 659–676. [CrossRef]
2. Hossain, M.; Islam, S.R.; Ali, F.; Kwak, K.S.; Hasan, R. An Internet of Things-based health prescription assistant and its security system design. Future Gener. Comput. Syst. 2018, 82, 422–439.
3. Badawi, H.F.; Dong, H.; Saddik, A.E. Mobile cloud-based physical activity advisory system using biofeedback sensors. Future Gener. Comput. Syst. 2017, 66, 59–70.
4. MarketsandMarkets Research. IoT Healthcare Market by Component (Medical Device, Systems & Software, Service, Connectivity Technology), Application (Telemedicine, Work Flow Management, Connected Imaging, Medication Management), End User, and Region—Global Forecast to 2022. Available online: https: //www.marketsandmarkets.com/Market-Reports/iot-healthcare-market-160082804.html (accessed on 21 December 2018).
5. Sahi, M.A.; Abbas, H.; Saleem, K.; Yang, X.; Derhab, A.; Orgun, M.A.; Yaseen, A. Privacy Preservation in e-Healthcare Environments: State of the Art and Future Directions. IEEE Access 2018, 6, 464–478.
6. Abrar, H.; Hussain, S.J.; Chaudhry, J.; Saleem, K.; Orgun, M.A.; Al-Muhtadi, J.; Valli, C. Risk Analysis of Cloud Sourcing in Healthcare and Public Health Industry. IEEE Access 2018, 6, 19140–19150.
7. Gordon,W.J.; Catalini, C. Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability. Comput. Struct. Biotechnol. J. 2018, 16, 224–230.
8. Rinner, C.; Sauter, S.K.; Endel, G.; Heinze, G.; Thurner, S.; Klimek, P.; Duftschmid, G. Improving the informational continuity of care in diabetes mellitus treatment with a nationwide shared EHR system: Estimates from Austrian claims data. Int. J. Med. Inform. 2016, 92, 44–53.
9. Hyppönen, H.; Reponen, J.; Lääveri, T.; Kaipio, J. User experiences with different regional health information exchange systems in Finland. Int. J. Med. Inform. 2014, 83, 1–18.
10. Yang, Y.; Li, X.; Qamar, N.; Liu, P.; Ke,W.; Shen, B.; Liu, Z. MedShare: A Novel Hybrid Cloud for Medical Resource Sharing among Autonomous Healthcare Providers. IEEE Access 2018, 6, 46949–46961.
11. Yang, Y.; Quan, Z.; Liu, P.; Ouyang, D.; Li, X. MicroShare: Privacy-Preserved Medical Resource Sharing through MicroService Architecture. Int. J. Biol. Sci. 2018, 14, 907–919.
12. Walker-Roberts, S.; Hammoudeh, M.; Dehghantanha, A. A Systematic Review of the Availability and Efficacy of Countermeasures to Internal Threats in Healthcare Critical Infrastructure. IEEE Access 2018, 6, 25167–25177.
13. Liu, Y.; Zhang, Y.; Ling, J.; Liu, Z. Secure and fine-grained access control on e-healthcare records in mobile cloud computing. Future Gener. Comput. Syst. 2018, 78, 1020–1026.
14. Wang, H. Anonymous Data Sharing Scheme in Public Cloud and Its Application in E-health Record. IEEE Access 2018, 6, 27818–27826.
15. Yao, X.; Lin, Y.; Liu, Q.; Zhang, J. Privacy-preserving search over encrypted personal health record in multi-source cloud. IEEE Access 2018, 6, 3809–3823.
16. Al Omar, A.; Rahman, M.S.; Basu, A.; Kiyomoto, S. MediBchain: A blockchain based privacy preserving platform for healthcare data, Security, Privacy, and Anonymity in Computation, Communication, and Storage, Guangzhou, China, 12–15 December,2017; Wang, G., Atiquzzaman, M., Yan, Z., Choo, K.K., Eds.; Springer: Cham, Switzerland, 2017.

AUTHORS PROFILE

R. Mythili is an Assistant Professor in Department of Information Technology, SRM IST, Chennai, Tamil Nadu, India.Email: mysakavin@gmail.com

Akkudalai Priyanka, Department of Information Technology,SRM IST,Chennai,Tamil Nadu,India. Email:raopriyanka2818@gmail.com

Ruchika Prasad, Department of Information Technology,SRM IST,Chennai,Tamil Nadu,India. Email:ruchika2180@gmail.com

Archit Bhandari, Department of Information Technology, SRM IST, Chennai, Tamil Nadu, India. Email: architbhandari.ab8@gmail.com