International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 02 | Feb 2020 www.irjet.net p-ISSN: 2395-0072

Health Record Transaction in Hospital Management Using Blockchain

D. Anto Sahaya Vinotha[1], G.Monisha[2]

[1]PG Student, Department of CSE, DMI Engineering College, Tamilnadu, India
[2]Assistant Professor, Computer Science & Engg., DMI Engineering College, Tamilnadu, India

---

Abstract - *In recent years, the block chain innovation considered as versatile contrasted with different procedures. A significant number of the business, understanding the block chain innovation is using for monetary administrations and its exchanges yet it likewise successful in different divisions like social insurance industry. Existing strategies are unsafe; where, information put away in untouchable servers may be listened stealthily, taken, or real way. All things considered, the reliability of capacity server design endless supply of single specialist organization. The security supervisor's identify which are client(s) can get to a particular piece of the information. Be that as it may, the current strategy is progressively neglected to keep up get to control, record exchange validations with unknown interferences. The paper proposes a safe and proficient wellbeing record exchange using square chain (SEHRTB) calculation for tending to wellbeing record data exchange between the patient, specialist, specialist organizations, and establishments in a protection safeguarding way. The work furnishes a human services area with square chain innovation. In medicinal services, the work empowers the patient to control and share their wellbeing record into distributed storage effectively in a verified way with no infringement of protection. It gives a compelling method to guarantee the patient information secretly in wise social insurance frameworks. The paper shows the framework worked in a decentralized processing framework to guarantee confided in outsider for leading calculation over patient information without disregarding the security. In light of Experimental outcome, the SEHRTB calculation lessens 2.05 dormancy, 1.08 ET (execution time), and improves 30.5% throughput thought about than existing methodologies.*

***Key Words*: Block chain technology, Health records, Privacy, Latency, Execution time, Throughput, Secure and efficient health record transaction utilizing block chain (SEHRTB) algorithm.**

1. INTRODUCTION

Block chain has gotten a genuine promotion and inspiration in the innovation than some other system. The block chain has begun its new upheaval in innovation, which will have at any rate as significant an impact on society as the innovative advancement. Block chain was at first made for the advanced cash Bitcoin and first depicted by Satoshi Nakamoto's whitepaper in 2008. In the record, Nakamoto particularly brings up the difficulties that happen in proprietorship related to cutting edge computerized money related frames and creates a few arrangements using a square chain going before the exchanges. The possession testing lies in uniting all essential data in a solitary database, which is further conveyed openly. The database isn't worked with any different proprietorship however at the same time possessed by everybody. The database was decentralized and made accessible to all gatherings included.

1.1 BLOCK CHAIN

The idea of Blockchain first came to distinction in October 2008, as a feature of a proposition for Bitcoin, with the plan to make P2P cash without banks. Bitcoin acquainted a novel arrangement with the deep rooted human issue of trust. The basic blockchain innovation enables us to confide in the yields of the framework without confiding in any entertainer inside it. Individuals and organizations who don't have the foggiest idea or trust one another, dwell in various nations, are dependent upon various wards, and who have no lawfully authoritative concurrences with one another, would now be able to interface over the Internet without the requirement for believed outsiders like banks, Internet stages, or different sorts of clearing establishments.

In any case, the Bitcoin white paper didn't leave slender air, and P2P systems are not another wonder. They are established in the early history of the PC and Internet, expanding on many years of research of PC systems, cryptography, and game hypothesis (see Appendix: Origins of Bitcoin). The Bitcoin white paper settled the issue of incorporated information stockpiling and data the board. All PCs in the system hold an indistinguishable duplicate of the record of exchanges, which goes about as a solitary perspective. Putting away information over a P2P organize takes out issues emerging from the powerlessness of concentrated servers while utilizing distinctive cryptographic strategies to verify the system.

2. PROBLEM DEFINITION

The block chain technology is highly utilized in many sectors like Internet of Things (IoT), finances, protection and many. Various public sectors and private businesses relied highly on the block chain technology in building the IoT system. Huh et al. (2017) managed the IoT system with the block chain technology by framing the keys in RSA public key cryptography systems. The work stored the public keys and private keys in Ethereum and individual devices respectively. Where, the Ethereum was a distributed computing platform, an open source for block chain technology due to the

advantage of the smart contract it possesses. Cha and Yeh (2018) described communication architecture with the block chain network technique and the construction of ISO/IEC 15408-2, which was a complaint security based auditing system. Intelligent applications comprised Internet of Things (IoT) and Artificial Intelligence (AI) robots were highly suitable to adopt the security auditing system. Iansiti and Lakhani (2017) explained a framework for block chain adoption with the analysis that suggested the two-dimensional effect for how a functional technology and the business uses evolved.

3. PROPOSED WORK

The block chain based health records monitoring system illustrates about the four issues called fragmented, slower accessibility to the data, system interoperability, and improved quality of data, health insurance agent, and set of quantity for medical data. The system adds other features like data integrity, individuals empowering towards record authenticity, data sharing, and auditability. Thus, the work considers as an innovative technology in providing a secure health record solution with block chain technology. In details, the SEHRTB algorithm is proposed to understand the workflow of the block chain methodology utilized in the health records application which details are displayed in Fig. 1.

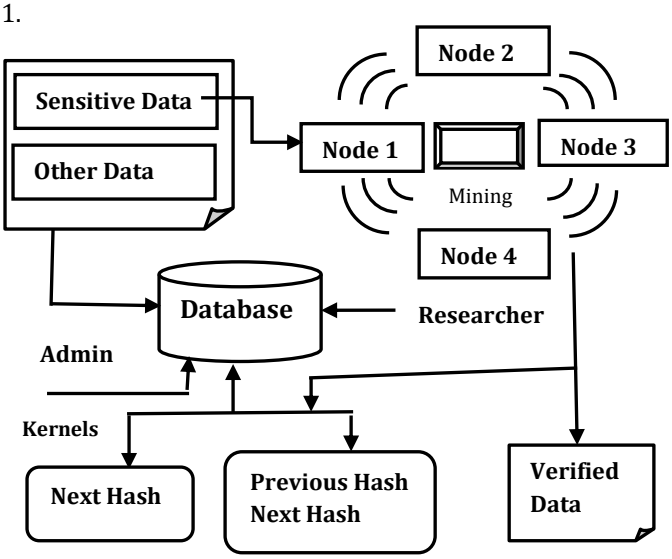

Fig-1: System Architecture

3.1 Patient

In patient module, patient needs to access the information which is stored in a storage server; he/she should enroll their information's first. The information's are maintained in a database or storage servers. When, patient enlisted, then patient send request or his/her inquiry to cloud database. Here, the patient can view the document list. Patient can recover the information in encrypted mode.

3.2 Doctor

The doctor will transfer the patient health record in encryption mode. Here, the doctor's facility can view patient health record. In this stage, the SEHRTB algorithm will effectively encode the health record information. During information transmission, there is no possibility for traded off with the aggressor. This health record information's are maintained in a database.

3.3 Insurance agent

If the insurance agent needs to access the information that is stored in a storage server then he/she should enroll their information first. The information is maintaining in a database or storage server. When, insurance operator enrolled then, they can send demand for his/her question to storage server or database. Here, the agent can view the document list, and she/he can recover the health record information in an encrypted manner. The agent cans also view hospital information's.

3.4 Record Upload

The doctor encodes the health record information dependent on the sub access control policies in proprietor and transfers them along with the comparing public/open data record to the database or storage server. The record encodes using SEHRTB algorithm and stored in storage server. The two parties execute an SEHRTB algorithm initially to create the symmetric key, the public information record and access tree for every sub access control policy. It explains a detailed explanation of the encryption procedure. The proprietor organizes the sub access control policy such that every data item has a unique access control policy.

3.5 Patient Health Record Search

Here, patient and insurance agent can enter their queries based on requirement from cloud server. Patient and insurance agent get the encoded data from server. Hence, they can request secret key to retrieve the original information. But, only register patient and insurance can retrieve the information.

3.6 Storage Server

Whenever, the system believed that authority full access and view all individual details, patient details, doctor's facility details, and insurance agent details. Hence, centralized storage server is required to share and retrieve the health records from anywhere and anytime.

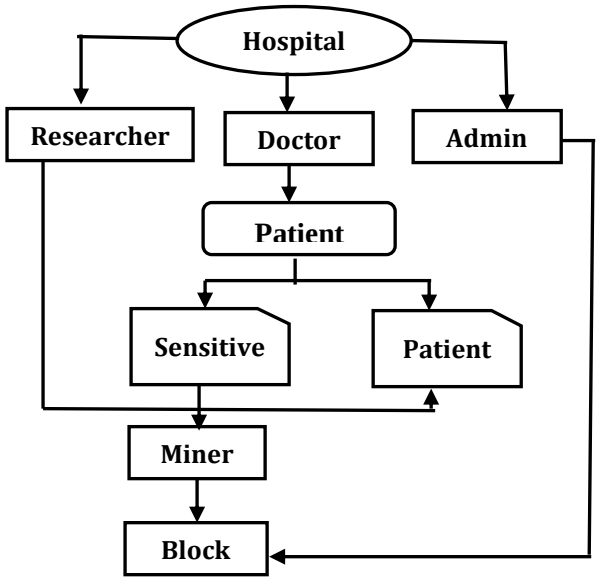

Fig-2: Flow Diagram

4. RESULTS

Fig-3: Login page

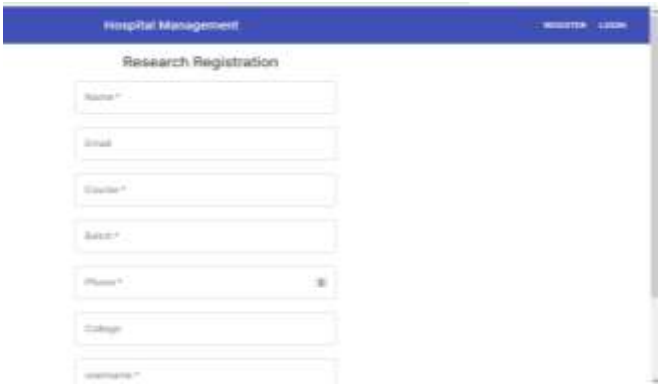

Fig-4: Registration page

Fig-5: Researcher details

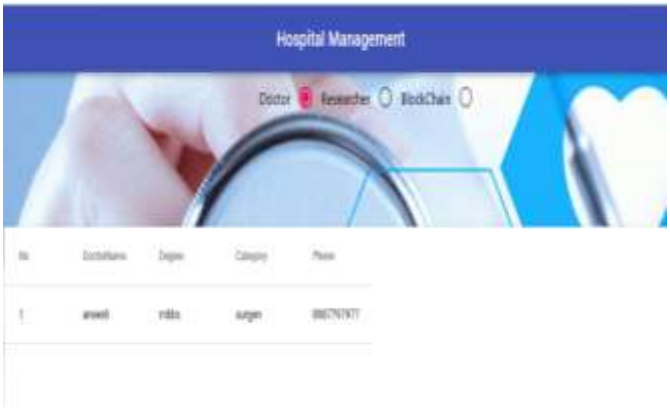

Fig-6: Doctor Details

5. CONCLUSION

The article presents SEHRTB algorithm adequately to control and the access to health record information and processed in storage framework in efficient way. The algorithm provides a proof-of-concept based framework, shows how standards of decentralization and block chain-based work could achieve security, interoperable health records frameworks. It accomplishes confidentiality protecting health record distribution. When, requirement matches to access the record then the smart contract is activated consequently to execute the comparing task. It can guarantee the legitimateness and fairness of health information sharing. The proposed structure is decreasing the overhead and maintaining dimensions of protection and privacy of sensitive data during the distribution of the block chain platform effectively. The SEHRTB reduces 2.05 Latency in seconds, 1.08 ET (Execution Time) in seconds, and improves 30.5% percentages of Throughput. Finally, the paper said that the proposed SEHRTB algorithm performs best on each evaluation matrix and several input dataset.

REFERENCES

[1] Aitzhan NZ, Svetinovic D (2016) Security and privacy in decentralized energy trading through multi-signatures, block chain, and anonymous messaging streams. IEEE Trans Dependable Secure Comput 15(5):840–852. https ://doi.org/10.1109/TDSC.2016.26168 61.

[2] Iansiti M, Lakhani KR (2017) The truth about block chain. Harvard Business Rev 95(1):118–127.

[3] Kiayias A, Panagiotakos G (2015) Speed-security tradeoffs in block chain protocols. IACR Cryptology ePrint Archive, pp 1–19 Kosba A, Miller A, Shi E, Wen Z, Papamanthou C (2016) Hawk: the block chain model of cryptography and privacy-preserving smart contracts. IEEE Symp Security Privacy SP. https ://doi. org/10.1109/sp.2016.55.

[4] Qu C, Tao M, Zhang J, Hong X, Yuan R (2018) Block chainbased credibility verification method for IoT entities. Security Commun Netw. https ://doi.org/10.1155/2018/78176 14.

[5] Shafagh H, Burkhalter L, Hithnawi A, Duquennoy S (2017) Towards block chain-based auditable storage and sharing of IoT data. Proc Cloud Comput Security Workshop. https ://doi.org/10.1145/31406 49.31406 56.

[6] Tian F (2016) An agri-food supply chain traceability system for China based on RFID and block chain technology. Int Conf Service Syst Service Manag ICSSSM. https ://doi.org/10.1109/ICSSSM.2016.75384 24.

[7] Tosh DK, Shetty S, Liang X, Kamhoua CA, Kwiat KA, Njilla L (2017) Security implications of block chain cloud with analysis of block withholding attack. Proc IEEE/ACM Int Symp Cluster Cloud Grid Comput. https ://doi.org/10.1109/CCGRI D.2017.111.

[8] Vukolić M (2015) The quest for scalable block chain fabric: proofof-work vs. BFT replication. International Workshop on Open Problems in Network Security, pp 112–125.

[9] Xu X, Weber I, Staples M, Zhu L, Bosch J, Bass L, Rimba P (2017) A taxonomy of block chain-based systems for architecture design. IEEE Int Conf Softw Archit ICSA. https ://doi.org/10.1109/ ICSA.2017.33.

[10] Yu X, Tan Y, Sun Z, Liu J, Liang C, Zhang Q (2019) A fault-tolerant and energy-efficient continuous data protection system. J Ambient Intell Hum Comput 10(8):2945–2954. https ://doi.org/10.1007/ s1265 2-018-0726-2.

[11] Zheng Z, Xie S, Dai HN, Wang H (2016) Block chain challenges and opportunities: a survey. Int J Web Grid Serv 14(4):352–375. https ://doi.org/10.1504/IJWGS .2018.09564 7.

[12] Cha SC, Yeh KH (2018) An ISO/IEC 15408-2 compliant security auditing system with block chain technology. IEEE Conf Commun Netw Security CNS. https ://doi.org/10.1109/CNS.2018.84331 85.

[13] Christidis K, Devetsikiotis M (2016) block chains and smart contracts for the internet of things. IEEE Access. https ://doi.org/10.1109/ ACCES S.2016.25663 39.

[14] D'Arienzo MP, Dudin AN, Dudin SA, Manzo R (2019) Analysis of a retrial queue with group service of impatient customers. J Ambient Intell Hum Comput. https ://doi.org/10.1007/s1265 2-019-01318.

AUTHORS

ANTO SAHAYA VINOTHA.D Pursuing M.E in computer science and Engineering at DMI engineering college, Aralvoimozhi, KanyaKumari, Tamilnadu.

MONISHA.G, currently working as Assistant Professor, Department of Computer Science & Engineering at DMI Engineering College, Aralvoimozhi, Tamilnadu, India.