Temporal Blockchain Approach based Secure Ehealth Framework

Shekh Jahid
M. Tech. Scholar
Department of Computer Science and Engineering
All Saints' College of Technology, Bhopal

Zuber Farooqui
Professor
Department of Computer Science and Engineering
All Saints' College of Technology, Bhopal

ABSTRACT
The advent of the internet and its impact on healthcare domain made it possible to store, access and update medical records anywhere and anytime. Medical discrepancies associated with Electronic Health Records (EHR) and concerns related to privacy and security issues need to be addressed. Perhaps the biggest issue of all was lack of standardization and indeed it is not the only challenge in EHR. Decentralized online ledgers with blockchain based platforms proposed and in use to address the interoperability and privacy issues. In this paper shows that the temporal shadow concepts and context-based properties have an impact on performance of the proposed Secure eHealth Framework (SeFra) to manage the Personalised Micro Ledger (PML) securely. Also it contributes to capture medical data in text format with temporal properties and share the data among all other peers as per the policies specified in the context-based smart contract. Significantly, the framework has the potential to address the issues in siloed data and provide tamper-proof, secure transactions in healthcare domain.

Keywords
Temporal blockchain, Personalised Micro Ledger, Electronic Health Records, SeFra

1. INTRODUCTION
Electronic health care is the patient information that stores the health information in a digital format. The patient-centered records allow accessing the data by any authorized user from anywhere and at any time. The electronic health system saves more than $81 billion annually (Hillestad et al., 2005). Electronic health care increases the social, health benefit and reduces medical errors. The Healthcare Information and Management System Society (HIMSS) is a non– profit organization to expand the health care protection, safety and transform the health information through the information technology. The HIMSS focused on North America, Asia Pacific, the United Kingdom, and the Middle East. The HIMSS contains 72,000 individuals and 630 organizations. The main aim of HIMSS is to improve healthcare throughout the world. The issues in the health care systems are attackers tries to change the health data, which leads to severe damage in the healthcare system, severe attacks like the ransomware attack, and lack of cybersecurity.

2. SECURITY ISSUES IN HEALTHCARE
The difficulty in expanding the utilization of IT frameworks in healthcare is presumably the worries about security when systems are to be trusted with healthcare information (Ermakova et al., 2013). Security It is the property of a system that is safe to deliberate attacks and control from outside of the framework. The system incorporates the part of information security. Avizienis et al. (2004) mention the common security issues in the health care system, such as confidentiality, authorization, and integrity.

i) Confidentiality Privacy is one of the core responsibilities of the medical provider. The healthcare information is a sensitive information need to protect from an unauthorized user. The system allows the authorized user to access the information and need to create a trusted environment so that the patient visits the hospital and willing to seek care. According to the HIPAA act of 1997, they required to protect the patient's health information.

ii) Integrity Maintaining the integrity of the eHealth record is essential because it is used to recognize and follow patients as they move from one provider to another provider. The integrity of medical services information is necessary to decide on patient care. It maintains the health information which should be accurate and unaltered over the entire life cycle. It keeps the accuracy, consistency, and trustworthiness of the data. Some random number is used to check the integrity of the data.

iii) Authorization EHR system agrees with the doctors to access the record and store, improving the medicinal recording process for an authorized user. The medical services associations attempt to relieve these risks, and they have to assume responsibility for their authorization. The authorization process restricted to external users, and it is essential to mention the access control mechanism to ensure the patient's privacy. It is a process; the system should specify the access privileges for accessing the eHealth data.

iv) Availability Availability is the property of a framework, the record being open, usable, and accessible upon interest by approved users. It implies that the information is continuously available to the clients when demanded by an authorized user. It has to be assured of the availability of health records by preventing service disruption due to hardware failures, framework upgrades, and power outages. The availability of health records is more important than securing it.

3. BLOCKCHAIN
Blockchain is a new technology, booming in most of the industries. Blockchain was first proposed for a cryptocurrency(Nakamota, 2008). Figure 1 shows with distributed peer – to – peer network. A novel element of distributed blockchain network has no central database. The blockchain information repeated over every one of the nodes in the circulated framework. The three components of the blockchain are decentralization, transparency, and immutable. All the transactions stored in the blocks. Once the block verified with peer nodes, then it is stored in the blockchain. Each block contains a list of transactions. The blocks arranged in

chronological order, permission, decentralized record management system, which allows people to share the information in a trustworthy manner. It is a secure database, where it is controlled by the whole network, not by a single user.

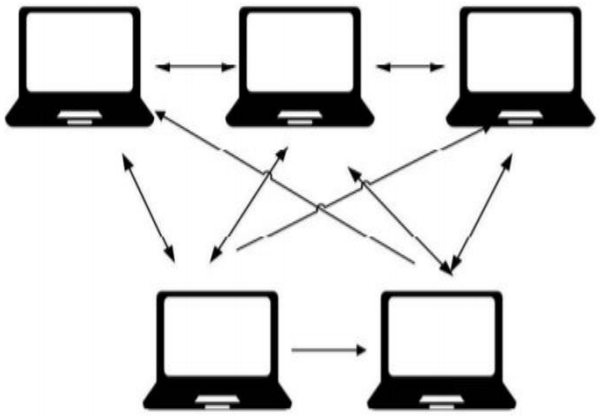

Fig. 1: Peer-to-Peer Network

Blockchain and IPFS is a perfect combination. Kept a large amount of data in IPFS, and the content address of the data is immutable and creates a permanent link, the content address given as input to the blockchain. The timestamp appended with the data in the blockchain. The data stored in the IPFS, and the link put in the blockchain. It is challenging to save a massive amount of data in the blockchain; instead, data stored in the IPFS network, and the hash value stored in the blockchain, so the integrity of the information is easily maintained.

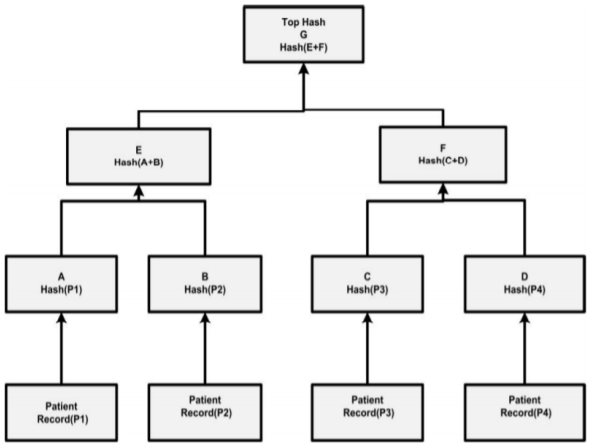

Fig. 2: Process of Merkle Tree

Blockchain is a distributed ledger, which is open and stores the record permanently. Blockchain which contains a list of blocks, each block linked with the previous block.

4. PROPOSED METHODS

The strong hash value generated with the help of temporal shadow. Each patient record hashed with temporal shadow, and the final aggregated hash value stored in the block header. Before the transaction stored in the Progressive temporal blockchain, each transaction verified by a miner and approved. The researcher will act as a miner and get anonymized health data as a miner reward for the research purpose. The two ledgers were maintained, General Public Ledger(GPL), and another one is a Personalized Micro Ledger(PML). The GPL maintains all patient hash value. Whereas in a PML maintains the personalized patient health hash value. The Merkle tree aggregates all the transactions and forms the root value. In the proposed work, to make the system more secure, a Merkle tree with the temporal shadow is used. The Merkle tree with the temporal shadow explained in Fig. 3. The Temporal Hash Signature(THS) is generated based on the path of the Context-based Merkle Tree(CBMT) and used for authentication. The proposed system makes the THS, which is used to secure the eHealth system to protect confidential information and maintain the privacy of sensitive data. Once the data stored in the Progressive temporal blockchain, then there is no chance to change the data. The integrity maintained by Progressive temporal blockchain. Each user authenticated by Etheruem address, and access privilege is attained by THS to access the health record, which is maintained in the Context-based Access Control (CBAC) in a Smart Contract.

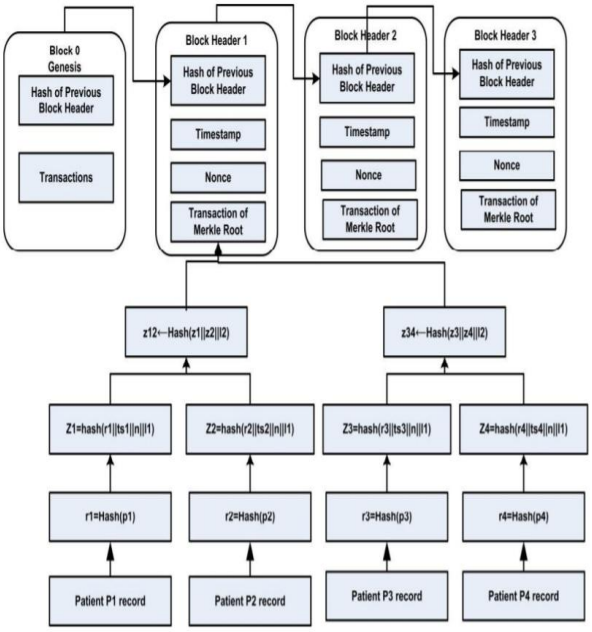

Fig. 3: Context-based Merkle Tree(CBMT) with Temporal Shadow

SeFra- Mining process:- The main work of the miner is to create a block and store the transactions; miner repeatedly tries to solve the mathematical puzzle until it gets to succeed. The miner tries to solve the mathematical puzzle by run the block header metadata through the hash function, just evolving the 'nonce value,' which impacts the hash value. If the hash is less than the target value, then the hash value is passed to all the peers, and all the peers validate it; if the hash value is correct, then the block is appended in the blockchain. This process is computationally expensive. The process of the block appended with the blockchain is explained in Fig. 3.

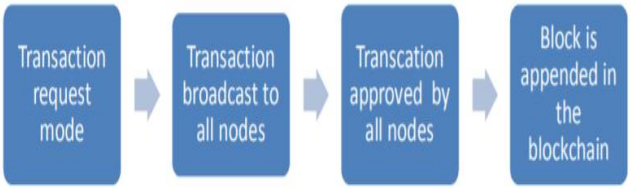

Fig. 4: Miner Validates the Transaction and Deployed in the Blockchain

The miner finds the hash that matches with the target, and the ether will be given as a reward for the miner and broadcast to the entire nodes to validate and maintain the copy of the ledger. The peer which solved the puzzle first will get the reward as ether. If one miner finds the result, then remaining miner work for the remaining block. In Ethereum blockchain, it takes 12-15sec to

find the block. It can handle 15 transactions per second. Ethereum block size depends on the gas limit, and it varies from block to block. In the proposed system, the researcher will act as a miner, and anonymized data will get as a reward. For example, miner1 find the answer for a mathematical puzzle, and a remaining miner will work for the next block. Once a miner finds the answer, then broadcast the value to all the miner, which is validated by all the peer.

The developer has to focus on six attributes while developing a Smart Contract.

i) Agreement identification Developers should know the agreement that supports everyone. Likewise incorporates the potential terms of exchange of rights and the conditions for swapping resources. For, eg. Everyone should accept the agreement like a patient, doctor, billing, insurance, Etc.

ii) Condition Setting The developer finds the condition based on the agreement. If the condition achieves automatically, it should respond. For, eg. Set to who wants to share the record.

iii) Business Logic Coding Developers develop code for the event-based trigger. When the condition occurs, automatically trigger, or response occurs. For example, if the condition met, then it allows the user to access or deny access.

iv) Digital Signature The digital signature used for verification purposes, and it is unique for all parties. For, eg. The doctor is one of the authorized users to access the record. The authorization ensured with a digital signature.

v) Executing Processes After verification, the Smart Contract completed, and results recorded for review and consistency.

vi) Updating the Network After the contract executed, each node updates a similar state. From that point onward, just the new updates can be added to the agreement and transfer the bytecode to the blockchain.

5. SIMULATION RESULT

The Integrity of the electronic health record ensured with the help of active hash function by appending temporal shadow properties before hashing. The integrity of the transaction is measured by comparing it with the Personalized Micro Ledger(PML) and without Personalized Micro Ledger(PML).

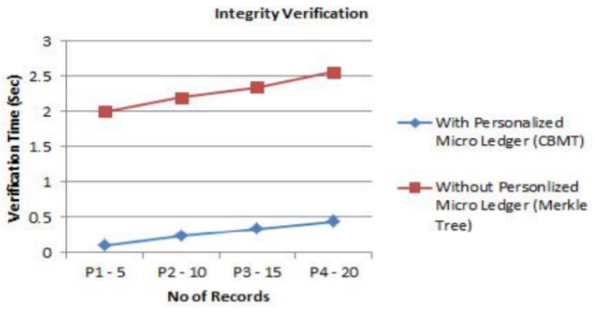

Fig. 5: Verification of Transaction

The time taken to check the integrity of the transaction explained in Fig. 5. The X-axis represents the number of records, and the y-axis refers to verification time measured in terms of the second. The Temporal Hash Signature(THS) takes less verification time when compared with the existing system.

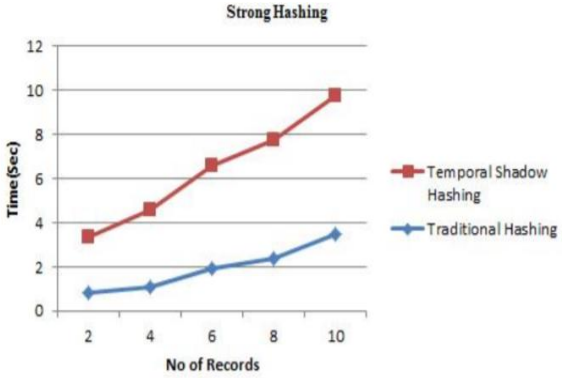

Fig. 6: Strong Hashing

The comparison of temporal shadow hashing and traditional hashing shown in Fig. 6. The X-axis represents no records, and Y-axis represents modification time (sec). The time taken to change the transaction is high when compared to existing work. The changing the transaction is difficult in blockchain, but still, the proposed work is more secure by providing a strong hash function. Each transaction appended with temporal properties; this makes the transaction more secure.

6. CONCLUSION

The Proposed work, Secure framework(SeFra) designed through Progressive temporal blockchain, which enhances the security of the eHealth record. The research work focused on data integrity, authentication, confidentiality, auditability, and privacy towards achieving users' trust and acceptance of eHealth systems. The proposed system supports the Interoperability and handling the scalability issues with the help of temporal properties. The permissioned blockchain decentralized network management system which allows people to share the information in a trustworthy manner with the temporal properties along with HL7 specification. The integrity of the eHealth record ensured with the help of Context-based Merkle Tree(CBMT). The security of the eHealth record achieved through Context-based Merkle Tree with temporal properties. Each record appended with the temporal property before hashing the record, so strong hash function was applied, this provides high security. It is difficult for the attacker to find the hash value for the given input. The authentication of the eHealth record done with Contextbased Access Control(CBAC) in the Smart Contract.

7. REFERENCES

[1] Cong Feng, Liang Tan, Huan Xiao, Keping Yu, Xin Qi5, Zheng Wen and You Jiang, "PDKSAP : Perfected Double-Key Stealth Address Protocol without Temporary Key Leakage in Blockchain", International Conference on Communications in China (ICCC Workshops), IEEE 2020.

[2] Zhang, Y., Kasahara, S., Shen, Y., Jiang, X. and Wan, J. (2019), 'Smart Contract-Based Access Control for the Internet of Things', IEEE Internet of Things Journal, 6(2), 1594– 1605.

[3] Zhang, A. and Lin, X. (2018), 'Towards Secure and Privacy-Preserving Data Sharing in e-Health Systems via Consortium Blockchain', Journal of Medical Systems, 42(8), 1-18.

[4] Xu, R., Chen, Y., Blasch, E. and Chen, G. (2019), 'Exploration of a blockchain-enabled decentralized capability-based access control strategy for space situation awareness', Optical Engineering, 58(4), 1-16.

[5] Xia, Q.I., Sifah, E.B., Asamoah, K.O., Gao, J., Du, X. and Guizani, M. (2017), 'MeDShare: Trust-less medical data sharing among cloud service providers via blockchain', IEEE Access, 5(1), 14757-14767.

[6] Liu, V., Musen, M. and Chou, T. (2015), 'Data Breaches of Protected Health Information in the United States'. 313(14), 1471-1473.

[7] Liu, W., Zhu, S. S., Mundie, T. and Krieger, U. (2017), Advanced block-chain architecture for e-health systems, in 'Proceedings of the IEEE 19th International Conference on e-Health Networking, Applications and Services (Healthcom)'. IEEE, pp. 1-6

[8] Hillestad, R., Bigelow, J., Bower, A., Girosi, F., Meili, R., Scoville, R. and Taylor, R. (2005), 'Can 1000 Electronic medical record Systems Transform Health Care? Potential Health Benefits, Savings, And Costs, Health Affairs, 24(5), 1103-1117.

[9] Hu, J., Chen, H.H. and Hou, T.W., 2010. A hybrid public key infrastructure solution (HPKI) for HIPAA privacy/security regulations. Computer Standards & Interfaces, 32(5- 6), 274-280.

[10] Dolin, R., Alschuler, L., Boyer, S., Beebe, C., Behlen, F., Biron, P., and Shabo (Shvo), A. (2006), 'HL7 Clinical Document Architecture', Journal of the American Medical Informatics Association, 13(1), 30-39.

[11] Brink, A., Messina, A., Feldman, C., Richards, G., Becker, P., Goff, D., Bauer, K., Nathwani, D. and van den Bergh, D. (2016), 'Antimicrobial stewardship across 47 South African hospitals: an implementation study', The Lancet Infectious Diseases, 16(9), 1017-1025.

[12] Cachin, C. (2016), Architecture of the Hyperledger Blockchain Fabric, in 'Workshop on distributed cryptocurrencies and consensus ledgers'. IBM, pp.1–4.