A Framework for Blockchain-based Smart Health System

Mousa Mohammed Khubrani[a]

[a]Department of Computer Science, College of Computer Science & IT, Jazan University, Jazan/KSAPhD scholar in Computer

Article History: Received: 10 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 20 April 2021

Abstract: Electronic health record (EHR) is patient data that store health information in digital format. Patient-centred data enables an authorized user to access the data at any time, anywhere. E-healthcare provides increasing social benefits, health benefits and reduced medical errors. The most difficult aspect of improving the use of IT frameworks in healthcare is the security issues of the systems that store health information. In the health sector, Blockchain is a revolution that may bring considerable changes in offered health services. It solves the issue of adapting and building a health care system in the healthcare community, pharmaceutical industry and insurance companies. This paper presents a framework for securing healthcare data. Public Ledger, private ledger, smart contracts and context-based access control are the basic principles behind the proposed framework. This proposed model further provides interoperability, secure storage, and reliable access to patient's data.

Keywords:*Blockchain, Healthcare, Smart Contracts, Distributed Ledger, Hashing, Electronic Health Record*

1. Introduction

Patient data that store personal health information in digital format is the core of electronic healthcare. Data focused on patients allow any approved user to access the data from anywhere and at any time. The electronic health system also saves money by minimizing the efforts and storage space (Simpson, 2015). Increased social and health benefits, as well as reduced chances of mistakes, are achieved through e-healthcare. The digital reproduction of paper-based health documents is the electronic medical record (EMR). EMR further evolved into EHR that help the various stakeholders to share medical information quickly. The primary goal is to exchange medical information between multiple doctors and diverse stakeholders, including the Government, patients, health service providers, insurers (Menachemi & Collum, 2011).

Healthcare Information and Management Systems Society, Inc. (HIMSS) is a non-profit corporation to extend health protection, security and convert health information through information technology. The main operation domain of HIMSS is North America, Asia Pacific, the UK and the Middle East. HIMSS' primary objective is to develop worldwide e-healthcare. Healthcare problems include attackers trying to modify health figures, leading to serious health system harm and severe attacks, such as a ransomware attack and a lack of cybersecurity. The challenge of increasing the use of IT frameworks in healthcare is probably security concerns when systems are supposed to have health information (Ermakova et al., 2013). The system includes the information security component (Samad et al., 2017)(Raghuvanshi et al., 2021). Researchers in (Avizienis et al., 2004) mention common health care security concerns such as privacy, approval and honesty. Following are the main requirements to consider the security of an EHR system:

1.1 Confidentiality

Confidentiality is one of the core tasks of the healthcare provider. The health data are confidential information that must be protected against unauthorized access (Bigini et al., 2020). The system gives the approved user access to the information and requires the creation of a trusted environment for the patient to seek healthcare. According to the 1997 HIPAA act, the patient's health information had to be protected (Shuaib, Alam, Shabbir Alam, et al., 2021a).

1.2 Integrity

Keeping eHealth record integrity is important because it is used to locate patients and pursue them when moving from one provider to another. In order to decide the level of patient care, the integrity of information in medical services becomes essential. It delivers precise and unaltered health information throughout the life cycle. It maintains data accuracy, consistency and reliability (M U Bokhari & Alam, 2013).

1.3 Authorization

The EHR system agrees to provide access to the record and to be recorded by physicians, thereby improving the process of medical recording for an authorized user (Shuaib, Alam, & Daud, 2021). The organizations of medical services are required to alleviate these risks and are responsible for authorization. It is important to mention the access control mechanisms to protect the privacy of the patient. The authorization process is limited to external users. The system needs to determine eHealth data access privileges and the user responsibilities.

1.4 Availability

The availability is an element that requires a framework to allow authorized users to open, use and access a record. It means that, if required by an approved user, the information is constantly accessible to customers. The

system must ensure that health records are available by preventing interruption to service due to hardware failures, improvements to the framework and safeguard the availability of health records (Mohammad Ubaidullah Bokhari et al., 2014).

The remaining part of this articles has been divided into three sections. Section 2 contains related work; section 3 contains blockchain description and advantages of using Blockchain in healthcare data security. Section 3 also contains a framework to secure healthcare data using Blockchain. Section 4 concludes the paper.

2. Literature Review

The patient's health information is generated and encrypted by the patient's public key (Shen et al., 2018). Based on unique information such as an e-mail address, etc., the public key is created. The patient now wishes to access the medical record, then authenticates the private key linked with the public key. This key is used only for a specific health record (Benet et al., 2018).

The authorized key issuer creates a public key and the user's private key. An access structure over attributes is linked with every private key. Doctors enable the decryption of data by private key; they should also comply with the access policy during the decryption process. A monotonic access structure like AS, OR, Etc. is kept in the attribute-based encryption process (Qian et al., 2015).

Techniques for attribute-based encryption policy permit non-monotonic access systems. The health record is encrypted and linked to a number of attributes, which are each private key linked to the attributes access structure. The physician attempts to access the encrypted record of health. It is only acceptable if the ciphertext has qualities and the access structure associated with a private key is satisfied (Shi et al., 2015). The downside is that the encrypter cannot determine who is able to decipher the data and that the data proprietor must also trust the key issuer. These problems have been overcome by encryption based on Ciphertext attributes.

The fine-grained encryption technology is used to encrypt the health record and preserve the access policies of each health record. In ciphertext, a user's private key is associated with the set of characteristics, and ciphertext has to do with attribute-base access policies (Jiang et al., 2018). The doctor should decrypt this ciphertext, for example, a doctor or patient trying to access the health record, access if and only if the doctor's attribute fulfils the access policy for the ciphertext.

Health records are encrypted and stored in the cloud by following these methods. It is the individual responsibility of the cloud servers to safeguard health information in the cloud. As the patient maintains confidential information in the cloud, it is important for the cloud service provider to keep the data secure and reliable (Shuaib, Alam, et al., 2020).

Although patient data are performed with various encryption techniques and stored in the cloud. The one central node is the most important portion of the job in a centralized network (Alam et al., 2019) . However, eHealth data in the cloud is inadequate since the cloud has confidence in the third party and a single failure point (Abdus et al., 2018). Nodes are distributed to other nodes in a decentralized framework. The distributed framework provides a stable and highly usable system and a fault-tolerant mechanism that stops the issue of a single point of failure. Included in the cloud is the accuracy of the eHealth record and done with Blockchain (Tanwar et al., 2020).

3. Blockchain for Securing eHealth Data

Blockchain is a new technology that is aggressively being used in many sectors, including healthcare, that guarantees secure and immutable record. Blockchain was first introduced by a researcher named Satoshi Nakamoto in his research work on the cryptocurrency Bitcoin (Nakamoto, 2008). Blockchain is a particular form of Distributed ledger that provides a distributed peer-to-peer network. The distributed peer-to-peer network is presented in Figure 1. There is no central database in this novel aspect of the distributed blockchain network. Decentralization, openness and immutability are the three main attributes of the Blockchain. All transactions in the blocks are recorded and stored in the Blockchain after each node has verified it. The list of transactions is included in each block (Shuaib, Alam, Shabbir Alam, et al., 2021b). The blocks are arranged in chronological order. It is a secure database where the network, not a single user, is operated (Shuaib, Alam, Shahnawaz Nasir, et al., 2021)(Shuaib, Daud, et al., 2020).

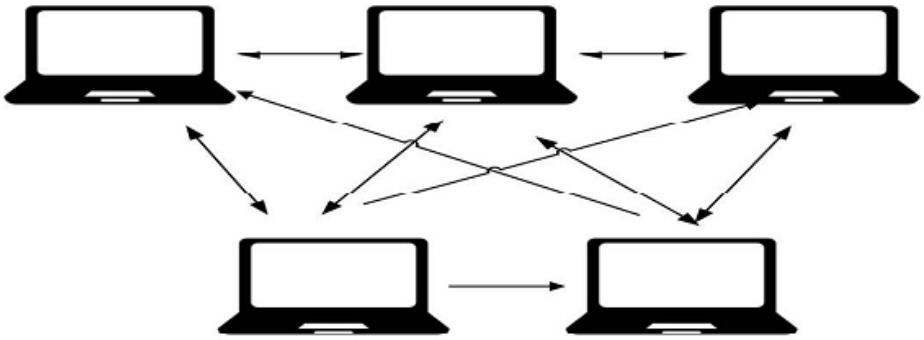

Figure 1. Peer-to-Peer (P2P) Network

The list of transactions called the block, linked with each other, generated using encryption techniques. Every block is connected to the previous header of the block. Block headers and transactions are contained in every block. The block header keeps the Hash of the earlier block header, timestamp, nonce and root value of Merkle. There can be no modification to the data stored on the Blockchain.

Blockchain is a joint transaction ledger. It enables members of a group to share data without the involvement of third parties and to monitor the transaction. It is stored over several machines rather than storing the record on a single server, making the information very difficult to mess with or delete. Most medical care companies are planning to implement Blockchain technology because of the decentralized database and inherent attributes. The public key encryption is used to produce unchangeable, timestamped content in Blockchain. All nodes receive the blockchain data.

In the health sector, Blockchain is a revolution and will bring significant changes in health services. It solves the issue of adapting and building a health care system in the healthcare community, pharmaceutical industry and insurance companies. Today, it is difficult to track the patients' data; the doctor does not have the right to access the medical record in due course because of deadly medical mistakes. Clinical preliminary data is difficult to get and share and are also susceptible to various types of hacks and leaks that can endanger the life and social value of a patient. A fundamental component of a blockchain is Merkle trees. A Merkle tree uses SHA-256 hazelnuts in a tree structure to associate information. Every record of patients is hashed and stored on the block. Once you have generated the transaction and saved it in the block, it is difficult to alter.

3.1 Blockchain-based Framework for Secure eHealthcare Data

General Public Ledger, personalized micro-ledge, smart contracts and context-based access control are the basic principles behind the proposed framework. It uses the Hash signature to monitor the authentication. Finally, in the Blockchain, the hash value is saved. Figure 2 describes the usefulness of the framework.

HL7 (Health Level Seven International) is a set of principles to create electronic health records, formats and definitions (EHR). HL7 principles have been developed and declared by the IT standard and adopted models of medical services in human services. HL7 was established in 1987, and the American National Standards Institute recognized this standard in 1994. HL7 helps global health care IT interoperability by guiding how standards should be implemented. The "7" belongs to Layer 7 of the OSI Reference Model.

The HL7 guidelines discuss and provide a format for exchange, decision-making, syntax, universal definition of health data and clinical records, electronic health, and personal health records. HL7 guidelines allow for information exchange. The HL7 standard is used for the transfer of eHealth records among two providers. HL7 is an international standard for transferring health record from software to different health providers (Dolin et al., 2006). The health system engages with one another establishes the approach, rules and standards. The other HL7 standard, such as Fast Healthcare Interoperability Resources (FHIR), is standard for resource exchange (Saripalle et al., 2019).

The InterPlanetary File System (IPFS) is a protocol and distributed file system (Singhal et al., 2020). The hash value of each record is shown. It swaps data within the Git repository and eliminates the data redundancy through the BitTorrent swarm (Benet, 2014). The relationship of the node in IPFS as a hash is carried out by Merkle DAG (Directed Acyclic Graph).

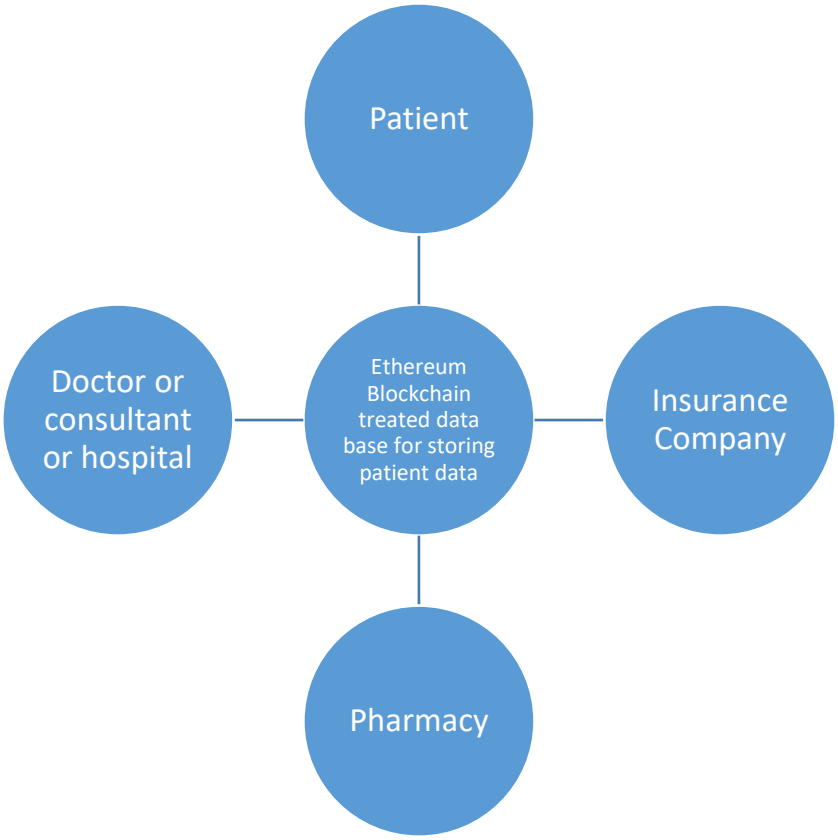

Figure 2. Blockchain-based Framework for securing eHealthcare Data

Each transaction relies on the next subsequent transaction in a progressive time-blockchain to fulfil the final transaction. Before the transaction has been completed, the length of the hash chain agreed prior to hashing should be attached to the concatenated hash value of the child node. With the help of the signature, each transaction was checked. Here, the Temporary Hash Signature (THS) without the assistance of a third party is used for authentication. Any modification will almost immediately be identified as long as the signature of the monitor changes.

4.Conclusion

The proposed theoretical blockchain-based framework highlights the concepts and techniques used and referenced for developing a blockchain-based reliable medical ecosystem and defines how complicated medical processes can be streamlined. We propose an innovative approach to medical record management through smart contracts that provide auditability, interoperability, and accessibility. In health data management, we have suggested potential uses of blockchain technology. We have adopted a data management and sharing system based on medical needs. It is possible to ensure that access to EHR data is guaranteed through blockchain technology, privacy, security, availability and refined control.

The ultimate aim of strengthening health procedures and patient records is to introduce Blockchain using smart contracts to simplify processes, minimize administrative burdens, and eliminate intermediaries. Blockchain may further strengthen patients' control over their personal data and support researchers in data collection, processing, and sharing health data reliably and securely while maintaining anonymity.

References

1. Abdus, S., Shadab, A., Mohammed, S., & Mohammad.Ubaidullah, B. (2018). *Internet of Vehicles (IoV) Global*
2. *Development, March, 4037–4040.*
3. Alam, S., Shuaib, M., & Samad, A. (2019). *A Collaborative Study of Intrusion Detection and Prevention Techniques in Cloud Computing.* In *Lecture Notes in Networks and Systems* (Vol. 55, pp. 231–240).*https://doi.org/10.1007/978-981-13-2324-9_23*
4. Avizienis, A., Laprie, J.-C., Randell, B., & Landwehr, C. (2004). *Basic concepts and taxonomy of dependable and* secure computing. IEEE Transactions on Dependable and Secure Computing, 1(1), 11–

33.

5. Arunkarthikeyan, K., Balamurugan, K., Nithya, M. and Jayanthiladevi, A., 2019, December. Study on Deep Cryogenic Treated-Tempered WC-CO insert in turning of AISI 1040 steel. In 2019 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE) (pp. 660-663). IEEE.
6. Arunkarthikeyan K., Balamurugan K. & Rao P.M.V (2020) Studies on cryogenically treated WC-Co insert at different soaking conditions, Materials and Manufacturing Processes, 35:5, 545-555, DOI: 10.1080/10426914.2020.1726945
7. Balamurugan, K., 2020. Compressive Property Examination on Poly Lactic Acid-Copper Composite Filament in Fused Deposition Model–A Green Manufacturing Process. Journal of Green Engineering, 10, pp.843-852.
8. Balamurugan, K., Uthayakumar, M., Ramakrishna, M. and Pillai, U.T.S., 2020. Air jet Erosion studies on mg/SiC composite. Silicon, 12(2), pp.413-423.
9. Benet, J. (2014). *Ipfs-content addressed, versioned, p2p file system. ArXiv Preprint ArXiv:1407.3561.*
10. Benet, J., Dolin, R. H., Alschuler, L., Boyer, S., Beebe, C., Behlen, F. M., Biron, P. V, Shabo, , Jiang, S., Cao, Wu, H., Yang, Y., Ma, M., He, J., Shi, Y., Zheng, Q., Liu, J., Han, Z., Qian, H., … Zarnekow, R. (2018). *A secure data sharing using identity-based encryption scheme for e-healthcare system. 2018 Ieee International Conference on Smart Computing (Smartcomp), 14(1), 221–231*
11. Bigini, G., Freschi, V., & Lattanzi, E. (2020). *A review on blockchain for the internet of medical things: Definitions, challenges, applications, and vision. In Future Internet (Vol. 12, Issue 12, pp. 1–16). MDPI AG. https://doi.org/10.3390/fi12120208*
12. Bigini, G., Freschi, V., & Lattanzi, E. (2020). *A review on blockchain for the internet of medical things: Definitions, challenges, applications, and vision. In Future Internet (Vol. 12, Issue 12, pp. 1–16). MDPI AG. https://doi.org/10.3390/fi12120208*
13. Bokhari, M U, & Alam, S. (2013). BSF-128: *a new synchronous stream cipher design.*
14. *Proceeding ofInternational Conference on Emerging Trends in Engineering and Technology, 541–545.*
15. *Bokhari, Mohammad Ubaidullah, Alam, S., & Hasan, S. H. (2014). A Detailed Analysis of Grain family of Stream Ciphers. International Journal of Computer Network & Information Security, 6(6).*
16. *Deepthi, T., Balamurugan, K. and Balamurugan, P., 2020, December. Parametric Studies of Abrasive Waterjet Machining parameters on Al/LaPO4 using Response Surface Method. In IOP Conference Series: Materials Science and Engineering (Vol. 988, No. 1, p. 012018). IOP Publishing.*
17. *Dolin, R. H., Alschuler, L., Boyer, S., Beebe, C., Behlen, F. M., Biron, P. V, & Shabo, A. (2006). HL7*
18. *clinical document architecture, release 2. Journal of the American Medical Informatics Association, 13(1),30–39.*
19. *Ermakova, T., Fabian, B., & Zarnekow, R. (2013). Security and privacy system requirements for adopting cloud computing in healthcare data sharing scenarios.*
20. *Garikipati, P. and Balamurugan, K., 2021. Abrasive Water Jet Machining Studies on AlSi 7+ 63% SiC Hybrid Composite. In Advances in Industrial Automation and Smart Manufacturing (pp. 743-751). Springer, Singapore.*
21. *Jiang, S., Cao, J., Wu, H., Yang, Y., Ma, M., & He, J. (2018). Blochie: a blockchain-based platform for healthcare information exchange. 2018 Ieee International Conference on Smart Computing (Smartcomp), 49–56.*
22. *Latchoumi, T.P., Dayanika, J. and Archana, G., 2021. A Comparative Study of Machine Learning Algorithms using Quick-Witted Diabetic Prevention. Annals of the Romanian Society for Cell Biology, pp.4249-4259.*
23. *Latchoumi, T.P., Vasanth, A.V., Bhavya, B., Viswanadapalli, A. and Jayanthiladevi, A., 2020, July. QoS parameters for Comparison and Performance Evaluation of Reactive protocols. In 2020 International Conference on Computational Intelligence for Smart Power System and Sustainable Energy (CISPSSE) (pp. 1-4). IEEE.*
24. *Menachemi, N., & Collum. (2011). Benefits and drawbacks of electronic health record systems. Risk Management and Healthcare Policy, 4, 47.* https://doi.org/10.2147/RMHP.S12985
25. *Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.*
26. *Qian, H., Li, J., Zhang, Y., & Han, J. (2015). Privacy-preserving personal health record using multi-authority attribute-based encryption with revocation. International Journal of Information Security, 14(6), 487–497.*
27. Raghuvanshi, A., Kumar Singh, U., Shuaib, M., & Alam, S. (2021). *An investigation of various applications and related security challenges of Internet of things. Materials Today: Proceedings.https://doi.org/10.1016/j.matpr.2021.01.821*
28. Samad, A., Shuaib, M., & Rizwan Beg, M. (2017). *Monitoring of Military Base Station using Flooding and ACO Technique: An Efficient Approach. International Journal of Computer Network and Information Security, 9(12), 36–44. https://doi.org/10.5815/ijcnis.2017.12.05*

29. Saripalle, R., Runyan, C., & Russell, M. (2019). *Using HL7 FHIR to achieve interoperability in patient health record. Journal of Biomedical Informatics, 94, 103188.*

30. Shen, W., Qin, J., Yu, J., Hao, R., & Hu, J. (2018). *Enabling identity-based integrity auditing and data sharing with sensitive information hiding for secure cloud storage. IEEE Transactions on Information Forensics and Security, 14(2), 331–346.*

31. Shi, Y., Zheng, Q., Liu, J., & Han, Z. (2015). *Directly revocable key-policy attribute-based encryption with verifiable ciphertext delegation. Information Sciences, 295, 221–231.*

32. Shuaib, M., Alam, S., & Daud, S. M. (2021).*Improving the Authenticity of Real Estate Land Transaction Data Using Blockchain-Based Security Scheme (pp. 3–10). Springer, Singapore. https://doi.org/10.1007/978-981-33-6835-4_1*

33. Shuaib, M., Alam, S., Mohd, S., & Ahmad, S. (2020). *Blockchain-Based Initiatives in Social Security Sector. EAI 2nd International Conference on ICT for Digital, Smart, and Sustainable Development (ICIDSSD), 8.*

34. Shuaib, M., Alam, S., Shabbir Alam, M., & Shahnawaz Nasir, M. (2021a). *Compliance with HIPAA and GDPR in blockchain-based electronic health record. Materials Today: Proceedings. https://doi.org/https://doi.org/10.1016/j.matpr.2021.03.059*

35. Shuaib, M., Alam, S., Shabbir Alam, M., & Shahnawaz Nasir, M. (2021b). *Self-sovereign identity for healthcare using blockchain. Materials Today: Proceedings. https://doi.org/10.1016/j.matpr.2021.03.083*

36. Shuaib, M., Alam, S., Shahnawaz Nasir, M., & Shabbir Alam, M. (2021). *Immunity Credentials using Self-Sovereign Identity for combating COVID-19 Pandemic. Materials Today: Proceedings. https://doi.org/10.1016/j.matpr.2021.03.096*

37. Shuaib, M., Daud, S. M., Alam, S., & Khan, W. Z. (2020). *Blockchain-based framework for secure and reliable land registry system. Telkomnika (Telecommunication Computing Electronics and Control), 18(5), 2560–2571. https://doi.org/10.12928/TELKOMNIKA.v18i5.15787*

38. Simpson, K. R. (2015). *Electronic Health Records. MCN, The American Journal of Maternal/Child Nursing, 40(1), 68. https://doi.org/10.1097/NMC.0000000000000089*

39. Singhal, N., Sharma, M. K., Samant, S. S., Goswami, P., & Reddy, Y. A. (2020). *Smart kyc using blockchain and IPFS. In Lecture Notes in Electrical Engineering (Vol. 643, pp. 77–84). Springer. https://doi.org/10.1007/978-981-15-3125-5_9*

40. Tanwar, S., Parekh, K., & Evans, R. (2020). *Blockchain-based electronic healthcare record system for healthcare 4.0 applications. Journal of Information Security and Applications, 50, 102407. https://doi.org/https://doi.org/10.1016/j.jisa.2019.102407*

41. Yarlagaddaa, J., Malkapuram, R. and Balamurugan, K., 2021. Machining Studies on Various Ply Orientations of Glass Fiber Composite. In Advances in Industrial Automation and Smart Manufacturing (pp. 753-769). Springer, Singapore.

42. Yookesh, T.L., Boobalan, E.D. and Latchoumi, T.P., 2020, March. Variational Iteration Method to Deal with Time Delay Differential Equations under Uncertainty Conditions. In 2020 International Conference on Emerging Smart Computing and Informatics (ESCI) (pp. 252-256). IEEE.