BLOCKCHAIN BASED SECURITY PRESERVING FRAMEWORK FOR HEALTHCARE4.0 USING HYPERLEDGER FABRIC

Jeevanantham M[1], Dev Anand S[2], Pranav Anand V[3], Kishore R[4], Padmashree A[5], Tharani Priya R[6]

[1,2,3,4,5] Bannari Amman Institute of Technology, [6] Capgemini Technology Services India Ltd

Abstract

Digital form of health records of the patients is called the electronic Health Record (EHR). These records highly contribute to enhance healthcare, improve clinical practices and encourage clinical research. However, the traditional environment uses client server architecture to maintain these records and make it inaccessible by the patients and the healthcare providers. It is the basic rights patients to understand how the data are stored and the purpose for which it is being used. Since these data are accessed over the internet, it is easy for the hackers or the unauthorized entities to gain access over the data and cause breaches. It is also important to eliminate third party interference and enable direct access between the patients' records and the healthcare providers to perform better diagnosis. The Blockchain technology is proposed to protect the Electronic Health Records of the patients that ensures security and privacy of healthcare data. The smart contract over decentralized peer-to-peer system allows distrustful entities to transact data securely without any third party intervention. Access Control is achieved by implementing permissioned Distributed Ledger Technology using Hyperledger Fabric and the performance of the system is evaluated using Hyperledger Caliper. Performance metrics for resource consumption including CPU, memory and network utilization and disk writes are evaluated.

Keywords: Blockchain, Electronic Health Records, Hyperledger Fabric, Healthcare, Distributed ledger technology, Security.

1. Introduction

From centuries ahead, there has been developments in the Industrial standards. During the first industrial revolution, Industry 1.0 focused on the usage of steam power and mechanization of production to increase the productivity. The second industrial revolution, Industry 2.0 focused on the usage of electric energy and assembly line production to promote mass production at lower cost. The third industrial revolution, Industry 3.0 introduced partial automation using programmable controls. But, with the evolution of internet and various wireless technologies, current form of Industries, i.e., Industry 4.0 evolved. The networking of all the systems leads to cyber-physical production systems and this leads to development of smart factories. Advances in Industries allow interaction with billions of objects across the world.[1] Today, these smart technologies are being used in the healthcare industry.

Healthcare industry also found its growth along with other industries. During Healthcare 1.0, due to lack of resources that coordinate with the digital system, the healthcare organizations used paper-based prescriptions and reports that consumed more time and cost. During the next era Healthcare 2.0, the healthcare system was created using health details and information technologies. Doctors used digital tracking along with imaging systems to analyze patients' health. Healthcare providers began to use social media to share knowledge and information through different groups and communities. Cloud servers were used to store the patients' data, mobile devices were used to provide access to the patient records. However, in many cases, the patient's privacy was compromised. During Healthcare 3.0, patient healthcare records were customized and delivered. Simple user interfaces, Electronic Healthcare Records (EHRs), wearable and implantable devices and ubiquitous healthcare tracking systems were introduced. Social media channels were used to store the data and to transfer the information between the patients and healthcare providers [2] .With the advent usage of today's technology, we are now at the Healthcare 4.0 era which mainly focuses on providing personalized healthcare.

Security and privacy are the important concerns in all applications. Healthcare industry is not an exemption. Being in medical advancements, the industry stores all the data as Electronic Health Records. It is easy for unauthorized actors to acquire access to the data. It is necessary to protect these data and HIPAA has suggested best practices for data protection

by healthcare organizations to preserve privacy and security of health records of the patients [6]. It also reports that, between 2009 and 2020, nearly 3,705 healthcare data breaches have been reported. The security requirements in the healthcare industry include confidentiality, integrity, ownership, privacy, authentication, non-repudiation, auditing, access control, data freshness, anonymity and secure data transit.

2. Related work

Yup et al. [18] proposed HGD architecture where the patient will have the full access control over their data. The ICS schema was used to easily organize the data. Secure multi-party computing was used to prevent intrusion. Zhang et al. [19] proposed a secure system for social network based healthcare system. They used IEEE 802.15.6 to enable authenticity and blockchain to share data between nodes. MeDShare system was suggested by Xia, Qi et al. [20], where the cloud service providers were able to achieve data provenance while sharing medical data in a trust-less environment. Liang et al. [21] deployed a blockchain based mobile application to collect healthcare data and stored it in cloud for data sharing. Large datasets were handled using tree-based data processing. Jiang et al. [22] proposed loosely - coupled blockchain based data exchange model and combined off-chain storage and on-chain verification to enhance data privacy. Li et al. [23] proposed data preservation system (DPS) using blockchain for healthcare data using Ethereum to perform memory management. Fan et al. [24] explored MedBlock, an information management system using consensus and distributed ledger to store patients' data. Wang and Song [25] proposed attribute-based/identity-based encryption and signature (C-AB/IB-ES) to encrypt medical data and to create digital signature for medical insurance application to ensure integrity and traceability of data. Guo, R. et al. [26] proposed an attribute-based signature scheme with multiple authorities to handle healthcare data using blockchain. Uddin et al. [27] designed a blockchain architecture with a patient centric agent to manage the components and a lightweight communication protocol was used to enhance security of data. Granular Access Authorization supporting Flexible Queries based blockchain architecture was proposed by Zhang and Poslad to support granular access control in Electronic health Records[29]. The computational performance was improved by using public key infrastructure. Plug and play optimization technique was proposed by Gorenflo et al. [30] to increase the transaction throughput in Hyperledger Fabric on focusing on performance bottlenecks beyond the consensus. The architecture was proposed to reduce computational and I/O overhead too. Griggs et al. [31] proposed Ethereum based private blockchain to remove the risks in remote monitoring system in medical field ensuring safe and secure access of patients' data from distant locations. Whereas, Ivan [32] proposed public blockchain based personal health record using encryption. The patients were given access rights and share their medical data with any medical personals. With the same idea and to avoid the intervention of any third party, Chen et al. [33] proposed a framework that integrated blockchain and cloud technology to enable secure exchange of health data. Wang et al. [34] proposed a blockchain framework for artificial intelligence based healthcare systems that tracks the therapeutic procedures and the computational trials for clinical decision making, to estimate the accurateness of diagnosis and efficacy of treatment. In [35], Shubbar proposed a blockchain framework that uses smart contacts to secure the data of cancer patients both in public medical cares and in private homes of the patients. Ianculescu et al. suggested a blockchain-based platform called ProActive Aging [36] to support the lives of aged people. The DNA data are stored on blockchain to perform research at genetic levels. Eric Affuldadzie et al. [37] proposed a framework with fuzzy VIKOR based method for ranking and validating the usefulness of online health records. It ensured reliability and usefulness of the health information.

3. Proposed approach

The Electronic Health records of the patient are typically shared among different departments of a hospital say, clinic, pathology laboratory, radiology, pharmacy, dietary etc.,. These information are accessed across all the departments within the hospital to analyze the condition of the patient before suggesting the prescription. However, these records are not shared among other hospitals or organizations unless the patients maintain a personal copy of the same. A model is proposed in which multiple organizations agree to share upon the patients' details in a secured channel within a consortium. The model uses Public Key Infrastructure (PKI) to securely share the data.

3.1 System architecture

Blockchain based Electronic Health Record (EHR) is proposed using Hyperledger fabric. It is a permissioned open-source distributed ledger technology (DLT) platform. The main components are Submitting client, Peer, Orderer, Certificate Authority (CA), Chaincode and Consensus [49] .The system includes actors like patients, doctors, nurses, pharmacist, dietitian and radiographer. Each organization has its own Certificate Authority (CA) that issues certificates

based on Public Key Infrastructure (PKI) to all the members and the nodes. It includes a root certificate and an enrolment certificate. When an actor tries to insert new data or monitor the update, a new transaction is created and the peer nodes are to endorse the transaction using consensus protocol. It verifies, if the issuer is an authentic user by verifying the validity of the issuer. It also ensures that the transaction is not duplicated. Smart contracts are executed individually by each peer node to sign the transaction. The application sends the signed transaction to the orderer node [50]. The transactions are then converted into blocks and are updated to the ledger. Fig 1. shows the sequence involved in handling a transaction.

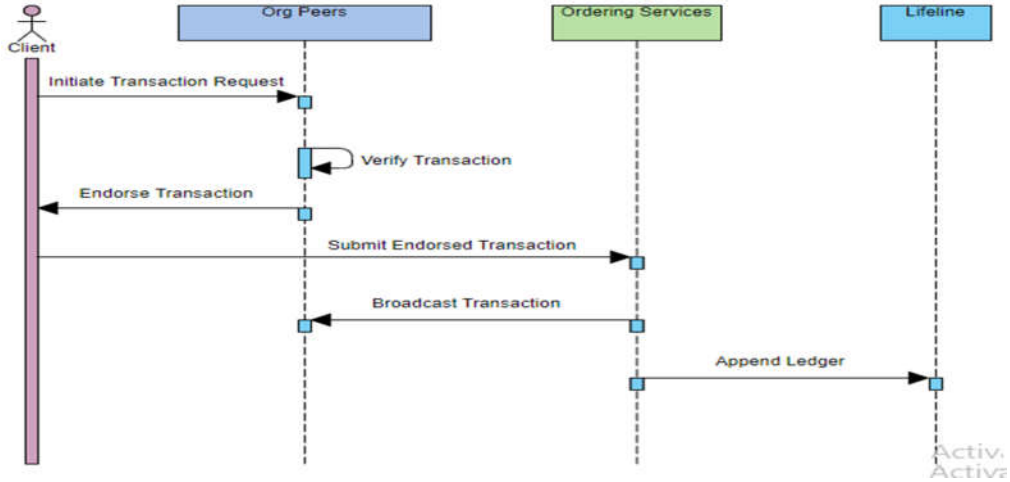

Fig 1. Sequence diagram for handling a new transaction

3.2 Proposed architecture

The proposed architecture depicted in fig.2 consists of two organizations R1 and R2 that works as a consortium over a channel C that is governed according to the Channel Configuration CC. Each organization has its own Certificate Authority (CA) and peer nodes. Each peer node has its own associated ledger that contains a block of data. The Network Configuration (NC) governs the entire network according to the policy rules of R1.The endorsing peers of both R1 and R2 are responsible for validating the new transaction. After verification, the transactions are sent to the ordering services (ODS) or simply the orderer peer which distributes the blocks to all peers connected to it. Gossip protocol is used to deliver the block to all the other peers in the blockchain.

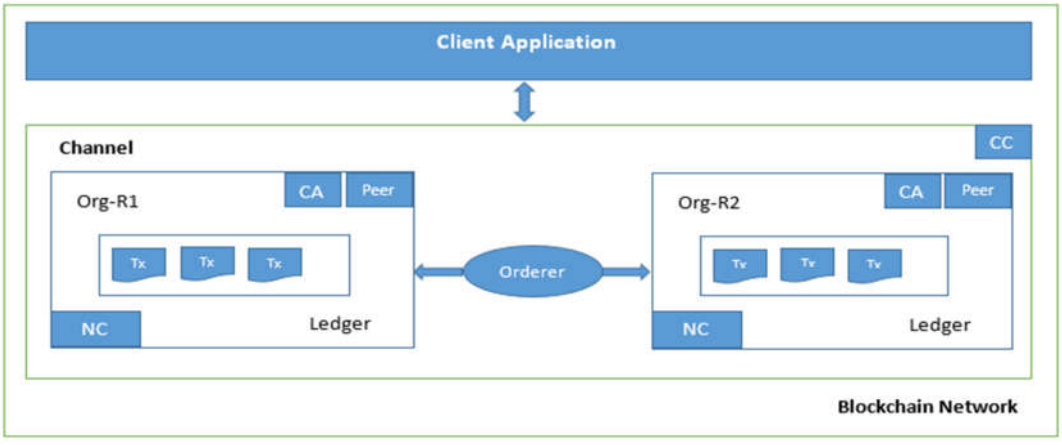

Fig 2. Proposed architecture

3.3 Deployment phase

The proposed model is deployed using Hyperledger fabric. It is an open source platform that uses permissioned distributed ledger. It helps to create transactions and to implement chaincode. The business network is modelled using

Hyperledger Composer that contains the transactions and the associated assets. It provides a consensus mechanism to provide secure interaction. Docker container is used to create, deploy and run hyperledger based networks.

3.4 Measurement phase

The performance metrics of the proposed model is measured using Hyperledger Caliper. It is a performance benchmark framework to measure performance of different use cases based on blockchain technology. It supports Hyperledger Besu, Ethereum, Hyperledger framework, FISCO BCOS etc. Transaction throughput and latency, read throughput and latency, resource consumptions like CPU, memory utilization, and network traffics can be measured using Caliper.

3.5 Performance analysis

A Simple benchmark to analyse the backend performance of the DLT is proposed using Hyperledger Caliper. Simple benchmark for Hyperledger Fabric for 2 organizations with 1 peer is proposed with the RAFT consensus protocol. The transaction mode is designed for 4 rounds with 1000 transactions per round. The rate of transaction is given as 50 to 250 per second.

The average consumption of CPU, memory, incoming and outgoing network traffic, memory read and memory write by different peers in the blockchain network is calculated.

3.6 Results and discussion

Table 1 shows the resource consumption for open transaction. The result shows that the orderer consumes minimum resources than the other peers. However it's the network traffic out is maximum than any other peers. It is also observed that the CPU utilization is more in peer0.org1.

Table 1. : Resource Consumption for open transaction

Name	RAM	CPU	Network Traffic in	Network Traffic out	Disk Write
peer0.org1	204.9MB	26.48%	6.3MB	3.6MB	8.5MB
peer0.org2	171.8MB	24.03%	6.3MB	3.5MB	8.5MB
peer1.org1	220.1MB	18.10%	6.0MB	420.2KB	8.4MB
peer1.org2	272.4MB	16.9%	6.1MB	424.0KB	8.5MB
orderer	64.4MB	8.18%	5.7MB	9.9MB	15.3MB

Table 2, shows the resource consumption for query operation, where disk read or disk write never consumes resource and it is observed that the network traffic of orderer node is minimum when compared with other peers. Table 3 shows the resource allocation for write transaction where the orderer consumes minimum resources.

Table 2. : Resource Consumption for query transaction

Name	RAM	CPU	Network Traffic in	Network Traffic out
peer0.org1	213.3MB	25.04%	6.2MB	6.5MB
peer0.org2	185.2MB	26.73%	6.6MB	7.0MB
peer1.org1	190.6MB	20.7%	6.3MB	6.2MB
peer1.org2	202.4MB	19.6%	6.2MB	6.3MB
orderer	116.7MB	0.51%	42.1KB	48.3KB

Table 3. : Resource Consumption for transfer transaction

Name	RAM	CPU	Network Traffic in	Network Traffic out	Disk Read	Disk Write
peer0.org1	220.2MB	20.48%	9.9MB	8.0MB	0MB	176.0KB
peer0.org2	186.6MB	22.54%	10.4MB	8.5MB	8.0KB	240.0KB
peer1.org1	178.3MB	16.2%	10.7MB	9.4MB	0MB	188.6KB
peer1.org2	189.8MB	17.5%	9.5MB	8.9MB	0MB	227.6KB
Orderer	118.3MB	4.17%	2.0MB	3.4MB	0MB	5.5MB

The above tables show that the resource consumption varies according to the mode of transaction and the number of transactions per second. Than implementing separate cryptographic algorithms, the consortium blockchain that works on the agreed upon consensus protocol and the immutable ledger provides better access control, authorization and data integrity for each transaction.

4. Conclusion

Blockchain in healthcare will change the future of the healthcare industry by providing secure sharing of patients' information between different organizations. The chaincode provides access control and the immutable ledger facilitates data security. The decentralized network of blockchain avoids a single point of failure in the network. Permissioned distributed ledger is implemented using hyperledger fabric and the performance is evaluated using hyperledger caliper. The performance metrics shows the resource consumption of different peer nodes of different mode of transaction. Blockchain technology will be a revolutionary technology for the secure healthcare industry.

References

[1] Aparna Kumari, Sudeep Tanwar, Sudhanshu Tyagi, Neeraj Kumar, Fog computing for Healthcare 4.0 environment: Opportunities and challenges, Computers & Electrical Engineering, Volume 72, 2018, Pages 1-13, ISSN 0045-7906.

[2] Vora, J. et al. "Blind Signatures Based Secured E-Healthcare System." 2018 International Conference on Computer, Information and Telecommunication Systems (CITS) (2018): 1-5.

[3] Aparna Kumari, Sudeep Tanwar, Sudhanshu Tyagi, Neeraj Kumar, Reza M. Parizi, Kim-Kwang Raymond Choo, Fog data analytics: A taxonomy and process model, Journal of Network and Computer Applications, Volume 128, 2019, Pages 90-104, ISSN 1084-8045.

[4] Desai S., Vyas T., Jambekar V. (2021) Security and Privacy Issues in Fog Computing for Healthcare 4.0. In: Tanwar S. (eds) Fog Computing for Healthcare 4.0 Environments. Signals and Communication Technology. Springer, Cham.

[5] Lanxiang Chen, Wai-Kong Lee, Chin-Chen Chang, Kim-Kwang Raymond Choo, Nan Zhang, Blockchain based searchable encryption for electronic health record sharing, Future Generation Computer Systems, Volume 95, 2019, Pages 420-429, ISSN 0167-739X.

[6] Alhadhrami Z, Alghfeli S, Alghfeli M, Abedlla JA, Shuaib K. Introducing blockchains for healthcare, International Conference on Electrical and computing technologies and applications (ICECTA), 2017;. p. 1–4.

[7] N. Abbas, M. Asim, N. Tariq, T. Baker, S. Abbas, A Mechanism for Securing IoT-enabled Applications at the Fog Layer, Journal of Sensor and Actuator Networks 8 (1) (2019).

[8] N. Tariq, M. Asim, F. Al-Obeidat, M. Z. Farooqi, T. Baker, M. Hammoudeh, I. Ghafir, The Security of Big Data in Fog-Enabled IoT Applications Including Blockchain: A Survey, Sensors 19 (8) (2019) 1788.

[9] N. Tariq, M. Asim, F. A. Khan, Securing SCADA-based critical infrastructures: Challenges and open issues, Procedia

Computer Science 155 (2019) 612–617.
[10] F. A. Khan, N. A. H. Haldar, A. Ali, M. Iftikhar, T. A. Zia, A. Y. Zomaya, A continuous change detection mechanism to identify anomalies in ECG signals for wban-based healthcare environments, IEEE Access 5 (2017) 13531–13544.
[11] H. Wang, K. Li, K. Ota, J. Shen, Remote data integrity checking and sharing in cloud-based health internet of things, IEICE TRANSACTIONS on Information and Systems 99 (8) (2016) 1966–1973.
[12] A. Strielkina, V. Kharchenko, D. Uzun, Availability models for healthcare iot systems: Classification and research considering attacks on vulnerabilities, in: 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), IEEE, 2018, pp. 58–62.
[13] S. F. Aghili, H. Mala, M. Shojafar, P. Peris-Lopez, Laco: Lightweight three-factor authentication, access control and ownership transfer scheme for e-health systems in IoT, Future Generation Computer Systems 96 (2019) 410–424.
[14] Y. Al-Issa, M. A. Ottom, A. Tamrawi, E-health cloud security challenges: A survey, Journal of healthcare engineering 2019 (2019).
[15] M. Talal, A. Zaidan, B. Zaidan, A. Albahri, A. Alamoodi, O. Albahri, M. Alsalem, C. Lim, K. L. Tan, W. Shir, et al., Smart home-based IoT for real-time and secure remote health monitoring of triage and priority system using body sensors: Multi-driven systematic review, Journal of medical systems 43 (3) (2019) 42.
[16] F. T. Jaigirdar, C. Rudolph, C. Bain, Can I trust the data I see? A physician's concern on medical data in IoT health architectures, in: Proceedings of the Australasian Computer Science Week Multiconference, 2019, pp. 1–10.
[17] R. Khan, X. Tao, A. Anjum, T. Kanwal, A. Khan, C. Maple, et al., θ-sensitive k-anonymity: An anonymization model for IoT based electronic health records, Electronics 9 (5) (2020) 716.
[18] Yue X, Wang H, Jin D, Li M, Jiang W. Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control. J Med Syst. 2016 Oct;40(10):218.
[19] Zhang J, Xue N, Huang X. A secure system for pervasive social network-based healthcare. IEEE Access 2016;4:9239–50.
[20] Xia, Qi et al. "MeDShare: Trust-Less Medical Data Sharing Among Cloud Service Providers via Blockchain." IEEE Access 5 (2017): 14757-14767.
[21] Liang, Xueping & Zhao, Juan & Shetty, Sachin & Liu, Jihong & Li, Danyi. (2017). Integrating Blockchain for Data Sharing and Collaboration in Mobile Healthcare Applications. 10.1109/PIMRC.2017.8292361.
[22] Jiang S, Cao J, Wu H, Yang Y, Ma M, He J. Blochie: a blockchain-based platform for healthcare information exchange. In: 2018 IEEE International conference on smart computing (SMARTCOMP); 2018. p. 49–56.
[23] Li H, Zhu L, Shen M, Gao F, Tao X, Liu S. Blockchain-Based Data Preservation System for Medical Data. J Med Syst. 2018 Jun 28;42(8):141.
[24] Fan K, Wang S, Ren Y, Li H, Yang Y. Medblock: efficient and secure medical data sharing via blockchain. J Med Syst 2018;42(8):136.
[25] Wang, H., Song, Y. Secure Cloud-Based EHR System Using Attribute-Based Cryptosystem and Blockchain. J Med Syst 42, 152 (2018).
[26] Guo, R. et al. "Secure Attribute-Based Signature Scheme With Multiple Authorities for Blockchain in Electronic Health Records Systems." IEEE Access 6 (2018): 11676-11686.
[27] M. A. Uddin, A. Stranieri, I. Gondal and V. Balasubramanian, Continuous Patient Monitoring With a Patient Centric Agent: A Block Architecture, in IEEE Access, vol. 6, pp. 32700-32726, 2018
[28] Sun Y, Zhang R, Wang X, Gao K, Liu L. A decentralizing attribute-based signature for healthcare blockchain. In: 2018 27th International conference on computer communication and networks (ICCCN); 2018. p. 1–9.
[29] Zhang X, Poslad S. Blockchain support for flexible queries with granular access control to electronic medical records (EMR). In: 2018 IEEE International conference on communications (ICC); 2018. p. 1–6.
[30] C. Gorenflo, S. Lee, L. Golab and S. Keshav, FastFabric: Scaling Hyperledger Fabric to 20,000 Transactions per Second, 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Seoul, Korea (South), 2019, pp. 455-463, doi: 10.1109/BLOC.2019.8751452.
[31] Griggs, K.N.; Ossipova, O.; Kohlios, C.P.; Baccarini, A.N.; Howson, E.A.; Hayajneh, T. Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring. *J. Med. Syst.* 2018, *42*, 130.
[32] Ivan, D. Moving toward a blockchain-based method for the secure storage of patient records. In *ONC/NIST Use of Blockchain for Healthcare and Research Workshop*; ONC/NIST: Gaithersburg, MD, USA, 2016.
[33] Chen, Y.; Ding, S.; Xu, Z.; Zheng, H.; Yang, S. Blockchain-Based Medical Records Secure Storage and Medical Service Framework. *J. Med. Syst.* 2018, *43*, 5.

[34] Wang, S.; Wang, J.; Wang, X.; Qiu, T.; Yuan, Y.; Ouyang, L.; Guo, Y.; Wang, F.Y. Blockchain-Powered Parallel Healthcare Systems Based on the ACP Approach. *IEEE Trans. Comput. Soc. Syst.* 2018, *99*, 1–9.
[35] Shubbar, S. Ultrasound Medical Imaging Systems Using Telemedicine and Blockchain for Remote Monitoring of Responses to Neoadjuvant Chemotherapy in Women's Breast Cancer: Concept and Implementation. Master's Thesis, Kent State University, Kent, OH, USA, 2017.
[36] Ianculescu, M.; Stanciu, A.; Bica, O.; Neagu, G. Innovative, Adapted Online Services that Can Support the Active, Healthy and Independent Living of Ageing People. A Case Study. *Int. J. Econ. Manag. Syst.* 2017, *2*, 321–329.
[37] E. Afful-Dadzie, S. Nabareseh, Z. K. Oplatková, and P. Klímek, ''Model for assessing quality of online health information: A fuzzy VIKOR based method,'' J. Multi-Criteria Decis. Anal., vol. 23, nos. 1–2, pp. 49–62, 2016.