Physical Education, Health and Social Sciences

https://journal-of-social-education.org E-ISSN: 2958-5996

P-ISSN: 2958-5988

Security Barrier against Integrity Based Attacks in Block Chain Health Care

Engr. Sana Tasleem Rao[1], Prof. Dr. Muhammad Shahbaz[2]

[1] Masters in Computer Engineering from Department of Computer Science and Engineering, University of Engineering and Technology, Lahore. Email: sanatasleemrao@gmail.com

[2] Professor in Department of Computer Science and Engineering, University of Engineering and Technology, Lahore. and technology, Lahore. Email: M.Shahbaz@uet.edu.pk

DOI: *https://doi.org/10.63163/jpehss.v4i2.1553*

Abstract

Healthcare data has grasp the attention cyber attacker because of the sensitivity of the data. Healthcare data has been the victim of many integrities based cyber-attacks recently. Further, patient's privacy has been adversely effected by keeping the data in a centralized manner as the data is valuable asset for the patients as well as for the medical staff. For the solution of aforementioned problems, we have addressed block chain as a barrier for integrity based attack son healthcare data stored in the block chain. We have designed Healthcare Block chain with a web-interface to keep the medical records of the patients safe against every integrity based attack and unauthorized access. Clients, patients, medical staff and miners can access the Healthcare Block chain via web-interface. The Healthcare Block chain have been divided into two views: Front End (Miner View) and Client End View. Miners can access the Healthcare Block chain via Front End View for the confirmation of valid medical data transactions. On the other hand, clients, patients and medical staff and access the Block chain for doing medical data transactions, viewing health records via Client End View. These web-based interfaces provided the functionality of accessing the data in a distributed manner. This security mechanism has provided the patient with the right of controlled data sharing with the concerned medical staff. Additionally, it provides the medical staff with the facility of managing the data in a decentralized and secure way.

Introduction

Block chain is a time-stamped series of unchangeable record of data which is managed by computer clusters and it is not owned by a single entity. Each of these data blocks (records) are secured and by the help of cryptographic principles these blocks are bound to each other. Network of block chain does not contain any central authority but it consists of democratized system. Since it is a mutual and permanent record, the data in it, is open for anybody and everybody to see. Henceforth, anything that is based on the block chain technology is transparent due to its nature and everybody who is involved, will be held accountable for his action. Once information enter in block chain record can never be erased. The most popular example of Block chain is Bitcoin which is a decentralized peer-to-peer digital currency. This bitcoin currency is extremely controversial in today's era but with the help of block chain technology, world can work without any flaws and found out a broad range of applications in non- financial and financial fields.

Literature Review

Abdullah Al Omar et al. [17] have developed a private platform for healthcare data record. It is a cloud based block chain system. According to them decentralization of cloud data could minimize the risk of cyber-attacks on data. In this paper, they have proposed a patient centric healthcare data management system. Block chain technology have helped to maintain the integrity and privacy of data. Smart contracts have been used in the development of this system. A set of security and privacy based requirements have been taken into consideration while the development of the system. However, interoperability between different diagnostic centers, hospitals, doctors and patients have not been taken into consideration.

Thomas McGhin et al. [18] have discussed the research challenges and opportunities of block chain while implementing for healthcare systems. Block chain has wide range of features which includes distributed ledger, decentralized storage system, authentication, integrity, privacy and immutability. Block chain application for healthcare is very suitable because of diverse data preserving and privacy features. On contrary to this, block chain technology have number vulnerabilities which can affect its performance while application in healthcare system such as mining incentives, mining attacks and key management system which needs to be taken into consideration. The main goal of the application of block chain technology for healthcare is to provide ownership to the medical data records in a secure environment. However, there are many areas of research which needs to be focused while implementing block chain for healthcare such as block chain mining incentives, scalability for healthcare, real-world data-sets availability for medical research and development.

BL Radhakrishnan et al. [19] have developed a electronic healthcare record management system using block chain. It provides multilevel authentication. The main purpose of this system is to provide protection to the medical records as leakage of such record could leads to a wrong medication, surgery or life loss. Although block chain with its distributed and decentralized property provides security to the healthcare data but block chain also suffers from attacks such as cold wallet, hot wallet and phishing-based attacks. In this paper, they have proposed a mechanism based on multi-level authentication which protects the block chain from the above-mentioned attacks and thus provides security to the healthcare data.

Tim K. Mackey et al. [20] have identified various challenges and opportunities for application of block chain technology for healthcare data management and privacy. According to the authors, block chain is a great source for data management, privacy and data provenance. Block chain technology has taken hype during the last decade and have revolutionized various technologies. In healthcare sector it has been explored abruptly to optimize lower cost requirements, patient outcomes, and enhancement of compliance and healthcare data provenance for better usage in future. However, it is critically analyzed that if the block chain has the capacity and capability to satisfy the hype of technology in terms of fulfilling actual healthcare needs, consumers, patients and providers.

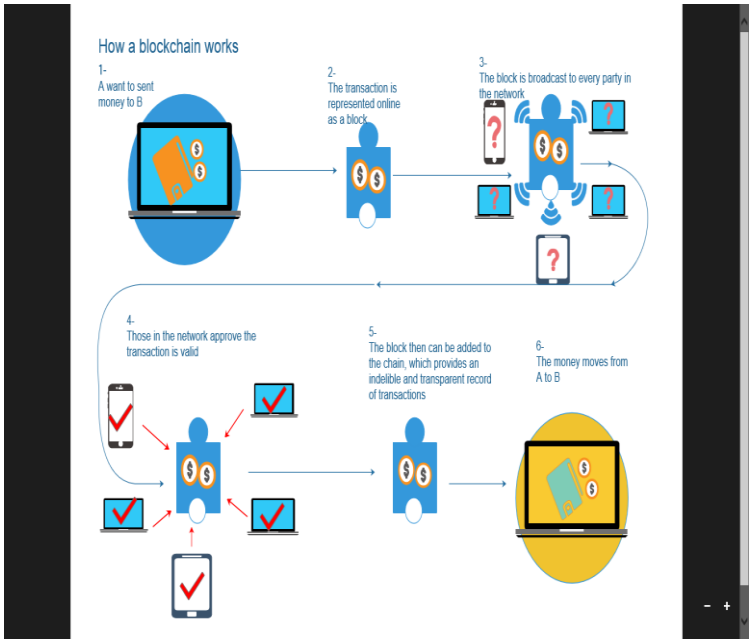
Dimiter V. Dimitrov et al. [21] have explored the applications of block chain for healthcare data management. The aim of this research is to provide an overview of applications of block chain technology in the healthcare sector. This review paper covers storing of healthcare records of patients through various applications and personal data ownerships. They have discussed the gap between block chain technology technical implementation for healthcare and on the other hand its economic impact. According to their results, they have concluded that block chain technology has proved to be a fast, simple and interactive platform for data providers and patients. Various applications of block chain have been discussed in this paper such as electronic medical record

data management, healthcare data protection, personal health record data management, point of care genomics and so on.

Tariq Abdullah et al. [22] have discussed challenges for integrating block chain within healthcare. This paper focus on the discussion of the use of block chain and IoT for healthcare domain. They have identified areas in healthcare which could flourish with the help of new technologies of block chain and IoT. While identifying the technological improvements, they have also paid attention on the practical aspects of such development. Practical aspects of implementation of such technology includes restricted funds, advance computer power requirements and considerations while investing in such new technologies. However, for the application of block chain in healthcare sector, design considerations with respect to its complexity, scope, funding and development must be taken into notice.

Patrick Li et al. [23] have used block chain for the management of medication histories. As effective patient care is needed so access to the accurate and complete medical history is necessary for healthcare institutions. Currently, management of history of medication is maintained using a centralized system. However, centralized mechanism of medical history management is not secure in terms of sharing and accuracy. Privacy and integrity of data can be affected. In this paper, they have developed a decentralized medical history management system with the help of block chain technology. Hyperledger Fabric framework is used. In this system, each prescriber can create prescriptions for each patient.

Block chain working in health Sector



Block chain System Taxonomy

In current vision, Block chain has been roughly classified into three major kinds named as: public block chain, private block chain and consortium block chain [1].

Public Block chain: It is a type of block chain that anyone in the world can see its records and could participate in its consensus process. Unexpectedly, just a cluster of pre-chosen nodes would take part in the consensus procedure of a consortium block chain. is considered as secured medium due to cryptoeconomics which is an economic incentives and cryptographic verification using

mechanisms such as proof of stake or proof of proof of work. Structure of this tyep of block chain is decentralized.

Private Block chain: With respect to this type of block chain only those nodes that originate from one explicit association would be permitted to join the consensus process. A private block chain is seen as a centralized structure since it is completely constrained by one association.

Consortium Block chain: The consortium block chain built by a few associations is in part decentralized since just a few nodes would be chosen to decide the consensus.

Comparison of Block Chain Types

Following is discussed comparison of three popular kinds of block chain through various aspects [2].

a) **Consensus Determination**: In public block chain, each node could put its contribution inconsensus process and only selected group of nodes are in charge of approving the block in consortium block chain. With respect to private block chain, completely constrained by one association and the association could decide the last consensus.
b) **Read Permission:** In Public block chains, transactions are visible or seen by public while its dependency with regards to a private block chain or a consortium block chain.
c) **Immutability**: It is almost difficult to alter transactions in public block chain since records are stored on an exapnsive number of participants. On the other hand, in private or consortium block chain transactions can be tempered in an easier manner as it consists of a limited number of participants.
d) **Efficiency:** It requires a lot of time to propagate blocks and transactions as public block chain consist of a large number of nodes. Therefore, transaction throughput is constrained and latency is high. With less validators, consortium block chain and private block chain could be increasingly effective.
e) **Centralized:** The primary distinction among the three kinds of block chains is that public block chain is decentralized, private block chain is completely centralized and consortium block chain is partially centralized.
f) **Consensus Process:** Everybody on the world could join the consensus process of public block chain while both private and consortium are permission.

Block chain Architecture Components

Following are the main components of block chain:

1) **Nodes:** These are computers or users within the architecture of block chain (each has an autonomous duplicate of entire block chain ledger).
2) **Transaction:** It is a smallest building block which is part of block chain system (information, records, etc.) whose duty is to serve as the purpose of block chain.
3) **Block:** It is called as the data structure utilized for keeping a transaction set and that set is distributed all nodes which are part of network.
4) **Chain:** It is called as a block sequence in a specified order.
5) **Miners:** These are specific nodes whose duty is to perform the verification process of block before doing addition to block chain structure.
6) **Consensus:** It is a protocol which consist of set of rules and arrangements for the sake of carrying block chain operations.

Block chain Working Scenario

1- A wants to send money to B.

2- A request for a transaction.
3- Block is created that represent the transaction.
4- This block is broadcast to every node in network.
5- Nodes in the network approve that transaction is valid.
6- A node is received by node for the proof of work.
7- This block is then added to chain which provides a transparent and incredible record of transactions.
8- At last, transaction is complete so money is moved from A to B.

Methodology

Interest in Block chain technology has been increased in health industrybecause it offers a secure, distributed database that has potential to operate without the presence ofany administrator or centralized authority. In my proposed methodology as dicussed in fig.1, block chain is presented as peer-to-peer and distributed network that is responsible to make a continuous records called blocks. Each transaction of amount that take place for block chain user is been represented in a cryptographically signed block which further automatically validated by the network itself. This cryptographically signed blocks and validation process works very well to maintain the transparency and authenticity of healthcare record or data.

Module 1: Wallet Generation Module for Public/Private Key

In this module, a Wallet is generated so we can add new patient or client or patient account. The generated Wallet contain two keys: Public key and Private key as shown in Fig.2.For Public/private key generation purpose, it will call an API which further calls a GetBitcoinSecret(built in library) function that is present inside RSA class algorithm.

Module 2: Transaction Module

In this module, hospital information is shared through Block chain network. while making transaction, a private encrypted signature is generated that contain its Sender Address, Private Address, Recipient Address, Amount or Medical Records ,for transaction purpose that was further decrypted in confirming transaction in system as shown in Fig. 3. After confirming transaction system, verify everything that has a relation(Sender Address, Private Address, Recipient Address, Medical Records or Amount).

Module 3: Wallet Transaction

In this module, client or patient history of transaction that took place within network is been verified as shown in Fig.4. When a sender address or public key is entered, it will give information of sender address, recipient address and amount or medical records.

Module 4: Miner View of Block chain Transaction

In this module, we can view the transaction of other node or miner. When we enter minor URL, it will show transaction detail: sender address, recipient address, amount or medical records with.

Implementation

Block chain Wallet Generation

A software program of Block chain wallet is generated (as shown in Fig.7, 8 &9) that enables our users to keep records of all transactions which are related to the amount and further

store them on Block chain. In our proposed work, this wallet mainly stores private and public keys for adding a patient or client account related information.

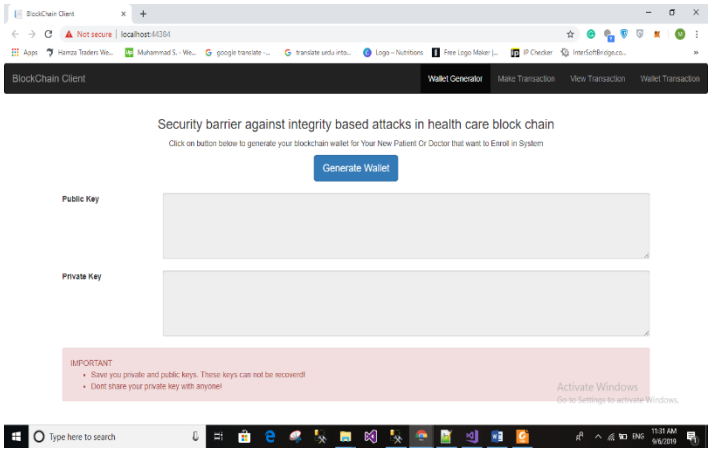


Figure.2. Wallet generate for security barrier against integrity based attacks in health care block chain

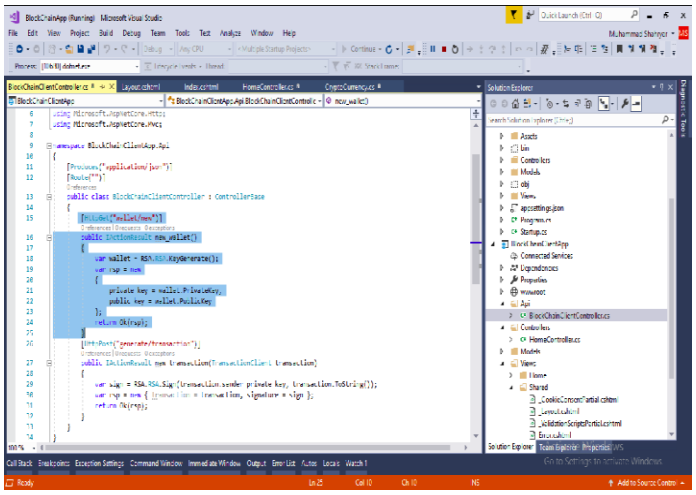


Figure.3. Generator for Public and private key RSA class

Block chain Transaction Module for Digital signature

A digital signature is generated in transaction module for assuring the authentication process of our medical digital records. Therefore, a valid digital signature is added in our proposed us to give our recipient, a trust that the message was actually created by a claimed client or user (authentication) and it is not possible that a message can be modified in transit (integrity). Additionally, a sender cannot deny regarding a message or medical record is sent by him. An asymmetric cryptography Digital signature also named as public key cryptography has been proposed to achieve integrity of our records in terms of encrypt and decrypt data. There are two keys: Public and Private which are not identical but paired together but are not identical. Public key can be shared with everyone and the private key is kept secret as shown. Either of the keys can be used to encrypt a message and the opposite key can be used to decrypt messages. This pair of keys provides a layer of security and validation to messages, sent through secure and non-secure channels it. The public key is freely shared with everyone and it is accessed as wallet's address. On the

other side the private key is used to sign transactions. This means, a client can only access or spend amount, present in wallet when he has associated private key.

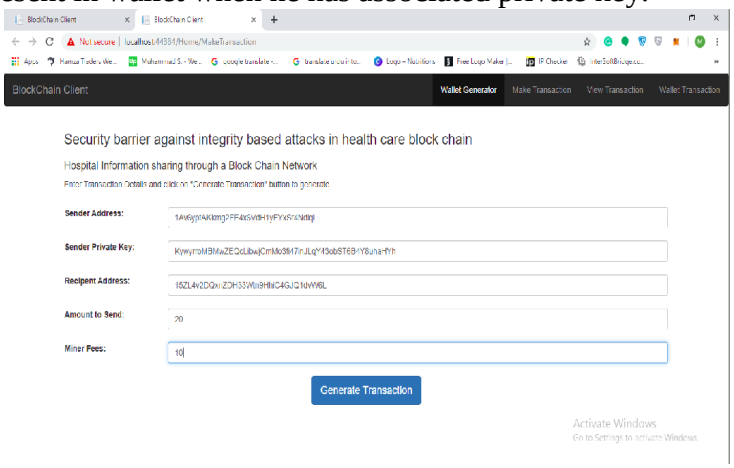
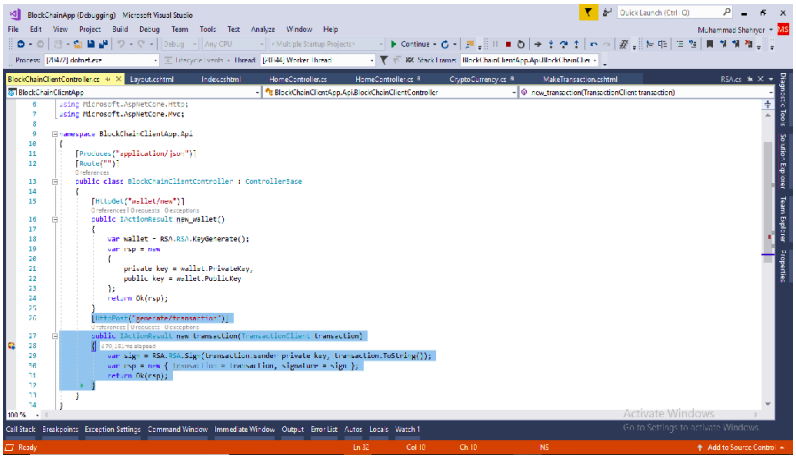


Figure.4. Portal or window of entering information regarding sender address, the sender's private key, the recipient's address, sending & fees of miner



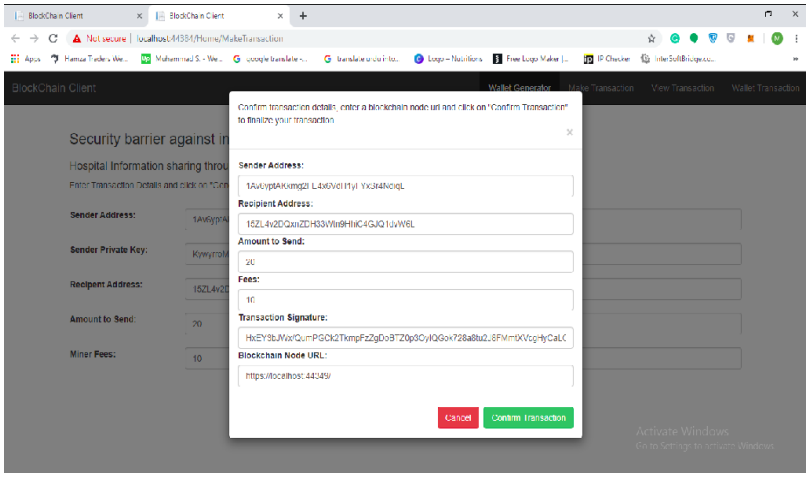
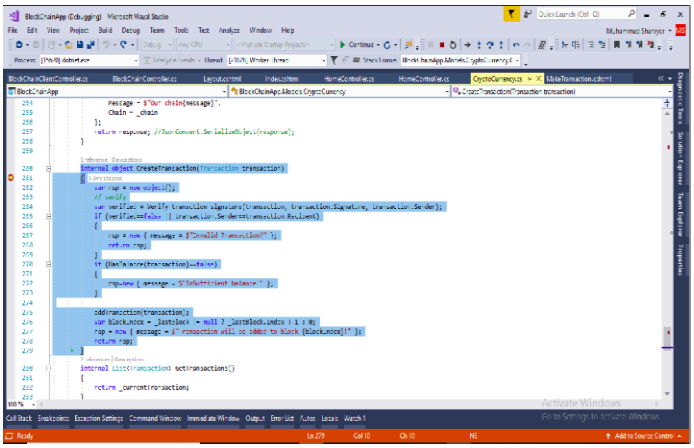
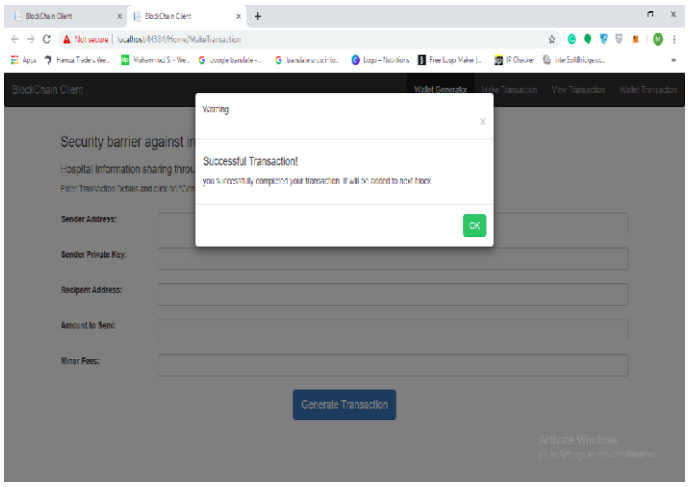


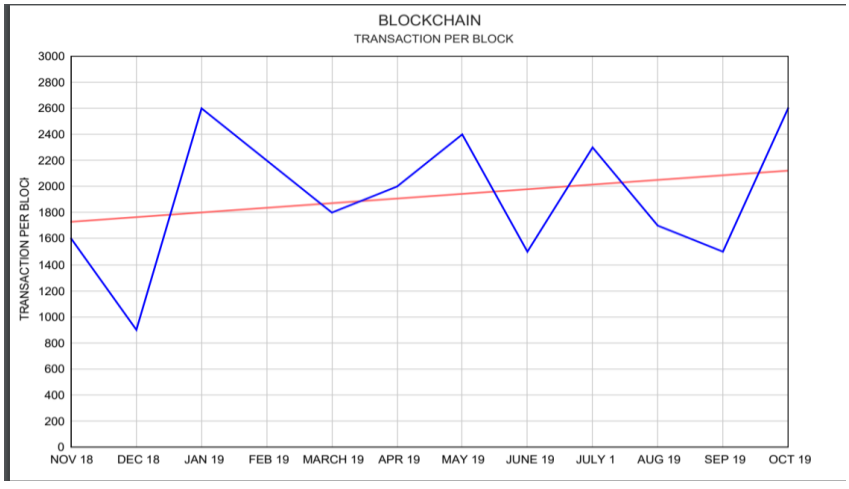
Figure.6. Confirmation of transaction details





Graphical Results

figure shows the recording of medical data records into healthcare block chain from a time period of almost 1 year (November, 2018 to October, 2019). The data has been recorded into the healthcare block chain via web-interface of the healthcare block chain. Privacy of the recorded data has been maintained by the block chain. Access control policy have been applied while recording the data. The data can only be accessed by the concerned medical staff and the patient itself.



Conclusion

In this work, we have proposed "Security barrier against integrity based attacks in health care block chain". Healthcare data is of major security concern due to increased ratio of cyber-attacks in the recent years. Healthcare data privacy, integrity, availability and confidentiality is of major concern. To keep the data safe from the aforementioned cyber-attacks, we have addressed Block chain as a security mechanism to preserve the privacy of the data. Healthcare Block chain has been designed to keep the medical records safe from cyber-attacks. Security barrier against integrity based attacks in Healthcare Block chain have been designed. For this we have provided a web-based interface for the Healthcare Block chain whose functionality can be divided into two components: Front End (Miner View), Client End View. With the help of client end view, the patients and concerned medical staff could enter their healthcare data into the Block chain and can keep record of the data safe. This client end view also ensures the availability of data anytime to the clients as well as medical staff for viewing the medical history of patients. Secondly, we have embedded the Front End view, which act as a security barrier against integrity based attack in Healthcare Block chain. These web-based interfaces provided the functionality of accessing the data in a distributed manner. This security mechanism has provided the patients with the autonomy in a way that they do not need to trust any third party and as well as they are always aware of who is accessing their data. Additionally, it provides the medical staff with the facility of managing the data in a decentralized and secure way.

References

[1] V. Buterin, "On public and private block chains," 2015. [Online]. Available: https://blog.ethereum.org/2015/08/07/ on-public-and-private-block chains/

[2] Zheng, Z., Xie, S., Dai, H., Chen, X., and Wang, H.,"An overview of block chain technology: Architecture, consensus, and future trends,"In 2017 IEEE international congress on big data (BigData congress), IEEE, pp. 557-564, June 2017.

[3] Panicker, S., Patil, V. and Kulkarni, D., "An Overview of Block chain Architecture and it's Applications," International Journal of Innovative Research in Science, Engineering and Technology, vol.5, no.11, 2016.

[4] Nakamoto, S.,"Bitcoin: A peer-to-peer electronic cash system."2008.

[5] Foroglou, G., and Tsilidou, A. L.,"Further applications of the block chain,"In 12th Student Conference on Managerial Science and Technology, May 2015.

[6] K. Fan, Y. Ren, Y. Wang, H. Li, and Y. Yang, "Block chain-based efficient privacy preserving and data sharing scheme of content-centric network in 5G," IET Commun., vol. 12, no. 5, pp. 527–532, Mar. 2018.

[7] X. Huang, C. Xu, P. Wang, and H. Liu, "LNSC: A security model for electric vehicle and charging pile management based on block chain ecosystem," IEEE Access, vol. 6, pp. 13 565–13 574, 2018.

[8] J. Gao, K. O. Asamoah, E. B. Sifah, A. Smahi, Q. Xia, H. Xia, X. Zhang, and G. Dong, "GridMonitoring: Secured sovereign block chain based monitoring on smart grid," IEEE Access, vol. 6, pp. 9917–9925, 2018.

[9] J. Gu, B. Sun, X. Du, J. Wang, Y. Zhuang, and Z. Wang, "Consortium Block chain-Based Malware Detection in Mobile Devices," IEEE Access, vol. 6, pp. 12 118–12 128, 2018.

[10] B. Lee and J.-H. Lee, "Block chain-based secure firmware update for embedded devices in an Internet of Things environment," J. Supercomput., vol. 73, no. 3, pp. 1152–1167, Mar 2017.

[11] Ferrag, M. A., Derdour, M., Mukherjee, M., Derhab, A., Maglaras, L., & Janicke, H.. "Block chain technologies for the internet of things: Research issues and challenges" IEEE Internet of Things Journal, 2018.

[12] C. Esposito, A. De Santis, G. Tortora, H. Chang, and K.-K. R. Choo, "Block chain: A Panacea for Healthcare Cloud-Based Data Security and Privacy? ," IEEE Cloud Comput., vol. 5, no. 1, pp. 31–37, Jan. 2018.

[13] R. Guo, H. Shi, Q. Zhao, and D. Zheng, "Secure Attribute-Based Signature Scheme with Multiple Authorities for Block chain in Electronic Health Records Systems," IEEE Access, vol. 6, pp. 11 676–11 686, 2018.

[14] X. Liang, J. Zhao, S. Shetty, J. Liu, and D. Li, "Integrating block chain for data sharing and collaboration in mobile healthcare applications," in 2017 IEEE 28th Annu. Int. Symp. Pers. Indoor, Mob. Radio Commun. IEEE, pp. 1–5, Oct 2017.

[15] Kotz, D., Gunter, C. A., Kumar, S., & Weiner, J. P., "Privacy and security in mobile health: a research agenda," Computer, vol. 49, no. 6, pp. 22-30, 2016.

[16] Al Omar, A., Bhuiyan, M. Z. A., Basu, A., Kiyomoto, S., and Rahman, M. S., "Privacy-friendly platform for healthcare data in cloud based on block chain environment," Future Generation Computer Systems, vol. 95, pp. 511-521, 2019.

[17] McGhin, T., Choo, K. K. R., Liu, C. Z., and He, D.,"Block chain in healthcare applications: Research challenges and opportunities," Journal of Network and Computer Applications, 2019.

[18] Radhakrishnan, B. L., Joseph, A. S., & Sudhakar, S., "Securing Block chain based Electronic Health Record using Multilevel Authentication," In 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS), IEEE, pp. 699-703, March 2019.

[19] Mackey, T. K., Kuo, T. T., Gummadi, B., Clauson, K. A., Church, G., Grishin, D., and Palombini, M., "Fit-for-purpose?'–challenges and opportunities for applications of block chain technology in the future of healthcare,"BMC medicine,pp. 17, no. 1, pp. 68, 2019.

[20] Dimitrov, D. V., "Block chain Applications for Healthcare Data Management," Healthcare informatics research, vol. 25, no. 1, pp. 51-56, 2019.

[21] Abdullah, T., and Jones, A., "eHealth: Challenges Far Integrating Block chain within Healthcare,"In 2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3), IEEE., pp. 1-9, January 2019.

[22] Li, P., Nelson, S. D., Malin, B. A., and Chen, Y., "DMMS: A decentralized block chain ledger for the management of medication historie," Block chain in Healthcare Today, 2019.

[23] Dwivedi, A. D., Srivastava, G., Dhar, S., and Singh, R., "A decentralized privacy-preserving healthcare block chain for iot," Sensors, vol.19, no. 2, pp. 326, 2019.

[24] Agbo, C. C., Mahmoud, Q. H., and Eklund, J. M., "Block chain technology in healthcare: a systematic review,"In Healthcare Multidisciplinary Digital Publishing Institute, vol. 7, no. 2, pp. 56, June 2019.

[25] Onik, M. M. H., Aich, S., Yang, J., Kim, C. S., and Kim, H. C., "Block chain in Healthcare: Challenges and Solutions," In Big Data Analytics for Intelligent Healthcare Management Academic Press, pp. 197-226, 2019.

[26] Griggs, K. N., Ossipova, O., Kohlios, C. P., Baccarini, A. N., Howson, E. A., and Hayajneh, T.,"Healthcare block chain system using smart contracts for secure automated remote patient monitoring,"Journal of medical systems, vol. 42, no.7, pp.130, 2018.

[27] Boulos, M. N. K., Wilson, J. T., and Clauson, K. A., "Geospatial block chain: promises, challenges, and scenarios in health and healthcare," International Journal of Health Geographics, 2018.

[28] Clauson , K. A., Breeden, E. A., Davidson, C., and Mackey, T. K., "Leveraging block chain technology to enhance supply chain management in healthcare," Block chain in Healthcare Today, 2018.

[29] Zubaydi, H. D., Chong, Y. W., Ko, K., Hanshi, S. M., and Karuppayah, S.,"A review on the role of block chain technology in the healthcare domain," Electronics, vol. 8, no.6, pp.679, 2019.

[30] Bhuiyan, M. Z. A., Zaman, A., Wang, T., Wang, G., Tao, H., and Hassan, M. M., " Block chain and big data to transform the healthcare," In Proceedings of the International Conference on Data Processing and Applications, ACM., pp. 62-68, May 2018.

[31] Sharma, A., Hung, Y. H., Agarwal, P., and Kalra, M., "A Study on Block chain Applications in Healthcare,"In International Conference on Frontier Computing, Springer, Singapore, pp. 623-628, July 2018.

[32] Ekblaw, A., Azaria, A., Halamka, J. D., and Lippman, A.,"A Case Study for Block chain in Healthcare:"MedRec" prototype for electronic health records and medical research data," In Proceedings of IEEE open & big data conference, vol. 13, p. 13, August 2016.

[33] Sharma, A., Hung, Y. H., Agarwal, P., and Kalra, M., "A Study on Block chain Applications in Healthcare," In International Conference on Frontier Computing (pp. 6 Springer, Singapore, pp. 623-628, July 2018.

[34] Zhang, P., Walker, M. A., White, J., Schmidt, D. C., and Lenz, G., "Metrics for assessing block chain-based healthcare decentralized apps," In 2017 IEEE 19th International Conference on e-Health Networking, Applications and Services (Healthcom), IEEE, pp. 1-4, October 2017.

[35] Liang, X., Zhao, J., Shetty, S., Liu, J., and Li, D.,"Integrating block chain for data sharing and collaboration in mobile healthcare applications,"*In 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), IEEE.,* pp. 1-5, October, 2017.

[36] Al Omar, A., Rahman, M. S., Basu, A., and Kiyomoto, S., "Medibchain: A block chain based privacy preserving platform for healthcare data*," In International conference on security, privacy and anonymity in computation, communication and storage*, Springer, Cham,pp. 534-543, Decemeber 2017.

[37] Yue, X., Wang, H., Jin, D., Li, M., and Jiang, W.,"Healthcare data gateways: found healthcare intelligence on block chain with novel privacy risk control,"*Journal of medical systems*, vol. 40, no.10, pp.218, 2016.

[38] El-Din, D. M. "A Pharmacy Block chain System Enhanced by Crowd Sourcing,"

[39] Witchey, N. J..*U.S. Patent Application No. 14/711*, 2015.

[40] Esposito, C., De Santis, A., Tortora, G., Chang, H., & Choo, K. K. R., "Block chain: A panacea for healthcare cloud-based data security and privacy?,"*IEEE Cloud Computing*, vol. 5, no. 1, pp. 31-37, 2018.

[41] Zhang, P., White, J., Schmidt, D. C., Lenz, G., and Rosenbloom, S. T., "FHIRChain: applying block chain to securely and scalably share clinical data,"*Computational and structural biotechnology journal*, vol. 16, pp. 267-278, 2018.

[42] Roman-Belmonte, J. M., De la Corte-Rodriguez, H., andRodriguez-Merchan, E. C.,"How block chain technology can change medicine,"*Postgraduate medicine*, vol.130, no.4, pp. 420-427, 2018.

[43] Kuo, T. T., Kim, H. E., and Ohno-Machado, L., "Block chain distributed ledger technologies for biomedical and health care applications," *Journal of the American Medical Informatics Association*, vol. 24, no.6, pp. 1211-1220, 2017.

[44] Pham, H. L., Tran, T. H., and Nakashima, Y.,"A secure remote healthcare system for hospital using block chain smart contract,"*In 2018 IEEE Globecom Workshops (GC Wkshps), IEEE.*, pp. 1-6, December, 2018.

[45] Angraal, S., Krumholz, H. M., and Schulz, W. L., "Block chain technology: applications in health care. *Circulation: Cardiovascular quality and outcomes*," *e003800,* vol.10, no. 9, 2017.