# TRANSACTION DELAY OF DATA TRANSMISSION BETWEEN SENSORAND BLOCKCHAIN TECHNOLOGY FOR THE HEALTHCARE DOMAINUSING CONSENSUS MECHANISM

**Puneeta Singh[1*], Dr. Shrddha Sagar[2]**

[1*], [2]Department of Computer Science and Engineering, Galgotias University, Greater Noida, U.P, India

***Corresponding Author:** Puneeta Singh
*Department of Computer Science and Engineering, Galgotias University, Greater Noida, U.P, India

**Abstract**

Blockchain is being used for sharing of data among the different nodes. In respect to maintain the confidentiality of data, the blockchain has been adopted with its high value data secrecy. Sensor nodes and blockchain nodes have been considered and concept of Diffie-Hellman is been employed in connection with both mentioned nodes. In this article/concept, Message authentication code (MAC) was adopted so that the secrecy of data can be protected thereafter, calculated the transition time i.e., time involved in transferring data from sensor nodes to blockchain nodes. One of the prominent methods which has come into the light smooth transaction of data and to ensure a stable security is blockchain Technology. Using the IoT with the backing of blockchain technology enables a system to work more smoothly. The Healthcare status of a patient can easily be tracked by using IoT. It is very big challenge in today's time to interlink block chain technology with Internet of things (IoT). Both the nodes are linked with shared key and it generate a common code referred as HMAC signature. The concept of machine learning introduced to remove theoutliers of data before feeding it into the sensor node. The outcomes/result/research shows thatas the test load is increasing, the corresponding throughout is getting advance/increase and after attaining a particular threshold it starts dropping. Thereafter the phenomenon is best suitablefor IoT system.

**Keyword:** Blockchain, MAC, HMAC, IoT, Healthcare, consensus, EHR, data transmission

## 1Introduction

In the era, the blockchain technology plays a vital role in the field of IoT in Healthcare sector has become very critical path in today's time. On the one side where it provides numerous help for the treatment of patient, where is on the other side there is always a concern about the security of data [1]. In a generalized term transferring the data is always subjected to theft, loss, or illegal use of the data [2-3]. There is a necessary requirement to establish a system where the data can be transferred from one device to another without any security concerns [4-5]. One of the prominent methods which has come into the light smooth transaction ofdata and to ensure a stable security is blockchain Technology. Using the IoT with the backing of blockchain technology enables a system to work more smoothly. The Healthcare status of a patient can easily be trackedby using IoT [6]. There are lot more medical devices which can relate to internet and a local system can be created for close monitoring of a patient.

The physical interaction with the doctor can also be avoided to any extent by using IoT. The exact data generated from patient body can directly be transmitted to a Healthcare organization where the feedback basedon the health situation, can be communicated to patient itself [7-8]. The only concern here is the transmissionof the data may be subjected to theft or loss If the data transmit through various local service. The datasecurity depends upon the trust of local servers. Blockchain technology is a ledger act as a distributed manner, sharable, immutable.

Whatever the information we are sharing it can store in ledger and transparent. All the blocks are to be connected each other. In each block, they can store all the information regarding transactions. Whatever the data are having it cannot be changed, tempered, or modified. If any node is updated in the blockchain it will affect to each node. Only when the additional block has been added into the

blockchain if the previous hash been verified. Previous hash value will be reflected into the next block. One of the important protocols that will be used in the blockchain is consensus algorithms. Every transaction would be completely verified, secured and transparent [9-10]. That will create trust worthy environment in the blockchain network. With the help of consensus protocol if any new block is added then each this protocol must be responsible for all the nodes that was agreed and for taking the authority of the blockchain network.

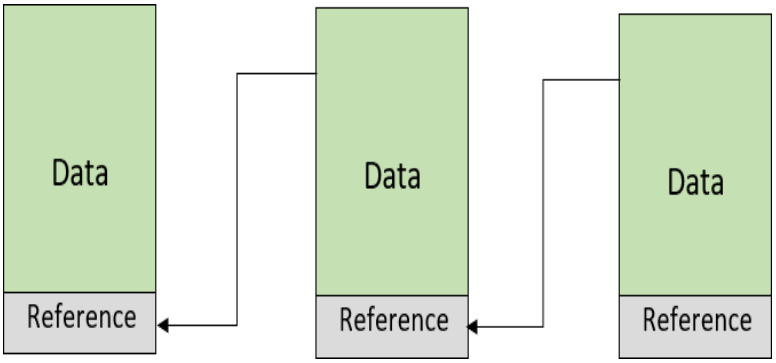


**Figure 1:** Representation of Blocks in Blockchain

In the Fig. 1 Represents blocks with data and reference. In blockchain technology, various consensus algo- rithm exists (proof of stake, Proof of work, practical byzantine fault tolerance, proof of burn, proof of capacity). Proof of work is used for mining purpose. Generally, Bitcoin can use this consensus algorithm. This algorithm was used in for solving mathematical puzzle that will give solution [11-12]. It can used more computational power at the same time it can mine the next block generation also. In the case of POS, here Ethereum was shifted from POF to POS. Instead using costly hardware for solving difficult problems, validators are to be used for solving the problems. These validators spend in the coins of the system, some of the coins are to be stake [10-13].

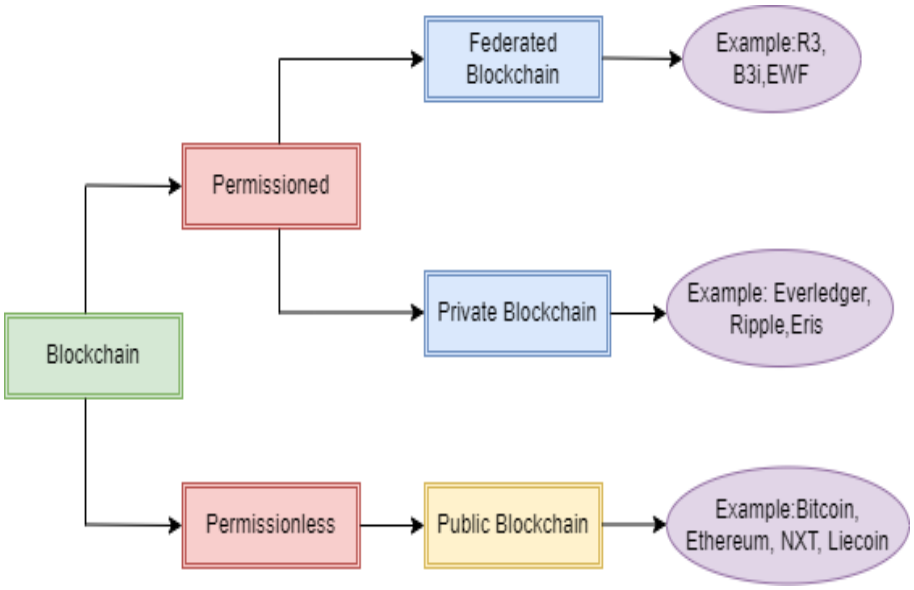


**Figure 2:** Representation of types of blockchain technology

In the Fig. 2, there are three types of blockchain: private blockchain, public blockchain and federated blockchain. Field of public blockchain, every node will take the participation and use their resources and eligible to take participate in the consensus mechanism [13]. The authority of the public blockchain is the de- centralized and having the transaction speed is slow. The mechanism that was used in this is the permission-less and their efficiency is low. Having to provide the read and write access to every user who participated in the blockchain network [14-15]. Every field like Internet of things (IoT), Health-care, Agriculture, Insurance, Real estate, Money transfers, Supply chain tracking, Missile data security etc. [20-21].

In the Fig. 3, it shows the application of Blockchain technology works as a block and these blocks are to be

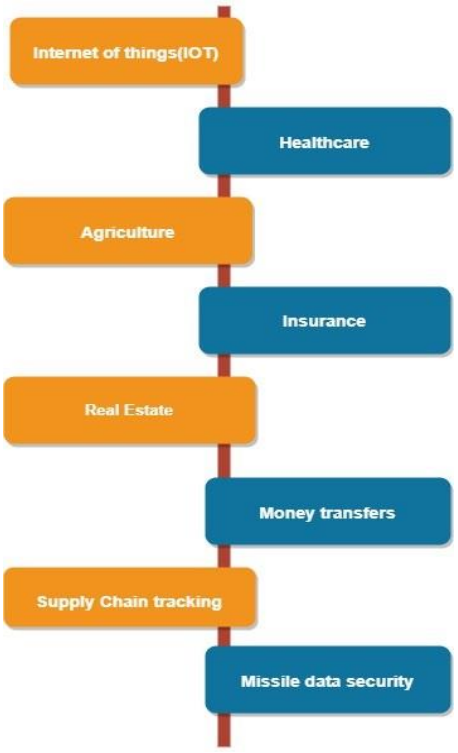


**Figure 3:** Applications of Blockchain Technology

connected to each other and their applications works in every field like Internet of things (IoT), Health-care, Agriculture, Insurance, Real estate, Money transfers, Supply chain tracking, Missile data security etc. [16-17].

## 2Related Work

Rathee, G et. al. [1] proposed that it can reduce the human effort with the help of preserving transparency and they will save the IOT smart sensors from hackers and give the transparency with the help of blockchain technology create into the number of blocks. We can see number of security issues like falsification attack, delay in authentication etc.

Mohanta, B. K. et. al. [2] proposed that resolve the security issue with the help of the formulae CIA (Confidentiality, Integrity, and availability) using the concept of machine learning and blockchain technology. It can remove the traditional IOT system. They can face number of challenges like integrity, confidentiality etc.

Haris, R. M. [3] proposed that embedded the 5G in IOT devices and using the function of control and management and via NFV it can implement the 5G technology. In this paper it can face number of issues in blockchain technology like regulation, standardization etc. that can be resolved with the help of Artificial intelligence, Blockchain technology.

Wu, Y. [4] proposed that it can use IOT devices and apply blockchain technology with the concept of con-sensus mechanism. Blockchain and their IOT sensors can share their key for creating Hash based authentication code and use to random function it can create block nodes. Block node is that node who won the election called offline fast election node. Before block nodes upgraded into the blockchain process, methods of AI are also introduced to remove the outliers of sensors.

Atlam, H. F [5] proposed about the IOT sensors are to be connected to each other and sharing the informa- tion to all nodes. Author sees the major issue regarding centralized infrastructure, it can be resolved with the help decentralized.

Da Xu, L. [7] about the Internet of things (IOT), faces the key challenges of security, reliability, and their transparency. With the help of blockchain and their most significant feature that is

decentralized. All the nodes are to connected and taking the property of smart contract, data encryption, decryption, proof of work, proof of stake, and taking the most important feature is consensus mechanism.

El Rahman, S. A. [8] proposed that all the patient's information was to be recorded with the help of internet of things (IoT). This paper more focused on security and their privacy when taking the information from patient data. Difficult to maintain the data integrity.

Singh, P. [26] describes about the blockchain technology which is distributed in nature containing different strategies i.e., private blockchain, public blockchain and consortium blockchain. In this paper they also pre- sented about the whole description of blockchain like authentication, privacy, confidential data.

Humayun, M. [27] proposed Smart logistic enables the easy and smooth way of transport the things. With new technology And involvement of IoT, the logistics has become very much easy going and reduced the lead time to a great extent. It requires less resources like men power, vehicles, paperwork etc. while being more reliable on digital technology. However, it may involve the concern of data theft and lead to privacy invasion. However, the application of blockchain with IoT will enhance the system of digital logistic with more security.

Fakhri, D. [28] proposed whatever the security issues in IOT. It can be resolved by blockchain technology gives the platform where secure communication taken place. Smart contracts are to be used in blockchain technology for security aspects.

Farouk, A. [29] explained that how the healthcare industry works and they impact the information technology. Effects the privacy of confidential data and their security. This technology improves the efficiency, robustness, and their transparency.

Kumar, N. M. [30] this paper tells that IoT is centralized via which their server fails then automatically all the data are to effected so blockchain is one of the technologies that comes under this and because of their nature it is decentralized. Their aspects resolve many problems of the IoT.

**Table1: Represents the different techniques used**

| Ref. | Year | Network function virtualization technique | Diffie-Hellman technique | Algo. Ethereum, Hyper-ledger and IOTA | Tool |
|---|---|---|---|---|---|
| Mohanta,B.K.et.al[2] | 2020 | yes | yes | | iFog simulator |
| Haris, R. M. et.al.[3] | 2020 | yes | yes | yes | Solidity |
| Wu, Y. et. al. [4] | 2020 | yes | | | iFog simulator |
| Atlam, H.F.et.al.[5] | 2020 | yes | | | Solidity |
| Atlam, H. F. et. al. [6] | 2018 | | | yes | iFog simulator |
| Da Xu. et. al. [7] | 2021 | | yes | | iFog simulator |
| Singh, P., et. al. [26] | 2021 | yes | | yes | Solidity |
| Humayun, M. et. al.[9] | 2020 | | yes | | Solidity |

Table1 specifies that how the authors contributed different technique in different technique proposed.

### Problem Statement

1. First issue was the nature of IoT is the central hub where all the nodes are to relate to the central node if any circumstances the central hub was failed then all the nodes are to be affected. That was the biggest challenge to be faced.
2. Second issue is their efficiency problem because all the connected nodes is having heavy resources in the network. With the help of these heavy resources faces the issue of efficient.
3. Third issue is the maintenance problem because there is a lot of nodes and that all the nodes are to be connected to only the single hub. It is also a very big challenge to face the issue i.e., maintenance via which the problem of security also come.

## 3Methodology

Combined blockchain with IoT is highly challenging. IoT sensors with high rate of data using the method of consensus. The nodes which can be used in blockchain using the Diffie-Hellman key exchange. In network layer, blockchain nodes and sensors nodes are to be used the key for same negotiation to create the Hash -Based Message Authentication Code (HMAC). This HMAC is used in sensors for valid transactions and random func-tion used for block nodes[18-19]. Blockchain and their IoT sensors can share their key for creating Hash based authentication code and use to random function it can create block nodes. Block node is that node who won the election called fast election offline node. Before the nodes that was blocked upgraded into a blockchain process, methods of AI are also described to eliminate the outliers of sensors.

## Consensus Mechanism

**3.1 Protocol (Shared Keys): According to Fig.4. In perception layer, sensors were attached with blockchain nodes and sharing the Diffie Hellman key in between these nodes.**

(a) Nodes that are in the layer of network and sensors in perception layer, both can share the prime number p and base q.

(b) Choose private key r in sensors and after that send public key S to the blockchain nodes.

$S = q^r modp$ (1)

(c) Blockchain nodes choose the private key t and after that send public key W to the sensor's nodes.

$W = q^t modp$ (2)

(d) In Sensor nodes, calculate the value of shared key:

$Xsensor = W^r modp$ (3)

(e) In Blockchain nodes, calculate the value of shared key:

$Xtc - node = S^t modp$ (4)

Including these two equations, X sensor = X tc-node the nodes of blockchain using the key and to create hash message.

(f) authentication code signatures for sensor transaction.

· Verification process in sensor: After receiving the whole process of transaction, that can be divided into further parts.

– In sensor, verify the whole signature (HMAC) of data.

– In whole process find out the abnormal data and label them.

· Verification in data of sensor signature.

– In this article, MAC was used to integrity and data source and HMAC key that was shared used for both the ends i.e., source or destination. HMAC is to be calculated as:

HMAC (key, data) =H ((Key0 XOR opad) —— (Key0 XOR ipad) —— data))

Where: H: Hash Function opad: outside complete data

ipad: inside the data the procedure for synchronization the sensors of the data in-between the transactions fx is as follows: info. =bytes (fx.sender) ——bytes(fx.time)——bytes(fx.value). where bytes used for byte-code stream

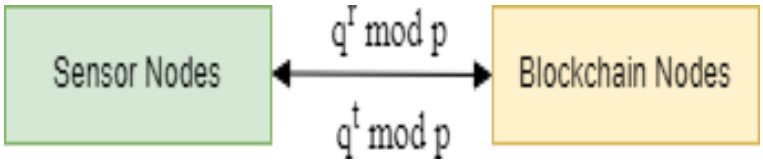


**Figure 4:** Agreement between sensor and blockchain nodes

In the Fig. 4 represents the sharing information between the blockchain nodes and sensor nodes, Diffie-Hellman exchange algorithm was used.

**Table 2:** Structure of transaction between sensor nodes and blockchain nodes

| S.No. | Domain | Data Types | Explanation |
|---|---|---|---|
| 1 | Transmitting Node | String | Identity of sensor node |
| 2 | Transmitting timing | Integer | Timestamp of Linux |
| 3 | Value of sensor node | Floating value | Data of sensor sampling |
| 4 | Message authentication code (MAC) | String | Code(MAC) |

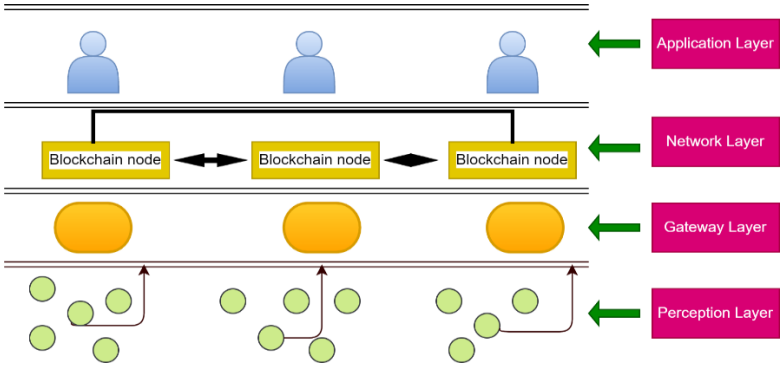


**Figure 5:** IoT system model based on blockchain

In the Fig.5, EHR is a digital form of the data, that include complete history about the medical treatment of a patient, genetic information related to another necessary information which can be helpful in order to give the effective treatment to that individual. It also includes the bio-metric data such as finger print, blood group and patient centric information within[22-23].The instant availability of all such data to the medical team can help to a great extent. Now the concern for the availability of the information in given point of period with full reliability without causing any damage and theft to the data. An attempt has been made to solve the problem with the help of BC and edge framework, which uses a decentralize mode of data storage would ensure reliability during data transmission and reduce concern about any data theft and manipulation. In the Fig.6, Edge framework is a concept which allow to compute the date and also store the data that too nearer to the source. It reduces the processing time as well as saves the bandwidth. Now, we need to build up a rigid structure by using IoT, Edge framework with the interaction of BC in order to realize the actual use of it[24-25].

1. **Layer in Blockchain**

(a) This layer is responsible for the primary services i.e., peer to peer communication, identity manage-ment and using the main important algorithm i.e., Consensus algorithm.

2. **Hyper-ledger**

(a) It is an open-source project which can used for or to create the distributed ledger. It can help to build the applications that can be used by the industries.

3. **Smart Contract**

Most probably because of their highly lot of resources are to be connected in the network.

**First concern**

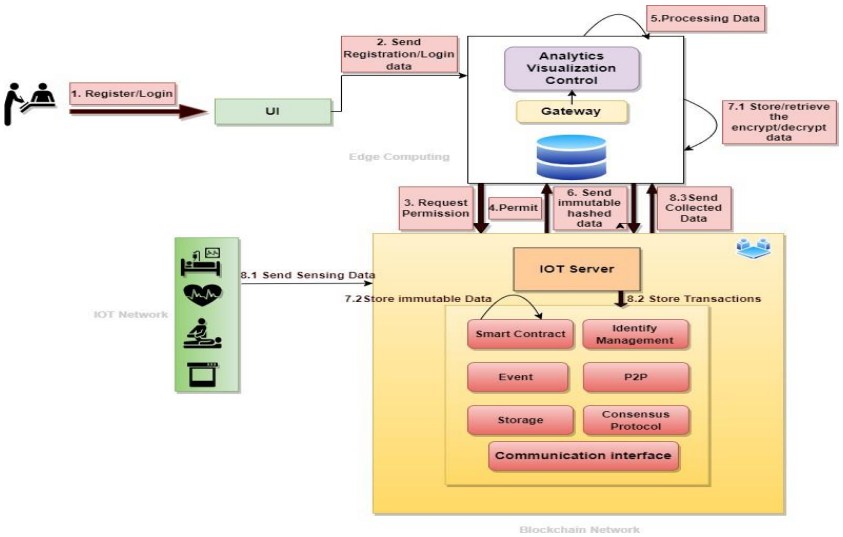


**Figure 6:** Framework of Blockchain network with IoT server of healthcare system

· The first concern in the IoT is the things where things are to be connected to the IoT network that are not scalable and their computing power is very small.

**Second concern**

· The second concern in the IoT is too difficult to manage all the things into the single one.

## Using the blockchain in IOT

With the nature of decentralization in blockchain, it does not rely on third party. In the Fig.7, All the nodes are transparent and maintains the record and achieve high availability of the system. It can work on access control, node to node communication and storage computability[26-27].

## 4Result

As we consider the blockchain with IOT we analysis after comparison our proposed to the xyz. There are somechanges in transaction delay in transaction time: In Fig.8, transaction time is the time when the data from

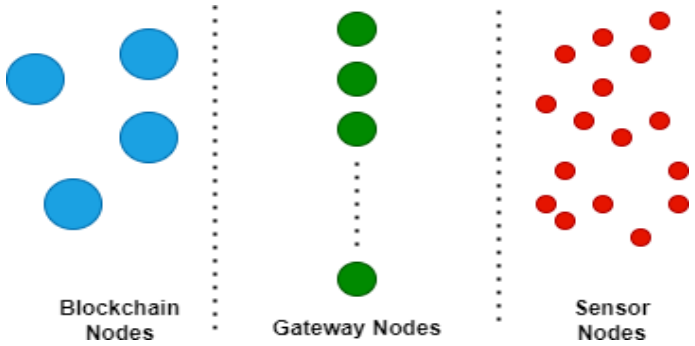


**Figure 7:** Transaction delay between the nodes

sensors to block nodes submitted. The delay in time is separated into the two sections.

$$Latency = Latency^1 + Latency^2 (5)$$

where latency1 is the time from the nodes in sensor into the completion in gateway and latency2 is the time when the transaction in gateway to block nodes. As shown in fig.6. shows that the systematic structure of transaction delay.

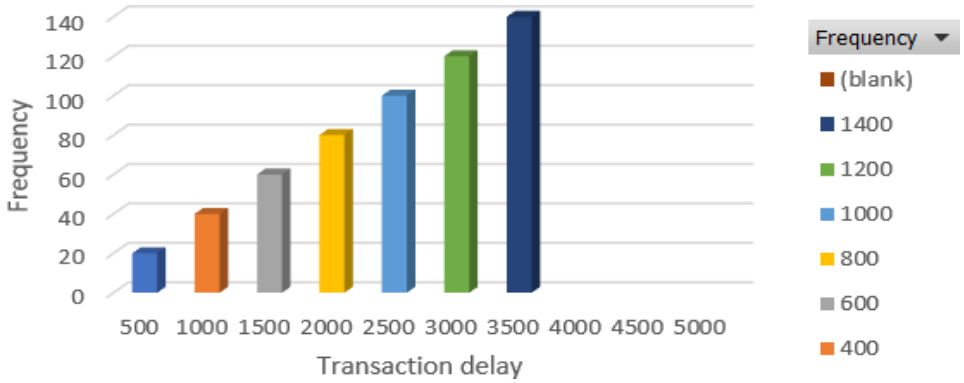


**Figure 8:** Analysis in transaction delay

In the Fig.9,the proposed system gave few positive results as compared to previous studies. Proven that transmission delay is comparatively low in fog cloud system than standalone IoT architecture but in blockchain networks turns almost zero if set efficiently[30-31].

In the Fig.10, it shows the transmission delay in between IoT, Fog and Blockchain and the Fig.11, it showsthe transaction time in IoT where all the nodes are to be connected. In the Fig,12, To compare different network architecture performances in this study we have conducted few tests on DevTools for operating system[28-29]. Network is simulated over range of 5 to 40 nodes. These nodes are low powered wireless personal/regional net- works in connection feature. From above transaction comparison between two stages, we can take an average transaction rate of 70 to 75 bytes. In the Fig.13, Assuming average transaction size be 72 bytes and fixed size number of nodes. We calculated communication time between nodes in blockchain and IoT only architecture.

Finally, we will be evaluating avalanche effect of hash function used in each architecture.Below results concludes that proposed consensus method has good hash result because changes in input produces low changes in its output too. HMAC has higher level of security that SHA-256[32-34].

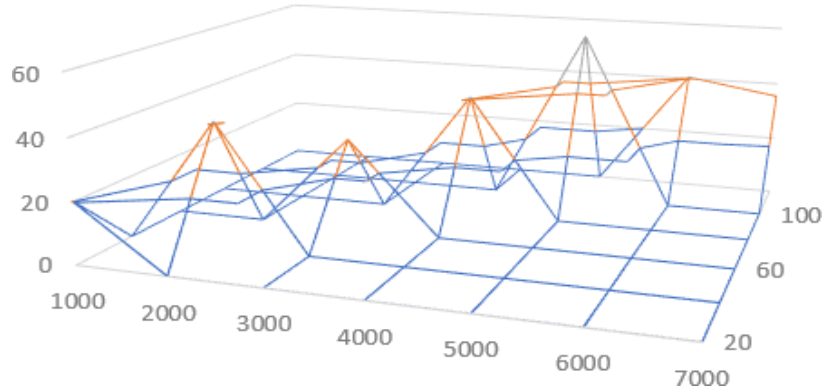


**Figure 9:** Comparison between the two stages

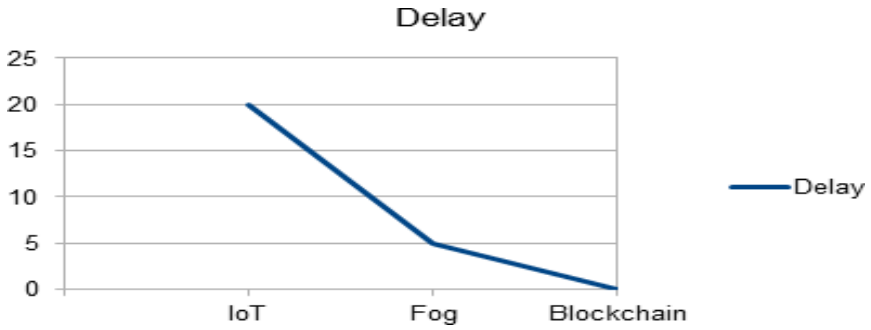


**Figure 10:** Transmission delay over different connection

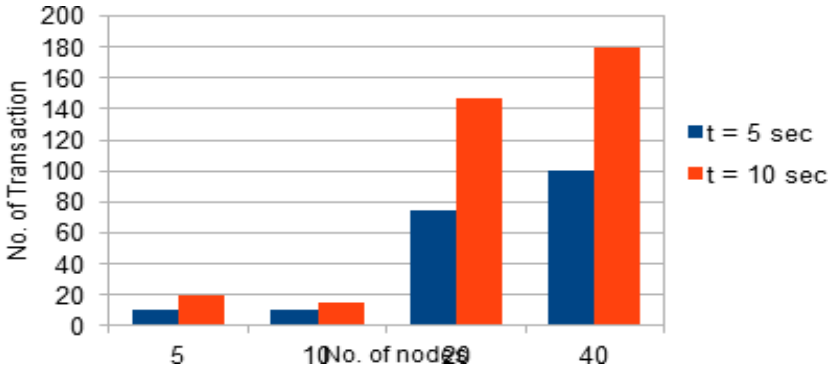


**Figure 11:** Average transaction time in IoT

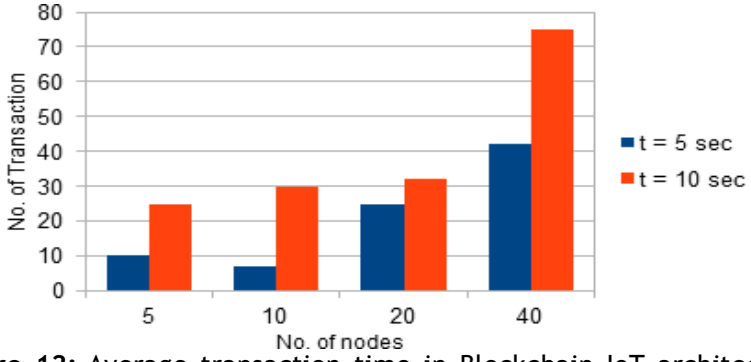


**Figure 12:** Average transaction time in Blockchain IoT architecture

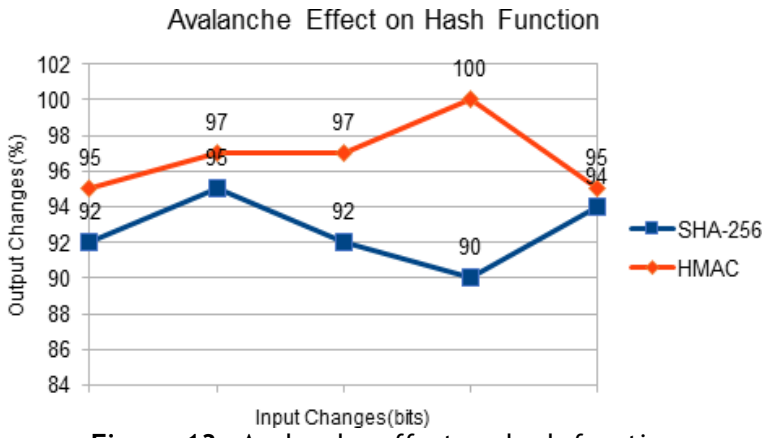


**Figure 13:** Avalanche effect on hash function

## 5Conclusion

Since the various tests carried out it can be proven that Blockchain - IoT system can solve many issues related to security feature in medical services, data exchange transmission problems and integrity guarantee. This can be seen through transmission delay, time estimation over different architecture and avalanche effect on hash function with and without blockchain in IoT.

**Data Availability:** The authors confirm that all data underlying the findings are fully available without restriction. Given simulation results are based on XCT results including data set for open-access use, are available at NSIT.
Digital Repository: https://doi.org/10.18434/mds2-2291.

## References

[1]. Rathee, G., Balasaraswathi, M., Chandran, K. P., Gupta, S. D., & Boopathi, C. S. (2021). A secure IoT sensors communication in industry 4.0 using blockchain technology. Journal of Ambient Intelligence and Hu-manized Computing, 12(1), 533-545.
[2]. Mohanta, B. K., Jena, D., Satapathy, U., & Patnaik, S. (2020). Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology. Internet of Things, 11, 100227.
[3]. Haris, R. M., & Al-Maadeed, S. (2020, February). Integrating blockchain technology in 5G enabled IoT: A review. In 2020 IEEE international conference on informatics, IoT, and enabling technologies (ICIoT) (pp. 367-371). IEEE.
[4]. Wu, Y., Song, L., Liu, L., Li, J., Li, X., & Zhou, L. (2020). Consensus mechanism of IoT based on blockchain technology. Shock and Vibration, 2020.
[5]. Atlam, H. F., Azad, M. A., Alzahrani, A. G., & Wills, G. (2020). A Review of Blockchain in Internet of Things and AI. Big Data and Cognitive Computing, 4(4), 28.
[6]. Atlam, H. F., & Wills, G. B. (2019). Technical aspects of blockchain and IoT. In Advances in computers (Vol. 115, pp. 1-39). Elsevier.
[7]. Da Xu, L., Lu, Y., & Li, L. (2021). Embedding blockchain technology into IoT for security: A survey. IEEE Internet of Things Journal, 8(13), 10452-10473.
[8]. ElRahman, S. A., & Alluhaidan, A. S. (2021). Blockchain technology and IoT-edxge framework for sharing healthcare services. Soft Computing, 25(21), 13753-13777.
[9]. Humayun, M., Jhanjhi, N. Z., Hamid, B., & Ahmed, G. (2020). Emerging smart logistics and trans- portation using IoT and blockchain. IEEE Internet of Things Magazine, 3(2), 58-62.
[10]. Rathee, G., Sharma, A., Kumar, R., & Iqbal, R. (2019). A secure communicating things network frame-work for industrial IoT using blockchain technology. Ad Hoc Networks, 94, 101933.
[11]. Niknejad, N., Ismail, W., Bahari, M., Hendradi, R., & Salleh, A. Z. (2021). Mapping the research trends on blockchain technology in food and agriculture industry: A bibliometric analysis. Environmental Technology Innovation, 21, 101272.
[12]. Rao, A. R., Clarke, D. (2020). Perspectives on emerging directions in using IoT devices in blockchain applications. Internet of Things, 10, 100079.

[13]. Wang, Q., Zhu, X., Ni, Y., Gu, L., Zhu, H. (2020). Blockchain for the IoT and industrial IoT: A review. Internet of Things, 10, 100081.
[14]. Ch, R., Srivastava, G., Gadekallu, T. R., Maddikunta, P. K. R., & Bhattacharya, S. (2020). Security and privacy of UAV data using blockchain technology. Journal of Information security and Applications, 55, 102670.
[15]. Mohanta, B. K., Jena, D., Ramasubbareddy, S., Daneshmand, M., & Gandomi, A. H. (2020). Ad- dressing security and privacy issues of IoT using blockchain technology. IEEE Internet of Things Journal, 8(2), 881-888.
[16]. Azbeg, K., Ouchetto, O., Andaloussi, S. J., & Fetjah, L. (2021). A taxonomic review of the use of IoT and blockchain in healthcare applications. Irbm.
[17]. Lo, S. K., Liu, Y., Chia, S. Y., Xu, X., Lu, Q., Zhu, L., & Ning, H. (2019). Analysis of blockchain solutions for IoT: A systematic literature review. IEEE Access, 7, 58822-58835.
[18]. Panda, S. S., Jena, D., Mohanta, B. K., Ramasubbareddy, S., Daneshmand, M., & Gandomi, A. H. (2021). Authentication and key management in distributed iot using blockchain technology. IEEE Internet of Things Journal, 8(16), 12947-12954.
[19]. Pavithran, D., Shaalan, K., Al-Karaki, J. N., & Gawanmeh, A. (2020). Towards building a blockchain framework for IoT. Cluster Computing, 23(3), 2089-2103.
[20]. Alfandi, O., Khanji, S., Ahmad, L., & Khattak, A. (2021). A survey on boosting IoT security and privacy through blockchain. Cluster Computing, 24(1), 37-55.
[21]. Rathee, G., Sharma, A., Saini, H., Kumar, R., and Iqbal, R. (2020). A hybrid framework for multime- dia data processing in IoT-healthcare using blockchain technology. Multimedia Tools and Applications, 79(15), 9711-9733.
[22]. Košťál, K., Helebrandt, P., Belluš, M., Ries, M., and Kotuliak, I. (2019). Management and monitoring of IoT devices using blockchain. Sensors, 19(4), 856.
[23]. Fotohi, R., and Aliee, F. S. (2021). Securing communication between things using blockchain technol- ogy based on authentication and SHA-256 to improving scalability in large-scale IoT. Computer Networks, 197, 108331.
[24]. Song, Q., Chen, Y., Zhong, Y., Lan, K., Fong, S., and Tang, R. (2021). A supply-chain system framework based on internet of things using Blockchain technology. ACM Transactions on Internet Technology (TOIT), 21(1), 1-24.
[25]. Akram, S. V., Malik, P. K., Singh, R., Anita, G., and Tanwar, S. (2020). Adoption of blockchain technology in various realms: Opportunities and challenges. Security and Privacy, 3(5), e109.
[26]. Singh, P., and Verma, S. (2019). Analysis on Different Strategies Used in Blockchain Technology. Jour- nal of Computational and Theoretical Nanoscience, 16(10), 4350-4355.
[27]. Humayun, M., Jhanjhi, N. Z., Hamid, B., and Ahmed, G. (2020). Emerging smart logistics and trans- portation using IoT and blockchain. IEEE Internet of Things Magazine, 3(2), 58-62.
[28]. Fakhri, D., and Mutijarsa, K. (2018, October). Secure IoT communication using blockchain technology. In 2018 International Symposium on Electronics and Smart Devices (ISESD) (pp. 1-6). IEEE.
[29]. Farouk, A., Alahmadi, A., Ghose, S., and Mashatan, A. (2020). Blockchain platform for industrial healthcare: Vision and future opportunities. Computer Communications, 154, 223-235.
[30]. Kumar, N. M., and Mallick, P. K. (2018). Blockchain technology for security issues and challenges in IoT. Procedia Computer Science, 132, 1815-1823.
[31]. Mohanta, B. K., Jena, D., Ramasubbareddy, S., Daneshmand, M., and Gandomi, A. H. (2020). Ad- dressing security and privacy issues of IoT using blockchain technology. IEEE Internet of Things Journal, 8(2), 881-888.
[32]. Rathee, G., Sharma, A., Saini, H., Kumar, R., and Iqbal, R. (2020). A hybrid framework for multime- dia data processing in IoT-healthcare using blockchain technology. Multimedia Tools and Applications, 79(15), 9711-9733.
[33]. Singh, P., and Verma, S. (2019). Analysis on Different Strategies Used in Blockchain Technology. Jour- nal of Computational and Theoretical Nanoscience, 16(10), 4350-4355.
[34]. Alam, T., and Benaida, M. (2020). Blockchain, fog and IoT integrated framework: review, architecture and evaluation. Tanweer Alam. Mohamed Benaida." Blockchain, Fog and IoT Integrated Framework: Review, Architecture and Evaluation.", Technology Reports of Kansai University, 62(2).
[35]. Singh, M., Singh, A., and Kim, S. (2018, February). Blockchain: A game changer for securing IoT data. In 2018 IEEE 4th World Forum on Internet of Things (WF-IoT) (pp. 51-55). IEEE.
[36]. Ratta, P., Kaur, A., Sharma, S., Shabaz, M., and Dhiman, G. (2021). Application of blockchain and internet of things in healthcare and medical sector: applications, challenges, and future perspectives. Journal of Food Quality, 2021.

[37]. Hussien, H. M., Yasin, S. M., Udzir, N. I., Ninggal, M. I. H., and Salman, S. (2021). Blockchain tech- nology in the healthcare industry: Trends and opportunities. Journal of Industrial Information Integration, 22, 100217.
[38]. Nguyen, G. N., Le Viet, N. H., Elhoseny, M., Shankar, K., Gupta, B. B., and Abd El-Latif, A. A. (2021). Secure blockchain enabled Cyber–physical systems in healthcare using deep belief network with ResNet model. Journal of Parallel and Distributed Computing, 153, 150-160.
[39]. Soni, M., and Singh, D. K. (2021). Blockchain-based security and privacy for biomedical and healthcare information exchange systems. Materials Today: Proceedings.
[40]. Azbeg, K., Ouchetto, O., Andaloussi, S. J., and Fetjah, L. (2021). A taxonomic review of the use of IoT and blockchain in healthcare applications. Irbm.
[41]. Hemalatha, P. (2021). Monitoring and securing the healthcare data harnessing IOT and blockchain technology. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(2), 2554-2561.
[42]. Alzubi, J. A. (2021). Blockchain-based Lamport Merkle digital signature: authentication tool in IoT healthcare. Computer Communications, 170, 200-208.
[43]. Wang, W., Qiu, C., Yin, Z., Srivastava, G., Gadekallu, T. R., Alsolami, F., and Su, C. (2021). Blockchain and PUF-based lightweight authentication protocol for wireless medical sensor networks. IEEE Internet of Things Journal.
[44]. Younis, M., Lalouani, W., Lasla, N., Emokpae, L., and Abdallah, M. (2021). Blockchain-Enabled and Data-Driven Smart Healthcare Solution for Secure and Privacy-Preserving Data Access. IEEE Systems Journal.
[45]. Singh, P., Singh, A.P. and Gupta, A. 2021. Design Strategies for Mobile Ad-hoc Network to Prevent from Attack. Proceedings of the 3rd International Conference on Advanced Computing and Software Engineer- ing. SCITEPRESS - Science and Technology Publications.
[46]. Veeramakali, T., Siva, R., Sivakumar, B., Senthil Mahesh, P. C., & Krishnaraj, N. (2021). An intelligent internet of things-based secure healthcare framework using blockchain technology with an optimal deep learning model. The Journal of Supercomputing, 77(9), 9576-9596.
[47]. Gupta, S., Yadav, B., & Gupta, B. (2022). Security of IoT-Based e-Healthcare Applications Using Blockchain. In Advances in Blockchain Technology for Cyber Physical Systems (pp. 79-107). Springer, Cham.
[48]. Haque, A. B., Muniat, A., Ullah, P. R., & Mushsharat, S. (2021, February). An automated approach towards smart healthcare with blockchain and smart contracts. In 2021 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS) (pp. 250-255). IEEE.
[49]. Ghayvat, H., Pandya, S. N., Bhattacharya, P., Zuhair, M., Rashid, M., Hakak, S., & Dev, K. (2021). CP-BDHCA: Blockchain-based Confidentiality-Privacy preserving Big Data scheme for healthcare clouds and applications. IEEE Journal of Biomedical and Health Informatics.
[50]. Srinivasu, P. N., Bhoi, A. K., Nayak, S. R., Bhutta, M. R., & Wo ́zniak, M. (2021). Blockchain Tech- nology for Secured Healthcare Data Communication among the Non-Terminal Nodes in IoT Architecture in 5G Network. Electronics, 10(12), 1437.
[51]. Nagarajan, G., & Kumar, K. S. (2021, March). Security Threats and Challenges in Public Cloud Storage. In 2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE) (pp. 97-100). IEEE.
[52]. Kirubakaran, J., Venkatesan, G. K. D., Sampath Kumar, K., Kumaresan, M., & Annamalai, S. (2021). Echo state learned compositional pattern neural networks for the early diagnosis of cancer on the internet of medical things platform. Journal of Ambient Intelligence and Humanized Computing, 12(3), 3303-3316.