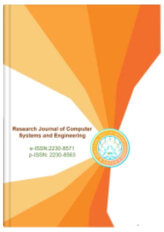
Research Journal of Computer Systems and Engineering

ISSN: 2230-8571, 2230-8563

Volume 01 Issue 02 - 2020 (July to December)

Page 26:30



Secure Internet of Things Environment Based Blockchain Analysis

Nouby M. Ghazaly
Professor, Faculty of Engineering,
South Valley University, Qena 83523, Egypt.
https://orcid.org/0000-0001-6320-1916

Article History	***Abstract***
Received: 15 July 2020 Revised: 20 September 2020 Accepted: 22 November 2020	Due to its indisputable nature and associated benefits of security and privacy, blockchain (BC) has attracted a lot of attention. BC has the potential to address IoT's shortcomings with data security and privacy. Due to the enormous scale and distributed nature of IoT networks, IoT security and privacy continue to be a significant concern. Because of sophisticated algorithms, security overhead, throughput, and latency, the BC described solutions are not workable to construct IoT applications. The proposed Blockchain based IoT is designed to handle mainly privacy and security threats, though consider many IoT devices resource-constraints. Keywords: Blockchain, IoT environment, Security, Privacy, untrusted parties.
CC License	CC-BY-NC-SA

1. Introduction

IoT has gained popularity over the past ten years in a variety of applications. Due to the incompatibility of traditional-based existing security protocols with IoT devices, the installation of the IoT system poses security and privacy challenges [1]. In order to address various security challenges, authors of this paper have selected three major technologies: ML, Blockchain, and AI. Blockchain technology is a distributed/decentralized network in which every node is interconnected with every other node in some way. The Blockchain network broadcasts the message. A block is made up of numerous legitimate transactions and the properties connected to them. The self-executing programmer known as a smart contract [2] is utilized on the network to implement business logic. To achieve consensus among the nodes, the Blockchain network uses a variety of consensus algorithms [3]. Blockchain is utilized for distributed data storage and sharing because it is immutable, auditable, and timestamp-enabled [4].

2. Related works

Review the research on the security challenges that affect the blockchain and IoT systems in this area. This survey's goal is to pinpoint the remedy required to deal with the security issue [5]. To be effective, blockchain and IoT applications must solve security, one of the most difficult issues. The authors of paper[6] provide a detailed explanation of the Blockchain's architecture and application areas. The technique and related work on IoT security, as well as Blockchain as a solution approach, were detailed by the authors in paper[7,8]. In [9,10], the authors put forth a safe framework based on a distributed Blockchain system for IoT applications.

3. Experimental Methodology

The experimental methodology shows the blockchain network with IoT device is shown in figure 1. Cloud storage system is verifies the data in blockchain network. The IoT devices are communicate through gateway to blockchain network. The data transmission among the network is secure manner.

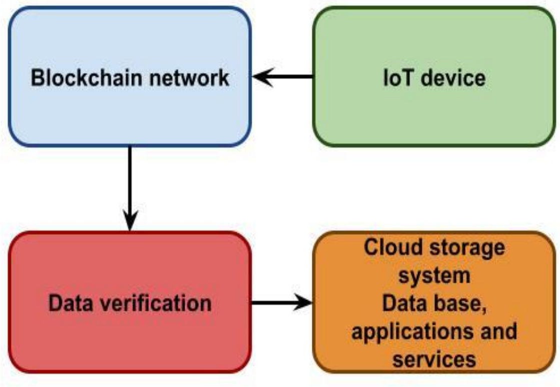


Figure 1: Experimental Methodology Model

3.1 Data Verification

Data verification is to reduce instrument and human errors, including those that occur during data processing, and to ensure that the data collected are as accurate as feasible. Data validation is a continuous process that must begin with data collection and continue through data entry and analysis.

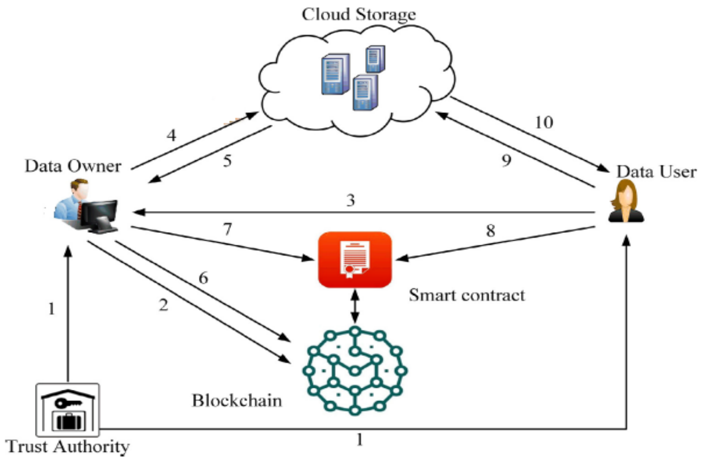


Figure 2: Proposed Network Model

Above figure 3 shows that every number describes a process as follows:

I. The Setup algorithm is used by TA to produce the keys. The Data Owner (DO) and Data User will use these keys (DU).
II. DO develop the blockchain smart contract. A smart contract must have encrypted data.
III. to make use of the cloud-based data. DU notifies DO of its desire to register.
IV. DO call for encryption, which transmits the data to the cloud after being encrypted in accordance with the access structure tree.
V. DO take note of the file location information that the cloud server returns.
VI. DO embeds the File Location Information (FLI) into the blockchain after hashing it.
VII. DO create the FLI index with hashes and save it in the smart contract.

4. Results and discussion

Performance of proposed system method is calculated based on four metrics one is average processing time for block and storage overhead, encryption and decryption. Table 1 shows average processing time for blocks. Data block is gradually increases then the storage overhead is also gradually increases which are shown in below graph.

Table 1: Comparative analysis between proposed and existing technique

Parameters	BC_IoT	DO_IoT	SIoT_BA
Average processing time	68	72	75
Storage overhead	75	78	85
Encryption	55	56	58
Decryption	44	43	52

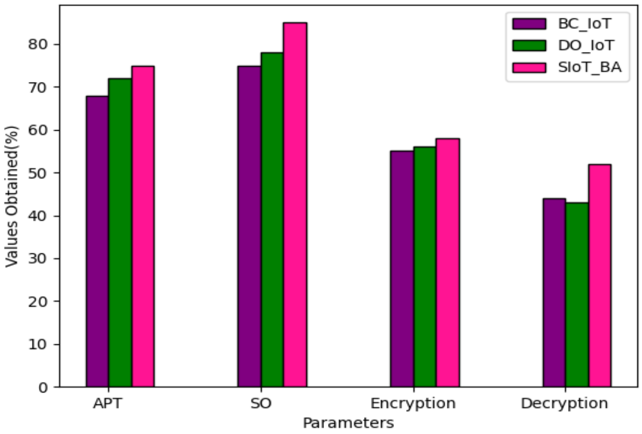


Figure 3: Overall comparison of proposed and existing methods

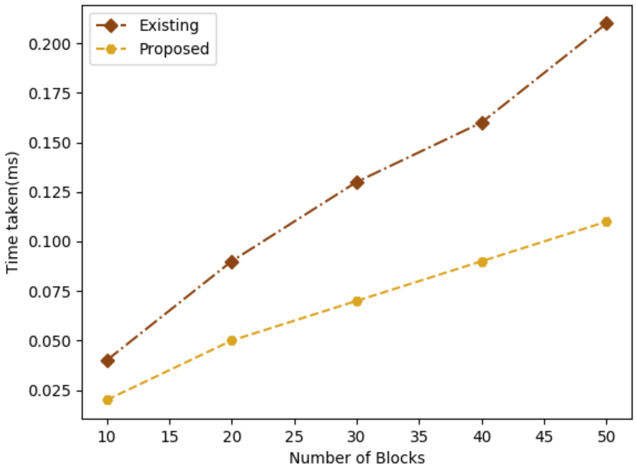


Figure 4: Average processing time of data blocks

The above figure 4 shows that existing and proposed model average processing time for data blocks. The data block is gradually increases then the storage overhead is gradually decreases which are shown in below graph.The below figure 5 shows that existing and proposed model storage overhead. Proposed model achieves good results when compared to existing model. The above figure 6 presented encryption and decryption performance of existing and proposed method. Existing model achieves encryption 90ms, decryption 48ms and proposed model achieves encryption 45ms, decryption 19ms. When compared to existing method proposed method achieves good results.

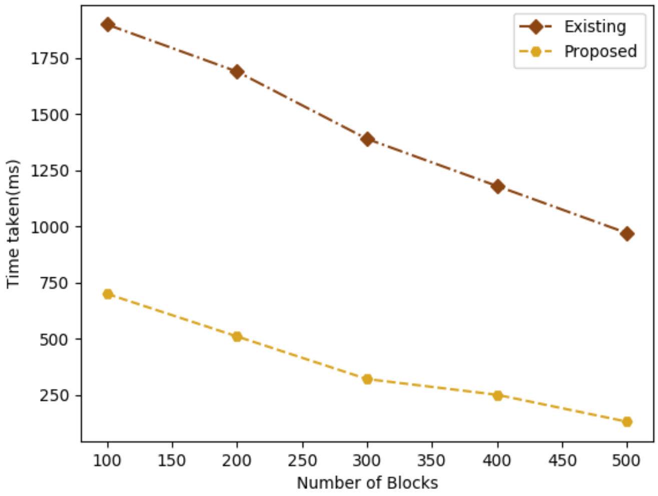


Figure 5: Storage overhead performance

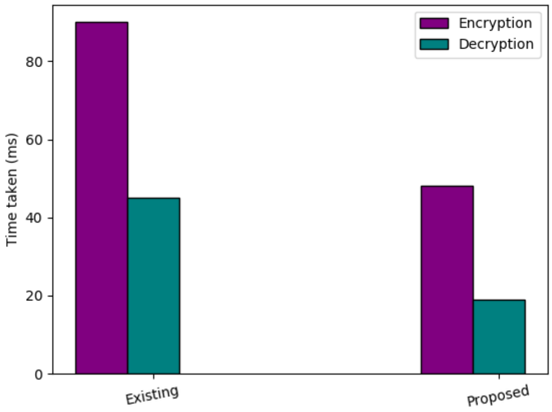


Figure 6: Encryption and Decryption performance

5. Conclusion

IoT has generated a lot of buzz in the tech industry. It has played a crucial role in offering cutting-edge solutions in a variety of industries. Researchers now comprehend the blockchain's (BC) potential in relation to security and authentication.Particularly, BC's decentralised structure makes it suitable for integration with IoT networks.The suggested approach is an alternative for IoT networks that uses blockchain technology to improve the security shortcomings of IoT.The combination of blockchain and IoT will pave the way for the creation of new applications because the IoT devices operate as physical world interaction points.Future benchmarking measures for platforms could include throughput, latency, scalability, and fault tolerance as more platforms become reliable and developed.

REFERENCES

[1] Atlam, H.F.; Wills, G.B. IoT Security, Privacy, Safety and Ethics. In Intelligent Sensing, Instrumentation and Measurements; Springer Science and Business Media LLC: Berlin, Germany, 2019; pp. 123–149.

[2] B. K. Mohanta, S. S. Panda, D. Jena, An overview of smart contract and use cases in blockchain technology, in: 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT), IEEE, 2018, pp. 1–4

[3] S. S. Panda, B. K. Mohanta, U. Satapathy, D. Jena, D. Gountia, T. K. Patra, Study of blockchain based decentralized consensus algorithms, in: TENCON 2019-2019 IEEE Region 10 Conference (TENCON), IEEE, 2019, pp. 908–913.

[4] A.Kosba, A. Miller, E. Shi, Z. Wen, C. Papamanthou, Hawk: The blockchain model of cryptography and privacy-preserving smart contracts, in: Security and Privacy (SP), 2016 IEEE Symposium on, IEEE, 2016, pp. 839–858.

[5] Choi, Y. J., Kang, H. J., & Lee, I. G. (2019). Scalable and secure internet of things connectivity. *Electronics*, *8*(7), 752.

[6] Gong, S., Tcydenova, E., Jo, J., Lee, Y., & Park, J. H. (2019). Blockchain-based secure device management framework for an internet of things network in a smart city. *Sustainability*, *11*(14), 3889.

[7] X. Yue, H. Wang, D. Jin, M. Li, W. Jiang, Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control, J. Med. Syst. 40 (10) (2016) 218.

[8] Ren, Y., Zhu, F., Sharma, P. K., Wang, T., Wang, J., Alfarraj, O., &Tolba, A. (2019). Data query mechanism based on hash computing power of blockchain in internet of things. *Sensors*, *20*(1), 207.

[9] Zhu, X., &Badr, Y. (2018). Identity management systems for the internet of things: a survey towards blockchain solutions. *Sensors*, *18*(12), 4215.

[10] Li, S., Qin, T., & Min, G. (2019). Blockchain-based digital forensics investigation framework in the internet of things and social systems. *IEEE Transactions on Computational Social Systems*, *6*(6), 1433-1441.