Turkish Journal of Computer and Mathematics Education Vol.12 No. 5 (2021), 1206-1215

Research Article

Hashing based Data Transaction and Optimized Storage for IoT Applications

Monika Parmar[a], Harsimran Jit Kaur[b]

[a]Chitkara University School of Engineering and Technology, Chitkara University, Himachal Pradesh, India.
E-mail: monika.parmar@chitkarauniversity.edu.in
[b]Chitkara University Institute of Engineering and Technology, Chitkara University, Punjab, India.
E-mail: harsimran.kaur@chitkara.edu.in

Article History: Received: 11 January 2021; Accepted: 27 February 2021; Published online: 5 April 2021

Abstract: Blockchain technology, which would be the underlying technology, has recently become very popular with the increase in cryptocurrencies and is being used in IoT and other fields. There have been shortfalls, however, which impede its implementation, including the volume of space. Transactions will be produced at a significant level due to the huge amount of Connected systems that often work in many networks as data processors. In IoT, the storage issue will become more intense. Current storing data platforms have a wide range of features to respond to an extensive variety spectrum of uses. Nevertheless, new groups of systems have arisen, e.g., blockchain with data version control, fork semantics, tamper-evidence or some variation thereof, and distributed analysis. They're showing new challenges for storage solutions to effectively serve such energy storage Systems by integrating the criteria mentioned in the processing. This paper discusses the potential security and privacy concerns of IoT applications and also it is shown that in first step the storage is enhanced by 50% and further in the next step, it is improved and it takes only 256 bytes irrespective of the input data size.

Keywords: Blockchain Technology, IoT, Storage Optimization, IoT Security

1. Introduction

The user interface for the cryptocurrency is BLOCKCHAIN. As described by Bitcoin, Blockchain initially emerged in 2008. This was introduced by Nakamoto [1] and the definition thereof is a form of the ledger to record the transactions. Users just talked about Cryptocurrency for a long period of time, so they knew nothing about the blockchain. Mostly with the popularity of online currencies, blockchain study has shown exponential development. Blockchain is a multi-field product that includes cryptographic, consensus protocol, and P2P (peer-to-peer) channels. At present, owing to its unique characteristics such as decentralization, untraceability, confidentiality, and security, a vast amount of research is based upon the applications of blockchain to banking, healthcare, education, IoT (Internet of Things), and other sectors. Many universities however have chosen to provide students and their faculty with blockchain digital wallets that retain their credentials to avoid educational and service record fraud simultaneously. While there are great growth opportunities for blockchain, there are still some shortfalls, including scalability and data storage space issues. To maintain the entire ledger, the decentralized system requires complete nodes, which definitely ensures security, but creates wastage of cloud infrastructure and generates storage constraint on nodes, compete for limited processing power. In certain IoT network that uses blockchain infrastructure, because of the constraint of IoT devices, they will often not specifically become a peer in blockchain, but instead, create a link with a particular platform or server. At this stage, the linked server will act as a node, and the focus is passed to the subsequent server to store the full blockchain database. In addition, a significant number of Connected devices create transfers at a significant level, making the volume of transactions enormous.

1.1. Motivation of the Work

The Internet of Things (IoT) is extending at a quick movement and a few reports anticipate that IoT gadgets will develop to 26 billion by 2020, which are multiple times the assessed number of gadgets sent in 2009 and is unmistakably more than the 7.3 billion cell phones, tablets and PCs that are required to be being used by 2020[8]. Internet of Things (IoT) and Block chain are viewed as rising ideas and innovations. Simultaneously they change ideas and make additional opportunities, each in their particular situations, and there is a chance to make applications that can share the inherent attributes of both, investigating how the IoT can profit by the decentralized idea of the Blockchain. Every gadget delivers and trades information on the Internet. Accordingly, thinking about these gigantic numbers of gadgets, it is straightforward that we are discussing a broad and consistent creation of information. Tending to the principal security issues for such a huge data framework is a test in itself. A fundamental test for IoT is its dispersed architecture. The IoT is an extensive term alluding to continuous endeavors to interface a wide assortment of physical things to correspondence organizations. Right now, the Internet has ordinary PCs associated as well as a huge heterogeneity of gear, for example, TVs, workstations, refrigerators, ovens, electrical machines, vehicles, and smartphones. Security arrangements and security ought to be executed

by qualities of heterogeneous IoT gadgets[9]. There is an interest for security arrangements that are fit for giving proportional degrees of security to different kinds of gadgets and requests components equipped for review and access control in these environments. Currently, most IoT arrangements depend on the incorporated worker customer worldview, associating with cloud workers through the Internet. In spite of the fact that this arrangement may work appropriately these days, the normal development recommends that new ideal models should be proposed. Among such recommendations, decentralized structures were proposed in the past to make huge Peer-to-Peer (P2P) Wireless Sensor Networks (WSNs), yet a few pieces were absent corresponding to protection and security until the appearance of blockchain innovation. Subsequently, as it is outlined in Figure 1, in the most recent years pre-IoT shut and concentrated centralized computer designs developed towards IoT open-access cloud-focused other options, being the following stage the appropriation of the cloud usefulness among numerous friends, where blockchain innovation can help. Blockchain advances can follow, facilitate, do exchanges and store data from a lot of gadgets, empowering the formation of utilizations that require no incorporated cloud[10]. The figure 1 shown below expresses the number of users in internet, mobile and networked device or connection from 2018 till 2023. The value expresses the need of IoT device and secured transmission of the data.

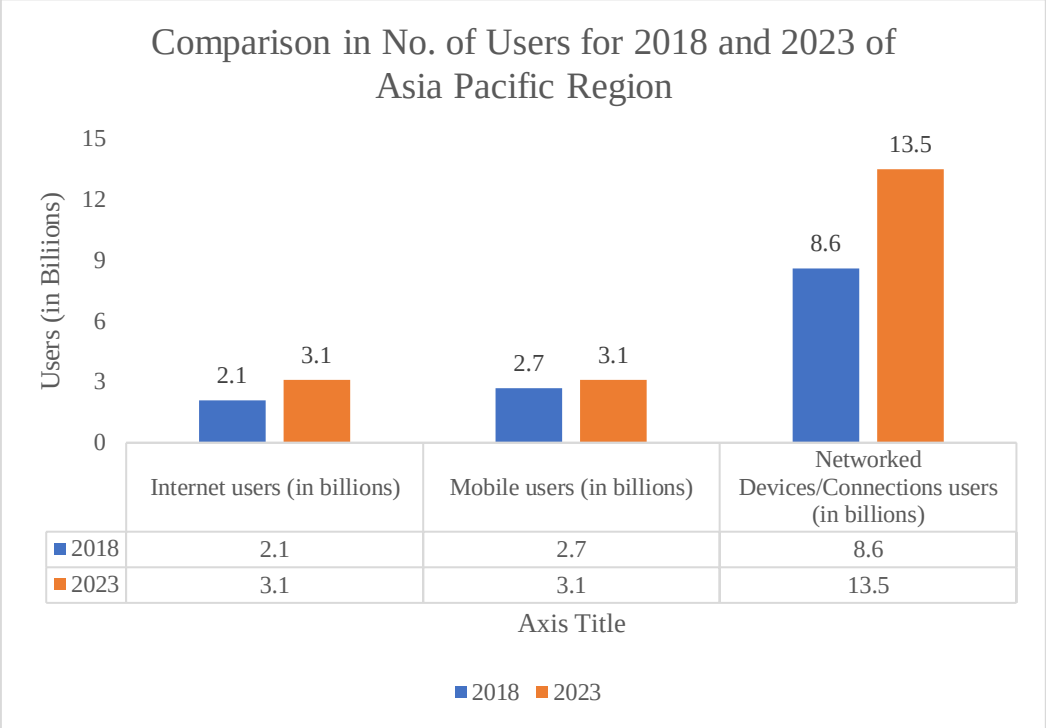

Figure 1. Comparison in Number of Users for 2018 and 2023 of Asia Pacific Region

2. Background and Related Work

Because of blockchain's rising interest in a smart home, numerous articles are being extensively studied in the literature. It is important to realize that a lot of Initiatives in the BIoT sector being worked out, however, many questions arise for instance:

- How to handle storage issues of IoT applications as number of IoT devices are increasing at a very fast pace?
- What and on which layer are the various threats/attacks can incur on IoT infrastructure?
- Is it feasible to use blockchain for IoT applications for its security, privacy, and storage optimization?
- How to manage massive volume of data generated by IoT devices in real-time?
- What are the various threats to blockchain technology in terms of security and transactions?

Quite recently, work has begun to answer above mentioned questions. For example, the blockchain concepts and its role in Internet of Things is being presented in [11] where the authors explained the integration of IoT and Blockchain and also presented its impact on other sectors. However, the security and the storage issues are understudied in this survey. Ref. [12] evaluates the different issues blockchain is facing in its development for universal functional implementation, taking account of security methodology to several attacks, selfish mining, and confidentiality disclosure with the blockchain efficiency vulnerabilities in consideration of scalability and

accessibility, frameworks. The work presented in [13] specifies the optimization of network coding-based Internet contact and secure storage of things. The authors suggested the adaptive network coding for the IoT applications in consideration with WSN. Simulation findings showed that the transmission efficiency of the proposed scheme will be higher than the one of existing infrastructure and also, they presented the optimum issue of optimizing the storage to distributed cloud computing but both storage and security issues of IoT is understudied however,[14] explored that it increases the reliability and intrusion detection frequency of data access and offers a more sophisticated technological platform for data accessibility management. In addition, the evaluation results revealed that IoT knowledge is improved by the method presented in this study, and also it is preferable in respect of the communication rate to the previous form. Furthermore, the IoT limit the performance of optimized transmission information processing can approach 99 percent, and the optimized algorithm's peak intrusion detection rating may hit 96.12 percent. The authors covered the security issues and address them but did not covered the storage optimization for IoT applications. Starting with the IoT context, Optimization of BC that removes the workload compared with the existing BC is presented in [15] by preserving its advantages in terms of protection and privacy. The authors proposed the BC that needs no mining and therefore does not impose any extra delays in computing the transactions produced , also, security concerns are partially covered in this whereas [16] proposed the optimized "sensor-chain" basically for resource-constrained BIoT framework for sensor applications with n. The authors presented the lightweight BIoT in three various layers that includes the spatial blockchains that is distributed into shorter discontinuous localized blockchains domain, so that there will be reduction in data storage capacity as compared to the existing blockchain. [9] presented a systematic review of the case study of smart home in respect of its security and privacy using blockchain and IoT. The authors highlighted the various fundamental elements of the home automation tier and addressed the various relevant processes and protocols by considering its confidentiality and protection. Also, the same is incurred in [17] where the authors broaden up open issues in BIoT and shown the research directions in the security in IoT applications. More precisely, there seems to be a lack of a shared vision about protection and privacy safety regulations in such a diverse world comprising various devices and networking protocols.

2.1. Blockchain Technology

Bitcoin's suggested alternative comprised of searching for the agreement of many of these network nodes, which attach the legitimate blocks to the blockchain. As its title indicates, a blockchain is a sequence of interlinked blocks with time-stamped connected by secured hashes. For the blockchain, a peer - to - peer system with all the entities involved in creating must first be established[21]. Two separate keys are received by each service node that is a public key, used by several nodes to encrypt files and a private key that enables those messages to be interpreted by the module. Thus, two separate keys have been used, one just for encryption and the other for decryption. The secret key is being used in practice to validate any transactions (i.e., to authorize certain transactions), whereas the public key serves as a unique identifier. The communications coded with either the primary key that is referenced can be decrypted only by the individual with the appropriate encryption key. Whenever a transfer of data is performed by a node, it signatures it first and then communicates it to its another-hop node peers. Signing a document in a special way (that used a secret key) allows this to be authenticated (it could only be signed by a person with a similar encryption key) and ensures confidentiality (whether there's a malfunction while transferring the data, the same will not be decoded)[22]. Even as module peers who communicate the transfer acquire the digitally signed transfers verified that it is legitimate while retransmission it to other nodes. The transactions promulgated within that manner and considered acceptable by the system are organized and packaged by specific nodes into a time-stamped block. Blockchain is getting popularity in almost every sphere because of its unique features and these are depicted in figure 2 that shows there are proper validation check, decentralized, distributed ledger, faster settlement, peer-to-peer network, immutable, Consensus, and highly secured network in blockchain framework[23].

Almost all miners' nodes are interested in the inadequacy phase and try to locate Nonce. The entity that detects the nonce first is entitled to validate and earn a bonus. In addition, the newly generated block will be distributed to certain other entities across the existing system. After a block is entered into the blockchain, it cannot be changed as it is immutable. In a blockchain framework, the consortium blockchain is utilized to give data protection. To create a personal system, nodes used for a specific purpose are merged simultaneously. A specific ID is allocated to every IoT system in order to monitor information in the public blockchain. Data obtained from a computer is labelled with its ID, and the information is sent to the overall infrastructure after computing the information hash.

Figure 2. Features of Blockchain

2.2. IoT Technology

At present, brought together design models broadly used to confirm, approve and interface various hubs in an IoT organization. Because of the basic part of IoT gadgets in detecting the encompassing scene and actuating properly, gathering dependable information has an indispensable bearing on the exact usefulness of these gadgets[26]. IoT information dependability can be accomplished by utilizing disseminated signal handling strategies which execute a confirmation cycle among every one of its members to guarantee that information stays changeless and untampered. A key part of IoT is information. This decentralized IoT organization may coincide with customary local center points or concentrated cloud based IoT models[27]. The decentralized evidence for IoT considers monetary reasonability and adaptation from IoT. Circulation of substance to gadgets - be it programming moves up to Things or food menu estimating substance to computerized shows in a diversified organization of cafés or promotion substance to leased screen space on huge configuration shows or flight status and door task substance to air terminal screen and versatile travel applications - in every one of these cases can be submitted, settled, and cleared in decentralized companion way from hubs on the Blockchain[28]. The layered architecture of IoT and its functions are depicted in figure 3.

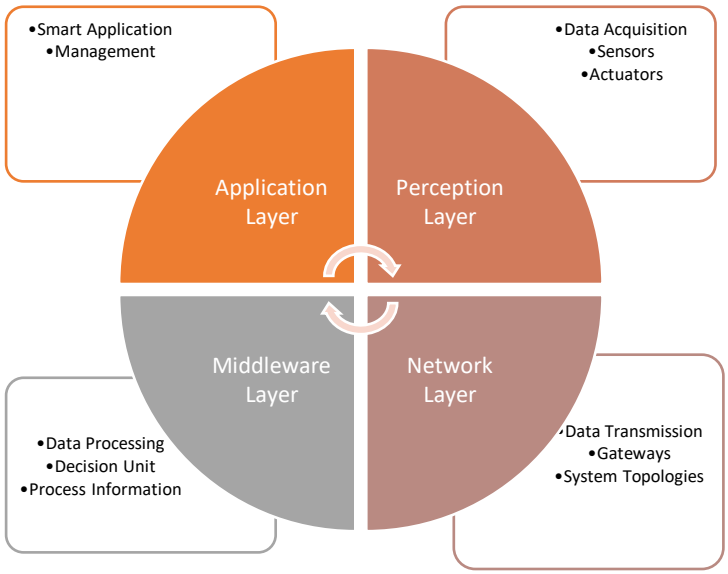

Figure 3. Layered Architecture of IoT and its Functionary Units

3. Proposed Framework

The proposed framework has its functionalities in two main parts namely Compressing technique and Decompressing technique.

3.1. Compressing Technique for the Framework

The information from multiple IoT smart applications will initially be collected at the activation of the application and unit integrity will be tested. During the first phase of processing, the device collects data regularly from the IoT sensor module. If the machine is not enabled, then the piece of data will be refused. Typically, inside an array, the data is registered over a certain period of time. In addition, the data is sorted in an ascending order using a sorting algorithm. Eventually, a calculation takes place in which the mean values of any 2 consecutive elements of the data set are calculated. That's how we get a mean parameter per each range of parameters. The data will be registered in spreadsheets just after the authentic node, but after arranging it in increasing order, the median of each set will be determined and the compressed file format saved. The compression technique is being depicted in Algorithm 1.

3.2. De-compressing Technique for the Framework

Initially, the Server approved the request for data in the decompression process. Alternatively, the Server receives the Source code according to the request bearing the data values. Though we have initially reduced the numerical value by fifty percent, we would have to increase the amount twice. After generating all the numbers, save the collected details in a set. Accordingly, the variables are documented in a report and the file is submitted for delivery. When there might be some disparity, which is called a mistake, between the actual sources and the collected data. By decreasing the deviation, we are able to raise the payload capacity as much as practicable. The decompression technique is being depicted in Algorithm 2.

Algorithm 1:
Algorithm for Sensor data compression and encryption
INPUT: Data from the IoT Sensors
OUTPUT: Compressed and Secured Data in blockchain

```
readData function (Url of sensor data.csv) returns the array of data
{
        define array
        declare variable i
        try
        {
                Read the data from the Url using the object of classes
                loop:
                        read the data till end of file
                        read the data splited by delimiter
                        read the splited contents
                        store in the array ith location
                        increase the value of i with 1
                loop ends
        }
        catch if error found
        print the error
 return the array
}
dataEncrypt (string, secret key) return the encrypted string
{
        declare the string
        try
        {
                use the predefined classes for string encryption with help of secret key using SHA-256 instance
and AES encryption
        }
        catch if error found
        print the error
return the string
}
CompressData function (array of data) returns the array
{
        declare an array
```

```
        declare the variable i and j initialize with 0
        loop:
                read the data at ith location
                find mean of ith and (i+1) th location data
                store the mean in the array
                loop continues till the length of data
        loop ends
return array
}
In the Main Function
{
        Define string variables to read sensor data from the.csv files
        Define a secret key
        send this address to readData function (string url of.csv) and returns the data in form of array
        send this data to the function CompressData(array) returns the data with half compression
        loop:
                Create string from all sensor data
                string encdata stores data from dataEncrypt (string, secret key)
                if array has no more contents
                        loop break;
        loop ends;
}
```

Algorithm 2:

Algorithm for Sensor Data Decompression at Receiver End

INPUT: Compressed and Secured Data in Blockchain

OUTPUT: Original IoT Sensor Data at Receiver end

```
   readData function (String Url of encrpted data,ith location) returns strings
   {
        declare string variable
        try
                {
                loop
                        read data the file using predefined class one line at time
                        store the data of ith location in the string variable
                        if data doesn't exist
                        loop break
                loop ends
                }
                catch if error found
                print the error
   return the string
   }
   dataDecrypt function (string variable, secret key) returns decrypted data string
   {
        declare the string
        try
        {
                use the predefined classes for string decryption with help of secret key using SHA-256 instance
and AES encryption
        }
        catch if error found
        print the error
```

```
return the string
}
in the Main Function
{
    declare string variable holds the Url of encrypted strings data
    declare the array variables for sensor data
    declare variable i and initialize with 0
    declare string array
    Loop:
        readData(Url of encrypted data,ith location) returns strings stores ith string ith location in string
array
        string variable stores dataDecrypt(string[ith], secret key) return string of decrypted data
        loop till end of line:
            split and read the string using delimeter
            stores the data in the array variables
        loop ends
        increase ith value with 1
        if data not available in file
        loop break
    loop ends
}
```

4. Result

Three sensors data is taken into consideration for compression and protection, which are Sensors for temperature, humidity, and carbon dioxide level in the air which are configured with Node MCU, and data analysis is done on Thing Speak. The readings are collected in the spreadsheets after the review of information in the cloud. The attributes gathered from each sensor are shown in Fig. For the failure rate, out of three sensor units, hundred sample values have been taken. The optimization for the storage is carried out in two phases, which are listed below.

Step I: Compression Technique for Improving Storage

Different sensors supply the sensory information as per the suggested approach to data encryption and standardisation in IoT cloud services utilising blockchain based technology, and this should be organised using any sorting methods. We have organised the information here using the technique of bubble sorting to identify the requirement selected from various actuators. Then measure the full set average for each data sources. With all device meta data, this method of computing the sum and storing it in another file will commence. In this, the three sensors and 100 recordings from each device database were registered. By implementing the average method mentioned above, each document's data is compressed to half the entire number of each record. With further verification and transmission into the network, this information can be accessed in some other documents. With the Compression technique for improving storage capacity, the storage is being optimized by 50%.

Step II: Transaction of Data through Encrypted Cryptography

Utilizing instances of SHA-256 and Advanced Encryption Standard authentication, compressed information is encoded and decoded using a private key created. Afterward, by removing the ith log within each document and constructing the sequence, the freshly created string is generated. The ciphertext with almost the same private key is processed in the cryptographic algorithm and the generated string is processed to secure the information in various files. By using SHA instance for optimizing the storage capacity, it is being reduced further from 50% to just 256 bytes. The Thingpeak analysis for the three sensors is depicted in figure 4, figure 5, and figure 6.

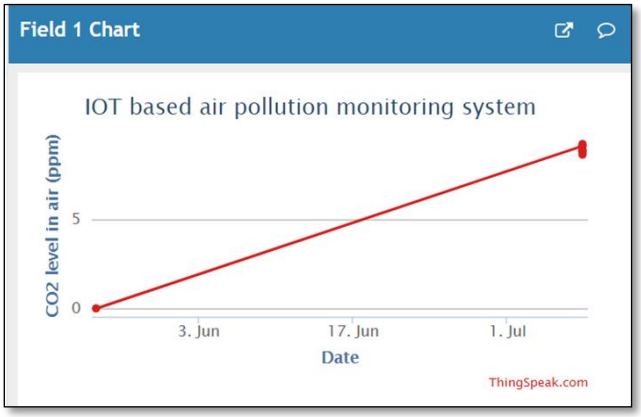

Figure 4. Analysis of CO2 Level in Air Sensor

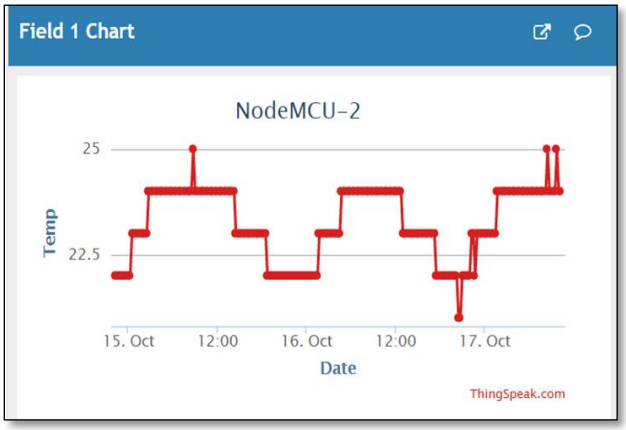

Figure 5. Analysis of Temperature Sensor

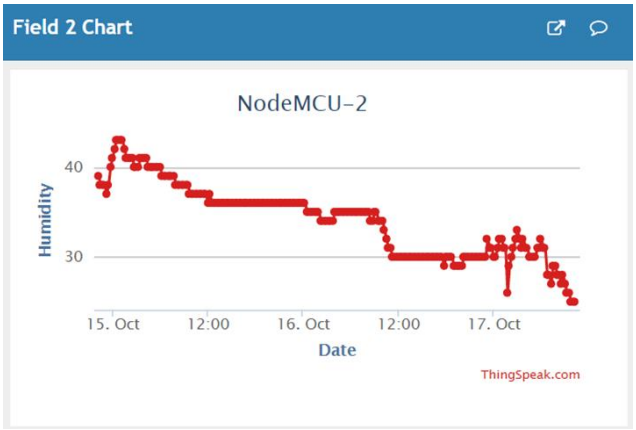

Figure 6. Analysis of Humidity Sensor

The IoT sensors data is being gathered and storage is optimized to 50% of the input and after applying the secured hash algorithms, it is reduced to 256 bytes irrespective of the input size, the output will always be 256 bytes only. The encrypted data which is sent onto the blockchain is shown below.

Secret Key: tSKVp3NASmFF2wYpjbghN9LqJFzvMpD7 (generated randomly)
Data before sending into Blockchain: 3.0 0.0 27.0 0.0 -5.0 33.55476379394531
Data in blockchain: bFDkdnD/kipyvslaKmfwekzHgDUmNVxoc7LntCQi8x4Tpt6L3Ar7vcnT5eZmrQ5d
Recovering data from Block chain:
bFDkdnD/kipyvslaKmfwekzHgDUmNVxoc7LntCQi8x4Tpt6L3Ar7vcnT5eZmrQ5d
Data decryption: 3.0 0.0 27.0 0.0 -5.0 33.55476379394531
After decrypting this data stored into the excel files and compared with the generated data for the accuracy check

5. Conclusion

Blockchain provides IoT security and anonymity with great hope. Because of many corresponding problems, including heavy power consumption, interoperability, and frame buffer, it is also not simple to adjust BC to IoT besides that. In this paper, it is proposed that an integrated blockchain offers security and privacy benefits through this observational investigation. The proposed BC does not require extraction so it does not create any further delays in the processing of the generated transactions. The proposed BC does not involve any spinning and does not really cause any further delays in the management of the transfers produced. The proposed BC does not involve any refining and thus does not cause any delays in the management of the transfers produced. It implements a common model that makes a centralized ledger at the IoT network level to optimize the storage issues and using a secured hashing for the security enhancements. A decentralized blockchain methodology is used to minimize new framework better process. The simulation result shows that the storage capacity is improved by fifty percent at the initial stage and thereafter it is just limited to 256 bytes which are not dependent on the input.

References

1. Suo, H., Wan, J., Zou, C., & Liu, J. (2012). Security in the internet of things: a review. *In international conference on computer science and electronics engineering*, *3*, 648-651.
2. Hongwen, H., Xingshuo, A., Haoyu, W., Weijia, J., Huixuan, Y., Hongjie, G., & Fuhong, L. (2019). Survey on blockchain for internet of things, *Journal of Internet Services and Information Security* (JISIS), *9*(2), 1–30. https://doi.org/10.22667/JISIS.2019.05.31.001.
3. Fernández-Caramés, T.M., & Fraga-Lamas, P. (2018). A Review on the Use of Blockchain for the Internet of Things. *Ieee Access*, *6*, 32979-33001. https://doi.org/10.1109/ACCESS.2018.2842685
4. Biswas, K., & Muthukkumarasamy, V. (2016). Securing smart cities using blockchain technology. *In IEEE 18th international conference on high performance computing and communications; IEEE 14th international conference on smart city; IEEE 2nd international conference on data science and systems*, 1392-1393.
5. Liu, B., Yu, X.L., Chen, S., Xu, X., & Zhu, L. (2017). Blockchain based data integrity service framework for IoT data. *In IEEE International Conference on Web Services (ICWS*) IEEE, 468-475.
6. Wan, L., Eyers, D., & Zhang, H. (2019). Evaluating the impact of network latency on the safety of blockchain transactions. *In IEEE International Conference on Blockchain (Blockchain)*, 194-201.
7. https://doi.org/10.1109/Blockchain.2019.00033.
8. Li, J., Wu, J., & Chen, L. (2018). Block-secure: Blockchain based scheme for secure P2P cloud storage. *Information Sciences*, *465*, 219-231. https://doi.org/10.1016/j.ins.2018.06.071
9. Huh, S., Cho, S., & Kim, S. (2017). Managing IoT devices using blockchain platform. *In 19th international conference on advanced communication technology (ICACT)*, 464-467.
10. https://doi.org/10.23919/ICACT.2017.7890132
11. Dorri, A., Kanhere, S.S., Jurdak, R., & Gauravaram, P. (2017). Blockchain for IoT security and privacy: The case study of a smart home. *In IEEE international conference on pervasive computing and communications workshops (PerCom workshops)*, 618-623. https://doi.org/10.1109/PERCOMW.2017.7917634
12. Hossain, K., Roy, S. (2018). A Data Compression and Storage Optimization Framework for IoT Sensor Data in Cloud Storage, *21st International Conference on Information Technology*, 1–6.
13. Gao, W., Hatcher, W.G., & Yu, W. (2018). A survey of blockchain: Techniques, applications, and challenges. *In 27th international conference on computer communication and networks (ICCCN)*, 1-11. https://doi.org/10.1109/ICCCN.2018.8487348
14. Alam, T. (2019). Blockchain and its Role in the Internet of Things (IoT). *Blockchain and its Role in the Internet of Things (IoT), International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, *5*(1). 151– 157, https://doi.org/10.32628/cseit195137
15. Li, J., Liu, Y., Zhang, Z., Ren, J., & Zhao, N. (2017). Towards green IoT networking: Performance optimization of network coding based communication and reliable storage. *IEEE Access*, *5*, 8780-8791. https://doi.org/10.1109/ACCESS.2017.2706328

16. Wang, M., & Zhang, Q. (2020). Optimized data storage algorithm of IoT based on cloud computing in distributed system. *Computer Communications*, *157*, 124-131. https://doi.org/10.1016/j.comcom.2020.04.023
17. Dorri, A., Kanhere, S.S., & Jurdak, R. (2017). Towards an optimized blockchain for IoT. *In IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI)*, 173-178.
18. https://doi.org/10.1145/3054977.3055003
19. Shahid, A.R., Pissinou, N., Staier, C., & Kwan, R. (2019). Sensor-chain: a lightweight scalable blockchain framework for internet of things. *In International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, 1154-1161.
20. https://doi.org/10.1109/iThings/GreenCom/CPSCom/SmartData.2019.00195
21. Sicari, S., Rizzardi, A., Grieco, L.A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of things: The road ahead, *Computer Networks*, *76*, 146–164. https://doi.org/10.1016/j.comnet.2014.11.008.
22. Wu, J., Dong, M., Ota, K., Li, J., & Yang, W. (2020). Application-aware consensus management for software-defined intelligent blockchain in IoT. *IEEE Network*, *34*(1), 69-75.
23. https://doi.org/10.1109/MNET.001.1900179
24. Gajbhiye, A., & Sen, D. (2020). Attacks and Security Issues in IoT Communication: A Survey, 1688–1693.
25. Buccafurri, F., Lax, G., Musarella, L., & Russo, A. (2019). Ethereum Transactions and Smart Contracts among Secure Identities. *In DLT@ ITASEC* 5-16.
26. Sigwart, M., Borkowski, M., Peise, M., Schulte, S., & Tai, S. (2019). Blockchain-based data provenance for the Internet of Things. *In Proceedings of the 9th International Conference on the Internet of Things*, 1-8. https://doi.org/10.1145/3365871.3365886
27. Ayoade, G., Karande, V., Khan, L., & Hamlen, K. (2018). Decentralized IoT data management using blockchain and trusted execution environment. *In IEEE International Conference on Information Reuse and Integration (IRI)*, 15-22. https://doi.org/10.1109/IRI.2018.00011
28. Liu, D., Ni, J., Huang, C., Lin, X., & Shen, X.S. (2020). Secure and efficient distributed network provenance for iot: A blockchain-based approach. *IEEE Internet of Things Journal*, *7*(8), 7564-7574.