European Journal of Molecular & Clinical Medicine
ISSN 2515-8260 Volume 07, Issue 08, 2020

Blockchain Based Iot Framework For Secure And Trustworthy Data Communication

Vikas ReddyS[1,], ChandrashekaraS N[2]*

[1]Department of Computer Science & Engineering, S J C Institute of Technology, Chickballapur, Karnataka, India
[2]Department of Computer Science & Engineering, C B Institute of Technology, Kolar, Karnataka, India

[1] vikasreddycs@gmail.com

Abstract

Internet of Things (IoT) is now an integral part of our daily life. Smart devices are common in place which makes our life easy. It has revolutionized the way human interacts with devices. No doubt the IoT enabled devices have significantly changed our life. However there are various obstacles which need to be addressed to fully exploit the benefits of IoT devices and IoT enabled networks. IoT devices are generally not meant for complex processing and large storage capacity. It has limited power, processing and storage capacity. IoT devices are used in critical infrastructure and to communicate sensitive data. Security and privacy of IoT devices and data communication are important issues. But, because of the resource constraints existing security approaches are unsuitable for IoT devices. Recent development in blockchain technology offers promising solutions to overcome the IoT security and privacy challenges. However, integration of IoT with blockchain technology is not an easy task. Blockchain itself demands high storage and processing capacity. This paper presents blockchain based IoT framework balancing the resource constraints of IoT devices and resource demand of blockchain technology.

Keywords: Internet of Things (IoT), Block chain, Privacy and Security

1. INTRODUCTION

Internet of Things (IoT) has become a part of our daily life. One of the main objective of IoT system was to facilitate real-time data collection and to provide remote control mechanism. Air Conditioner, Fridge, and Power Inverters almost all the house hold devices are currently IoT enabled. Smart City, Smart Manufacturing, Smart Home, Environment Monitoring, Smart Agriculture all possible because of IoT enable d devices and sensors. The exponential growth in IoT enabled devices require advancement in IoT architecture, protocol and technology. The IoT devices and sensors generate huge amount of data. Normally these data are stored in centralized database for generating meaningful information through analysis. However with growing number of IoT devices, centralized system may get overloaded and potential target for cyber-attack. It also raise the scalability issue. In case of any break down and failure of centralized server, the entire system will be unavailable [11][14]. Most of the IoT devices are designed for real-time data acquisition and processing. These devices features with limited processing capacity and memory resources. The limited battery and processing capacity create a constraint for the IoT devices to implement complex cryptography algorithm to secure the information. IoT devices are used for communicating sensitive data and connecting critical infrastructure. Lack of strong security fea-

tures are major concerns which needs to be addressed [8][9]. Currently many techniques have been implemented to secure the data communication among the IoT devices. However there are significant challenges such as real-time communication, high maintenance cost, and trust issues which need to be addressed [2][4][7]. IoT data reliability, authenticity, trust, and security can be enhanced using a blockchain technology. Recent development in blockchain technology has emerged as promising technology to strengthen the security of IoT device communication. The key thing of this paper is to design and develop a scalable blockchain based IoT architecture to provide secure and trustworthy data communication.

2. Blockchain Technology

Blockchain is an immutable ledger of transactional record. Blockchain maintains a distributed ledger of transaction shared among all the participating nodes. Every new transactions are verified by all the participating nodes before adding it in to the transactional records. One of the popular application based on Blockchain is Bitcoin. Because of the potential advantages of blockchain, it is used for various services like supply chain management, banking, insurance, land record management, assets management etc. In blockchain all the participating nodes update the copy of distributed ledger for every valid transactions. Each node generally contains three main components:

Data:
Normally the data in blockchain nodes contain only the transactional information. It can be any type of data. However, it is important to understand that blockchain is not the substitution of database. Data portion of blocks are not meant for large volume of data.

Hash:
Hash function generate a unique value of fixed length for the block. Any modification and alteration in the block will change the hash value. Hash value is used for verifying the integrity of data stored in block.

Previous Block Hash:
Every block except the genesis block keep the hash value of previous block. It connects the current block with the previous block and makes chain format as shown in figure 1.

Advantages of Blockchain :
There are various advantages of blockchain. Some of the major advantages are as follows:

Decentralize:
Blockchain store the transaction record in a decentralized system. All the participating nodes in the blockchain network maintain the copy of transactional record. It makes the overall system robust and fault-tolerant.

Transparency:
Since every node in the blockchain maintains the transactional record, it makes the entire system very transparent. It is practically impossible to hide any transaction from any peer members on the network.

Immutability:
Blocks in blockchain cannot be added without the consensus of participating members in network. Once the block is added in blockchain, it is secured and tampered proof. No blocks can be deleted or altered in the blockchain. It makes the entire system tamper proof and trustworthy.

Blockchain Implementation Challenges:
Although blockchain has many advantages and looks simple in implementation, it has many implementation challenges.

Storage Capacity:
Blockchain keeps adding blocks for every transaction. With growing number of transactions the size of blockchain also increases and needs a significant storage capacity. It may not be feasible to meet the storage requirement at IoT devices as generally IoT devices have small storage and processing capacity.

Block Processing Time:
Block cannot be added on the blockchain without the consensus of the peer members. Due to the increased size of blockchain, the validation time to add the blocks also increase. It also need more computational time to add the nodes on network.

IoT Device Security Challenges:
Currently the IoT devices are controlled through centralized server. Data collected through IoT devices are either stored in the local central server or cloud server. The centralized approach has many issues like cost, scalability, privacy, security, maintenance etc. [3][6]. The traditional privacy and security measures adopted for IoT devices are ineffective due to the following reasons:

Limited Resource:
Generally the IoT devices have limited resources. Whereas the security algorithms are complex in nature and resource intensive.

Centralize Control:
Currently IoT devices are controlled through centralized nodes. This system has a major issue as this model is unlikely to scale as billions of devices are connected.

Lack of Privacy:
Most of the IoT devices communicate sensitive data among peer devices without any encryption.

3. Related Work

Recently many researchers have focused on blockchain based IoT architecture. Some of the researchers have discussed impact of blockchain implementation for IoT devices. Majority of the work is focused on integrating the blockchain with IoT, access control, trust management, security and privacy. Some researchers have focused on the resource constraints of the IoT devices. The authors in the paper [5][13] have highlighted the advantages of blockchain and its integration with IoT. Authors have elaborated the benefits of trust and security features with the implementation of blockchain and IoT, along with the overheads of blockchain. The author has also discussed about various types of consensus algorithms with its advantages and disadvantages. The paper contains in-depth about the resource consumption, throughput limitations and confirmation delay.

In the papers [10][12] authors have highlighted various issues for IoT blockchain integration. It is suggested that a set of protocols and standards should be developed to support the basic essential requirements of all IoT applications instead of introducing application specific IoT networks. In paper [15] authors have mainly focused on blockchain-based secure service provisioning mechanism to protect the lightweight client. Author has introduced the blockchain on edge computing to reduce the direct overhead on IoT devices. Authors have used permissioned blockchain with the PoA consensus engine.

Authors in the paper [13], have discussed about the possibilities of using blockchain for securing and assuring data integrity in IoT. Authors in this paper have mainly focused on the pros and cons of different consensus methods used in blockchain implementation. Authors have also discussed how private blockchain can be a better alternative to the public blockchains for IoT network. In the paper [1] authors have proposed a light weight scalable “Sensor-Chain” framework for the resource constrained IoT devices.

Many researchers work is going-on for the blockchain and IoT integration. Some of the researchers have achieved partial success. However demand of high processing and storage capacity is a big challenge for the integration of blockchain with IoT. The main objective of this paper is to address this issue.

4. BLOCKCHAIN BASED IOT FRAMEWORK

This section discusses about the integration of IoT sensors and devices with blockchain. We have analyzed the strength and weakness of the proposed framework. Next section highlights strength, weakness and the motivation behind the proposed framework.

Conventional Blockchain :
In the conventional approach, blocks in the blockchain are managed by all the participating nodes in the network (Figure 2). With the lifespan of the network the blockchain will keep on growing. The growing blockchain will need high storage capacity which is not technically feasible with the small IoT devices.

Clustered Blockchain Approach:
The major problem with the IoT device is resource constraint. Convention block chain implementation with IoT device requires significant storage capacity at the individual nodes. Technically the individual IoT device do not have sufficient processing and storage capacity and hence clustered approach seems to be a feasible solution (Figure 3).
The cluster network could potentially consists of a large number of IoT sensors. The clustering algorithm is used to group nodes into clusters. Each cluster has a cluster head which is responsible for managing the blockchain. Cluster heads are responsible to record the incoming and outgoing transactions generated among the cluster members. The cluster heads are specialized nodes having sufficient processing and storing resources.

5. IMPLEMENTATION AND PERFORMANCE ANALYSIS

To analyze the feasibility of proposed architecture, experimental analysis has been done. We have conducted the performance analysis of IoT integration with conventional blockchain and IoT integration with clustered network. We used IBM Hyperledger to develop a prototype blockchain model.

Consensus Algorithm:
Consensus is one of the core process in blockchain. Consensus is the process through which the nodes are added on the blockchain network. It ensures guaranteed ordering, validation and authenticity of the nodes added into the blockchain. The consensus algorithm must confirm the correctness of all the transactions and ensure its authenticity. Consensus can be implemented in different ways. It may be lottery-based algorithms or through the use of voting-based methods. Each method has its own approach and fault tolerance models. We have used lottery-based algorithm. The main advantage of choosing lottery-based algorithm is that they can scale to a large number of nodes. However in lottery-based algorithm when two “winners” propose a block, it may lead to fork. Our priority was more on scalability than finality time and hence we used lottery-based algorithm for consensus.

Performance Analysis:
Basic objective of our research work is to test the feasibility of our proposed cluster based blockchain-IoT architecture. We have focused on three basic parameters for the performance analysis i.e. processing overhead, network traffic overhead and block processing time. We have compared these parameters with the conventional approach of blockchain-IoT architecture and cluster based blockchain-IoT architecture.

Processing Overhead:
We have analyzed the test on CPU (Intel Core i5) usage for adding new blocks on convention blockchain platform and clustered based blockchain-IoT architecture. The prototype model was simulated with ten IoT sensors/smart devices. Each device was generating random number of transactions within the network. Figure 4 displays the processing overhead for conventional approach and clustered approach.

Network Traffic Overhead:
The blockchain implementation will increase the overhead on the network. In our experimental analysis we tried to analyze the network traffic overhead with the implementation of conventional blockchain and the clustered blockchain approach (Figure 5).

Block Processing Time:
We simulated our experiment for 3 Hours. We observed that as the number of blocks started increasing, the block processing time for the conventional approach also started increasing (Figure 6).

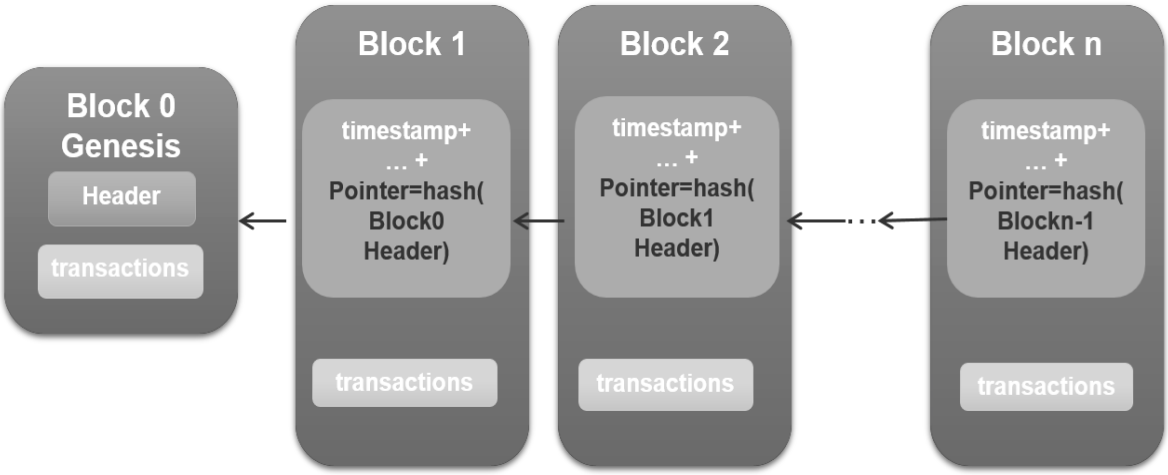

Figure 1: General Format of Blocks in Blockchain.

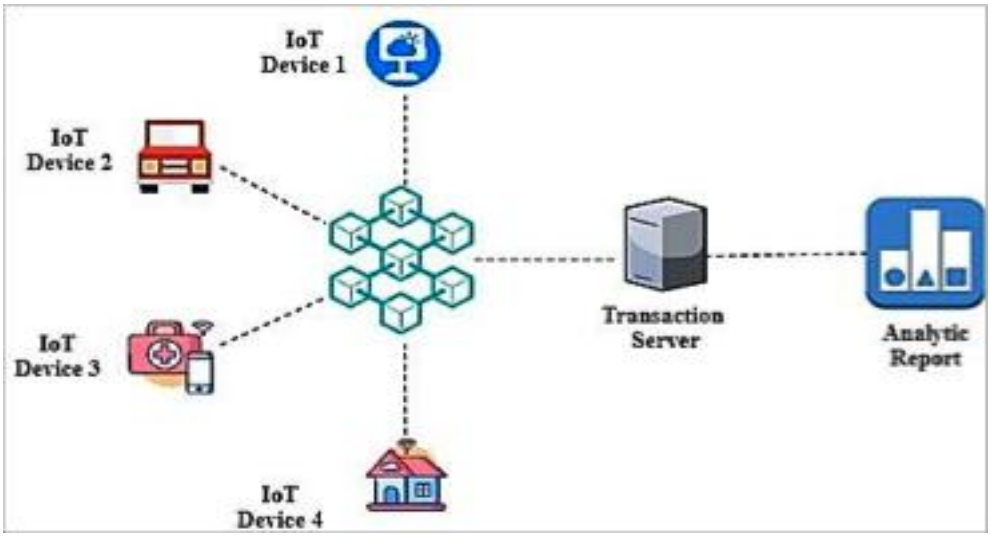

Figure 2:Conventional Blockchain and IoT Integration

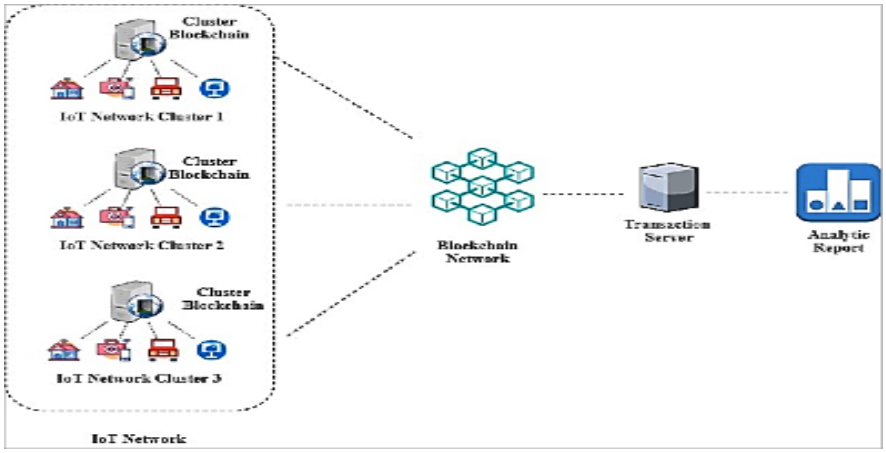

Figure 3: Cluster Based Blockchain and IoT Integration

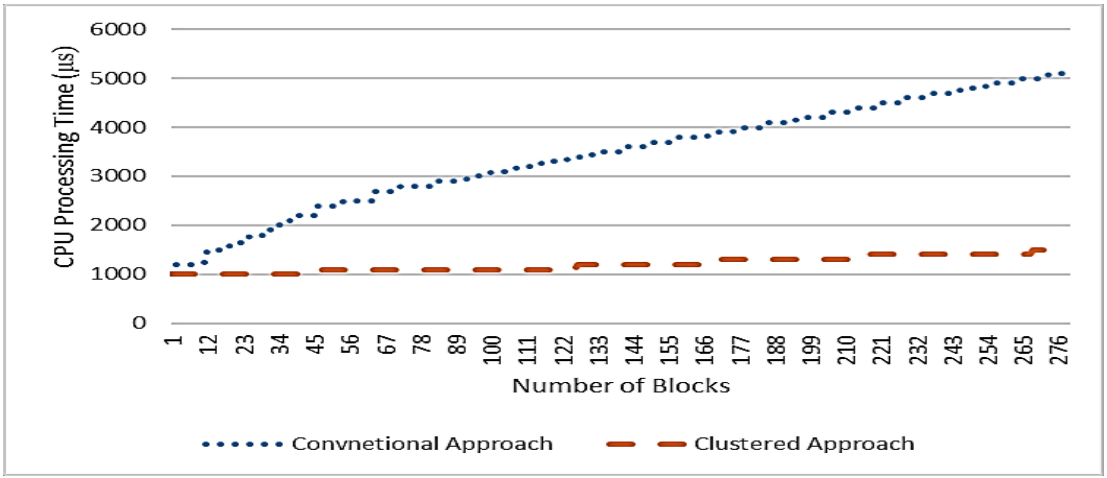

Figure 4: CPU Processing Overhead

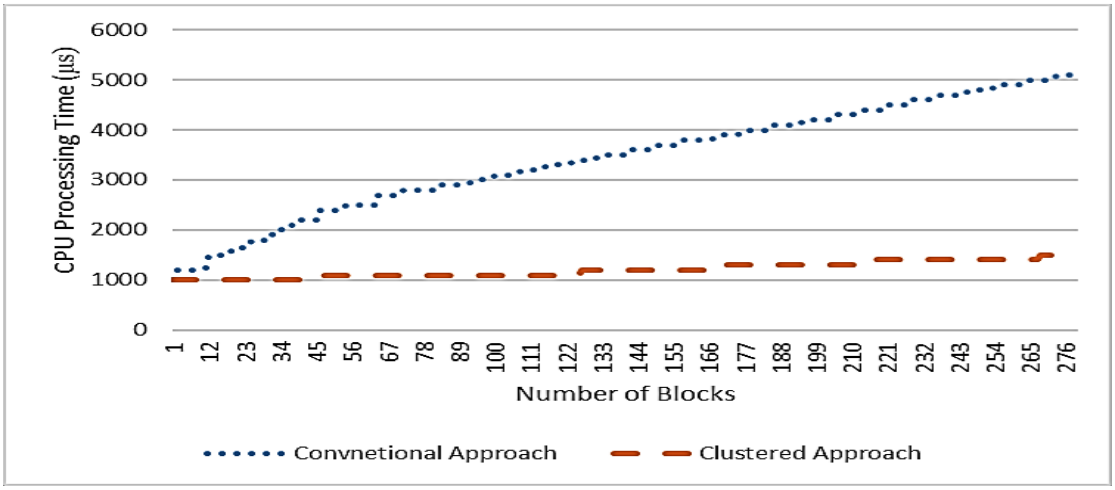

Figure 5: Network Traffic Overhead

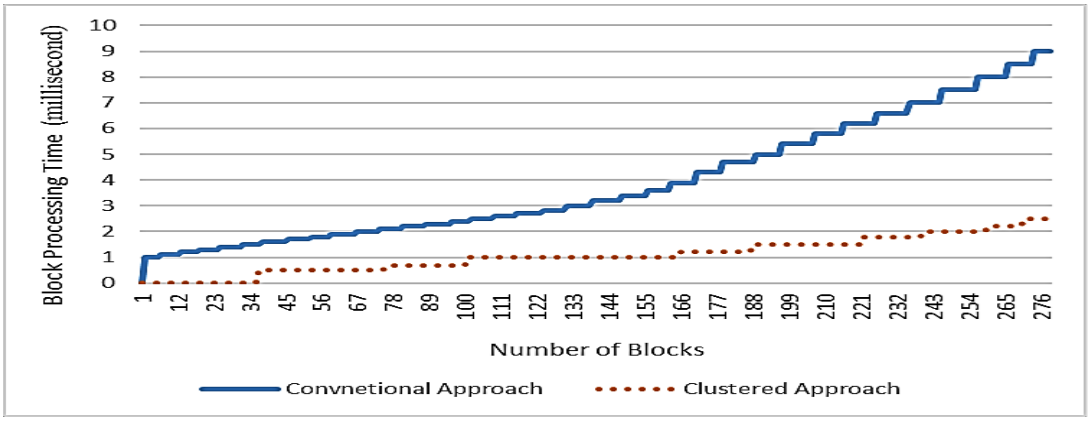

Figure 6: Block Processing Time

6. CONCLUSION AND FUTURE RESEARCH

In recent days IoT devices have witnessed rapid growth. With the exponential growth in number of connected IoT devices, privacy and security has become a major cause of concern. In this paper we have proposed a blockchain based architecture to strengthen the privacy and security of IoT device and data communication. The distributed ledger of the blockchain makes the overall system scalable and trustworthy. We have implemented a clustered approach to balance the resource constraints of IoT devices and to meet the processing capacity and storage demand of blockchain system. Though we have achieved basic objectives of our research, there are many other issues which can be addressed in future research. Formation of dynamic cluster, joining the IoT devices dynamically in cluster are some of the complex issues need to be discussed in detail. Since in-depth discussion of each and every issue will slightly divert the main focus of our work it is not covered in this paper and planned for future work.

REFERENCES

[1] A. R. Shahid, N. Pissinou, C. Staier and R. Kwan, "Sensor-Chain: A Lightweight Scalable Blockchain Framework for Internet of Things," 2019 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), Atlanta, GA, USA, 2019, pp. 1154-1161.

[2] Aafaf Ouaddah, Anas Abou Elkalam, and Abdellah Ait Ouahman. 2017. Harnessing the power of blockchain technology to solve IoT security & privacy issues. In Proceedings of the Second International Conference on Internet of things, Data and Cloud Computing (ICC '17). Association for Computing Machinery, New York, NY, USA, Article 7, 1–10.

[3] Abid Sultan, Muhammad Azhar Mushtaq, and Muhammad Abubakar. 2019. IOT Security Issues Via Blockchain: A Review Paper. In Proceedings of the 2019 International Conference on Blockchain Technology (ICBCT 2019). Association for Computing Machinery, New York, NY, USA, 60–65.

[4] Ana Reyna, Cristian Martín, Jaime Chen, Enrique Soler, Manuel Díaz, "On blockchain and its integration with IoT. Challenges and opportunities", Future Generation Computer Systems, Volume 88,2018, Pages 173-190.

[5] B. Cao et al., "When Internet of Things Meets Blockchain: Challenges in Distributed Consensus," in IEEE Network, vol. 33, no. 6, pp. 133-139, Nov.-Dec. 2019.

[6] D. Fakhri and K. Mutijarsa, "Secure IoT Communication using Blockchain Technology," 2018 International Symposium on Electronics and Smart Devices (ISESD), Bandung, 2018, pp. 1-6.

[7] Jollen Chen. 2018. Hybrid blockchain and pseudonymous authentication for secure and trusted IoT networks. SIGBED Rev. 15, 5 (November 2018), 22–28.

[8] M. Singh, A. Singh and S. Kim, "Blockchain: A game changer for securing IoT data," 2018 IEEE 4th World Forum on Internet of Things (WF-IoT), Singapore, 2018, pp. 51-55.
[9] Mehedi, S.K.T., Shamim, A.A.M. & Miah, M.B.A. Blockchain-based security management of IoT infrastructure with Ethereum transactions. Iran J Comput Sci 2, 189–195 (2019).
[10] Mohammad Maroufi, Reza Abdolee, and Behzad Mozaffari Tazekand, "On the Convergence of Blockchain and Internet of Things (IoT) Technologies." Journal of Strategic Innovation and Sustainability 14, no. 1 (November 2019). https://doi.org/10.33423/jsis.v14i1.990.
[11] Pankaj Mendki. 2019. Blockchain Enabled IoT Edge Computing. In Proceedings of the 2019 International Conference on Blockchain Technology (ICBCT 2019). Association for Computing Machinery, New York, NY, USA, 66–69.
[12] Riya Thakore, Rajkumar Vaghashiya, Chintan Patel, Nishant Doshi, "Blockchain - based IoT: A Survey", Procedia Computer Science, Volume 155, 2019, Pages 704-709.
[13] Salimitari, Mehrdad and Mainak Chatterjee. "A Survey on Consensus Protocols in Blockchain for IoT Networks." (2018).
[14] Y. Gupta, R. Shorey, D. Kulkarni and J. Tew, "The applicability of blockchain in the Internet of Things," 2018 10th International Conference on Communication Systems & Networks (COMSNETS), Bengaluru, 2018, pp. 561-564.
[15] Y. Xu, G. Wang, J. Yang, J. Ren, Y. Zhang and C. Zhang, "Towards Secure Network Computing Services for Lightweight Clients Using Blockchain", Wireless Communications and Mobile Computing, vol. 2018, pp. 1-12, 2018. Available: 10.1155/2018/2051693.