ALLEVIATING DATA STORAGE CHALLENGE THROUGH VIRTUALIZATION OF BLOCKCHAIN EMBEDDED WITH INTERNET OF THINGS

M. Vivek Anand

Research Scholar, School of Computing Science and Engineering, Galgotias University, Gautam buddh Dist, Greater Noida, Uttar Pradesh-201308, India
vivek395@gmail.com

Dr. Munish Sabharwal

Professor & Dean, School of Computing Science and Engineering, Galgotias University, Gautam buddh Dist, Greater Noida, Uttar Pradesh-201308, India
mscheckmail@yahoo.com

Dr. S Vijayalakshmi
Associate Professor, Dept of Data Science, Christ university
412112, India
svijisuji@gmail.com

Abstract

Internet of things is evolving day by day with connected devices with continuous advancement in the devices but the security of IoT is not assured due to its trusted third party with centralized servers. Blockchain is a peer-to-peer network, where each peer is responsible for their task without centralized server, and no need to trust anyone in the network. Blockchain is integrated with IoT to improve their security, because of its feature of tamper-proof. Few issues are happening while integrating blockchain to IoT. The main issue that has to be resolved for a blockchain is the storage issue. Whenever the blockchain is evolving the storage of the blockchain is also increasing. IoT peers in the network have to store the entire blockchain to perform the verification of data and the IoT nodes are not having the capability to store the entire data. In this paper, we are discussing the storage issue of blockchain while integrating it into IoT. We proposed a navel approach to resolve the issues of storage by the virtualization technique. The result shows that virtualization reduces the storage capacity for the IoT peers as compared with the previously proposed methods.

***Keywords*: Blockchain; IoT; Bitcoin; Disruptive Technology; BIoT.**

1. Introduction

Although various architecture styles have been proposed for IoT such as client-server architecture, cloud-based architecture, Fog computing architecture they are deficient to handle data breaching. IoT is not only involved in a sophisticated application but is also involved in the emergency application. The data breaching in emergency applications such as a remote patient health monitoring system, where the patient's health condition is monitored through a wearable chip kept inside the patient's body. The wearable chip will send the notification to the hospital when there is a change in the patient's body condition. Based on the data analytics, hospital management will call for the ambulance in a critical situation to save the life of the patient. In this case, IoT is contributing majorly to monitoring health conditions through the sensor and giving the notification to the device that is embedded in the hospital. (In this kind of scenario, if IoT is failing to perform the task because of data breaching, the patient life would not be saved. The failure of IoT in this task may lead to a patient's life in a dangerous state). The application of IoT in the Medical field is high in its impact.

2. Challenges in IoT

IoT is based on a centralized server such as client-server architecture, cloud-based architecture, and fog computing architecture. In a client-server architecture, the client requests every process to the server where the server is having big data storage. Providing the DNS service for each client's request for the service is difficult. If the server is affected by any unauthorized person the entire system will fail to do the task. In cloud-based architecture, the application residing on the internet, and the data is stored online. The request will be given by the client whenever the data is required. Privacy of data is questionable in public cloud architecture. A small organization cannot able to maintain the hardware and data storage in a private cloud are 30 times the expected number of devices deployed. In the case of the public cloud, the data may be misused by cloud service providers. Centralized server architecture is vulnerable to data breaching through the internet.

IoT devices will not perform the task without receiving commands or associated data from the centralized server. The entire system will fail if the server is hacked by an unauthorized person. This will lead to the misuse of data by hackers by tampering with the data intentionally to spoil the system. Fog computing is rectifying some of the issues addressed in cloud computing such as latency, volume, etc., that also works in the base of cloud servers. Although various security measures proposed for security in centralized servers are not enough to secure the system and also the maintenance of the server is expensive because of upgraded security tools and techniques in the network. Privacy of the network is not maintained due to the data available in the servers. [Alenezi et al. (2017)]. Since the centralized server architecture is not enough to handle data breaches such as DDoS [Conoscenti et al. (2017)]. In-flexibility to handle the workload of the server due to large storage in the centralized server [Atlam and Wills, 2019]. The maintenance cost for securing the network is high and it is showing the failure of centralized architecture [Atlam et al. (2018)]. Centralized servers are restricting the diversity in the network [Fernandez-Carames and Fraga-Lamas (2018)] So, the important challenge is to propose new architectural styles that are saving the data from an unauthorized person. In a decentralized architecture, the maintenance of the server is not required. In the way of looking for an architecture that is free from hacking and decentralized in nature, many suggestions are given by experts to go for blockchain.

3. Solution to IoT Challenges with Blockchain

A The blockchain is a peer-to-peer decentralized network, where the users who are involved in the network will have the responsibility of controlling their own peers only. The blockchain is an anonymous network where the user can hide their identity from the remaining peers in the network. In Blockchain Network all the data and transactions are stored and distributed among all the peers. Tampering of data in the distributed ledger is highly impossible because it has to get approval from most of the peers. Blockchain provides security to the application with its cryptographic hashing [Atlam et al. (2017)]. In the blockchain, no need of installing the hardware for maintaining and monitoring the security [Atlam and Wills (2019)]. Blockchain is providing more address space when compared to IPV6. Blockchain is applied in Most the IoT application which is getting more secure in the real world

4. Storage issues while Integrating blockchain and IoT

Blockchain was introduced by "Satoshi Nakamoto" in 2008 (Nakamoto, 2008) who released windows 32 software bitcoin.exe with 6 MB size of data with its first application called bitcoin [Pascal Urien (2018)]. The blockchain was small when it was started. The difficulty of storing the data is not at all a problem. In 2014 the blockchain size was close to 20 GB but it was manageable at that time. In the blockchain, blocks consist of data and it will be chained with another block when the miners of the network verify and got consensus from the network. The storage of a block is approximately 2MB in the bitcoin network. When the network is evolving the size of the blockchain is also increasing. In a bitcoin network now the size of the blockchain nearly 250 GB. Statistics of the blockchain data are available in (Blockchain.info). If anyone wants to join the bitcoin network as a full node, they have to download the entire blockchain to verify the data of another node [Saito and Iwamura, (2018)]. The node has to have the capability to store the entire blockchain. Internet of things is the network of nodes with different sizes of devices and different storage capacities. A small node or lightweight node cannot store the entire network. The storage capacity is the major problem while we integrate blockchain into IoT. For minimizing the size of the blockchain the switching of Berkeley DB to LevelDB [(Andresen (2013)]. LevelDB is providing a major performance boost in case of block synchronization and block verification speeds. The ultimate blockchain compression technique was aimed to achieve the compressed blockchain with pruning technique with balance tree information [Reiner (2012)]. The pruning was provided with compressed blockchain but the results are limited and it is not having any idea that how it can be merged with bitcoin. Another process which will increase the block size to get more transaction to be done but it will increase the storage in lightweight nodes [Todd (2013)]. In bitcoin, the transaction can be taken up to 7 in a second. This is not enough. Block size can be increased at some

point but how it will be compatible with the previous block with different sizes is questionable. Increasing block size can reduce transaction fees and increase the number of transactions but it would not be helpful to reduce the storage. It will increase the size of the blockchain and it will be an additional burden for lightweight nodes. Block size has to be increased to get more transactions in a period [Bitcoin Wiki (2020)].

In bitcoin, some people considered the variation of the block in size as a spamming of the network and some more even tell that it is a stress test for the blockchain network. We can leave the system as the way it is growing in a blockchain by considering some points such as not every node has to store the entire blockchain other than full node, transaction data can be pruned, off-chain transitions can be done and it can be applied to the main blockchain, changing the transaction fees can minimize or maximize the transaction and it can reduce data according to the size. All these things are not a big solution for minimizing storage. Pruning results are limited and not accurate. In proof of work consensus, when the networks keep on mining the network it becomes a larger server farm to control the entire network but it will lead to centralization and becomes getting no participation from light nodes.

Data compression also becomes the problem to get the original data from the blockchain and if there is a loss of data that is not suitable for proper verification of data. Mini blockchain schemes have been proposed to avoid the problem of storage in light nodes where the recent transactions can be stored as an account tree [França (2018)]. [Bruce (2018)]. Even though the lightweight nodes which are not having enough data to store the entire blockchain can also be able to participate in the network but it cannot able to validate the transaction. Lightweight nodes of the bitcoin network can have Participation and initiation transactions in the network [Conti, Lal and Ruj (2018)]. Reliability is low when the lightweight nodes are not able to check the validation of the data in the network. At least some portion of the data in the blockchain has to be visible to do the confirmation. A Memory-optimized scheme [Dorri et al. (2019)] has been proposed and it is solving the privacy issues also. However, there is no proper solution for the storage issue. IoT requires more security with blockchain such as some crucial medical applications [Kirubakaran et al. (2020)]. Transparency among the devices is required for IoT devices to decide on their applications. IoT devices are not capable of storing all entire blockchain devices cannot validate the transactions without the blockchain information. Here the historical data is required to initiate the new transactions [Reyna et al. (2018)]. The cost of storing the data on the blockchain is also costly, for instance storing 1GB of data in Ethereum is about USD 200,000. Data storage in IoT devices with underlying blockchain is a problem

5. Solution for the storage issue of blockchain in IoT

Even though the blockchain is providing a Secure solution to the IoT [Alkurdi (2018)], so many issues are occurring while integrating blockchain into the IoT environments [Banafa (2017)]. So many issues are listed in the previous section and the important issue of the adaptability of the blockchain is storage [Samaniego and Deters (2016)]. IoT devices have to store the entire blockchain if they want to actively participate verify all the data in the network. IoT devices are not having enough memory space to hold the entire blockchain. The growing application of blockchains such as bitcoin and Ethereum is required a large amount of blockchain data that is not possible to hold in IoT devices. Lightweight nodes of IoT devices are not having enough memory capacity to hold the entire blockchain. Even those lightweight nodes no need to have an entire blockchain for their storage to verify the data and also the IoT nodes are not interested in storing the entire blockchain. Nowadays the Light nodes can participate in the network to initiate the transaction but they can't able to verify the entire blockchain data. The full node is the peer which can have all the blockchain data capacity of memory to verify the data in the blockchain and can able to verify the data and can mine the data.

6. Proposed Method-MEmory Reduced Blockchain light node of Internet of Things(MERBIoT)

Security for some crucial applications such as Army applications can be assured when all the nodes of the blockchain network have to know other transactions or data in the blockchain. Nowadays only the full node of an IoT only can able to see all the blockchain data. If there is any light node in the network, they can only initiate the transaction in the network. If the light node in such an IoT application can verify all the data of the network without having a storage issue our proposed method will provide the solution. All the full nodes in the application can see every data and can mine other data. Light node is not having full blockchain data due to storage issues. Whenever the blockchain data is stored in the blockchain, it will be available to all the nodes in the network. When the data are storing then the blockchain size also will be increased. A light node cannot store all the blockchain data due to its minimum capacity in the memory. If the light node is the remote location if it wants to identify all the data of the blockchain to take any important decision in the network, it is not possible because the IoT light node can have only the recent data of the blockchain. If the light node wants to see the previous data of the blockchain our proposed solution will be useful in such a scenario.

The Architecture diagram Fig 1 shows that how the light node has the connectivity in the network and it can find the full node near to the light node it can get the data by doing memory virtualization. The figure shows blockchain full node data and how it can be achieved through memory virtualization with the help of swapping the data between a full node and light node. Security of the data will not be assured when we are using blockchain as a separate data storing platform for IoT Environment Capturing all the data through IoT devices and storing the data in a blockchain is not assuring the original data from the origin of the IoT devices. The separation of blockchain and IoT is not assuring 100% security in crucial applications such as medical applications and army applications.

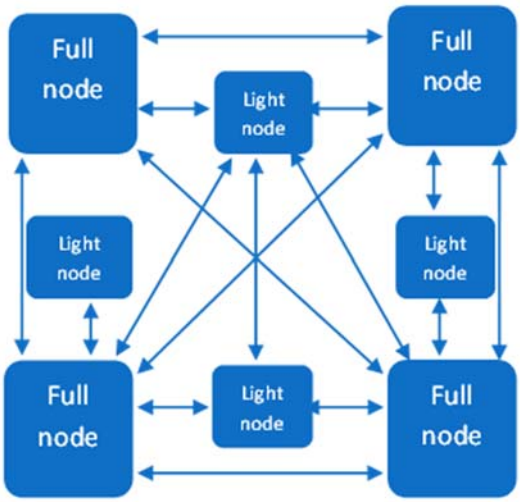


Fig.1. Architecture Diagram for a proposed method

Keeping the blockchain inside the node of the IoT will give more security for the IoT environment and Every node can access the blockchain data. To have access to the light node, this work will be giving a solution and security can be achieved. To achieve that we have to make the light node to be active and the memory virtualization has to be done.

7. Implementation Algorithm (MERBIoT)

Format Symbol	Description
DN	Decentralized Network
DNs	Formation of internal Network
Fn	Full node
Ln	Light Node
rg	Register a node
Brg	Bulk Register
Tn	Total nodes
TFn	Total Full nodes
TLn	Total Light nodes
Trg	Total Registered nodes
TBrg	Total Bulk Registered nodes
Mn	Miner node
Fx	Full node transaction
Lx	Light Node transaction
PH	Previous Hash
CBD	Current Block Data
Mne	Mining
Pg	Page

Table 1. Notation used for MERBIoT

Table 1 refers the notation used in this algorithm

Step 1: Register a new node to connect with previous node

Fig.2. connection of two full nodes

$$DNs1 = (Fn1 + Fn2) + (rgFn2 \rightarrow Fn1) + (BrgFn1 \rightarrow Fn1 \rightarrow Fn2) \quad (1)$$

IoT full node can be connected with another node. Here Full node 2 is registered with Full node1 and also Full node1 will do bulk registration with Full node2. Here Bulk registration refers to the data of all the previous nodes in the network is registered to the new node in the network. Figure 2 refers to the Registration and bulk registration that happens with two Full nodes.

Step 2: Form a Registration and bulk registration with all previous nodes to a new light node 1

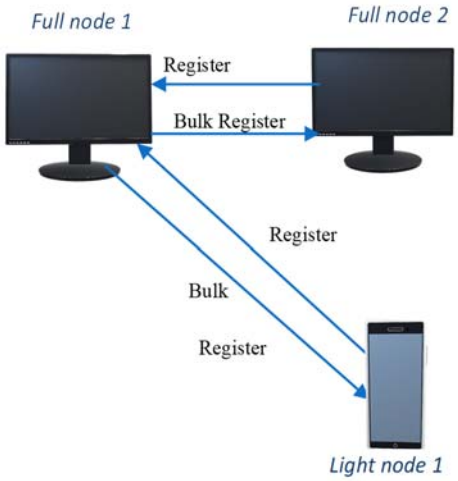


Fig.3. Adding light node1 to the network

$$DNs2 = DNs1 + (rgLn1 \rightarrow Fn1) + rgLn1 \rightarrow Fn2) + (Brg(Fn1 + Fn2) \rightarrow Ln1) \quad (2)$$

Figure 3 refers to the Registration and bulk registration happens with two Full nodes and a light node

Step 3: Form a registration and bulk registration with all previous nodes to a new light node 2

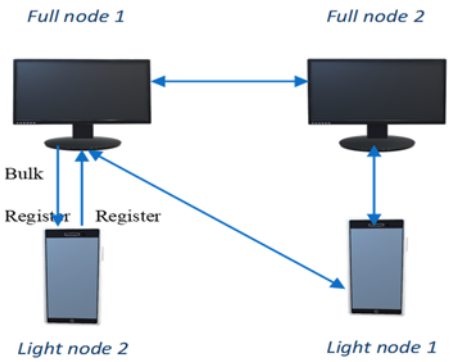


Fig.4 Adding light node2 to the network

$$DNs3 = DNs2 + \big((rgLn2 \rightarrow Fn1) + (rgLn2 \rightarrow Fn2) + (rgLn2 \rightarrow Ln1)\big) + Brg(Fn1 + Fn2 + Ln1) \rightarrow Ln2)) \quad (3)$$

Figure 4 refers to the Registration and bulk registration happens with two Full nodes and two light nodes

Step 4: Broadcast each node data to other nodes in the and for a peer-to-peer network.

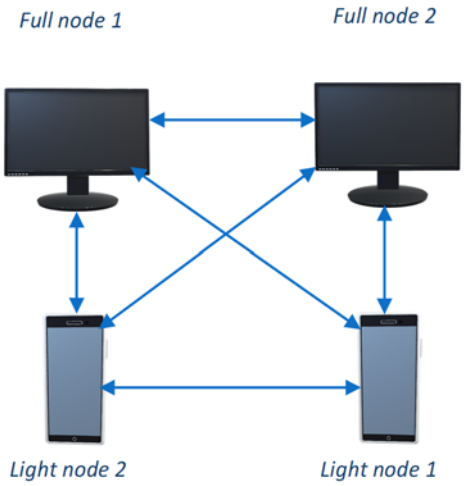


Fig.5. formation of peer-to-peer network

Figure 5 refers to the Registration and bulk registration happens with two Full nodes and two light nodes and form a peer-to-peer network.

$$DN = \sum_{i=1}^{n} (DNs) + \sum_{i=1}^{n} (Trg + TBrg) \quad (4)$$

The Whole network of blockchain architecture can be taken as the sum of all light nodes, full nodes, the registration of nodes, and bulk registration of previous nodes. The total number of nodes is equal to the total number of full nodes and Light nodes

$$Tn = TFn + TLn \quad (5)$$

Step 5: Initiate transaction to the network

$$Fx|Lx \rightarrow Tx \quad (6)$$

The transaction can be initiated to the blockchain network.

Step 6: Broadcast Transaction to all the nodes in the network

Transaction of IoT nodes Broadcasted to all the nodes in the network.

$$Tx \in \forall Fn\&Ln \quad (7)$$

Step 7: Mine the transaction with miner node

Mining node mine the transaction with previous hash, current block data, nonce. Mining will be done up to the of hash matching with nonce.

$$Mn = \{PH, CBD, Non, GH\} \quad (8)$$

$$Mne \rightarrow Non \quad (9)$$

Step 8: Adding blocks into Blockchain:

$$BC = CBD + BC \quad (10)$$

$$Fn = \{BC, CBD\} \quad (11)$$

$$Ln = \{CBD\} \quad (12)$$

The block will be added to the current blockchain after mining where the full node is having the blockchain data and the light node can have the current blockchain data. Miner node will get rewards as a bitcoin after successfully adding the blocks into the previous block

Step 9: Verify the full node has all blockchain data.

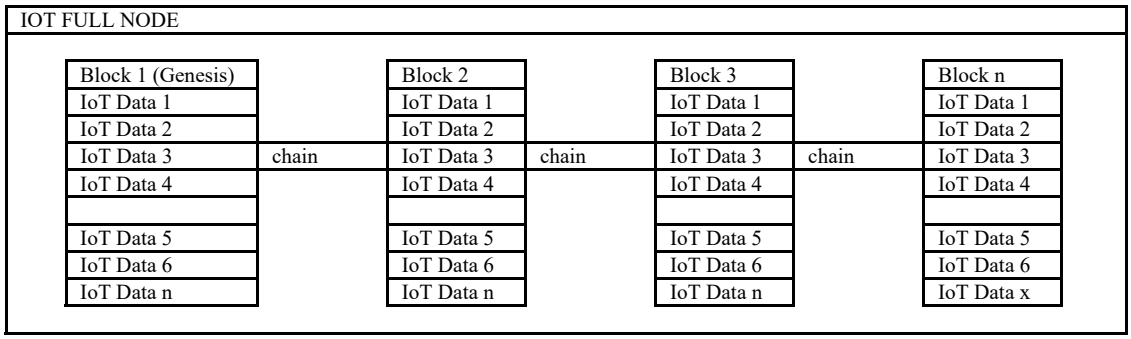


Fig.6. Full node with IoT data

Full node of the IoT network has all the blockchain data. Figure 6 shows the data in the blockchain

Step 10: find the Adjacent full node and make the virtualization to receive the previous data.

Here the light node can initiate a transaction to get data from the Full node and it will be approved by the network nodes and the miner node can provide data to the light node. The request of the light node will be taken as one of the transactions in a block and it will also be added in a block and blockchain. So here what are all the light nodes get the details from the miner node also will be visible.

Fig. 7. Swapping between full node and light node

$$Ln \rightarrow Tx \quad (13)$$

$$CBD \leftarrow Tx \quad (14)$$

$$Mne \rightarrow Non \quad (15)$$

$$BC = CBD + BC \quad (16)$$

The requesting transaction will be added to the block and it will be mined by the miner node.

A light node can easily get the data from Full node through Virtualization and the IoT light node can take any decision according to the data in the blockchain. The trust among all the peers is ensured through virtualization. Figure 7 shows the swapping of memory from full node and light node.

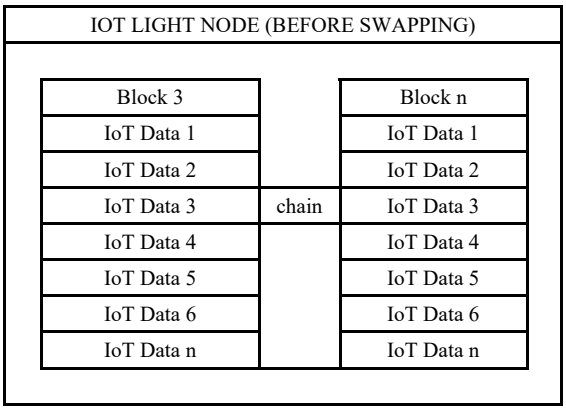


Figure 8 IoT Light node before Swapping

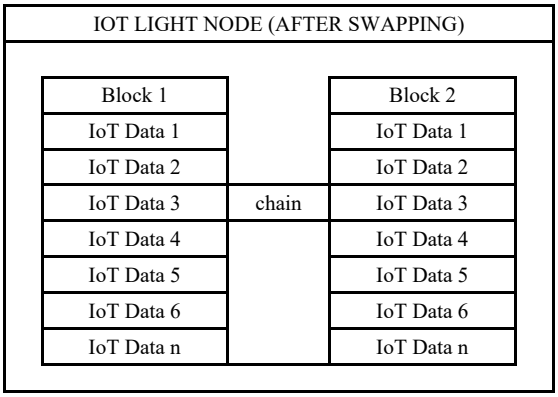


Figure 9 IoT Light node After Swapping

Step 11 Ensure that the light node can take all the blockchain data from full node.

$$CBD \rightarrow CLn \tag{17}$$

$$Pg(Fn) \notin \mathrm{Pg(Ln)} \tag{18}$$

$$Pg(Fn) \rightarrow Pg(Ln) \tag{19}$$

$$Pg(L(n) \rightarrow Pg(Fn) \tag{20}$$

The current blockchain data can be given to the light node from the Full node after checking the capacity of the Light node and also will check whether the data of blockchain is already available in the light node. If the data are required from the light node the pages will be swapped Full node blockchain data can be taken as a page and it can be swapped with Light node. Figure 8 and Figure 9 show the before and after swapping.

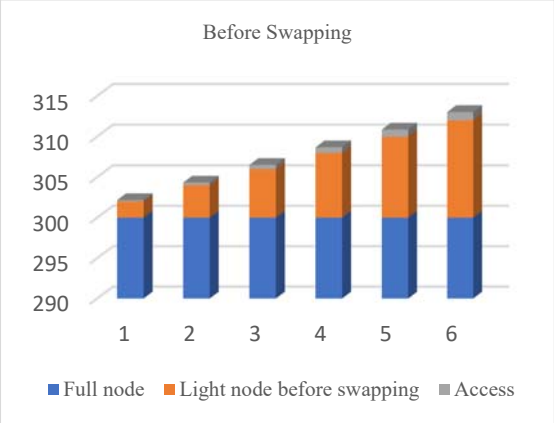
8. Results and Discussion

Blockchain has implemented in the IoT Network and the Light node can able to get the data of the entire blockchain with memory virtualization techniques and it provides a very good impact on the performance to show the results that the light node can actively participate in the network and it can able to see all the data available in the network by swapping the pages one by one.

Graph1 and Graph 2 shows the values before and after swapping. Table 2 and Table 3 refers to the corresponding values.

Full node	Light node before swapping	Access
300	2	0.17
300	4	0.34
300	6	0.51
300	8	0.68
300	10	0.85
300	12	1.02

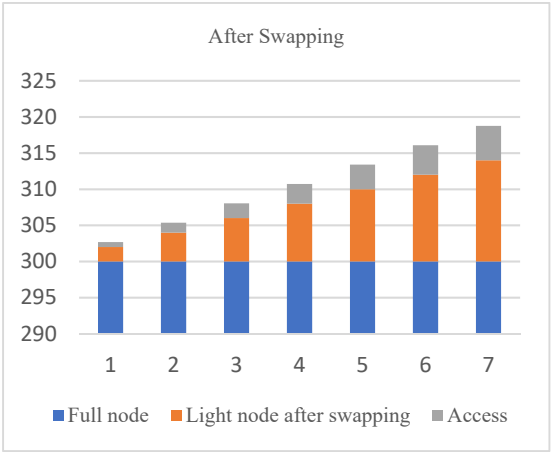
Table 2 Access values before Swapping



Graph 1 Performance before Swapping

Full node	Light node after swapping	Access
300	2	0.68
300	4	1.36
300	6	2.04
300	8	2.72
300	10	3.4
300	12	4.08
300	14	4.76

Table 3 Access values after Swapping

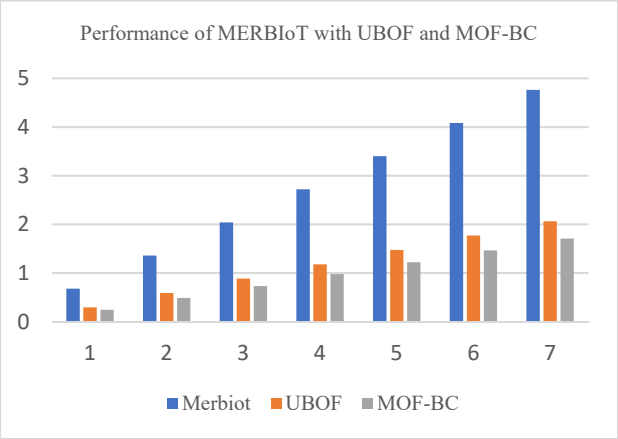


Graph 2 Performance after Swapping

The performance of MERBIoT is increased when after swapping the page from Full node to Light node. To analyze our Algorithm, we have taken two previous algorithms which were proposed recently in 2019. One is UBOF which was proposed as a light chain and those proposals performed well that time. MOF-BC (memory-optimized and flexible blockchain for large-scale networks) is another algorithm that was proposed in 2019 to reduce the memory of blockchain.

Full node	Light node	Merbiot	UBOF	MOF-BC
300	2	0.68	0.29478	0.24412
300	4	1.36	0.58956	0.48824
300	6	2.04	0.88434	0.73236
300	8	2.72	1.17912	0.97648
300	10	3.4	1.4739	1.2206
300	12	4.08	1.76868	1.46472
300	14	4.76	2.06346	1.70884

Table 4 Access values of MERBIoT



Graph 3 Performance of MERBIoT with UBOF and MOF-BC

Graph 3 shows MERBIoT performance over other algorithms. Table 4 refers to the access of MERBIoT values. The Results shows that the performance of MERBIoT is better than UBOF and MOF-BC.

9. Conclusion

Blockchain is providing more security than other platforms such as a centralized network in IoT environments. Even in centralized cloud storage, so many security measures have been proposed to obtain the security of the application, the security is not assured and there is a possibility of tampering the data in the network. To secure the Internet of things in very crucial applications blockchain should be implemented, to achieve transparency and data access will ensure the data is available in all the peers including Light node through Virtualization. The result shows that virtualization will be more helpful in blockchain adaptation to the Internet of things is a crucial application. Our future work is to test the light nodes with various heterogeneity in the network and to look for a solution to increase the number of transactions in IoT networks.

Acknowledgments

I would like to express thanks to my supervisor Dr. Munish Sabharwal, Prof., School of Computing Science & Engineering, Galgotias University for his tremendous support and been tremendous mentor for me. His immense knowledge and plentiful experience have encouraged me to complete this research. I owe him with lot of gratitude shown me during the way of research. I would also like to thank to my Co-supervisor Dr.Vijayalakshmi, Associate professor, christ university, india for always encouraging, motivating, enthusiasm, and allowing me to do what I think and continuous support throughout this research work. I have learned much knowledge from her and those helped me to including how to raise new possibilities, how to regard an old question from a new perspective, how to approach a problem by systematic thinking. This section should come before the References. Funding information may also be included here.

References

[1] Alenezi.; Zulkipli.; Atlam.; Walters.;Wills.(2017): *The Impact of Cloud Forensic Readinesson Security*, In Proceedings of the 7th International Conference on Cloud Computing and Services Science, Porto, Portugal, 24–26 April 2017, pp. 539–545. doi: 10.5220/0006332705390545
[2] Alkurdi.; Elgendi.; Munasinghe.; Sharma.; Jamalipour (2018): *Blockchain in IoT Security: A Survey*, In Proceedings of the 28th International Telecommunication Networks and Applications Conference (ITNAC), Sydney, Australia, 21–23, pp. 1–4. doi: 10.1109/ATNAC.2018.8615409.
[3] Andresen. (2013): *Bitcoin-Qt* / bitcoind version 0.8.0 released. Retrieved from https://bitcointalk.org/index.php?topic=145184
[4] Atlam.; Wills. (2019): *An efficient security risk estimation technique for Risk-based access control model for IoT*. Internet Things, 6, 1–20. doi: https://doi.org/10.1016/j.iot.2019.100052.
[5] Atlam.;Wills. (2019). *IoT Security, Privacy, Safety and Ethics*. In Intelligent Sensing, Instrumentation and Measurements; Springer Science and Business Media LLC: Berlin, Germany, pp. 123–149. doi: 10.1007/978-3-030-18732-3_8
[6] Atlam.; Alenezi.; Walters.; Wills.;Daniel. (2017): *Developing an Adaptive Risk-Based Access Control Model for the Internet of Things*. In Proceedings of the 2017 IEEE 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), Exeter, UK, 21–23, pp. 655–661. doi: 10.1109/iThings-GreenCom-CPSCom-SmartData.2017.103.
[7] Atlam.;Walters.;Wills. (2018): *Fog Computing and the Internet of Things: A Review*. Big Data Cogn. Computing, 2, 10. doi: https://doi.org/10.3390/bdcc2020010.
[8] Banafa. (2017): *IoT and Blockchain Convergence: Benefits and Challenges*. IEEE IoT Newsletter. Retrieved from http://iot.ieee.org/newsletter/january-2017/iot-and-blockchain-convergence-benefits andchallenges.html
[9] Bitcoin Wiki. (2020): *Scalability*. Retrieved from https://en.bitcoin.it/wiki/Scalability
[10] Blockchain.info. *Blockchain Size Data*. Retrieved from https://blockchain.info/charts/blocks-size
[11] Bruce. (2018): *The Mini-Blockchain Scheme*. Retrieved from https://www.weusecoins.com/assets/pdf/library/The\%20MiniBlockchain\%20Scheme.pdf
[12] Conoscenti.; Vetro.; De Martin (2017): *Peer to Peer for Privacy and Decentralization in the Internet of Things*. In Proceedings of the 2017 IEEE/ACM 39th International Conference on Software Engineering Companion (ICSE-C), Buenos Aires, Argentina, 20–28, pp. 288–290. doi: 10.1109/ICSE-C.2017.60.
[13] Conti.; Lal.; Ruj. (2018): *A Survey on Security and Privacy Issues of Bitcoin*," IEEE Communications Surveys Tutorials, pp. 1–1. doi: 10.1109/COMST.2018.2842460.
[14] Dorri.; Kanhere.;Jurdak. (2019): *MOF-BC: A memory optimized and flexible blockchain for large scale networks*. Future Generation Computer Systems, vol.92, pp357373. Retrieved from http://www.sciencedirect.com/science/article/pii/S0167739X17329552. doi:https://doi.org/10.1016/j.future.2018.10.002
[15] Fernandez-Carames.; Fraga-Lamas. (2018): *A Review on the Use of Blockchain for the Internet of Things*. IEEE Access 2018, 6, 32979–33001. doi: 10.1109/ACCESS.2018.2842685.
[16] França. (2015): *Homomorphic Mini-blockchain Scheme*. Retrieved from http://cryptonite.info/files/HMBC.pdf
[17] Kirubakaran.; Prasanna Venkatesan.; Sampath Kumar.; Kumaresan.; Annamalai. (2020): *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. doi: https://doi.org/10.1007/s12652-020-02218-1.
[18] Nakamoto. (2008): *Bitcoin: A peer-to-peer electronic cash system*. Retrieved from http://bitcoin.org/bitcoin.pdf
[19] Pascal Urien. (2018): Blockchain IoT (BIoT): A New Direction for Solving Internet of Things Security and Trust Issues. IEEE, doi: 10.1109/CIOT.2018.8627112
[20] Reiner. (2012): *A. Ultimate blockchain compression*. Retrieved from https://bitcointalk.org/index.php?topic=88208
[21] Reyna.; Martín.; Chen.; Soler.;Díaz. (2018): *On blockchain and its integration with IoT. Challenges and opportunities*. Future Gener. Comput. Syst, 88, 173–190. doi: https://doi.org/10.1016/j.future.2018.05.046.
[22] Saito.; Iwamura. (2018): *How to make a digital currency on a blockchain stable*. arXiv preprintarXiv:1801.06771. doi: https://doi.org/10.1016/j.future.2019.05.019.
[23] Samaniego.; Deters. (2016): *Blockchain as a Service for IoT*. IEEE Int. Conf. Internet Things IEEE Green Comput. Commun. IEEE Cyber, Phys. Soc. Comput. IEEE Smart Data, pp. 433–436. doi:10.1109/iThings-GreenCom-CPSCom-SmartData.2016.102
[24] Todd. (2013): *Bitcoin Blocksize Problem Video*. Retrieved from https://bitcointalk.org/index.php?topic=189792Akerkar, R. A.; Lingras, P. (2008). An Intelligent Web: Theory and Practice, 1st edn. Johns and Bartlett, Boston.

Authors Profile

M. Vivek Anand is a research scholar in Department of CSE, Galgotias University, Greater Noida, Uttar Pradesh, India. He received M.E in Software Engineering from Anna University, Chennai, Tamilnadu in 2013. Bachelor of Engineering in the stream of Computer Science from Anna University, Coimbatore, Tamil Nadu in 2011, He has more than 7 years of teaching experience. His research interests are Blockchain and Internet of Things

Dr. Munish Sabharwal is Qualified PhD (CS), PhD (Management [MIS]) and contributing over 22.5+ years in Teaching (CS and MIS), Education Management, Research as well as S/W Development. Currently spearheading efforts as Dean & Professor (CSE), Galgotias University, Greater Noida (UP) INDIA. Possessing a flair for teaching with the proven ability to apply the best practice based & innovation-oriented teaching learning practices in engineering education as well as collaborative approach for research and decentralized &supportive style to academic administration. Current research interests include Data Science-AI& ML, Biometrics & E-Banking.

Dr. S. Vijayalakshmi completed Bachelor of Science in the stream of Computer Science from Bharathidasan University, Tiruchirappalli, Tamil Nadu in 1995, Master of Computer Application in same University in 1998 and Master of Philosophy in same University in 2006. She received her Doctorate in 2014. She has been working as an Associate Professor in the Dept of Data Science, Christ university, India., She has more than 20 years of teaching experience and more than 10 years of research experience. She has published many papers in the area of image processing especially in medical imaging.