IoT-Fog: A Communication Framework using Blockchain in the Internet of Things

Tanweer Alam[1]

[1]Islamic University of al-Madinah al-Munawarah

June 8, 2020

Abstract

The fog computing is the emerging technology to compute, store, control and connecting smart devices with each other using cloud computing. The Internet of Things (IoT) is an architecture of uniquely identified interrelated physical things, these physical things are able to communicate with each other and can transmit and receive information. This research presents a framework of the combination of the Internet of Things (IoT) and Fog computing. The blockchain is also the emerging technology that provides a hyper, distributed, public, authentic ledger to record the transactions. Blockchains technology is a secured technology that can be a boon for the next generation computing. The combination of fog, blockchains, and IoT creates a new opportunity in this area. In this research, the author presents a middleware framework based on the blockchain, fog, and IoT. The framework is implemented and tested. The results are found positive.

Keywords: Internet of Things (IoT), Fog Computing, Cloud Computing, Blockchains, Communication Security.

1.0 Introduction:

The blockchains technology (BT) and IoT are pondered emerging approaches that can change our lives in the next generation computing. The BT is much secured and authentic than other technologies. It can be optimistic to provide us high trust in the secure transactions in the heterogeneous network where everything with connecting and talks to each other [1]. Fog computing can play an important role in IoT and BT network. It can compute, store and control the transaction. The IoT is the ongoing research to connect the physical objects, machines and embedded devices to wireless communication and the internet. According to the Statista report, the IoT connected devices will reach more than 75 billion up to 2025 [2]. This report shows us the importance of the proposed framework.
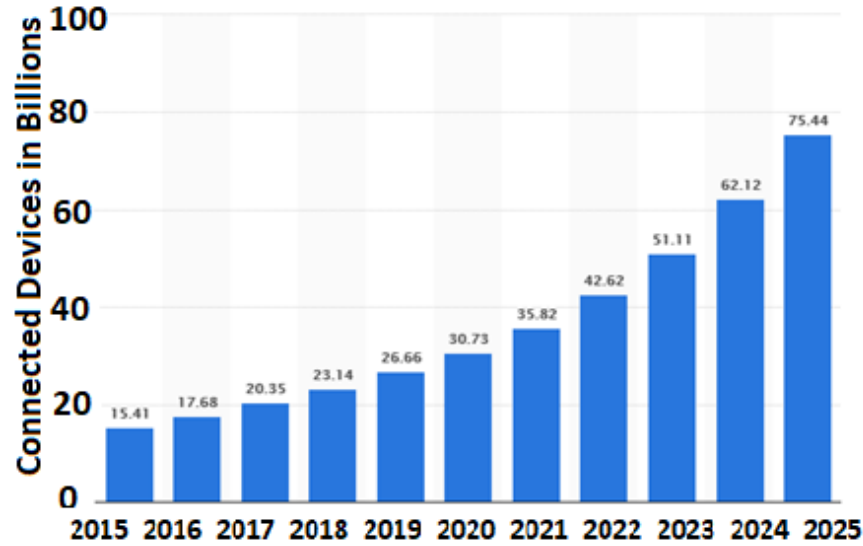
Figure 1. Statista report of connecting devices between 2015-2025 [1]

The blockchain is considered as validating and selecting a chain of blocks. Every IoT node is able to perform validation and selection criteria. The transactions fired by the IoT node are converted into blocks. The blocks are transmitted to the public network and this block will reach every IoT node but this block will be selected by the valid node and verify the hash code. The hyper ledger stores the transaction records publicly with security. Every transaction is digitally signed before transmitting to the network. So, the transactions are much more secured that shows its authenticity and integrity of the Hyperledger. The following points can be considered for the blockchain:

i) A blockchain is a decentralized, public, distributed and secure database among IoT nodes.

ii) Each IoT node has the ability to validate the blocks.

iii) Sometimes some IoT nodes (Miners) are considered as a controller in the block chains.

iv) The peer-to-peer topology is used in blockchains.

v) The hyper ledger stores all recorded transactions. The blockchains update after recorded.
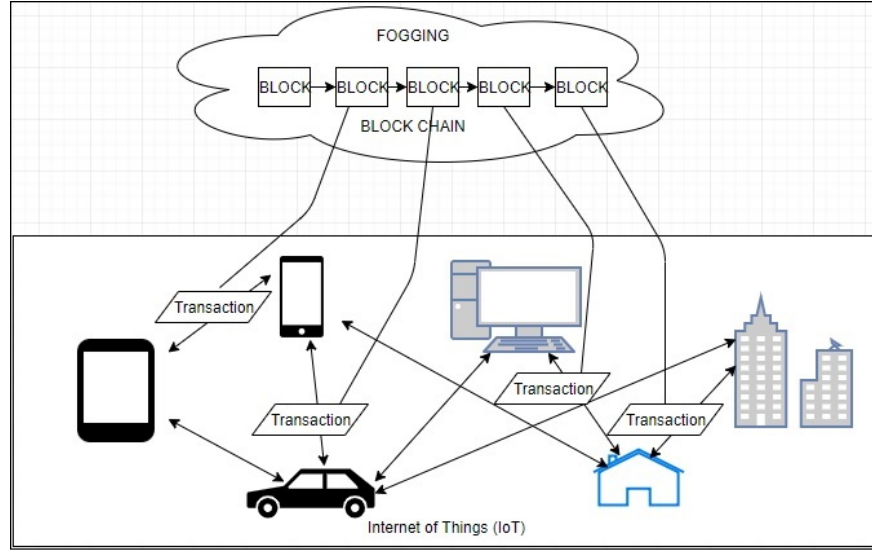
vi) BT is always on. No any IoT node off the BT.

Figure 2: IoT-Fog

The above are the positive points about blockchains but there are a lot of challenges such as:

i) the processing speed of IoT device and BT

ii) Time durability

iii) storage the big data

iv) real-time connectivity

v) IoT device Intelligence power

vi) and so on...

The aim of this research is to introduce the new area of research where the top emerging technologies combined together and form a group for the ultimate goal of our proposal. It enhances the area of IoT and provides secure and authentic communication among the physical things.

The rest of the paper is organized into different sections. Section 1 introduce the research, section 2 represents the literature review, section 3 represents the proposed study and results of the proposed study and section 4 represents the conclusion of the proposed research.

2.0 Literature review

Fog Computing is also represented as Fogging that is a term created by Cisco. The role of fogging is to extend the cloud computing into the edge computing. The fogging is supported to the IoT network that is the main idea to develop this term. The Fogging has improved the accuracy of the system and the quality of the services. It can support the physical things that are connected together. In 2015, Cisco represented fogging for the cloud computing in the edge of the network to process the information in a more accurate way. It is used to reduce the workload of cloud computing [3]. Flavio Bonomi et. al. was presented the role of fogging and its characteristics in the internet of things [4]. Fog computing is used to minimize the information transmitted to the cloud to process, analyze and store. It is also improved the efficiency and security of the framework. In 2017, Jianbing Ni has presented an article on secure fogging for IoT. In this paper, the authors were focused on security and privacy issues faced in the communication among IoT nodes with fogging [5]. In 2017, Joy Dutta and Sarbani Roy have published an article [6] on IoT-Fog framework for smart cities. In this paper, they presented the smart building structure with the use of fog and IoT

3

networks. In 2017, Muhtasim M., et. al. was published the thesis report [7], they have presented the security of transmitted data transactions in the internet of things network by using the blockchains technology. In the article [8], various consensus algorithms discussed and compared. They compared the algorithms such as Proof-of-Work (PoW), Proof-of-Stake (PoS), Delegated Proof-of-Stake (DPoS), Leased Proof-Of-Stake (LPoS), Proof of Elapsed Time (PET), Practical Byzantine Fault Tolerance (PBFT), Simplified Byzantine Fault Tolerance (SBFT), Delegated Byzantine Fault Tolerance (DBFT), Directed Acyclic Graphs (DAG), Proof-of-Activity (PoA), Proof-of-Importance (PoI), Proof-of-Capacity (PoC), Proof-of-Burn (PoB), and Proof-of-Weight (PoW) [9].

Table 1: Comparison of the Consensus Algorithms [9,10]

Algorithms	Blockchain Platform	Launched Year	Languages	Smar
PoW	Bitcoin	2009	C++	No
PoS	NXT	2013	Java	Yes
DPoS	Lisk	2016	JavaScript	No
LPoS	Waves	2016	Scala	Yes
PoET	Hyperledger Sawtooth	2018	Python, JavaScript, Go, C++, Java, and Rust	Yes
PBFT	Hyperledger Fabric	2015	JavaScript, Python, Java REST and Go	Yes
SBFT	Chain	2014	Java, Node, and Ruby	No
DBFT	NEO	2016	Python,.NET, Java, C++, C, Go, Kotlin, JavaScript	Yes
DAG	IOTA	2015	Javascript, Rust, Java Go, and C++	In Pro
POA	Decred	2016	Go	Yes
PoI	NEM	2015	Java, C++XEM	Yes
PoC	Burstcoin	2014	Java	Yes
PoB	Slimcoin	2014	Python, C++, Shell, JavaScript	No
PoWeight	Filecoin	2017	SNARK/STARK	Yes

3.0 Proposed Framework and results

The proposed framework has represented the use of Fog computing with IoT devices on the edge of the network using the blockchain technology to connect, transfer and exchange information among the IoT nodes. The transactions in the proposed framework are transmitted in the point-to-point network topology. In the network, there are some special IoT nodes called Miners. They are generally used to verify the transactions in the network. If the transactions are verified then it converts into the block and added in the blockchains that previously exist and relayed to the network. The miners play the important role to adjust the newly created block in the blockchain.
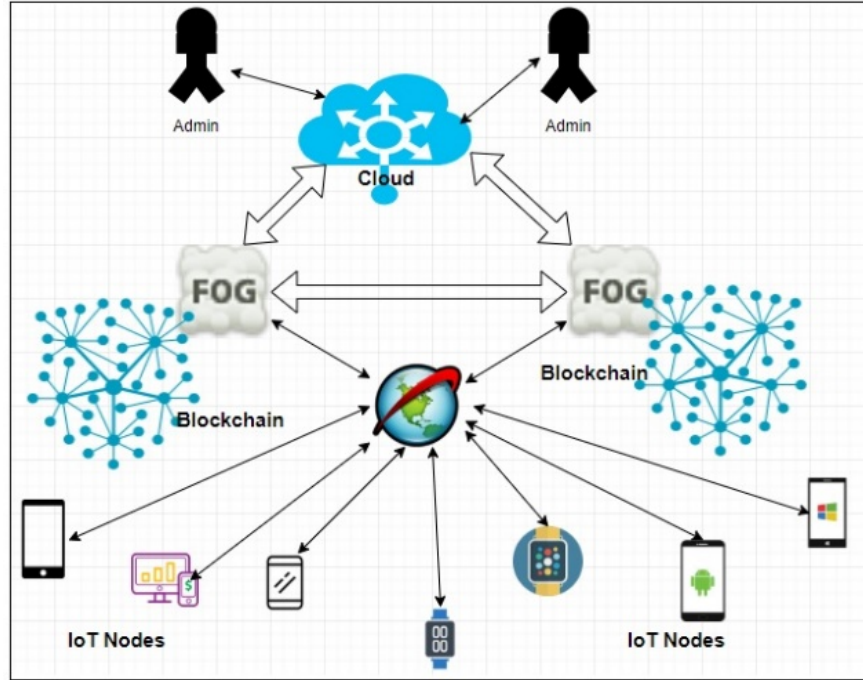
4

Figure 3: IoT-Fog middleware architecture using Blockchain

In this research, we have evaluated the framework using several tests. The blockchains are implemented using Hyperledger IROHA tool. The docker and docker-compose are installed on the machine. The main parameters are described in table 1 [11]. Icov coverage testing tool is used to evaluate the IoT device coverage in the range of the network.

Parameter	Possible values	Default	Description
COVERAGE	ON/OFF	OFF	Enables or disables lcov setting for code coverage generation
BENCHMARKING		OFF	Enables or disables build of the Google Benchmarks library
TESTING		ON	Enables or disables build of the tests
SWIG_PYTHON		OFF	Enables or disables the library building and Python bindings
SWIG_JAVA		OFF	Enables or disables the library building and Java bindings

Table 2. Main parameters for performance evaluation.

The Hyperledger IROHA tool is included many facilities such as distributed Hyperledger, Proof of Work (PoW) algorithms, P2P network, etc., Sumeragi in Hyperledger IROHA algorithm is implemented to rum blockchains. The Android and iOS packages in IROHA provide the facility to interact the IoT nodes to the blockchain. According to the Sumeragi algorithm, the IoT nodes request the transaction, and follow the following steps:

Step 1. Broadcasting: the leaders verify, orders and sign the transaction and transmit to the network.

Step 2: Verification and signing: It verifies, orders and sign the transaction and broadcasting to the authorized IoT node of the peer to peer network.

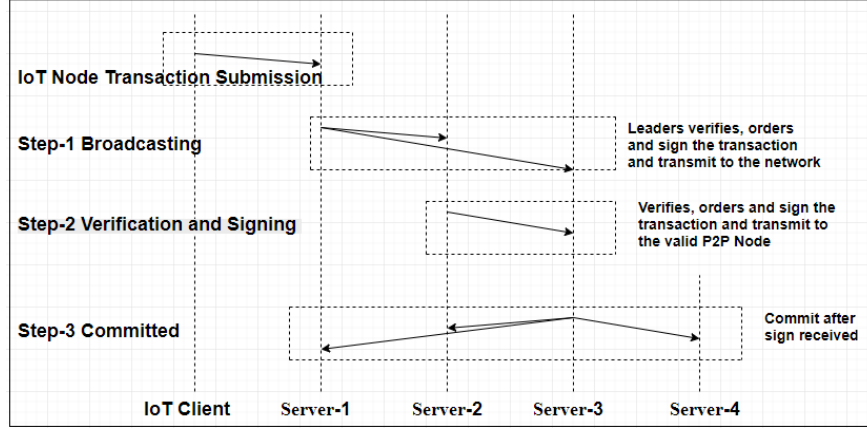Step 3: Committed: Commit after signing.

Figure 4: Sumeragi in Hyperledger IROHA algorithm [12]

In case of server failure, the algorithm adds one another step called error control. For controlling the errors, the algorithm works with the additional server to control the errors.
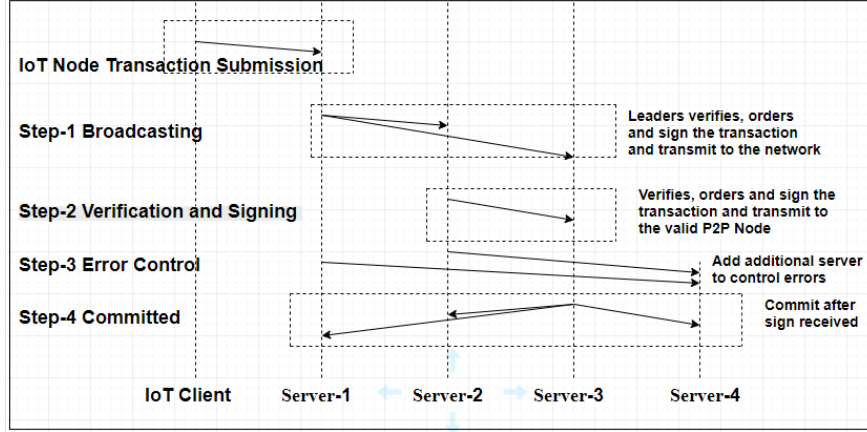

Figure 5: Sumeragi in Hyperledger IROHA algorithm with error control

We have evaluated the performance of 10, 50 and 100 IoT nodes using the different parameters in the proposed framework.

Table 3: Performance of 10 IoT-nodes against searching, Examine and Selecting

	IoT-Node-1 ON	IoT-Node-1 OFF	IoT-Node-3 ON	IoT-Node-3 OFF	IoT-Node-5 ON	IoT-Node-5 OFF
Searching	0.11	0.22	0.12	0.18	0.08	0.15
Examine	0.01	-	0.01	-	0.01	-
Selecting	0.01	0.01	0.01	0.01	0.01	0.01

[CHART]

Figure 6: Performance of 10 IoT-nodes

Table 4: Performance of 50 IoT-nodes against searching, Examine and Selecting

6

	IoT-Node-1 ON	IoT-Node-1 OFF	IoT-Node-3 ON	IoT-Node-3 OFF	IoT-Node-5 ON	IoT-Node-5 OFF
Searching	0.12	0.23	0.10	0.21	0.12	0.22
Examine	0.01	-	0.02	-	0.02	-
Selecting	0.02	0.02	0.02	0.02	0.01	0.01

[CHART]

Figure 7: Performance of 50 IoT-nodes

Table 5: Performance of 100 IoT-nodes against searching, Examine and Selecting

	IoT-Node-1 ON	IoT-Node-1 OFF	IoT-Node-3 ON	IoT-Node-3 OFF	IoT-Node-5 ON	IoT-Node-5 OFF
Searching	1.81	2.25	1.97	2.54	2.2	3.6
Examine	0.53	-	0.81	-	0.72	-
Selecting	0.24	0.25	0.37	0.56	0.29	0.47

[CHART]

Figure 8: Performance of 100 IoT-nodes

4.0 Conclusion

The proposed framework acted as a combination of the Internet of Things (IoT) and fog computing. The Blockchain is used to create a hyper-distributed public authentic ledger to record the transactions. The research opened a new opportunity in this area. The framework is implemented using a different set of IoT nodes and tested. The results are found positive.

Acknowledgment

References

[1] Alam, Tanweer, and Mohammed Aljohani. "Design a new middleware for communication in ad hoc network of android smart devices." In Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies, p. 38. ACM, 2016. DOI: https://doi.org/10.1145/2905055.2905244

[2] Statista. Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions), 2019. https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

[3] Computing F. the Internet of Things: Extend the Cloud to Where the Things are. Cisco White Paper. 2015.

[4] Bonomi F, Milito R, Zhu J, Addepalli S. Fog computing and its role in the internet of things. InProceedings of the first edition of the MCC workshop on Mobile cloud computing 2012 Aug 17 (pp. 13-16). ACM.

[5] Ni J, Zhang K, Lin X, Shen XS. Securing fog computing for internet of things applications: Challenges and solutions. IEEE Communications Surveys & Tutorials. 2017 Oct;20(1):601-28.

[6] Dutta J, Roy S. IoT-fog-cloud based architecture for smart city: Prototype of a smart building. In Cloud Computing, Data Science & Engineering-Confluence, 2017 7th International Conference on 2017 Jan 12 (pp. 237-242). IEEE.

[7] Muhtasim M, Fariha SR, Islam N, Rashid R. Secure data transaction and data analysis of IOT devices using blockchain, Doctoral dissertation, BARC University, 2017.

[8] https://101blockchains.com/consensus-algorithms-blockchain/

[9] A. Shanti Bruyn, "Blockchain an introduction", research report, University AMSTERDAM, 2017

[10] Florea BC. Blockchain and Internet of Things data provider for smart applications. In2018 7th Mediterranean Conference on Embedded Computing (MECO) 2018 Jun 10 (pp. 1-4). IEEE.

[11] https://iroha.readthedocs.io/en/latest/guides/build.html

[12] https://www.hyperledger.org/wp-content/uploads/2017/08/Hyperledger_Arch_WG_Paper_1_Consensus.pdf

Other Bibliographies:

[13] Wang, Tian, Jiyuan Zhou, Anfeng Liu, Md Zakirul Alam Bhuiyan, Guojun Wang, and Weijia Jia. "Fog-based computing and storage offloading for data synchronization in IoT." IEEE Internet of Things Journal (2018).

[14] Alam, Tanweer, and Mohammed Aljohani. "An approach to secure communication in mobile ad-hoc networks of Android devices." In 2015 International Conference on Intelligent Informatics and Biomedical Sciences (ICIIBMS), pp. 371-375. IEEE, 2015. DOI: https://doi.org/10.1109/iciibms.2015.7439466

[15] Aljohani, Mohammed, and Tanweer Alam. "An algorithm for accessing traffic database using wireless technologies." In Computational Intelligence and Computing Research (ICCIC), 2015 IEEE International Conference on, pp. 1-4. IEEE, 2015. DOI: https://doi.org/10.1109/iccic.2015.7435818

[16] Alam T, Benaida M. The Role of Cloud-MANET Framework in the Internet of Things (IoT). International Journal of Online Engineering (iJOE). 2018;14(12):97-111. DOI: https://doi.org/10.3991/ijoe.v14i12.8338

[17] Alam, Tanweer. (2018) "A reliable framework for communication in internet of smart devices using IEEE 802.15.4." ARPN Journal of Engineering and Applied Sciences 13(10), 3378-3387.

[18] Alam T, Benaida M. CICS: Cloud–Internet Communication Security Framework for the Internet of Smart Devices. International Journal of Interactive Mobile Technologies (iJIM). 2018 Nov 1;12(6):74-84. DOI: https://doi.org/10.3991/ijim.v12i6.6776

[19] Alam, Tanweer. "Middleware Implementation in Cloud-MANET Mobility Model for Internet of Smart Devices", International Journal of Computer Science and Network Security, 17(5), 2017. Pp. 86-94

[20] Tanweer Alam, "A Reliable Communication Framework and Its Use in Internet of Things (IoT)", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), Volume 3, Issue 5, pp.450-456, May-June.2018 URL: http://ijsrcseit.com/CSEIT1835111.

[21] Alam, Tanweer. "Fuzzy control based mobility framework for evaluating mobility models in MANET of smart devices." ARPN Journal of Engineering and Applied Sciences 12, no. 15 (2017): 4526-4538.

[22] Alam, Tanweer, Arun Pratap Srivastava, Sandeep Gupta, and Raj Gaurang Tiwari. "Scanning the Node Using Modified Column Mobility Model." Computer Vision and Information Technology: Advances and Applications 455 (2010).

[23] Alam, Tanweer, Parveen Kumar, and Prabhakar Singh. "SEARCHING MOBILE NODES USING MODIFIED COLUMN MOBILITY MODEL.", International Journal of Computer Science and Mobile Computing, (2014).

[24] Alam, Tanweer, and B. K. Sharma. "A New Optimistic Mobility Model for Mobile Ad Hoc Networks." International Journal of Computer Applications 8.3 (2010): 1-4. DOI: https://doi.org/10.5120/1196-1687

[25] Singh, Parbhakar, Parveen Kumar, and Tanweer Alam. "Generating Different Mobility Scenarios in Ad Hoc Networks.", International Journal of Electronics Communication and Computer Technology, 4(2), 2014

[26] Sharma, Abhilash, Tanweer Alam, and Dimpi Srivastava. "Ad Hoc Network Architecture Based on Mobile Ipv6 Development." Advances in Computer Vision and Information Technology (2008): 224.

[27] Alam, Tanweer, and Mohammed Aljohani. "Design and implementation of an Ad Hoc Network among Android smart devices." In Green Computing and Internet of Things (ICGCIoT), 2015 International Conference on, pp. 1322-1327. IEEE, 2015. DOI: https://doi.org/10.1109/ICGCIoT.2015.7380671

[28] Stanciu, Alexandru. "Blockchain based distributed control system for edge computing." In Control Systems and Computer Science (CSCS), 2017 21st International Conference on, pp. 667-671. IEEE, 2017.