A Survey of Internet of Things node's transactions Secure through Blockchain Technology

Mahesh Arse
PG Scholar
Department of Information Technology
Shri Vaishnav Institute of Information Technology,
SVVV Indore M.P

Jigyasu Dubey
Professor
Department of Information Technology
Shri Vaishnav Institute of Information Technology,
SVVV Indore M.P

ABSTRACT
Internet of Things is widely used in various sectors in recent years, due to its efficiency, scalability, feasibility, etc. Thus, need such type of network infrastructure for reducing the human effort from unwanted work like household chores, information gathers or repeated work, etc. That is possible from the Internet of Things. Internet of Things is a collection of smart nodes that collect the data and produce a result by systematically analyzed them. Therefore it can reduce the dependability from humans and expect the best result in any worst condition. Now the Internet of Things is a rapidly growing industry in the world and also there are lots of vulnerability have occurred in recent years. Thus, need to secure Internet of Things nodes during communicating between each other device as well as saving or processing information, without precaution from the attacks, it cannot safe, sensitive information from the attacker, because enhancing of technology there will be increased computational overhead. Therefore, need security measures like Confidentiality, Integrity, Authentication, Non-repudiation, Availability, etc. in any transactions of IoT devices. And such security measures can provide now the only Blockchain technology. And it can safe from the attacker's intention. Blockchain is a decentralized, distributed ledger technology that overcomes the data's tamper and provides the availability from its decentralization environment. This technology can use in the IoT environment to protect them from malicious, unauthorized user/node and make it able to take action against them. In this study, introduced the concept of a secure IoT node's transaction through Blockchain technology.

Keywords
Internet of Things, Blockchain, Security Measurement

1. INTRODUCTION
Internet of Things is one of the most prominent technology emerged in the 21st century. This technology is leading all over the world within a few times that makes it possible with its efficiency, scalability, and feasibility etc. But the most important loophole of this technology is that there are no such security measures available to protect data/information during the communication as well as on stores on both sides. Because the Internet of Things (IoT) devices is very small in size as well as processing too. Thus, need such mechanism to overcome the vulnerabilities of IoT devices. Blockchain is a decentralized, distributed ledger technology, which is widely used in today's era. From 2009 to the current date is gaining popularity from its working scenarios, due to this Bitcoin used in its implementation made popular in the world of cryptocurrency. Most cryptocurrencies also have developed to use Blockchain technology. In Blockchain there are most of the parts are provide security, but some of them are now vulnerable like proper authentication, provide non-repudiation etc. Blockchain provides the massive security solution to break impossible jobs for attackers, but some part in the Blockchain need for redefining.

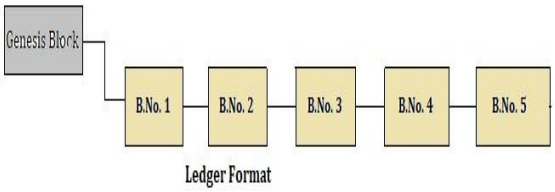

Fig.1 Ledger Format

In this study, we will use the home appliance devices to connect each other through Internet for communication amongst them and the outdoor node. In general smart home appliances like fridge, air conditioner, microwave, fan, smart bulb etc. These nodes must have the computing power for processing, memory for storage, and energy. If these nodes will communicate with each other, then they will be passing messages from each other on that condition, need the protection for securing transaction, and also the entire network through Blockchain technology. Internet of Things needs protection in all stages of communication from begging to end the communication as well as ensure the stored information into the distributed ledger. In recent years lots of research work already have been done in the field of IoT and blockchain, but few of the problems did not touch in a proper implementation phase in a combination of the Internet of Things and Blockchain technology.

2. LITERATURE REVIEW
Existing security arrangements are not suited for it because of high vitality utilization, what's more, handling overhead [1]. The author recently proposed a technique that tends to these difficulties by utilizing the Bitcoin BC, which is a permanent record of squares [2]. Execution examination of the Blockchain stages gave bits of knowledge into the engineering's attainability and further contemplations for sending a usable usage [3]. A contextual analysis was additionally accommodated the access control in an IoT framework with one workstation, one workstation, and two Raspberry Pi single-board PCs [4]. In light of the structure, the author builds up a model framework for its information trade with Ethereum Blockchain and related Internet innovation [5]. These highlights are accomplished in the author's proposition by utilizing the eccentric properties of Blockchain innovations, joined with another engineering structure that maintains a strategic distance from the entanglements acquired by this innovation while releasing its

points of interest. [6] An extraordinary consideration towards Blockchain has been as of late given by the two analysts and organizations, because of its high practical power, chiefly depending on the possibility that Blockchain can actualize an open, shared record without committing any confided in substance [7]. [8] Author structured an IoT-driven PKI. The author recognizes adaptability issues emerging from distributing authentications straightforwardly on the blockchain and propose an elective model roused by the snare of trust. Given this model, the author plan to insightfully break down the versatility of our answer contrasted with different PKIs. Moreover, a protected open key dissemination conspire requires secure provisioning the way toward stacking a one of a kind private key and different authentications to give character to a device. An IoT device and server correspondence structure on Ethereum utilizing is doing a smart contract that empowers a superior protection instrument against D DoS and rebel device assaults. The proposed framework can give qualification among trusted and untrusted devices and distributes a static asset limit to every device above which it can't work [9]. Our framework takes into consideration fine-grained get to control and sharing of time arrangement sensor information of different out applications. Starting execution assessment results are promising and demonstrate a moderate overhead because of our framework [10]. In any case, unscrambling engaged with the ABEs is normally excessively costly for asset compelled front-end clients, which significantly obstructs it's down to earth prevalence. With the end goal to lessen the unscrambling overhead for a client to recuperate the plaintext, Green et al. Recommended redistributing most of the unscrambling work without uncovering real information or private keys [11]. The model demonstrates that the blockchain system can record the exchange in an auditable, straightforward, and changeless ways [12]. Now in time, the author doesn't have natty gritty outcomes on the adaptability or the execution of blockchain in it arranges [13].

Table 1: Comparison between different types of blockchain services available:

S.No.	Features	Bitcoin	Ethereum	Hyperledger Fabric
1.	Fully developed	✓	✓	✓
2.	Miner participation	Public	Public, Private, Hybrid	Private
3.	Trustless operation	✓	✓	Trusted validator Nodes
4.	Multiple applications	Financial only	✓	✓
5.	Consensus	PoW	PoW, PoS ("Casper")	PBFT
6.	Run smart contracts	×	✓	✓
7.	TX integrity and authentication	✓	✓	✓
8.	Data Confidentiality	×	×	✓
9.	ID management	×	×	✓
10.	Key management	×	×	(Through CA)
11.	User authentication	Digital Signatures	Digital Signatures	Based on enrolment Certificates
12.	Vulnerability to attacks	51%, linking Attacks	51%	> 1/3 faulty Nodes
13	TX throughput	7TPS	7-9TPS	Can achieve Thousands TPS (Depending upon Number of endorsers, Orderers And commuters)
14.	Latency in the single confirmation For a TX	10 min	20-25 Sec	Less than Bitcoin And Ethereum

1.1.Security Requirement in IoT

Confidentiality: - To protect data from unauthorized user.

Authentication: - Without permission one can enter into it for modification.

Non-repudiation: - No one can deny after committing transactions.

Authorization: - To give permission for read/write operation over the transactions.

3. PROPOSED METHODOLOGY

3.1 Block format

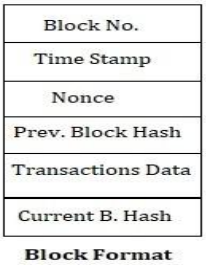

Fig. 2 Block Format

Block No: which represents the block number by which easily identifies any block in the ledger. This will helpful for searching.

Time Stamp: which also an important factor in searching any block from the entire ledger.

Nonce: This field also important for providing consensus among the node as well as make the hash identical from the different ledger.

Previous Block Hash: This field for linking one block to another block and make a link list of a block in the ledger which makes the data immutable.

Transactions Data: In this field number of transactions stores via Markle tree concept, by which easily find any transaction from the block.

Current Block Hash: This field shows the integrity of the block. Here the hash function is used e.g. MD5, SHA 256, etc.

Genesis Block: This is the first block of any ledger which doesn't have the previous block hash & transaction too. After that, all block links via previous block hash which makes the data immutable.

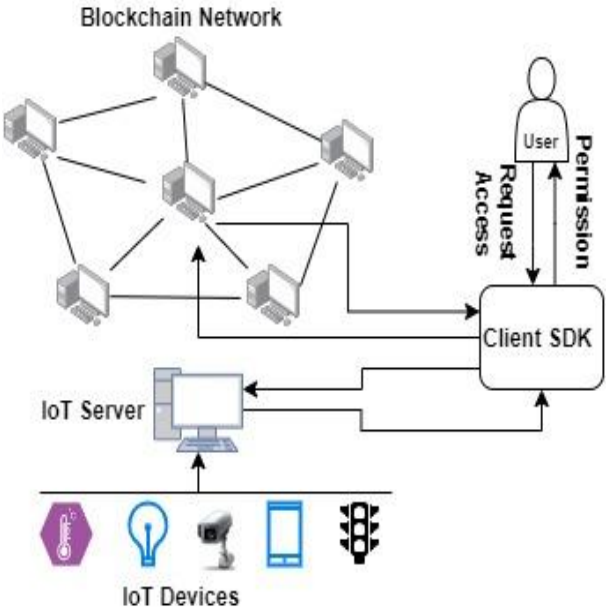

Fig. 3 Proposed Solution Architecture

The fig. 3 shows the proposed solution architecture where in bottom IoT devices are situated which produced the data and that data collected by IoT server. And then send it to blockchain network with the help of client SDK. By SDK user can also interact with blockchain network and do any things want. Without credentials no one can interact with the blockchain network. So, firstly user has to enroll itself into it and then receive credentials. Such credentials useful for accessing the network. But most important is that user also don't change the block content instead it has to make new transaction for changing any things into the block. Blockchain network node connected like a P2P network node thus no one can change entire network ledger at a time. Because every block contains the previous block hash which makes it immutable. Blockchain technology provides the decentralized environment through which consensus achievement is hard task. But this study try to resolve such problems. In this proposed methodology, used the hyperledger fabric as a blockchain technology framework to secure the data of Internet of Things. Authentication is a security measure to provide the ability to node do anything in the network, which must be legal and approve by others to show the trust between them with the help of username & password provided in the hyperledger fabric network. Non-repudiation is also a security which provides the way of no one can deny its work that has been done, with a digital certificate and public, private key infrastructure that provided by certificate authority onto fabric wallet. The all history of transactions is stored in a distributed ledger (Couch DB) no one can tamper or delete from the ledger, because ledger provides the read only command instead of CRUD command. Once sender makes the transaction and send it to the destination, then this transaction will pass from the hyperledger fabric network where one peer will mine this transaction this can happen through voting method or PBFT for consensus achievement, if verification find correctness in the message then it will save on the block otherwise discard permanently & that time it store into the buffer. Due to this process it takes time, thus one block use the time, 100-150 MS (Depending upon the system configuration) from creation itself to complete final commit.

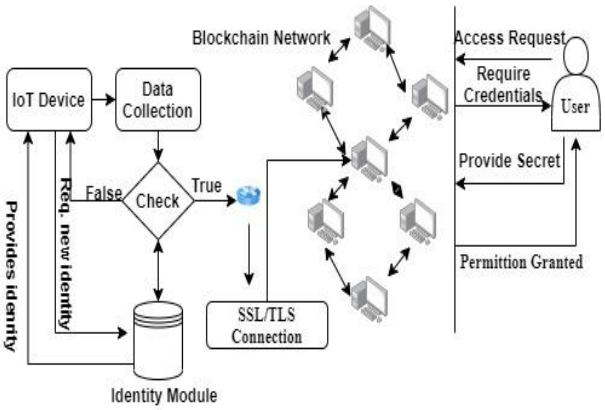

Fig. 4 Flow Diagram of Proposed solution

Fig. 4 shows the flow diagram of proposed solution where IoT devices send their sensing data to data collection module or IoT server. This time every IoT devices has to present their identity for authentication purpose. All the identity stored into the identity module if doesn't exit then transaction failed and return to IoT devices. Then IoT devices are register and get identity then finally send to gateway. If legitimated IoT devices send their data then checks found true and data received into the blockchain network through internet connection and all the connection enable secure through SSL/TLS protocols. Now, after reaching data into the network miner node has to first check its validity and authentication of node's transaction and after satisfy allow to store into the block. In this mechanism miner became through voting process where individual node elect the leader who takes decision for any transaction and miner decision have to comply by all node and get the consensus in the network. If client want to interact with the implemented network then it has to enroll itself. And then granted permission able to communicate with the blockchain network otherwise not. But more important things is that user/client also don't change any block's data it can make new transaction only. For all the transaction done with smart contract mechanism for getting better efficiency of the blockchain network.

4. EXPECTED OUTCOME

Internet of Things is widely used technology so this research will boost their acceptance and increase its demand, as usual nowadays is being. All the transactions will be secure during communication. Before communicating with other nodes, the sender will identify the legitimate right receiver easily through a two-way authentication mechanism or mutual TLS authentication in hyperledger fabric network. All the data which saved on to the distributed ledger will be immutable by the use of hash function into the blockchain technology, no one can change without the hacked off over the 51% node's ledger at the same time. This is impossible nowadays because neither made such hardware nor software for such work.

1. Free from data centralization.
2. Improve scalability, if less no of peer.
3. Achieve authentication & confidentiality with the help of username and password as well as PKI domain.
4. Easily find the corresponding node's data with the help of timestamp and node id which put into the every transaction.
5. In Blockchain technology nonce will be useful for different hash with respect to same data comes again and again.
6. And get security measurements in every single transaction of IoT devices.

5. CONCLUSION

This proposed methodology creates secure communication between IoT and blockchain network, by which its data will be secured & fulfil the requirement of IoT security. Along with increase the acceptance and demand of IoT devices in various areas, due to its smartness, efficient and convenient. Also with hyperledger fabric could be improved scalability if number of peer has to use less. This study prominent for security in IoT device without any computational overhead onto it. In future this study will further enhance according to the requirements and implement onto the real physical IoT device to calculate its various characteristic. Because this study mainly design for working on the simulator not actual IoT actual devices.

6. REFERENCES

[1] Dorri, A., Kanhere, S., Jurdak, R., & Gauravaram, P. (n.d.). *Blockchain for IoT Security and Privacy: The Case Study of a Smart Home.*

[2] Schmitt, C., Kothmayr, T., Hu, W., Stiller, B., Schmitt, C., Stiller, ·., . . . Kalaiselvi, M. (2017). Two-Way Authentication for the Internet-of-Things. *Studies in Big Data*, *25*.

[3] Ali, M., Dolui, K., & Antonelli, F. (2017). IoT data privacy via blockchains and IPFS. *Proceedings of the Seventh International Conference on the Internet of Things - IoT '17.*

[4] Zhang, Y., Kasahara, S., Shen, Y., Jiang, X., & Wan, J. (2018). Smart Contract-Based Access Control for the Internet of Things. *IEEE Internet of Things Journal*.

[5] Wu, L., Du, X., Wang, W., & Lin, B. (2018). An Out-of-band Authentication Scheme for Internet of Things Using Blockchain Technology. *2018 International Conference on Computing, Networking, and Communications, ICNC 2018.*

[6] Bdiwi, R., De Runz, C., Faiz, S., & Cherif, A. (2017). Towards a New Ubiquitous Learning Environment Based on Blockchain Technology. *Proceedings - IEEE 17th International Conference on Advanced Learning Technologies, ICALT 2017.*

[7] Huang, Z., Su, X., Zhang, Y., Shi, C., Zhang, H., & Xie, L. (n.d.). *A Decentralized Solution for IoT Data Trusted Exchange Based-on Blockchain.*

[8] Gupta, Y., Shorey, R., Kulkarni, D., & Tew, J. (2018). The applicability of blockchain in the Internet of Things. *2018 10th International Conference on Communication Systems and Networks, COMSNETS 2018.*

[9] Stanciu, A. (2017). Blockchain-Based Distributed Control System for Edge Computing. *Proceedings - 2017 21st International Conference on Control Systems and Computer, CSCS 2017.*

[10] Choi, S., Burm, J., Sung, W., Jang, J., & Reo, Y. (2018). A Blockchain-based Secure IoT Control Scheme. *Proceedings on 2018 International Conference on Advances in Computing and Communication Engineering, ICACCE 2018.*

[11] Chen, P.-W., Jiang, B.-S., & Wang, C.-H. (n.d.). *Blockchain-based Payment Collection Supervision System using Pervasive Bitcoin Digital Wallet.*

[12] Di Pietro, R., Salleras, X., Signorini, M., & Waisbard, E. (2018). A blockchain-based Trust System for the Internet of Things. *Proceedings of the 23nd ACM on Symposium on Access Control Models and Technologies - SACMAT '18.*

[13] Alphand, O., Amoretti, M., Claeys, T., Dall'Asta, S., Duda, A., Ferrari, G., . . . Zanichelli, F. (2018). IoTChain: A blockchain security architecture for the Internet of Things. *IEEE Wireless Communications and Networking Conference, WCNC.*

[14] Buccafurri, F., Lax, G., Nicolazzo, S., & Nocera, A. (2017). Overcoming Limits of Blockchain for IoT Applications. *Proceedings of the 12th International Conference on Availability, Reliability and Security - ARES '17.*

[15] Shandilya, A., Gupta, H., Khatri, S., & Pradesh, U. (n.d.). *Role and Applications of IoT in Online Transactions using Blockchain Technology.*

[16] Özyılmaz, K., & Yurdakul, A. (2017). Integrating low-power IoT devices to a blockchain-based infrastructure. *Proceedings of the Thirteenth ACM International Conference on Embedded Software 2017 Companion - EMSOFT '17.*

[17] Durand, A., Gremaud, P., & Pasquier, J. (2017). Decentralized web of trust and authentication for the internet of things. Proceedings of the Seventh International Conference on the Internet of Things - IoT '17.

[18] Javaid, U., Siang, A., Aman, M., & Sikdar, B. (2018). Mitigating loT Device based DDoS Attacks using Blockchain. *Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems - CryBlock'18.*

[19] Medwed, M. (2016). IoT Security Challenges and Ways Forward. *Proceedings of the 6th International Workshop on Trustworthy Embedded Devices - TrustED '16.*

[20] Song, J., Demir, M., Prevost, J., & Rad, P. (2018). Blockchain design for trusted decentralized IoT networks. *2018 13th System of Systems Engineering Conference, SoSE 2018.*

[21] Lazaroiu, C., & Roscia, M. (2017). Smart district through IoT and blockchain. *2017 6th International Conference on Renewable Energy Research and Applications, ICRERA 2017.*

[22] Lin, S., Zhang, R., Ma, H., & Wang, M. (2015). Revisiting Attribute-Based Encryption with Verifiable Outsourced Decryption. IEEE Transactions on Information Forensics and Security.