Blockchain Technology for Secure IoT Communication

Manjunath S, Meghana A, Dharmapuri Mahidhar

¹Assistant Professor, Dept. of CSE, SJCIT, Karnataka, India
²Student, Dept. of CSE, SJCIT, Karnataka, India
³Student, Dept. of CSE, SJCIT, Karnataka, India

---***---

Abstract - *In recent days, the evolution of the Internet of Things is increasing quickly. This condition put up security problems because of many violations of security strategies. Besides, the evolution of blockchain is also increasing rapidly reason being it was first accessible in Bitcoin. Security dispute on this IoT can be solved by make use of blockchain, Specific approach that can be fullfilled is to make secure communication in between IoT devices. In this study, an IoT system would be created without blockchain and using blockchain, which will then equated between the two. MQTT is the communication protocol used in IoT systems without blockchain. In the meantime, the blockchain platform used is Ethereum together with a smart contract. These two IoT systems will be examined for their security level by counterfeit attacks and perceive their security aspects. The results of the analysis show that IoT system based upon blockchain technology has a leading level of security than the IoT system without blockchain technology.*

Key Words: **Blockchain, Ethereum, MTTQ, Smart contract, Etherium Virtual Machine (EVM)**

1. INTRODUCTION

By using Internet of Things (IOT), various devices are connected to a network. It is used in various intelligent applications including the embedded systems, software, sensors and artificial intelligence. Researchers said that the IOT devices that are connected will increases by 140%   from 21 billion 2018 to 50 billion 2023. IOT has a large demand in the field of IT. Blockchain growing rapidly and is increasingly being used since it was first introduced by Bitcoin. Blockchain has been used in various fields such as healthcare, transportations etc.

IOT devices are vulnerable to cyber-attacks. Security policies are also violated to make IOT devices inexpensive. Blockchain technology can be used to strengthen our IOT security. There are four ways for doing this, first providing secure communication, user authentication, legitimating IOT and configuration. This research main aim is to make strong IOT connection by using blockchain technology. By taking two devices we can conduct simulation with or without using Blockchain. Here we are using smart contract. Then the simulation attacks of two IOT devices are carried out then we check the results. Along with that, hash functions and cryptographic algorithms are also used.

2. LITERATURE SURVEY

2.1 Internet of Things (IoT)

Internet of Things (IoT) is an object used to connect various devices in a network to get data through the internet, which is used in diverse intelligent applications with the help of embedded systems, sensors, software, and artificial intelligence and other technologies. Each connected device will have its own unique identity [1].
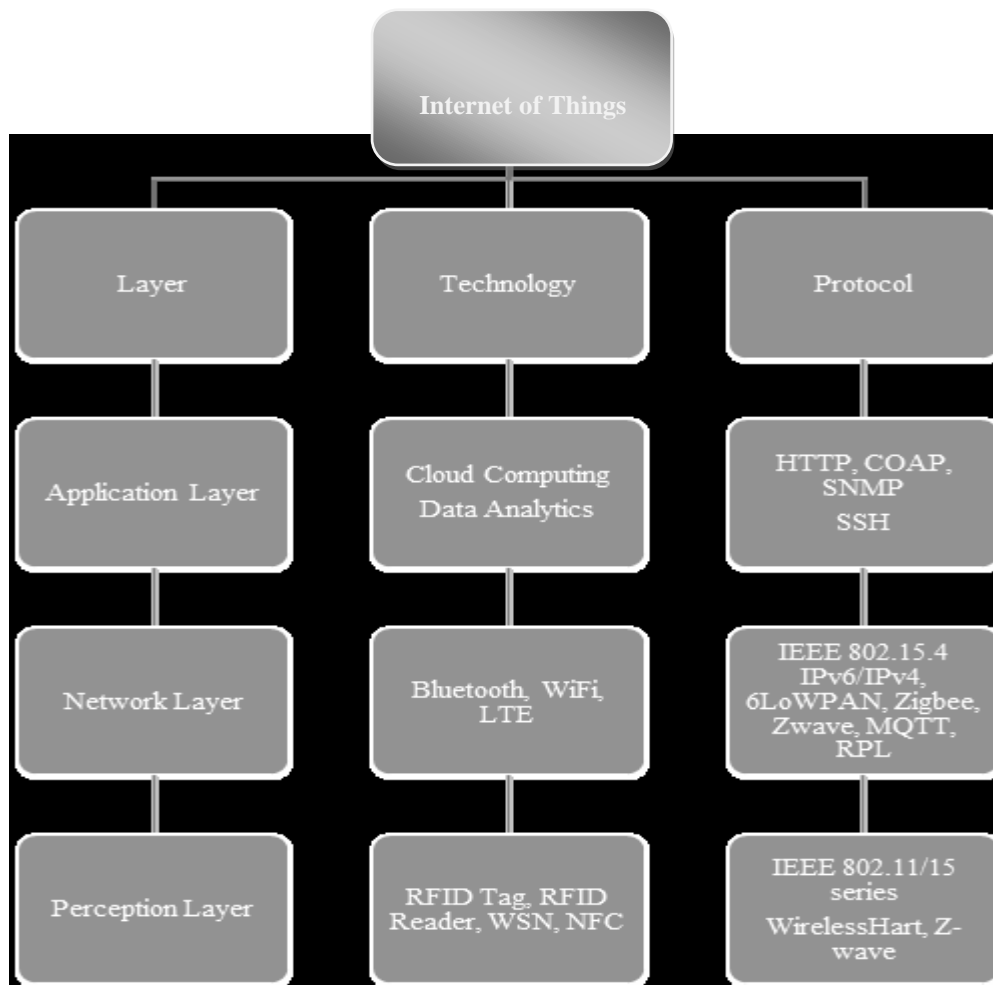
Fig -1: Architecture[1]

Above figure is architecture of IoT in which each layer has an important role. The figure also displays the technologies and protocols used on IoT. Improving the quality of human life is the main aim of IoT by connecting objects with humans to make it easier to get the data needed through the internet. In this instance, IoT provides a new way of communication between objects and humans, or betwixt objects themselves [2].

Anyhow, despite IoT having many benefits for humans, there are security threats that arise from IoT. These IoT devices are the prey of attacks by hackers to fetch sensitive data. This security problem takes place in all three IoT layers, specifically application layer, network layer, and perception layer. The exposure of this security problem is to a certain extent due to the security policies that are barratries to make IoT devices that are cheap, easy, and small in size [3].

2.2 Blockchain

At first, bitcoin was created with blockchain technology to keep away from double spending, But now blockchain is acclimate for other purposes. One of the examples is IoT in this work. The term "blockchain" is generally used to mention to data structures occasionally to networks or systems. Blockchain is a list of ordered blocks, where every block contains transactions. Each block in the blockchain is linked to the preceding block, containing a hash from the previous block. As a result, the transaction history on the blockchain cannot be changed or erased without completely changing the contents of the blockchain. This is what leads blockchain to be safe from hackers[4].

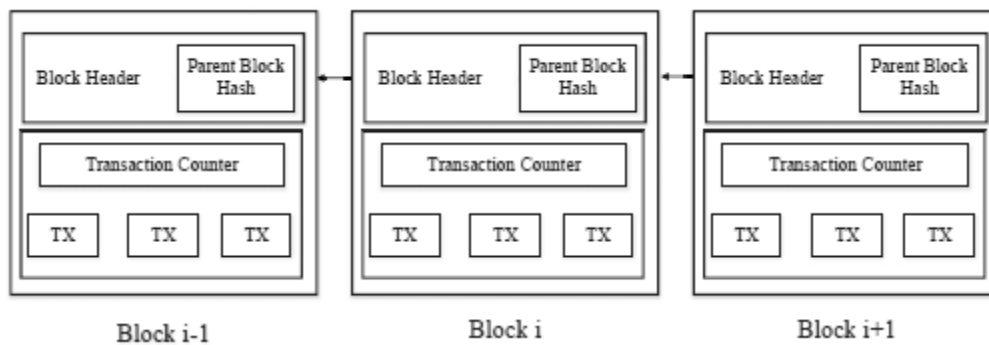The shape of the blockchain and the block structure are as follows.
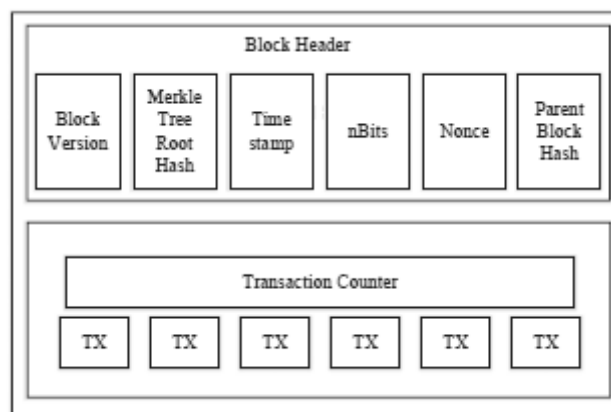
Fig -2: Blockchain [4]

Fig -3: Block Structure [4]

Several main characteristics of Blockchain are as follows [4].

• *Persistency*. In blockchain, transactions can be quickly validated and invalid transactions will not be recognized by miners. Hence, it is not possible to erase transactions that have already take place.

• *Auditability*. Every transaction on the blockchain refers to the previous transaction. This leads to each transaction to be easily verified and tracked.

• *Decentralization*. In blockchain, third forces are not required to verify transactions. The algorithm used to maintain data consistency on blockchain networks is Consensus algorithm.

• *Anonymity*. Every user on the blockchain network can interact with each other by using a generated address. Hence, the real identity of the user is not displayed in the interaction[4].

2.3 Ethereum

Ethereum is a blockchain platform created by Vitalik Buterin and discusses some restrictions of Bitcoin. The main benefit of Ethereum is that it supports full Turingcompleteness, which means Ethereum keep up all types of computing. Ethereum is a transaction-based state machine [5].

The following are the Ethereum important elements [5].

• *Currency*. To do the computation in the network in the form of data transmission, "Ether" or ETH is used as intrinsic currency on Ethereum.

• *Transaction*. Transaction in Ethereum refers to a signed data package, which stores messages that will be sent from EOA. Message call and account creation are the 2 types of transactions in Ethereum. This transaction contains the recipient of the

message, the sender's signature, the number of Ether and the data to be sent, and the number of Starts (Gas limit) and Gas price.

• **Technology used**. Ethereum uses several technologies including web technology, client/node implementation, and data storage.

• **Account**. Each account on Ethereum has a 20-bytes address and consists of four parts, Specifically noncecounter, ether balance, storage, and contract code. Externally Owned Account (EOA) and Contract Account are the 2 types of accounts in Ethereum. EOA is controlled by the private key and Contract Account is controlled by contract code. Besides, Contract Account can only be activated by EOA.

• **Consensus algorithm**. Ethereum has 3 types of consensus algorithms, specifically Proof Proof of Authority (PoA), Stake (PoS), and Proof of Work (PoW)[5].

2.4 Smart Contract

Smart contract is one important element in Ethereum. A smart contract is an application that is applied to the blockchain network and executed automatically as part of transaction validation. Special creation on the transaction must be executed to implement a smart contract on Ethereum, which is a contract on the blockchain. Smart contracts on Ethereum are basically written in a highlevel language and compiled via the Ethereum Virtual Machine (EVM). Solidity is the most widely used programming language [6].

3. CONCLUSION

Latterly, the evolution of the Internet of Things has expedited but has been followed by security problems. Insecurity of communication is the one of the security problems that occurs between IoT devices. In this study, the design and implementation of the IoT system have been carried out without blockchain and using blockchain technology to compare the results. MQTT is used as communication protocol for The IoT system without blockchain technology. For the time being, Ethereum is used as the platform of the blockchain network for the IoT system with blockchain. Besides, smart contracts are also used to store and retrieve desired data from the blockchain network. Based on various examinations that have been carried out, it can be validated that the IoT system using blockchain technology can fix security problems that appear in communication between IoT devices, because it has a greater level of security than the IoT system without blockchain technology so that data integrity can be assured. This can be seen from the testing of attack simulations and observations of deluge effects carried out where the IoT system using blockchain technology has better security.

REFERENCES

[1] Naved Alam, Prashant Vats, and Neha Kashyap, "Internet of Things: A Literature Review," in *2017 Recent Developments in Control, Automation & Power Engineering (RDCAPE)*, October 2017.

[2] Ashvini Kamble and Sonali Bhutad, "Survey on Internet of Things (IoT) Security Issues & Solutions," in *2018 2nd International Conference on Inventive Systems and Control (ICISC)*, January 2018.

[3] Madhusudan Singh, Abhiraj Singh, and Shiho Kim, "Blockchain: A Game Changer for Securing IoT Data," in *2018 IEEE 4th World Forum on Internet of Things (WF-IoT)*, February 2018.

[4] Zibin Zheng et al., "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," in *2017 IEEE 6th International Congress on Big Data (BigData Congress*), June 2017.

[5] Chinmay Saraf and Siddharth Sabadra, "Blockchain Platforms: A Compendium," in *2018 IEEE International Conference on Innovative Research and Development (ICIRD)*, May 2018.

[6] Maximilian Wöhrer and Uwe Zdun, "Smart Contracts: Security Patterns in the Ethereum Ecosystem and Solidity," in *2018 International Workshop on Blockchain Oriented Software Engineering (IWBOSE)*, March 2018.