

Blockchain for Large-Scale Internet of Things Data Storage and Protection

Ms. Neha Jain (GUIDE), Asst Prof, SLRTCE, Rahul Singh, Bhavesh Chari, Pankaj Chohan,
Jay Valangar

^{1,2,3,4}Computer Engineering Dept Shree LR Tiwari College of Engineering

Abstract - With the increasing growth of IOT (internet of things) devices, storing and securing a large amount of IOT data have become major issues, Blockchain offers a convenient platform for distributed data storage and protection. Due to increasing high computation and storage demands from cloud server problem such as cloud-based IOT structures has been arisen, for solving such issues distributed data storage has been introduced which helps to employ blockchain. We present a description of the transaction in a non-cryptocurrency system and specify how the transactions are processed. Our scheme eliminates the centralized server by replacing with a decentralized server which performs "Transaction" verification. Using certificate-less and blockchain we ensure more security to the IOT data.

notifying the data owner. A decentralized structure will properly handle these issues. Data can be transferred and controlled in a distributed manner as opposed to that in a centralized structure.

1.3.2 No Centralized Trusted Server :

As in previous systems, centralized systems had interventions from trusted servers. Now, after the introduction of Centralized Trusted Server, the access to IoT data is controlled by the majority of the blockchain miners, without any intervention from a trusted server.

1.3.3 Traceability and Accountability :

Tracing the changes made in the previous systems were not possible. But, after the introduction of blockchain in IoT, every change made in the system will be traced. Users do not need to worry about unauthorized access to his/her data. No malicious attempts can be made undetected.

1.3.4 Edge computing :

IoT devices have low computational power.

The computations done by the IoT devices in previous systems were very slow. With the help of edge computing, computations are done faster. Edge computing brings real-time computations and communications by leveraging nearby edge servers. [4]

1.4 Project Objectives

The basic objective of Blockchain is to offer a convenient platform for Distributed data storage and protection.

a) To achieve Distributed data storage and protection through storing data DHT (Distributed hash tables).

b) To achieve complex computations using. Edge computing.

2. LITERATURE REVIEW

Here we will elaborate the aspects like the literature survey of the project and what all projects are existing and been actually used in the market which the makers of this project took the inspiration from and thus decided to go ahead with the project covering with the problem statement.

1. INTRODUCTION

Here we will elaborate on the aspects like problem statement, scope, motivation and also the objectives of our project

1.2 Problem statement

With the increase in the copious amount of IOT devices, a tremendous amount of interactions are occurring between the physical objects which improves efficiency. It reduces human interventions. IOT devices send all the data to centralized servers. The problem with centralized systems is that they collect and manipulate all the data. Sensitive or important data can be easily leaked, hence making the system vulnerable.

1.3 Scope and Motivation

1.3.1 De-Centralized System:

IOT applications such as smart grid and implantable medical system, involve tremendous data aggregations. In a traditional cloud-based IOT structure, a centralized cloud server collects and controls all the data, which brings two drawbacks:

1) The cloud server needs a very high storage capacity to store the IOT data;

2) Sensitive data can be easily leaked from the server. So, to prevent these drawbacks, we convert the centralized system into a decentralized system. For example, a server might trade sensitive data with other entities without

2.1 Secure Data Sharing in Public Clouds

AUTHOR: Seung-Hyun Seo, Mohamed Nabeel.

An Efficient Certificate-less Encryption for Secure Data Sharing in Public Clouds mCL-PKE scheme is used to construct a practical solution to the problem of sharing sensitive information in public clouds. The clouds are employed as secure storage as well as a key generation center. The data owner encrypts the sensitive data using the cloud generated user's public keys based on its access control policies and uploads the encrypted data to the cloud. After successful authorization, the cloud partially decrypts the encrypted data for the users.

2.2 Data Storage in Cloud Computing Platform

AUTHOR: Lihong Jiang, Boyi Xu.

This network brings a series of challenges for data storage and processing in a cloud platform. IOT data can be generated quite rapidly, the volume of data can be huge and the types of data can be various. In order to address these potential problems, this paper proposes a data storage framework not only enabling efficient storing of massive IOT data but also integrating both.

2.3 Smart Contracts for the Internet of Things

AUTHOR: Konstantinos chirstidis, Michael Devetsikiotis.

Motivated by the recent explosion of interest around blockchains, we examine whether they make a good fit for the Internet of Things(IoT)sector. We review how this mechanism works and also look into smart contracts—scripts that reside on the blockchain that allow for the automation of multi-step processes. We then move into the IoT domain, and describe how a blockchain-IoT combination: 1) facilitates the sharing of services and resources leading to the creation of marketplace of services between devices and 2) allows us to automate in a cryptographically verifiable manner several existing, time-consuming work flows.

2.4 Blockchain For Internet of Things

AUTHOR: Ruinian Li, Tianyi Song, Hong Li.

Traditional cloud-based IoT structures impose extremely high computation and storage demands on the cloud servers. Meanwhile, the strong dependencies on the centralized servers bring significant trust issues. To mitigate these problems, we propose a distributed data storage scheme employing blockchain. Our scheme eliminates the traditional centralized servers by leveraging the blockchain miners who perform "transaction" verifications and records audit with the help of certificate-less cryptography. We present a clear definition of the transactions in a non-cryptocurrency system and illustrate how the transactions are processed. Additionally, we

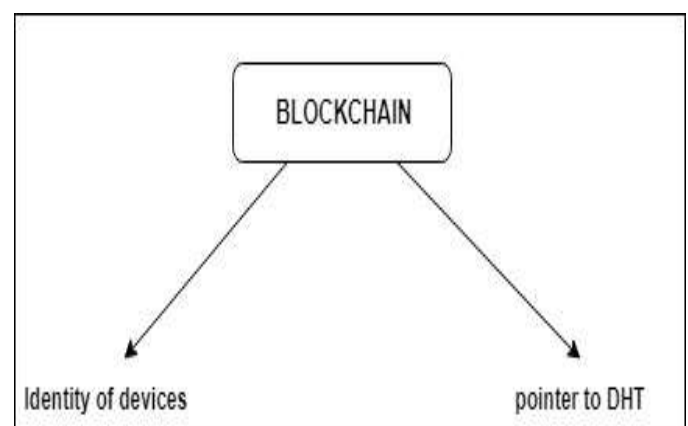
extend our scheme to enable data trading and elaborate on how data trading can be efficiently and effectively achieved.

3. PROPOSED SYSTEM

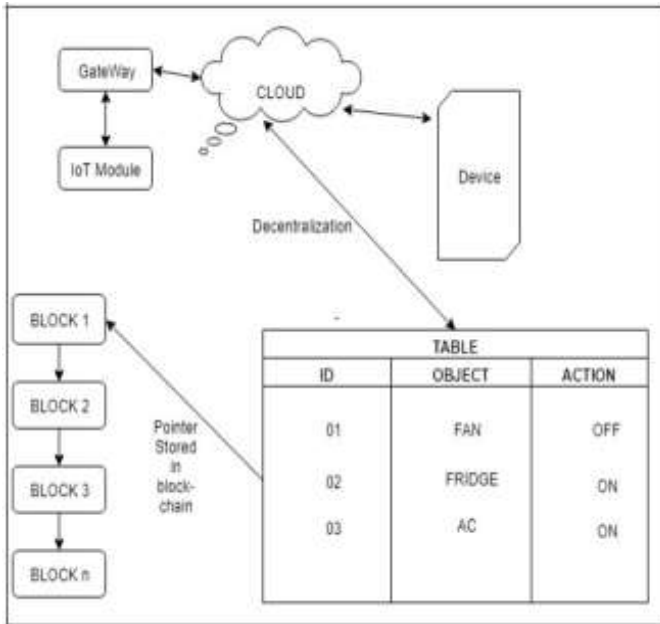
Due to, day by day increase in usage of IoT devices the traffic of data transaction is increasing that results in an overloaded centralized system. The IoT implementation at present does not excel in security. The previous implementation of old IoT includes certificate-based security. It utilizes PKI(Public key infrastructure) which introduces too much redundancy. This paper proposes the implementation of blockchain in combination with IoT for developing a secure, robust and reliable decentralized system. This paper Consists of hashing techniques, edge computing for security and decentralization of the system.

A)Storing data: Before an edge device forwards data to DHT, it posts a "transaction" to the blockchain, announcing that the data belonging to certain IOT device will be stored in an address of DHT. Blockchain verifies the transaction and records the identity of the IOT device and the storage address. In this way, blockchain helps manage data storage.[5]

B)When an IOT device requests data from DHT, it posts a "transactions" to the blockchain. The blockchain will work as a "trusted third party" to authenticate the requester. If the transaction is validated and written into a block, the DHT node storing the data will send data to the requester. Therefore, authentication is performed through the blockchain, without a trusted server.



4. APPLICATION ARCHITECTURE



4.1 IOT devices

The IoT module makes all the IoT devices in the network to be connected to each other. The registration and authentication of devices is a part of the process handled by the IOT module. The module is capable of making transactions among IOT devices and the database.

4.2 DHT

The location at which the data must be stored is recorded in DHT(Data Hash-table) which is part of the blocks of transactions and remain secured in the network and is only to be accessed by the rightful authority and not other in and out of the network.

4.3 Blockchain

The data coming from the IoT device is stored in a block sequence and every block contains device id, device data, previous hash, current hash and time-stamp.

4.4 Edge Computing Device

As the IoT module is not capable of processing such high computations at an astonishing rate with an increasing number of IoT devices in the network. Edge devices do the job calculating the hash values and for all the blocks in the blockchain.

5. RESULTS AND DISCUSSION.

The deployment of the proposed machine is based heavily at the layout of blockchain system. Without incredibly scalable blockchain system, it is hard to set up the IoT garage system. This is the alternate-off brought through

disposing of the centralized server. Scalability is a chief trouble in blockchain's layout. There are a lot of ongoing studies operating on it. To find the maximum scalable tool that exists currently, we need to examine the blockchain systems that have already been deployed in very huge networks. Some very new blockchain generation together with Ripple should machine hundreds of transactions in step with per second, however the layout is partly decentral-ized. Decentralized designs together with Ethereum have to take handiest 13 transactions in keeping with per second. However, there exists new-rising blockchain layout built primarily based on Ethereum that have a whole lot better scalability. For example, Tomochain is supposed to method as much as a thousand transactions in step with per second.

6. CONCLUSION

In this paper, we propose A relaxed scheme for IoT facts storage and safety based totally on blockchain. Edge computing is included to help control facts storage and small IoT devices carry out computations. Edge computing device is adopted to set up a convenient authentication gadget for the blockchain-primarily based IoT applications, and blockchain overcomes the drawback of certificateless cryptography. We give exact algorithms on the way to procedure transactions in any such system and a way to gain authentication and accountability. To the exceptional of our understanding, that is the first paper tackling the hassle of constructing a relaxed large-scale IoT facts, and the first to combine facet computing and blockchain as a whole to serve lot .

REFERENCES

- [1] 1. M. F. Kaashoek and D. R. Karger, "Koorde: A simple degree-optimal distributed hash table," in International Workshop on Peer-to-Peer Sys-tems. Springer, 2003, pp. 98–107.
- [2] S. S. Al-Riyami and K. G. Paterson, "Certificateless public key cryp-tography," in Asiacrypt, vol. 2894. Springer, 2003, pp. 452–473.
- [3] S. S. Chow, C. Boyd, and J. M. G. Nieto, "Security-mediated certi-icate-less cryptography," in Public key cryptography, vol. 3958. Springer,2006, pp. 508–524.
- [4] M. Satyanarayanan, "The emergence of edge computing," Computer,vol. 50, no. 1, pp. 30–39, 2017.
- [5] Blockchain For Large-Scale Internet of Things Data Storage and Protection AUTHOR: Ruinian Li, Tianyi Song, Hong Li.
- [6] L. Jiang, L. Da Xu, H. Cai, Z. Jiang, F. Bu, and B. Xu, "An iot-oriented data storage framework in cloud computing platform," IEEE Transactions on

Industrial Informatics, vol. 10, no.2, pp.1443-1451,2014.

- [7] L. Jiang, L. Da Xu, H. Cai, Z. Jiang, F. Bu, and B. Xu, "An iot-oriented data storage framework in cloud computing platform," IEEE Transactions on Industrial Informatics, vol. 10, no.2, pp.1443-1451,2014.