SECURING COMMUNICATION AMONG IOT DEVICES USING BLOCKCHAIN PROXY

Vishal Bhalerao[1*], Akanksha Mandlik[2], Swapnil Nehere[3], Namrata Shingapure[4], Sulbha Ghadling[5]

[1]Computer Engineering, NMIET, SPPU, Pune, India
[2] Computer Engineering, NMIET, SPPU, Pune, India
[3] Computer Engineering, NMIET, SPPU, Pune, India
[4] Computer Engineering, NMIET, SPPU, Pune, India
[5]Computer Engineering, NMIET, SPPU, Pune, India

---***---

Abstract - *Data is central to the Internet of Things ecosystem. Most of the current IoT systems are using centralized cloud-based data sharing systems. Involvement of such third party service provider requires trust from both sensor owner and sensor data user and to tackle both the scalability and trust issues or to automatize the payments. This system presents a blockchain based proxy scheme. The proxy only requires a slim proxy SDK on the device that holds a regular blockchain identity with its own private key, retaining full control of the transactions in the device. The security implications and present supply chain monitoring is used as a use case. Preliminary results show significant savings in CPU time and communication bandwidth for the IoT device. The proposed system is implemented in an custom based blockchain to analyze the performance and security properties.*

Key Words: Proxy Re-Encryption, Blockchain, Smart Contracts, IoT Data Sharing, Security

1. INTRODUCTION

Many IoT systems has affected with network attacks as well as some vulnerable en-vironment attacks, hence it's not able to defend such attacks. Sometimes lightweight attacks can't be identified by middleware trustworthy systems but in research system proxy verification is provided which can easily eliminate such attacks. This system reduces the time complexity of existing systems and achieves data decentralization for proposed system.

IoT sensors having strengths like computational power, memory size and bandwidth. This system propose to minimize the foot print of connecting an IoT device to a permission blockchain by the communication with the blockchain to a proxy server. As the blockchain identity rests with the sensor, even the proxy server cannot modify the readings without detection as it cannot copy the sensor device's signature.

2. RELATED WORK

2.1 Objectives

This system is proposed to study and to analyse of lightweight attack on IoT devices in collaboration with cloud servers and to develop an own blockchain with n peer nodes for parallel execution, which contains own smart contract as well as mining respectively. This project is to deploy the proxy server to commit incoming transaction in blockchain environment and validate its execution. It also validate the system performance and trustworthiness with multiple experiment analysis.

2.2 Problem Statement

This research work system is introducing the concept of a blockchain proxy to an IoT devices for secured communication. The proxy only requires a slim proxy SDK on the device that holds a regular blockchain identity with its own private key, retaining full control of the transactions in the device.

3. LITERATURE SURVEY

1. A Blockchain Proxy for Lightweight IoT Devices.

This research demonstrates the blockchain proxy as a service for lightweight IoT devices to offload communication with a blockchain while retaining full control of all transactions committed to the shared ledger. System have argued that the approach is robust against tampering with the device data in transit and delivers trustworthy readings to the blockchain. Preliminary results of a proxy for Hyperledger Fabric demonstrate the potential for the IoT device to save significant CPU time and communication bandwidth using the proxy.

Advantages:

All participants have the ability to see all transactions and blocks as each participant has its own ledger.

Disadvantages:

The distributed ledger will increase in size as time passes and with increasing number of nodes in the network.

Limitation:

Multiple resource dependency which is hard to manage in decentralized architecture.

2. Blockchain in IoT Security

There are two types of blockchains, a public blockchain and a private one. A Public blockchain is permission less blockchain. Anyone can join it successfully and productively. They can engage by viewing or inputting within the blockchain. On the other hand, a private blockchain is a permission blockchain. Only someone permission can join it and each member has restricted participations depending on the authorizations given by the network.

Advantages:

1. Eliminating centralized traffic flows and single point of failure of the current centralized IoT architecture.
2. Each node has its own copy of the ledger that contains all transactions that have ever made in the network.

Disadvantages:

The blockchain scales poorly as the number of nodes in the network increases.

Limitation:

The system needs to take permission to access private blockchain.

3. Blockchain with Internet of Things: Benefits, Challenges, and Future Directions

This research demonstrates provided an overview of integrating blockchain with IoT with highlighting benefits and challenges. It defines that integrating blockchain with IoT can bring many advantages that improve many of IoT issues but at the same time it introduces new challenges that should be addressed.

Advantages:

Eliminating centralized traffic flows and single point of failure of the current centralized IoT architecture.

Disadvantages:

The blockchain scales poorly as the number of nodes in the network increases.

Limitation:

IoT systems have different types of devices which have very different computing capabilities and not all of them will be able to run the same encryption algorithms at the required speed.

4. RESULTS AND DISCUSSION

Architecture:

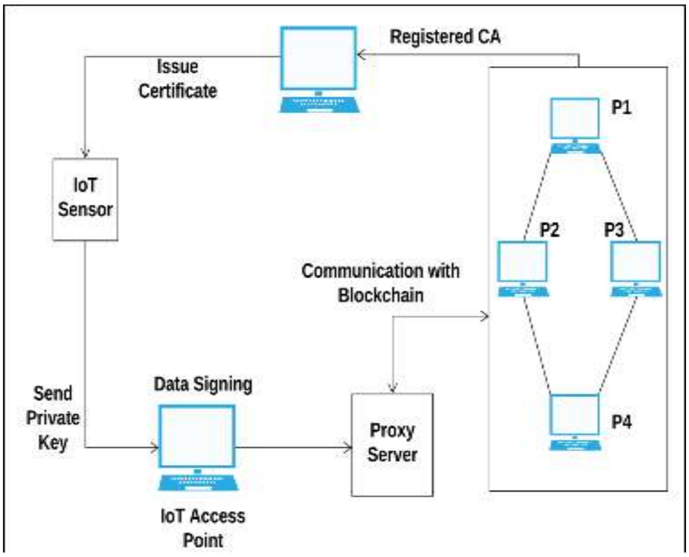

Fig.1

Certificate Authority : This module generates the private key which is send to IOT sensors. This private key is used for unique identification and validation of the user.

IOT Module: This module consists of various types of IOT sensors which are used for data sensing and transmitting data over the server through network.

Proxy Server: The sensor sends the transactions along with its private key to the blockchain proxy which executes the required protocols with the blockchain nodes to save the transactions to the ledger.

Blockchain : Blockchain on a server with identity that receives data from the sensor and signing that data to blockchain. The main purpose of blockchain is to provide security for IOT sensor's data for transmitting data securely over the network.

ER Diagram:

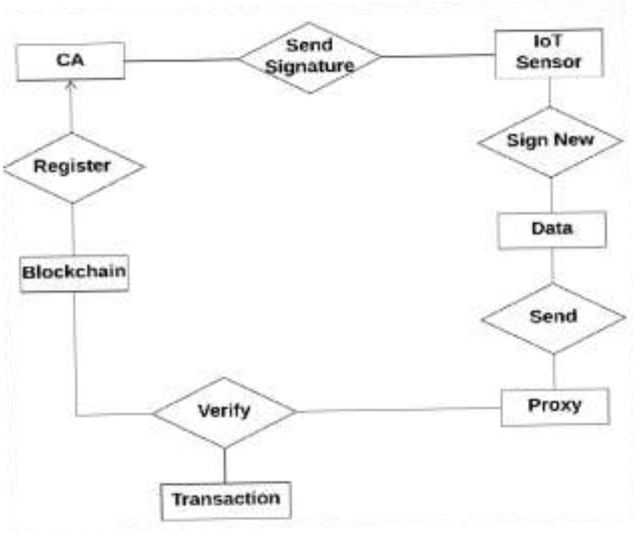

Fig.2

5. CONCLUSION AND FUTURE SCOPE

This system introduced a blockchain proxy as a service for lightweight IoT devices to communication with a blockchain while retaining full control of all transactions committed to the shared ledger. This system argued that the approach is robust against tampering with the device data in transmit and delivers trustworthy readings to the blockchain. Preliminary results of a proxy for Hyperledger Fabric demonstrate the potential for the IoT device to save significant CPU time and communication bandwidth using the proxy. Here system deploy manual blockchain to proposed IoT and cloud infrastructure will provide transaction execution in minimum time complexity.

As future work, the system will support subscribing to Fabric events via the Proxy to harden the system against DoS attacks. Events also provide a channel back from the blockchain to the device that can be used to control the device and trigger actions. Having transactions write sequence numbers to a shared ledger variable would protect the system against DoS attacks, malicious reordering and selective dropping of transactions.

REFERENCES

[1] Das, Manik Lal, ”Privacy and Security Challenges in Internet of Things,” Distributed Computing and Internet Technology. , pp. 33-48, 2015.

[2] Ho, G., Leung, D., Mishra, P., Hosseini, A., Song, D. and Wagner, D., , ”Smart locks: Lessons for securing commodity internet of things devices.,” in Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security.

[3] Fahad Alkurdi1, Ibrahim Elgendi1, Kumudu S. Munasinghe1, Dharmendra Sharma1 and Abbas Jamalipour2, “Blockchain in IoT Security: A Survey,” *In the Proceedings of the 2018* International Telecommunication Networks and Applications Conference. *(ITNAC 2018)*, Australia **2018.**

[4] M. Amoozadeh et al.,, ”Security vulnerabilities of connected vehicle streams and their impact on cooperative driving,” IEEE Communications Magazine, vol. 53, no. 6, pp. 126-132, 2015.

[5] Skarmeta, Antonio F., Jose L. Hernandez-Ramos, and M. Moreno., ”A decentralized approach for security and privacy challenges in the internet of things,” in internet of Things (WF-IoT), 2014 IEEE World Forum on, 2014.

[6] H. Gross; M. Holbl, D. Slamanig, and R. Spreitzer, ”Privacy-Aware Authentication in the Internet of Things,” Cryptology and Network Security. Springer International Publishing, pp. 32-39, 2015.

[7] A. Ukil, S. Bandyopadhyay and A. Pal, ”IoT-Privacy: To be private or not to be private,” in Computer Communications Workshops (INFOCOM WKSHPS), 2014 IEEE Conference on., Toronto, 2014.

[8] S. Nakamoto, ”Bitcoin: A peer-to-peer electronic cash system,” 2008. Decker, Christian, Jochen Seidel, and Roger Wattenhofer., ”Bitcoin Meets Strong Consistency.”

[9] Wu, Axin, et al. ”Hidden policy attribute-based data sharing with direct revocation and keyword search in cloud computing.” Sensors 18.7 (2018): 2158.

[10] Khan S, Khan R. Multiple authorities attribute-based verification mechanism for Blockchain mircogrid transactions. Energies. 2018 May;11(5):1154.

[11] Guo, Rui, et al. ”Secure attribute-based signature scheme with multiple authorities for Blockchain in electronic health records systems.” IEEE Access 776.99 (2018).