International Journal of Scientific Research and Engineering Development-– Volume X Issue X, Year

Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

Block Chain Based Securing IOT Enabled Devices

Harsha Manohar Girdhani,Kirti Madansingh Pardeshi,Priyanka Manohar Thakare, Swati Shekhar Korde

Department of Computer Engineering ,Late G.N. Sapkal College of Engineering, University of Pune,Nashik,India

----------**********----------

Abstract:

The buss words block chain and internet of things have been floating around the tech world for quite a while. IoT has already proved that it can have a significant impact on our daily life. A significant amount of data is collected and transmitted through the internet from various devices across the globe. IoT consists of heterogeneous devices communicating over a wide range of networks transmitting lots of critical and non-critical data, which raises concern about the security of such collected data from the users and the ownership of the data. This paper introduces a security framework for the internet of things implementation in a confined environment, such as smart city, power grid, or metro rail systems, etc. The framework ensures the secure communication and authentication of the data across such diversified networks and devices. The framework is built upon the underlying mechanism of block chain technology combined with the use of a secure hashing algorithm.

Keywords **—Block chain, IoT, Cyber Security.**

----------**********----------

I. INTRODUCTION

There are two types of block chains, a public block chain and a private one. A public block chain is a permission lessblock chain. Anyone can join it successfully and productively. They can engage by viewing or inputting within the block chain. This public chain does not have a single unit controlling it over the network because they are decentralized. This means once the data on the block chain is validated it can't be changed. This public block chain is beneficial because within it the user can openly input and view data, the ledger is not centralized, and it is distributed, it is immutable to avoid any tampering with data attempts, and it is secure because of the 51% rule ''no one can obtain dominant power on this network'' On the other hand, a private block chain: is a permission block chain. Only someone's permission can join it and each member has restricted participation depending on the authorizations given by the network.

II. RELATED WORK

PROBLEM STATEMENT:

The technological industry and information security have been evolving so fast and developing at an exponential rate. Every day lots of new devices are being surfaced with various capacities to aid humans in various fields. At the same rate, technology becomes obsolete at another end.

Considering the examples of cell phones today, which no longer gets a security update or patch after three years. There won't be a complete security solution for a device or system which can cover it for its lifetime. Security needs to be regularly updated. It should be considered as a continuous process rather than as a product. So Hacking can increase and control all the hardware. So it should be secured.

SYSTEM OVERVIEW:

We proposed a new paradigm using the Ethereum Smart Contracts to enable secure user authentication for fog-enabled IoT devices. Each participant is identified on the network with a unique Ethereum address and also associated with a private and public key. Our main focuses are the usage of smart contracts, event execution, and enable fog devices to allow only authenticated users to access IoT devices. In Ethereum, events are broadcasted to all participants and miners when an event in a smart contract is triggered. In case of any violation of pre-defined smart contract conditions, events rebound immediately and revert the condition to a previous optimal state. The main participants include admin, End users, Fog enabled IoT devices, Block chain with EVM (Ethereum Virtual Machine) that executes the smart contract.

III. SYSTEM DESIGN

Admin-Admin is the system's primary entity that creates and deploys a Smart contract, associates each device to a fog node and creates a permission list mapping that specifies which user is permitted to access which device. An Admin is identified by an Ethereum address. Admin also issues tickets to end-users in an off-chain mode.

End Users- End Users are identified on the network with an Ethereum address. These users request tokens through block chain to access IoT devices. Once the token is issued, they request access by contacting the designated fog node.

Smart Contract- We used a single smart contract in our scheme to authenticate users. Smart Contracts contain functions, modifiers, events, mappings. It also stores tokens on the block chain which are later utilized by fog nodes to provide authenticated access to IoT devices.

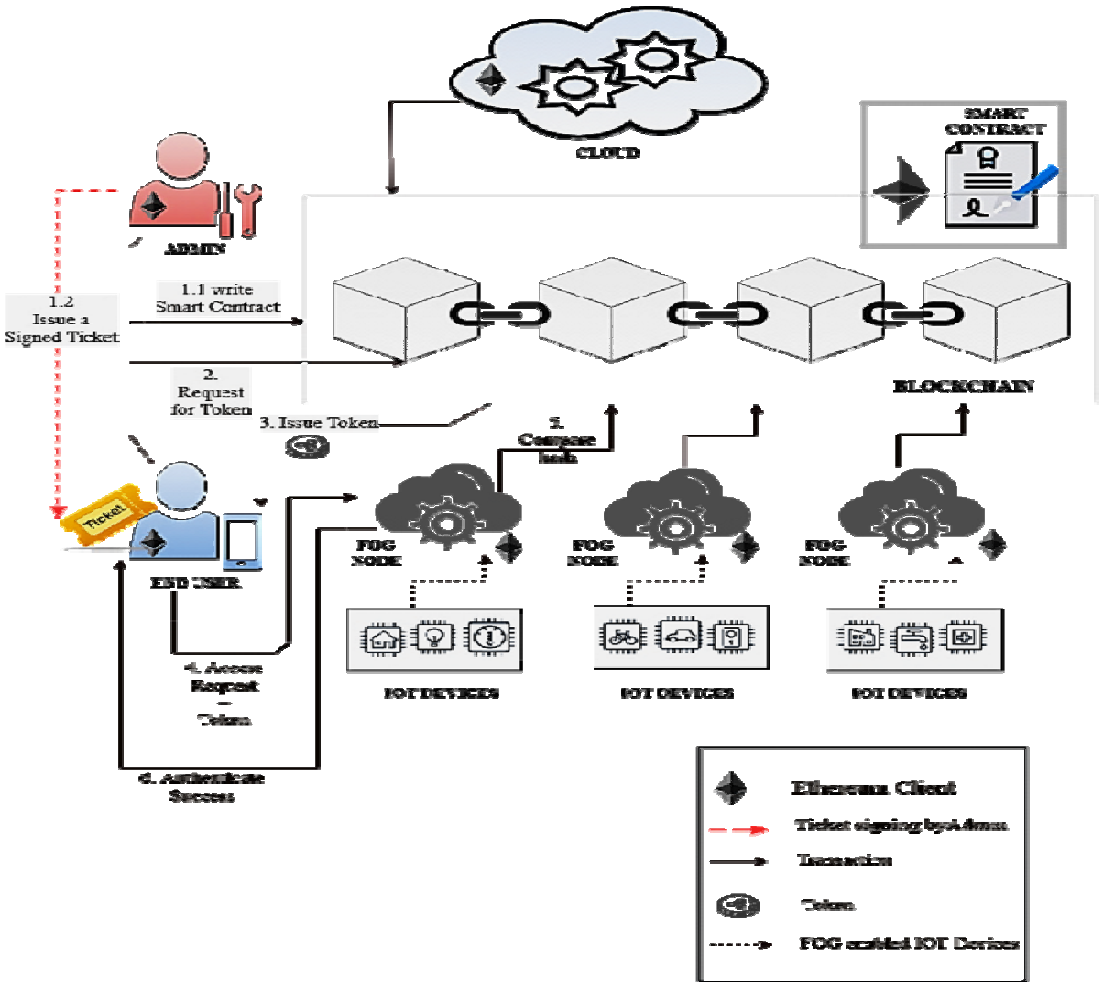
Fog Node- A Fog node carries out edge storage and processing for IoT devices with reduced latency and response time as compared to Cloud-IoT integration. Fog nodes perform processing, storage and carry out security mechanisms on behalf of IoT devices.

IoT Devices- IoT Devices are incapable of securing, computing, storing data all by themselves due to the property of resource-constrained devices. Thus, each IoT device is associated with one fog node in our scheme. Each IoT device is identified by an Ethereum address in our scheme.

IV. GOALS AND OBJECTIVES

The IoT offers enormous opportunities and also brings some challenges. Authentication considered one of the main challenges introduced by IoT. IoT devices are not able to protect themselves due to there limited processing and storage capabilities. Researchers proposed authentication algorithms with either a lack of scalability or vulnerable to cyberattacks. In this paper, we propose a decentralized token-based authentication based on fog computing and block chain. The protocol provides a secure authentication protocol using access token, ECC cryptography, and also block chain as decentralized identity storage. The block chain uses cryptographic identifiers, records immutability, and provenance, which allows the implementation of a decentralized authentication protocol.

V. BLOCKCHAIN ARCHITECTURE



VI. CONCLUSION

We proposed a Decentralized block chain-based scheme for secure authenticated access to Iot devices. The proposed system is completely secure, decentralized, and independent of trusted third parties, resilient. Our scheme fulfills CIA-triads defined by Confidentiality, Integrity, and Availability security requirements of IoT devices. We implemented our smart contract using solidity programming on Remix-IDE and tested its functionalities using Test RPC Ganache and Rinke by Test Network.

ACKNOWLEDGMENT

We are very thankful to our guide Prof.J.V.Shinde, project coordinator Prof.S.S. Shinde & H.O.D Prof. (Dr.)N. R. Wankhade, Computer Engineering, Late G.N Sapkal College of Engineering for guidance and advice which help to improve the present and for reading the paper and giving the valuable suggestions to improve the paper.

REFERENCES

1. M. Hung, “Leading the IoT,” p. 29, 2017. [Online]. Available: https://www.gartner.com/imagesrv/books/iot/iotEbook digital.pdf [Accessed: September 2017]
2. C. Yang, X. Chen, and Y. Xiang, "Blockchain-based publicly verifiable data deletion scheme for cloud storage," Journal of Network and Computer Applications, vol. 103, pp. 185–193, 2018.
3. G. Zyskind, O. Nathan, and A. S. Pentland, "Decentralizing Privacy: Using blockchain to protect personal data,” Proceedings - 2015 IEEE Security and Privacy Workshops, SPW, pp. 180–184, 2015
4. D. Puthal, R. Ranjan, and J. Chen, “Big data stream security classification for IoT applications," 2019
5. S. Nakamoto et al., “Bitcoin: A peer-to-peer electronic cash system,” http://bitcoin. Org/bitcoin. pdf, 2008
6. G. Wood, “Ethereum: a secure decentralized generalized transaction ledger,” Ethereum Project Yellow Paper, pp. 1–32, 2014
7. S. Amani, M. Be´gel, M. Bortin, and M. Staples, “Towards verifying smart contract bytecode in Isabelle,” in Proceedings of the 7th ACM SIGPLAN International Conference on Certified Programs and Proofs. ACM, 2018, pp. 66–77
8. M. A. Khan and K. Salah, “IoT security: Review, blockchain solutions, and open challenges,” Future Generation Computer Systems, vol. 82, pp. 395–411, 2018.

