

Security Of Internet Of Things Using Blockchain

Nilam K. Kadale,

COMPUTER ENGINEERING, NBN Sinhgad School of Engineering, PUNE, INDIA

Abstract

Internet of Things (IoT) is used now by various organizations, industries for completing their many works. Obviously it will influence everyone to use IoT for completing their various day to day life activities. Increasing use of it will result in increase in vulnerabilities. There is very urgent need to secure IoT devices otherwise it will be bigger platform for attacks on various organizations, homes, etc. As per many researcher whatever existing solution are there which not that much efficient to tackle all security problems. Now blockchain is new emerging technology and its main motive is only to give security In this paper, first an overview of the IoT and blockchain technology is discussed then solutions which are now available for securing internet of things using blockchain are discussed.

Keywords — *Internet of Things; Blockchain; Security.*

1. INTRODUCTION

Internet of Things (IoT) is the way through which many devices are connected each other. Use of IoT is increased day by day as our society is moving towards it for completion of their various daily activities. A. Kevin [1] introduced this IoT term in 1999, he is the initiator of IoT idea. Internet of Things (IoT) connects many small devices each other like sensors, smart watches, alarms through which information or data is getting shared within devices. Many people as switching to IoT it will introduce many threats towards it. Therefore many researchers now are working in this area to provide good solution. For providing security to IoT many researcher are saying blockchain technology is one of the good solution. Nowadays Blockchain technology is one of the new technologies and it is therefore centre of attention of many researchers. Blockchain is nothing but collection of blocks which are connected to each other through cryptography. Blockchain technology is having ability to transform and optimize the performance of infrastructure which is connected to the internet. Infrastructure consists of two important things:

a. Decentralised System

Creates point to point connection i.e. decentralised system

b. Transparency in database

Create transparent databases while designing system.

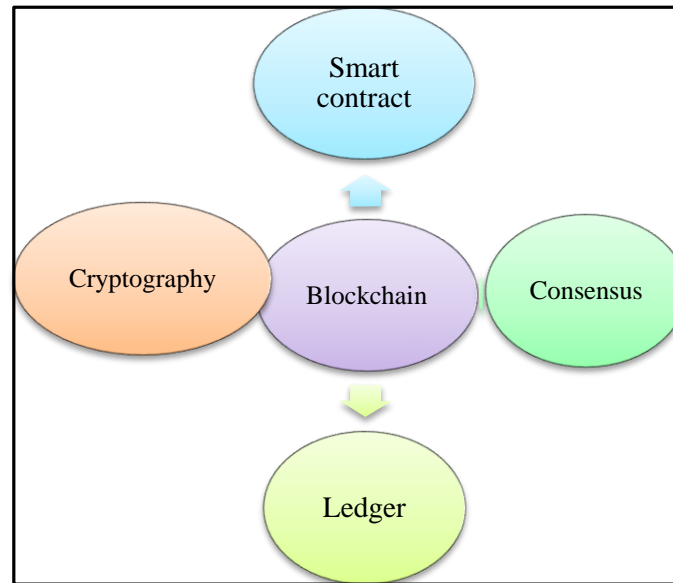


Figure 1. Blockchain Pillars [12]

Through 4 pillars blockchain technology is connected to internet world, blockchain pillars are shown in figure 1. a. Consensus – The main function of consensus is to give the proof of work and verifies the action in the networks,

b. Ledger - The ledger gives the complete transaction records within the network.

c. Cryptography- The cryptography confirms all the data encrypted in ledger and network, and decrypt the information by authorised users only.

d. Smart contract- The main function of smart contract is to verify and validate the participants in the network.

IoT is developing very fast and growing in every sector of technology .Due to its rapid growth, it is most prone to cyber-attacks. Now making IoT secure is on priority[12].

The nature of IoT systems is inherent like having limited storage and low processing a capability which makes them an unsuitable for the use of complex and highly computational in cryptographic algorithms. Because of AWS and Google reduced the cost of setup and also reduced the some security issues. But still there is problem of authentication of data and access control. Blockchain technology is one of the decentralized mechanisms which is used for managing security and also used for switching data of IoT devices. Therefore blockchain is nowadays a good solution to provide authenticity, access control to IoT devices [6].

In this paper survey of various blockchain technology based solutions are discussed which provide solution to various IoT security problems. Organization of paper is as follows: Section II gives an overview of blockchain technology based solutions for IoT security issues. Section III gives conclusion of the paper.

2. BLOCKCHAIN TECHNIQUES

In this section, existing Blockchain based solutions is discussed for IoT security.

G. Dittmann and J. Jelitto [2] designed a system in which they used blockchain proxy through which they can able to offload very huge part of considered application footprint. Proxy which they are using only required a slim proxy SDK. Using slim proxy SDK they can store blockchain identity with their private key. As a result maintaining control over transactions of that device. Their system is decreasing CPU processing time and also bandwidth required by that device for communication.

M. Son and H. Kim [3] designed firmware using blockchains and IPFS (The InterPlanetary File System) for managing architecture. Integrity of firmware is maintained by using IPFS. It is not giving surety of integrity of IoT device version management and IPFS URL. Firmware information provided by IoT devices and for surety of integrity of IPFS URL blockchain networks information is getting updated. As a result of system gives safe firmware which increases the security of IoT devices.

R. Yetis and O. K. Sahingoz [4] designed an authorization system for IoT devices. Set up consists of various distributed nodes. Blockchain system and blocks kept in these nodes. For communication purpose UDP (User Datagram Protocol) used for creation of connection with nodes. For communication establishment between multiple nodes encryption is applied in the system for creating secure framework. As a result of system it is observed that by using blockchain technology confidentiality of network traffic is improved for communicating securely with different nodes in network. Also system is providing authentication system as it is coded with python language.

C. Lee, N. Sung, L. Nkenyereye and J. Song [5] designed this system basically for M2M platform. The system is having blockchain-enabled IoT service layer platform based on oneM2M IoT standards and an blockchain hybrid application. They were used Logchain named blockchain technology which is more appropriate for IoT because of to its consensus algorithm. IoT users are getting enabled to store their data into database when oneM2M optional platform attribute and hybrid application is added to the system. They developed a layer which is used for completing IoT services by embedding blockchain high level architecture. As a result of system in IoT can able to modify and upload data without getting infected.

Rahul Agrawal, Pratik Verma, Rahul Sonanis, Umang Goel, Dr. Alok Nath De, Sai Anirudh Kondaveeti, Suman Shekhar [7] designed a system to do analysis and for evaluation of authenticate user in IoT network. All type of transaction of IoT is stored using blockchain. Also all type of interaction of IoT devices is stored as transaction or series of transaction for security purpose. For user to be legitimate in system a distinct digital crypto token is generated. This generated token is then used to give access to the user so that access control is managed. As a result of this unauthenticated user access will be denied. System will able to improve the access control things for IoT device. This is one of the good advantages of this designed system possible only because of blockchain technology.

D. Fakhri and K. Mutijarsa [8] designed a system in which they developed two system one which considering blockchain technology and second one without considering blockchain technology. For evaluation purpose they have designed these two systems. In the first system for communication purpose Ethereum protocol is used considering smart contract which one pillar of blockchain technology. For second system MQTT protocol is used for communication purpose. For experimentation and for evaluation both the system is observed. Both systems security is evaluated based on attack detection. As a result of system the first system which is using blockchain technology is showing good results.

M. Banerjee, J. Lee, K.-K.R. Choo [9] designed a system in which they have incorporated blockchain technology in IoT framework for detecting and curing system. Blockchain technology is mainly used for securing RIM. Blockchain technology is having main purpose as security. It is giving security to all the type of database transaction. In the designed system, they have already considered

that system is already authenticated by taking help of existing tools. It updates the flash memory and computes the RIM. The RIM, metadata, and the new firmware are stored in the blockchain and repository by the blockchain hardware. As a result of system RIM is secured by using blockchain technology.

B. T. Asare, K. Quist–Aphetsi and L. Nana [10] designed a system in which GOST algorithm is used. In system one of the good secured algorithm is used which is GOST, it is mainly used in fund type of section like pension fund, commercial application, in transfer of electric fund, in various payment system, in various online payment things, etc. In GOST algorithm encryption method used is most of the time using various combination of modes like stream mode, again stream mode with feedback thing, simple substitution mode, authenticity mode, encrypting electronic data mode, and validation of received hash value from hash function of GOST. System gives result as improved verification of received and transmitted data and also improved authentication of transmitted and received data.

S. Khanji, F. Iqbal, Z. Maamar and H. Hacid [11] designed system in which blockchain is integrated into IoT model to improve security, to overcome some existing system limitations. This system is mainly designed for smart transportation of cars. In this system in blockchain platform private fork on Ethereum is designed to connect IoT devices (Raspberry pi) deployed to detect car crashes. Because of it process of claim of insurance can be expedited.

M. Singh, A. Singh and S. Kim [12] discussed that by using blockchain in IoT, It will become more trustworthy. Blockchain technology is having various advantages that can be utilised in IoT like APIs, which offered by network of connected nodes. By using various functionality of blockchain IoT will become more secure. Authors designed a system in which they have used blockchain technology embedded infrastructure with IoT. Because of it IoT security is increased and also trust of IoT device is improved. In this system IoT devices are connected to each other in network and security is provided with blockchain. Through blockchain system becomes decentralised and then every system is having copy of chain of growing data. As the system is not centralised no single point of authority is there. For any type of access or transaction all nodes in network must validate it then it will go for further processing. As a result of system it is more secure than previous version.

P. Urien [13] designed an IETF draft ("Blockchain Transaction Protocol for Constraint Nodes") the BIoT paradigm. Main aim of this system is to place data collected from sensors into blockchain transaction. BIoT paradigm are having four advantage as sensor data publication and distributed ledger, authentication of data, using blockchain framework time stamping and non repudiation.

CONCLUSION

Nowadays IoT is growing rapidly as it is current trend. Therefore IoT is center of attention for many researchers, academicians and commercial organizations. Many people are using IoT for their daily life activity. Now everyday IoT requirement is increasing drastically, with this it is also raising security issue. Recently many researchers are switching to blockchain technology for security purpose. So in this paper various security solutions for IoT using blockchain technology is discussed.

REFERENCES

- [1] Ashton K, "That 'internet of things' thing.", RFID Journal 22, no. 7, 2009, pp.97-114.
- [2] G. Dittmann and J. Jelitto, "A Blockchain Proxy for Lightweight IoT Devices," 2019 Crypto Valley Conference on Blockchain Technology (CVCBT), Rotkreuz, Switzerland, 2019, pp. 82-85.

- [3] M. Son and H. Kim, "Blockchain-based secure firmware management system in IoT environment," 2019 21st International Conference on Advanced Communication Technology (ICACT), Pyeong Chang Kwangwoon_Do, Korea (South), 2019, pp. 142-146.
- [4] R. Yetis and O. K. Sahingoz, "Blockchain Based Secure Communication for IoT Devices in Smart Cities," 2019 7th International Istanbul Smart Grids and Cities Congress and Fair (ICSG), Istanbul, Turkey, 2019, pp. 134-138.
- [5] C. Lee, N. Sung, L. Nkenyereye and J. Song, "Blockchain Enabled Internet-of-Things Service Platform for Industrial Domain," 2018 IEEE International Conference on Industrial Internet (ICII), Seattle, WA, 2018, pp. 177-178.
- [6] M. S. Urmila, B. Hariharan and R. Prabha, "A Comparative Study of Blockchain Applications for Enhancing Internet of Things Security," 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kanpur, India, 2019, pp. 1-7.
- [7] Rahul Agrawal, Pratik Verma, Rahul Sonanis, Umang Goel, Dr. Alok Nath De, Sai Anirudh Kondaveeti, Suman Shekhar, "Continuous Security in IoT Using Blockchain," 2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Calgary, AB, 2018, pp. 6423-6427.
- [8] D. Fakhri and K. Mutijarsa, "Secure IoT Communication using Blockchain Technology," 2018 International Symposium on Electronics and Smart Devices (ISESD), Bandung, 2018, pp. 1-6.
- [9] M. Banerjee, J. Lee, K.-K.R. Choo, "A blockchain future to Internet of Things security: A position paper, Digital Communications and Networks (2017), doi: 10.1016/j.dcan.2017.10.006.
- [10] B. T. Asare, K. Quist–Aphetsi and L. Nana, "Nodal Authentication of IoT Data Using Blockchain," 2019 International Conference on Computing, Computational Modelling and Applications (ICCA), Cape Coast, Ghana, 2019, pp. 125-1254.
- [11] S. Khanji, F. Iqbal, Z. Maamar and H. Hacid, "Boosting IoT Efficiency and Security through Blockchain: Blockchain-based Car Insurance Process - A Case Study," 2019 4th International Conference on System Reliability and Safety (ICSRS), Rome, Italy, 2019, pp. 86-93.
- [12] M. Singh, A. Singh and S. Kim, "Blockchain: A game changer for securing IoT data," 2018 IEEE 4th World Forum on Internet of Things (WF-IoT), Singapore, 2018, pp. 51-55.
- [13] P. Urien, "Blockchain IoT (BIoT): A New Direction for Solving Internet of Things Security and Trust Issues," 2018 3rd Cloudification of the Internet of Things (CIoT), Paris, France, 2018, pp. 1-4.