Recent Trends in Intensive Computing
M. Rajesh et al. (Eds.)

doi:10.3233/APC210250

Architecture for Secure Communication Among IoT Devices with Ethereum Blockchain

Bawankar Chetan D [a,1], Dr. Sanjeev Kumar Sharma [b]

[a] *Sanjivani COE, Dept. of IT & Research Scholar Dept. of Computer Science and Engineering Oriental University Indore, India*
[b] *Dept. of Computer Science and Engineering Oriental University Indore, India*

Abstract. The paper aims to clarify the relationship between Internet-of-Things devices and Ethereum blockchain. It proposes the arrangement to ensure information transmission among parties in an open system of IoT must be secure using Ethereum. The accompanying joining strategy utilized terminal gadgets as system innovation and Ethereum blockchain stage that delivered back-end, which guarantees high security, accessibility, and protection, supplanting conventional back-end frameworks. The following issues should be considered to prevent the malicious hub from attacking, resist distributed denial-of-service attacks, and prevent firmware backdoor access. This paper proposed a system in which the Peer-to-Peer authentication model, where every IoT node in the system must be authenticated and verified by the proposed framework. The paper provides empirical insights into IoT nodes manufactured in bulk, and they are remaining with their default username and password.

Keywords. Performance Measurement Authentication, Botnet, Blockchain, Data Protection, Ethereum, Smart contacts

1. Introduction

Ethereum Blockchain and Internet of Things (IoT) are used for creating new ideas and innovations. All the while, they change contemplations and make extra chances, each in their individual conditions, and there is an opportunity for applications that can be shared with standard attributes of IoT and Ethereum, the significant advantage of decentralized for IoT hub/nodes is with Blockchain.[1] Right now, Blockchain likewise falls along this line of research may be used to authorize, authenticate and audit the data generated by IoT hub/nodes. Like- wise, thinking about decentralized nature takes out the need to trust in the untouchable and doesn't have a particular clarification behind failure. In proposed IoT Hub/hubs are relied upon to be online and ought to speak with one another.

[1] Bawankar Chetan D, Research Scholar Dept. of Computer Science and Engineering Oriental University Indore, Email: chetan251htc@gmail.com.

In Private blockchains, hubs/nodes are foreordained, while in Public blockchains, any hub/node can leave or join the network. Ethereum is a Public blockchain variation where each exchange has a cost estimated in the wording of" Gas." Ethereum receives the PoW consensus algorithm.[2]

To manage the security issues of IoT, one needs a few stages which could give both security and integrity of the information being imparted between the IoT gadgets. In the Beginning, the advancement which is exhibiting an enormous achievement in the area of assurance and security of data for clients in Blockchain is improved. Blockchain innovation has a decentralized network with trustless in more minor conditions. It doesn't require outside interference. Having this sort of condition, the information is still verified in the Blockchain as it uses Cryptographic hashing to verify information in the distributed ledger. Blockchain as a passed-on record advancement makes a trustless situation that can thoroughly clean the dependence of trusted third parties. Each IoT hubs has the stability to cutoff information through a Consensus computation in the Ethereum blockchain network. The structure is secure if the reasonable center points control inside and out more hash rate than any interest social affair of aggressor hub. The informational index aside of Blockchain can't be changed, regardless of whether the aggressor begins from the internal framework.[3]

The blockchain advancement gives reasonable courses of action to the verification and security protection of IoT hub/node. The edge arrangement and board (management) of Blockchain is moderately below average.[4] Regardless of whether intelligent gadgets have constrained processing assets, Blockchain may be developed. Using Blockchain in the IoT makes the system decentralized, which can significantly improve the system's security. It is essential to spare contraption ID, public key, and the hash value of critical information in the record before gadget access to the IoT network. Using cryptography, shared certification with partners to check the rightness of the data out between a public key and a contraption ID. [5] Comparing hash values of contraption ID information, any difference in the data can be perceived promptly.[6]

The paper is arranged as mentioned:

2. Section Presents Background and Related work done in the field of Botnet Internet of Things (BIoT)

3. Section Presents the Problem Identification and Proposed System architecture

4. Section Proposed System Implementation details

5. Section Addressed the challenges in implementations

6. Section Concludes and the future scope.

2. Background and Related Work

Blockchain is a decentralized appropriated database of changeless records, where exchanges are ensured by robust Cryptographic calculations, and the system status is

kept up by the Consensus algorithm. Examination and investigation of security gaps in the brilliant home system layer and proposed arrangements. It is conceivable to oversee and confirm gadgets utilizing an ISP and oversee intelligent home gadgets in an external web condition. In any case, because of the absence of client information for examination, this methodology isn't successful in guaranteeing the security of the inside Internet condition. Use Wireshark to check home horizons and lack of confidential data for devices such as free detectors when building intelligent home devices. This approach offers software-specific solutions but cannot compete with software other than Wireshark.

3. Problem Identification and Proposed Methodology

1. A novel authentication method for IoT hub/node based on Ethereum for secure communication over IoT network.
2. To Implement smart contract and validation of node in proposed authentication framework.

The Proposed system comprises of two main parts as follows

3.1. Peer-to-Peer Authentication Method

Blockchain is an open, secure, and distributed exchange ledger innovation, can flexibly adjust to complex also changing system conditions. The failure of a few hubs/nodes doesn't influence the ongoing activity of the framework. Distributed authentication between hubs prevents malicious hubs from attacking the system. Regardless of whether few hubs are undermined, the ledger won't be altered. In a multi-node network, the identity data of the hub/node should be enlisted in the blockchain each time a new hub/node is included. Every hub/node ID, public key, a hash of basic information, and other data are put away in the blockchain ledger.

Simultaneously, every IoT hub/node is a major component in the Ethereum blockchain network, and the consensus component ensures that every hub stores similar data. At whatever point, Peer-to-Peer Authentication Method correspondence happens via public-key cryptography, which can be utilized for validation in IoT networks.[5] The framework process is mainly divided into three stages. All gadgets need to finish the enlistment in the blockchain before authentication. When a new node wishes to access, it will first check the list mentioned in the blockchain. Once getting authentication from the blockchain gadget will be checked for trustworthiness with the hash value of data to find the potential intrusion behavior.

3.2. Independent Framework to detects Botnet

The proposed framework contains three significant parts Ethereum Blockchain, Hosts, and Self-governing System (SS).

- **Hosts:** Nodes which are associated with the web using an SS. Two types of hosts are their general and IoT nodes. IoT nodes have devices like sensors, actuators, and many more devices, which may play an important role in the network and send/receive data remotely. As botnet misuses the vulnerabilities of IoT has; consequently, they are increasingly helpless against attacks. [2]
- **Self-governing System:** SS is one of the significant segments of the proposed framework. The botnet moderation component is executed in the SS. An SS is mindful

of advancing the packets outside of the system. SS stores the list of host and threshold values per IoT hub/nodes. Four records are looked after" Blacklist"," Whitelist"," Reckoned Attacker List" and" Conceivable Victim List". The SS are associated with one another using the Ethereum blockchain and exchange arrangements of IP address. Each SS monitors the number of packets sent and received by the host. This edge esteem is invigorated at regular intervals.

- **Blockchain:** The SS is associated with the Ethereum blockchain. They communicate with one another in the type of blockchain ex- changes. For the most part, in Ethereum information is communicated when the block exchanges.

4. Implementation Details

This section addresses the particular usage of the framework, which includes the Ethereum blockchain, the procedure of the asymmetric key generation; at last, security analysis of the framework is given as below. Session key KSAB is shared with both. This received key will be used by both parties for secure communication.

Algorithm 1: Proposed method for Key Exchange

1 Aryan will request to Ethereum for public-key of Agrani PuKB
2 Ethereum will check for authentication of IoT hub/node
3 if IoT hub/ node is in 'BlackList' then
4 go to step 23
5 else if IoT hub/ node is in 'reckoned Attacket List' then
6 go to step 23
7 else
8 Send the Public-key of Agrani PuKB to Aryan
9 Aryan will encrypt a" Number only used once (Nonce)" N1 that solely identifies a transaction and Aryans IDA with the PuKB of Agrani is given by EPuKB (N 1, IDA)
10 Agrani will request to Ethereum for PuKA of Aryan
11 Ethereum blockchain will check the authentication of IoT hub/node
12 if IoT hub/ node is in 'BlackList' then
13 go to step 23
14 else if IoT hub/ node is in 'reckoned Attacket List' then
15 go to step 23
16 else
17 Send the Public-key of Aryan PuKA to Agrani
18 Agrani will encrypts a" Number only used once (Nonce)" N2 that solely identifies a transaction and Agranis IDB with the PuA key of Aryan is given by EPuKA (N 2, IDB)
19 Agrani send to Aryan the already received Nonce (N 1) and second Nonce (N 2) is encrypted with Aryan PuA key. EPuA (N 1, N 2)
20 Aryan acknowledge with received Nonce(N2) to Agrani which is encrypted by Agrani's public-key PuB. EPuKB (N 2)
21 Aryan will now be generated secure key KSAB which is signed with Aryan PrKA and the complete message is encrypted with Agrani PuKB EPuKB (PrKAKSAB, N2)

22 Agrani will decrypts the received message by accessing both key of Agrani PrKB and verifies the digital signature using Aryan PuKA key
23 Add the user in Black list and report the same.

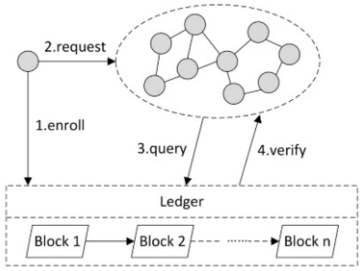

Figure 1. Working Process of Proposed method

4.1. Framework of blockchain network

Each SS keeps up four unique types of records. Since botnet explicitly focuses on the IoT hub/nodes, IP locations of IoT hub/node have SS, which includes the list of the reckoned attacker; meanwhile, other hosts' IP addresses are included in the whitelist. Different lists are updated to SS using the Ethereum blockchain.

4.2. Private key generation

Random number generator likewise needs a seed from a source with ad- equate entropy count. An irregular seed is gathered by different data of the IoT gadgets, for example, free space, I/O delay, memory status, procedures running, CPU frequency, and many more. By using the RSA algorithm, the Public key is generated from the Private key.

5. Challenges of IoT hub/node with proposed blockchain solutions

Many applications use blockchain in IoT framework. A few difficulties are with security of IoT hub/nodes and their solutions with use of blockchain Privacy of IoT Hub/nodes IoT hubs are helpless against uncovering the private information of the user. To address this issue permission Ethereum used to provide security to IoT hub/nodes. [8] Traffic and Cost To deal with rapid changes in IoT gadgets. For this purpose, decentralization using Ethereum. All devices present in the system are directly connected and communicate with a peer rather than a central server. Shoddy architecture Every component of IoT gadgets has a state of washout that influences the network. Using blockchain, all nodes in the web will be verified. The data is also cryptographically secure. Verification is a framework by which a framework decides whether the customer has certain benefits. Verification arranged into a group of three as mention below: what-you-have (possession), who-you-are (ownership), and what-you-know (data).[10]

Data Protection/manipulation In IoT hub/nodes, guaranteeing the unwavering quality of the IoT gadgets gives security assurance. Regardless of whether a gadget has passed the authentication of different hubs, it, despite everything, has the danger of being assaulted by intruder clients because of programming or framework

vulnerabilities during the execution of the task. The intruder normally will change the system element to leave the second passage in the gadget to get ready for consequent invasion and adjust the key arrangement record in the gadget and prompt harm to the whole system. Due to the use of blockchain the Data protection/Manipulation, if any node updates the data, the framework will reject the manipulation.[11]

6. Conclusion and Future Scope

This paper addressed various challenges of IoT hub/node, which are having possible solutions using blockchain. Additionally, investigated the downside of the present IoT center/hubs in personality confirmation and security zone. The structure of multi-chain gives add-on security between various IoT hubs in a network. This paper proposes an Ethereum based response for the issue present in secure communication between IoT Hub/center points. Future work will concentrate more on the administration of IoT sensors versus the customary budgetary database in the blockchain. We aim to employ Edge computing, Fog computing, and Machine learning algorithms for the botnet detection method.

Acknowledgement

The authors are thankful to the Department of Computer Science and Engineering, Oriental University, Indore, for their contentious supports. This work has also been supported by the Department of Information Technology, Sanjivani College of Engineering, Kopargaon.

References

[1] S. G. Kumar, A. Murugan, B. Muruganantham, and B. Sriman, “IoT–smart contracts in data trusted exchange supplied chain based on block chain,” International Journal of Electrical and Computer Engineer- ing (IJECE), vol. 10, no. 1, p. 438, feb 2020.

[2] Z. Ahmed, S. M. Danish, H. K. Qureshi, and M. Lestas, “Protecting IoTs from mirai botnet attacks using blockchains,” in 2019 IEEE 24th Interna- tional Workshop on Computer Aided Modeling and Design of Communica- tion Links and Networks (CAMAD). IEEE, sep 2019.

[3] S. K. T. Mehedi, A. A. M. Shamim, and M. B. A. Miah, “Blockchain-based security management of IoT infrastructure with ethereum transactions,” Iran Journal of Computer Science, vol. 2, no. 3, pp. 189–195, jul 2019.

[4] K. Koˇsˇt´al, P. Helebrandt, M. Belluˇs, M. Ries, and I. Kotuliak, “Manage- ment and monitoring of IoT devices using blockchain,” Sensors, vol. 19, no. 4, p. 856, feb 2019.

[5] D. Li, W. Peng, W. Deng, and F. Gai, “A blockchain-based authentication and security mechanism for IoT,” in 2018 27th International Conference on Computer Communication and Networks (ICCCN). IEEE, jul 2018.

[6] M. El-Hajj, A. Fadlallah, M. Chamoun, and A. Serhrouchni, “Ethereum for secure authentication of IoT using pre-shared keys (PSKs),” in 2019 International Conference on Wireless Networks and Mobile Communica- tions (WINCOM). IEEE, oct 2019.

[7] H. Akhundov, E. van der Sluis, S. Hamdioui, and M. Taouil, “Public-key based authentication architecture for IoT devices using PUF,” in 6th In- ternational Conference on Computer Science, Engineering and Information Technology (CSEIT-2019). Aircc Publishing Corporation, nov 2019.

[8] O. Alphand, M. Amoretti, T. Claeys, S. Dall'Asta, A. Duda, G. Ferrari, F. Rousseau, B. Tourancheau, L. Veltri, and F. Zanichelli, “IoTChain: A blockchain security architecture for the internet of things,” in 2018 IEEE Wireless Communications and Networking Conference (WCNC). IEEE, apr 2018.

[9] M. D. A. Dhaya and R. Ravi, “Multi feature behavior approximation model based efficient botnet detection to mitigate financial frauds,” Journal of Ambient Intelligence and Humanized Computing, jan 2020.

[10] L. Hang and D.-H. Kim, "Design and implementation of an integrated IoT blockchain platform for sensing data integrity," Sensors, vol. 19, no. 10, p. 2228, may 2019.
[11] J. H¨oglund, S. Lindemer, M. Furuhed, and S. Raza, "PKI4iot: Towards public key infrastructure for the internet of things," Computers & Security, vol. 89, p. 101658, feb 2020.
[12] O. Pal, B. Alam, V. Thakur, and S. Singh, "Key management for blockchain technology," ICT Express, aug 2019.