IARJSET

ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 5, May 2024

DOI: 10.17148/IARJSET.2024.115116

Securing the IoT with the Blockchain

Mr.Rahul Chandrayan

Research Scholar

Abstract: IoT is the boon for industries with capabilities to digitize complete industry process, system, software's and machineries on one single platform. The capability enables the 360 degree view of the industry. The security concerns is very important while implementing the IoT, since it become crucial for any IoT or IIoT project to implement the security else since IoT application has direct access on internet hence it become more prone to internet attacks hence to avoid we need to have high security which ensures full proof system for this we can have integration of block chain technologies with IoT.

Keywords: IoT, IIoT, Blockchain, Privacy, Security.

INTRODUCTION

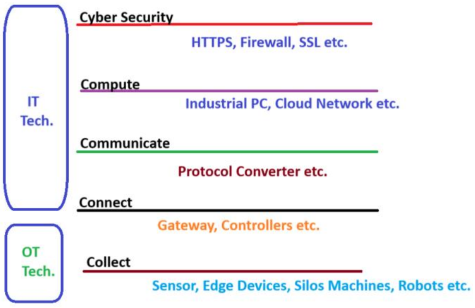
IoT is a layered architecture it follow the OSI model for its implementation. There are many challenges while implementing the IIoT / IoT application and varies case to case. If can identify the common challenge and try to mitigate it will further ensures 360 degree implementation of the services of IoT application. The common challenge while implementing the IoT based solution is cyber attacks which get easily initiated since the complete system is available on the Internet.

The advantage of silos system in industries are that they are very less prone to cyber attacks or viral attacks since the access is restricted and hence ensuring the tight security where as when we attach the system or machine to the internet it get more prone to cyber attacks since the system can be accessed from any place any time via internet. Thus the role of security is topmost concern in such scenarios where your system, equipment or machine is available on public domain.

Today, to address IoT security we have various approaches includes encryption techniques, edge computing, fog computing, cloud computing, machine learning and block chain etc. The IoT solution architect has to choose the best suited model to mitigate the security issues for the particular application. Here, we are discussing the most secure way for implementing the IoT application using integrated approaches with IoT and block chain technologies.

IoT / IIoT building blocks

We know that the IoT architecture is very dynamic and varies case to case hence to simplify the implementation approach we have 5C approach of implementation. The 5Cs provides the layered architecture and bottom up approach for its implementation starts from sensing unit at the base and ends at control and monitoring unit at top. The 5Cs approach helps to implement the IoT application from start to end ensuring 360 degree feedback of the system.


IT Tech.
Cyber Security
HTTPS, Firewall, SSL etc.
Compute
Industrial PC, Cloud Network etc.
Communicate
Protocol Converter etc.
Connect
Gateway, Controllers etc.
OT Tech.
Collect
Sensor, Edge Devices, Silos Machines, Robots etc.

5C - Approach of IIoT Implementation

Block Chain building blocks

Block chain technology has been proposed to provide the security to the IoT applications. The Block chain technology brings worldwide revolution to optimize and secure the global infrastructure of the technologies on the internet. Block chain creates a decentralized system which avoids the indulgence of central servers and provides peer-to-peer interaction. It provides a fully transparent system and open to all database, which records every transaction made on a network.

The centralized ledger distributed over a network of nodes. This network can be public or private.

Components of a Block chain system

Following are the block chain components

Network of Nodes : All the nodes connected through the internet to form a block chain network. Each node has been added, its record are added to the ledger of past transaction which is known as mining.

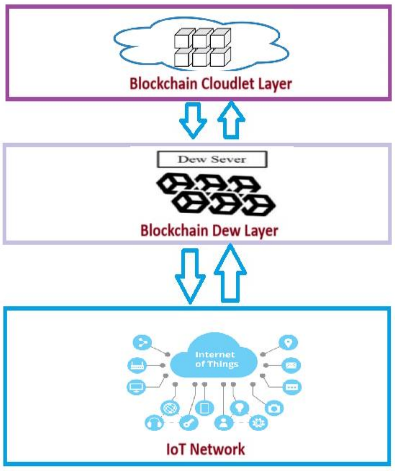
Distributed database: The database is composed of blocks of information and is copied to every node of the system. Every data block stores list of transaction and timestamp and the information which links to the previous blocks.

Shared Ledger: The ledger is public and is available for storage of any transaction done on the network.

Cryptography: Every node data is encrypted by crypto mechanism for unauthorized access.

Integration and Security Implementation

To strengthen the IoT network with blockchain technology need to create a decentralized system, which means there is no single authority which can approve any transaction on the network. Here, each and every device will have a copy of the ever growing chain of data or transaction made on the network. This means that whenever someone wishes to access the device and do some transaction, then all the members of the network must validate it. After the validation is done, the performed transaction is stored in a block and is sent to all the nodes of the network. Thus by adding the validation stage the complete block chain network become more secure and impossible for the un-authorized sources to breach into the security.



Proposed IoT-blockchain Integrated Architecture

To secure IoT application with block chain following points are considered

1. **Ensuring Communication Security:** IoT devices have to communicate to exchange data required to process a transaction and to store it in a ledger. Ledgers can also be used to store encryption keys to make the data exchanges more confidential. IoT device sends an encrypted message using the public key of the final destination device, which is then stored in the block chain network. The sender then asks its node to get public key of the receiver from the ledger. Then the sender encrypts the message using public key of the receiver, in this way, only the receiver will be able to decrypt the sent message using their private key only which ensures security in the whole network.

DOI: 10.17148/IARJSET.2024.115116

2. **Users Authentication:** The sender device digitally signs the message before sending them to the network. The receiver device then gets the public key from the ledger and uses it to verify the digital signature of the received message.

   The digital signature work as follows:

   • Firstly, the sender encrypt the message with its private key.

   • Then, the digital signature along with the message is transmitted on the network

   • Further, the receiver then decrypts the digital signature using the public key of sender stored in the ledger to obtain the hash value as calculated by the sender.

   • Finally, the message is validate with the calculated hash and the protected hash of the message are same.

   • Due to the centralize ledger storage the trust in the network get improved.

3. **Discovering IoT device:** As soon as a new IoT device initiated on the network, it asks root servers to give a list of trusted nodes in the network. This device then registers itself in a node, and the exchange of information starts.

   DNSSec has to be implemented to secure name resolution of root servers by avoiding any spoofing attacks. Every communication made must be authenticated and encrypted efficiently.

   This can be done based upon:

   - Credentials already installed on the device during setup.
   - Credentials could be given by the owner of the IoT device.

4. **Configuring IoT Devices on the Network:**

   - Properties of IoT devices like configuration details and the latest firmware version has been validated and hosted on the ledger.
   - During bootstrap, the block chain node is asked to get its configuration from the centralized ledger.
   - The configuration is required to be encrypted in the ledger to prevent the discovery of IoT network topology or its properties by analysis of the information stored in the public ledger.
   - The hash value of latest configuration file for every device can be hosted in the ledger.
   - Using a cloud service the IoT device will have to download the latest and trusted configuration file after every fixed interval of time. Then the device can use the blockchain node API to retrieve and match the hash value, which is stored in the blockchain. If it was found un matching node the administrators removes such any bad configurations node regularly and reboot each and every IoT device in the network with latest and trusted configurations.

CONCLUSION

This research paper presents an approach of securing the IIoT application with the help of Block chain technologies. This paper also provides an overview of a the current state of the art of IoT, block chain and the implementation challenges. Since the IoT market is growing rapidly it is necessary to streamlined the integrating process with block chain so as to ensure primitive security measures by considering the distributed and heterogeneous environment thereby increasing the confidentiality, authenticity and availability.

Thus, through collaborative efforts in space of IoT and block chain technologies and optimized policymaking, we can build a more inclusive and sustainable future for all.

REFERENCES

[1] S. Mohapatra, D. Mohanachandran, G. Dwivedi, et al., A comprehensive study on the sustainable transportation system in India and lessons to be learned from other developing nations, Energies 16 (4) (2023) 1986, https://doi.org/10.3390/ en16041986

[2]J. Holmgren, The effect of public transport quality on car ownership–A source of wider benefits? Res. Transport. Econ. 83 (2020) 100957 https://doi.org/ 10.1016/j.retrec.2020.100957.

[3]N. Tapas, G. Merlino, and F. Longo, "Blockchain-based iot-cloud authorization and delegation," in 2018 IEEE International Conference on Smart Computing (SMARTCOMP). IEEE, 2018, pp. 411–416. [181]

[4]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, 2018, pp. 1–6. [182]

[5]L. Seitz, G. Selander, E. Wahlstroem, S. Erdtman, and H. Tschofenig, "Authentication and authorization for constrained environments (ace)," Internet Engineering Task Force, Internet-Draft draft-ietf-aceoauthauthz-07, 2017. [183]

[6]M. Vucini ˇ c, B. Tourancheau, F. Rousseau, A. Duda, L. Damon, and ´ R. Guizzetti, "Oscar: Object security architecture for the internet of things," Ad Hoc Networks, vol. 32, pp. 3–16, 2015. [184]

[7]J. Pouwelse, P. Garbacki, D. Epema, and H. Sips, "The bittorrent P2P file-sharing system: Measurements and analysis," in IPTPS, vol. 5. Springer, 2005, pp. 205–216.

[8] J. J. Xu, "Are blockchains immune to all malicious attacks?" Financial Innovation, vol. 2, no. 1, p. 25, 2016. [275]

[9] P. Koshy, D. Koshy, and P. McDaniel, "An analysis of anonymity in bitcoin using p2p network traffic," in International Conference on Financial Cryptography and Data Security. Springer, 2014, pp. 469– 485. [276]

[10] J. Herrera-Joancomart´ı, "Research and challenges on bitcoin anonymity," in Data Privacy Management, Autonomous Spontaneous Security, and Security Assurance. Springer, 2015, pp. 3–16. [277]

[11] F. Reid and M. Harrigan, "An analysis of anonymity in the bitcoin system," in Security and privacy in social networks. Springer, 2013, pp. 197–223. [278]

[12] M. Rahouti, K. Xiong, and N. Ghani, "Bitcoin concepts, threats, and machine-learning security solutions," IEEE Access, vol. 6, pp. 67 189– 67 205, 2018.