SRI RAMACHANDRA

INSTITUTE OF HIGHER EDUCATION AND RESEARCH

(Category - I Deemed to be University) Porur, Chennai

SRI RAMACHANDRA ENGINEERING AND TECHNOLOGY

CSE-450 IOT SECURITY

CA4- Securing IOT data via Blockchain Technology and Service-Centric Networking

Submitted to

SRI RAMACHANDRA INSTITUTE OF HIGHER EDUCATION AND RESEARCH
SRI RAMACHANDRA ENGINEERING AND TECHNOLOGY

For the Award of the Degree of

BACHELOR OF TECHNOLOGY
In
COMPUTER SCIENCE AND ENGINEERING
(Cyber Security and Internet of Things)

By
SHRIRAM K.P(E0219007)
UMESH KUMAR M(E0219019)

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
SRET, PORUR, CHENNAI- 600116
OCTOBER 2022

Abstract:

Blockchain and IoT are two of the most widely discussed technologies in today's world. They're in their early stages of maturity, and there's a lot going on in terms of development and finding interesting applications for the technologies. Data transmitted by IoT devices is critical and must be secure. Based on the IoT security issues, this paper proposed a Blockchain-based model for secure IoT data, known as service-centric networking (SCN). SCN provides communication by service names rather than addresses, as well as a decentralised network that allows network users to communicate quickly and securely. However, the users' identities will be stored in an encrypted format on their device and will be backed up by Interplanetary File System (IPFS).

Introduction:

The Internet of Things (IoT) refers to the process of connecting devices via the Internet network; each device has an internet protocol (IP address), and all of these devices can send and share data from anywhere and at any time [1].

IoT is used for a variety of purposes, including healthcare, smart homes, wearable sensors, self-driving cars, banking, E-commerce, and surveillance systems [2].

The data were collected during transmission while facing some security issues that may cause it to lose its value because the Internet of things are small devices that cannot install a system to be more secure, as well as memory limitations and the use of centralised service providers through which the IoT data may be illegitimately used [3].

The most common issue in IoT security is Distributed Denial of Service (DDOS), which prevents users from accessing the server because the attacker sent a large number of requests to the server [4].

As a result, the data requires some security measures. Blockchain provides a decentralised model that allows the network to be dependable, safe, flexible, and capable of supporting real-time services [5].

Using IoT with blockchain improved network connectivity and provided users with more opportunities to communicate with one another directly (P2P) without the use of a third party [6].

Blockchain models include the Directed Acyclic Graph (DAG), which is known as the next generation of decentralised ledger technology, and the Service-Centric Network (SCN), which provides a service-aware network stack that allows each application to communicate by service names rather than addresses[7].To avoid cyber-attacks, blockchain technology provides decentralised Technique security and privacy [8].

Survey:

We went over some previous research on IoT threats and how to secure IoT using blockchain technology. M. S. Ali, K. Dolui, and colleagues [9]

Using Blockchain and IPFS, they created a network architecture to provide IoT data privacy. They used a "Modular consortium," which divided the network into small networks and connected all devices in the networks as peer-to-peer. As a result of using this architecture, users can access the network without relying on a third party. C. Li and L. J. Zhang [10]

Using Blockchain Technology, we created a multi-layer model for IoT network security. He classified IoT networks as multilevel decentralised networks. By utilising a peer-to-peer connection, this model reduces the overcome of using a centralised network while also increasing network safety and speed. Fan, K., Wang, S., et al. [11, 20]

Proposed a system for securing IoT data during time synchronisation using Blockchain technology. This system is made up of five modules: communication authentications, consensus, a time source, internet of things devices, and a common time node. This proposed system can avoid network attacks and accidents by using a multi-time source and minimising communication overhead. D. Fakhri and colleagues .[12]

They implemented and compared Message Queuing Telemetry Transport (MQTT) and Blockchain technology to test the efficiency of security during internet of things communication. They recognised that implementing Blockchain technology in IoT communication makes it more secure and efficient. Muhtasim, M. A., et al. [13]

Proposed using Blockchain Technology to protect the network and prevent DDOS. R. Agrawal et al .[14]

Proposed a method for ensuring continuous data security by utilising IoT-Zone Identification and IoT-token Generation The IoT-Zone tracks user activity. Every IoT-Token user must register and obtain an Enrollment Certificate Authority (ECA). They used a dataset of one building with floors and 1000 data points generated by the user for training. The Blockchain framework was tested using Hyperledger Fabric v0.6. They used two models, Markov and LSTM, and the results showed that the Markov model was more accurate than the LSTM model. Wrona, K., et al. [15]

Proposed an architecture to secure civil-military metadata. The architecture is built on the Hyperledeger fabric. This architecture will improve the security of civil-military metadata collected by IoT sensor members in the workplace. A. Dorri et al.[16]

Proposed a method for smart home security based on Blockchain technology They used the Cooja simulator to simulate the smart home. They compared the use of Blockchain with smart homes to another implementation that did not use hash, encryption, or Blockchain. This simulation resulted in reduced time and energy consumption in various traffic flows. Y. Qian et al .[17]

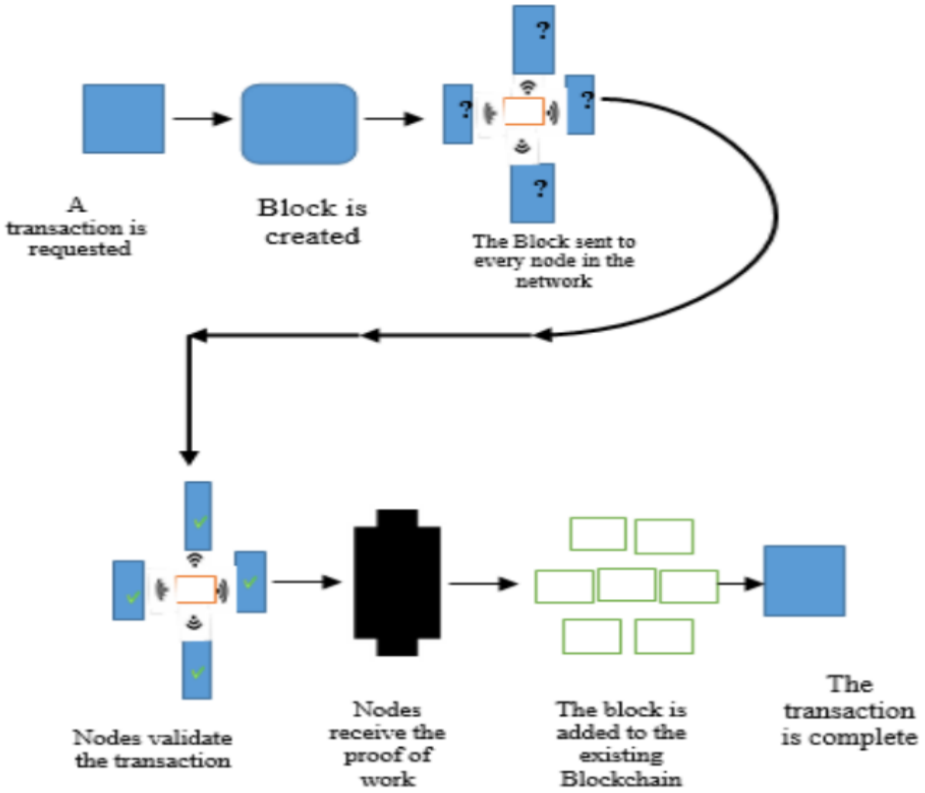
Proposed three IoT layers for security enhancement The first is the application layer, where they focused on three issues: cloud security, user data privacy protection, and secure computing. The second layer is the network layer, which IoT devices use to communicate data. The third layer is the perception layer, which has two issues: a large number of terminal sensors with open ports, which may be caused by DDoS, and IoT devices. Because it is connected via short-distance protocols such as Zigbee, Bluetooth, and Wi-Fi, it may be targeted by hackers. Based on those issues, they proposed solutions such as traffic monitoring using machine learning and verification. S. Chakraborty and colleagues .[18]

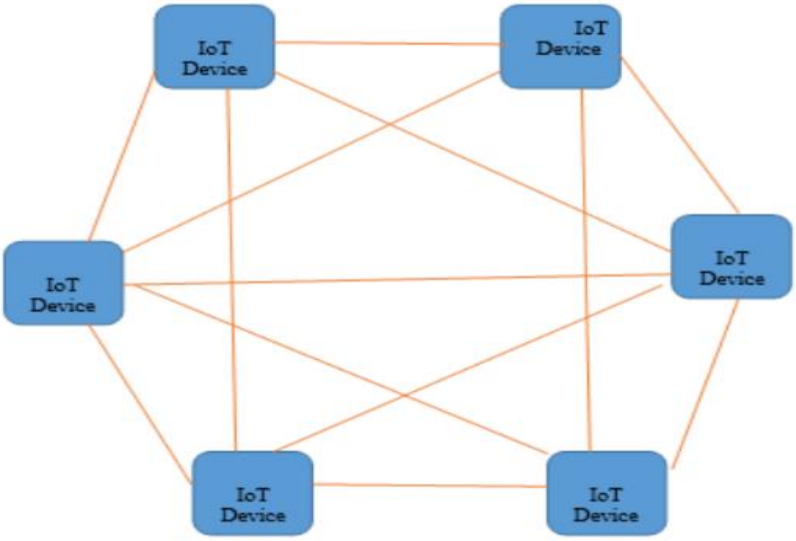
Proposed method for storing healthcare information using Blockchain Technology To prevent unauthorised access, healthcare information collected from patients via wearable sensors and sent to doctors via IoT and machine learning must be secure and private. The state of patients will update continually to the doctor who observes his statutes, and all this information is secured by Blockchain. Li, D., et al.[19]

Discussed the disadvantages of using traditional internet of things security methods and their centralised nature, and then proposed a method based on Blockchain technology to secure IoT and a prototype based on Blockchain technology platform Hyperledger Fabric to validate the proposed system.

Implementation :

The Internet of Things has become increasingly popular and has a wide range of applications, including smart cities, banking, self-driving cars, healthcare, smart homes, and marketing. The implementation of IoT is increasing, as are the vulnerabilities. These kinds of applications are essential in our lives, and data must be kept private and secure. When users use IoT without using security techniques, their data and privacy are in the hands of the attacker. To avoid these threats, we are employing Blockchain and SCN technology.


A transaction is requested
Block is created
?
?
?
?
The Block sent to every node in the network
Nodes validate the transaction
Nodes receive the proof of work
The block is added to the existing Blockchain
The transaction is complete



Blockchain network of IOT device .

Recommendation :

Traditional security techniques demanded three things: integrity, confidentiality, and availability.

- Integrity means that the data will arrive in the receiver unaltered by an unauthorised user.
- Confidentiality: The data must be kept private and secure from unauthorised access.

When will the necessary data be available for use? Traditional security techniques have a centralised system limitation; Blockchain technology provides a decentralised system to overcome those limitations. In Blockchain, if one node is attacked, all other nodes in the network continue to function normally. The privacy provided by Blockchain makes IoT more secure in the event that an unauthorised user wishes to change the access permission he/she requires by forging a digital signature; however, this is not possible because Blockchain requires a pair of keys; public and private keys. Even if the owner's key is compromised, the hacker cannot alter the data on the blockchain. Blockchain technology is currently receiving a lot of attention. It has the potential to revolutionise and improve the global infrastructure of technologies linked together via the internet.

It will have an impact on two fields:

It creates a decentralised system rather than using central servers and it provides peer-to-peer networks.

It creates a completely open and transparent database for all databases, allowing for greater transparency in governance and elections.

Conclusion :

This project covered Blockchain-based IoT and its implementation. Using Blockchain, this study proposed a model (SCN) for IoT data security. Because IoT data is very important and requires some security techniques, the SCN model is the best modern technology that can be used. This model avoids a centralised network model that requires a third-party service provider. The disadvantage of a traditional model is that data on IoT could be compromised. This model's characteristics include a decentralised network, encryption of the user's identity, and a peer-to-peer network that allows data to be stored on a user device.

Reference :

[1] D. Christin, A. Reinhardt, P.S. MogreandR. Steinmetz, “Wireless Sensor Networks and the Internet of Things: Selected Challenges," Multimedia Proceedings of the Fifth International Conference on Inventive Computation Technologies (ICICT-2020) IEEE Xplore Part Number:CFP20F70-ART; ISBN:978-1-7281-4685-0978-1-7281-4685-0/20/$31.00 ©2020 IEEE 20 Authorized licensed use limited to: University of Edinburgh. Downloaded on June 15,2020 at 03:11:32 UTC from IEEE Xplore. Restrictions apply.Communications Lab, Technische Universität Darmstadt, Merckstr.25, and 64283 Darmstadt, Germany.

[2] Dorri,s. s. Kanhere,and R. jurdak,”Towards an optimized Blockchain for IoT,” in Proceedings of the Second International Conference on Internet-of-Things design and implementation, ser. IoTDI ’17,2017,pp. 173-178.

[3] Ouaddah, A., ELkalam, A. A., and Ouahman, A.A. (2017).Towards a novel privacy-preserving access control model based on Blockchain technology in IoT. In Europe and MENA cooperation Advances in Information and Communication Technologies s (pp.523-533). Springer, Cham.

[4] Tawfik, M., Almadni, A. M., & Alharbi, A. A. (2017). A Review: the Risks And weakness Security on the IoT. IOSR Journal of Computer Engineering (IOSR-JCE).

[5] Mehaseb Ahmed Mehaseb, Hadia El-Hennawyand Yasser Gadallah "A Software-Defined Device-to-Device Communication Architecture for Public Safety Applications in 5G Networks" Special section on recent advances in software defined networking for 5G networks.

[6] Jeon, J. H., Kim, K.-H., & Kim, J.-H. (2018). Block chain based data security enhanced IoT server platform. 2018 International Conference on Information Networking (ICOIN). doi:10.1109/icoin.2018.8343262.

[7] Olivier Alphand, Michele Amoretti, Timothy Claeys, and Simone Dall ’Asta, Andrzej Duda, et al.. IoTChain: A Blockchain Security Architecture for the Internet of Things. IEEE Wireless Communications and Networking Conference, Apr 2018, Barcelona, Spain. 2018.

[8] M. Pilkington, Blockchain technology: principles and applications. Research handbook on digital transformations, F. X. Olleros and M. Zhegu, Eds., 2016.

[9] Ali, M. S., Dolui, K., & Antonelli, F. (2017, October). IoT data privacy via blockchains and IPFS. In Proceedings of the Seventh International Conference on the Internet of Things(p. 14). ACM.

[10] Li, C., & Zhang, L. J. (2017, June). A blockchain based new secure multi-layer network model for Internet of Things. In 2017 IEEE International Congress on Internet of Things (ICIOT)(pp. 33-41). IEEE.

[11] Fan, K., Wang, S., Ren, Y., Yang, K., Yan, Z., Li, H., & Yang, Y. (2018). Blockchain-based secure time protection scheme in IoT. IEEE Internet of Things Journal.

[12] Fakhri, D., & Mutijarsa, K. (2018, October). Secure IoT Communication using Blockchain Technology. In 2018 International Symposium on Electronics and Smart Devices (ISESD) (pp. 1-6). IEEE.

[13] Muhtasim, M. A., Fariha, S. R., Rashid, R., Islam, N., & Majumdar, M. A. (2018, December). Secure data transaction and data analysis of IOT devices using blockchain. In 2018 International Conference on Circuits and Systems in Digital Enterprise Technology (ICCSDET) (pp. 1-8). IEEE.

[14] Agrawal, R., Verma, P., Sonanis, R., Goel, U., De, A., Kondaveeti, S. A., & Shekhar, S. (2018, April). Continuous security in IoT using Blockchain. In 2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) (pp. 6423-6427). IEEE.

[15] Wrona, K., & Jarosz, M. (2019, April). Use of blockchains for secure binding of metadata in military applications of IoT. In 2019 IEEE 5th World Forum on Internet of Things (WF-IoT)(pp. 213-218). IEEE.

[16] Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017, March). Blockchain for IoT security and privacy: The case study of a smart home. In 2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops) (pp. 618-623). IEEE.

[17] Kumar, R. P., & Smys, S. (2017). Analysis of dynamic topology wireless sensor networks for the Internet of Things (IOT). Int. J. Innov. Eng. Technol.(IJIET), 8, 35-41.

[18] Qian, Y., Jiang, Y., Chen, J., Zhang, Y., Song, J., Zhou, M., & Pustišek, M. (2018). Towards decentralized IoT security enhancement: A blockchain approach.Computers & Electrical Engineering, 72, 266-273.

[19] Chakraborty, S., Aich, S., & Kim, H. C. (2019, February). A Secure Healthcare System Design Framework using Blockchain Technology. In 2019 21st International Conference on Advanced Communication Technology (ICACT) (pp. 260-264). IEEE.

[20] Li, D., Peng, W., Deng, W., & Gai, F. (2018, July). A blockchain-based authentication and security mechanism for iot. In 2018 27th International Conference on Computer Communication and Networks (ICCCN) (pp. 1-6). IEEE.