International Journal of Innovative Research in Computer Science and Technology (IJIRCST)
ISSN(Online): 2347-5552, Volume-12, Issue-2, March 2024
https://doi.org/10.55524/ijircst.2024.12.2.18
Article ID IJIRD-1280, Pages 106-110
www.ijircst.org

Blockchain for Enhancing IoT Privacy and Security

Shweta Sinha

Associate Professor, Department of Computer Science and Engineering, Amity School of Engineering & Technology, Amity University, Gurugram, Haryana, India

Correspondence should be addressed to Shweta Sinha; shwetakant.sinha@gmail.com

Received 8 March 2024; Revised 21 March 2024; Accepted 30 March 2024

ABSTRACT- The technological advancements in the network technologies that deal with interconnected computing devices has led to the dramatic increase in the number of Internet of Things (IoT) devices. It promises to improve the convenience of our lives by leveraging to modernize the way day to day items are connected to various elements of existence by converting it to smart object. However, with the unprecedented convenience, accessibility, and efficiency, IoT has caused acute security and privacy threats in recent years, and it must be addressed properly. Due to the massive scale and distributed nature of IoT networks, overlooking these privacy and security issues will negatively impact many elements of our existence that involves our surroundings, and these effects will influence our own masses too. The national or jurisdictional boundaries are not restricted to the centralized cloud infrastructure that provides interconnectivity of IoT items, hence maintaining robustness, authentication and security becomes crucial. Recently, the development of blockchain technology is a plausible solution to offer such features. Security, authentication, and maintenance issues can be solved by the secure decentralization of blockchain and overcome the current IoT ecosystem's drawbacks. This paper highlights the IoT features and presents a IoT security and privacy problems are examined and classified in accordance with the IoT layered architecture. Further, we explore the IoT security and privacy challenges and examine blockchain technology towards a solution that help solve many of the IoT privacy and security issues.

KEYWORDS- Internet of Things, Blockchain, Privacy, IoT Features, Blockchain Characteristics.

I. INTRODUCTION

The Internet of Things (IoT) is an evolving domain and the devices along with the technology governing it has become widely used in numerous applications that seek to do away with human interaction. By transforming each physical object in our environment into a smart object that can detect the environment, communicate with the other smart objects, use reasoning, and appropriately respond to changes in the environment, it promises to make our lives more convenient. These intelligent items range in complexity from straightforward wearables like the smart wrist watches for recording and evaluating fitness data to much more complicated systems using complex infrastructures like auto-driven cars (SDV) for vehicular systems, surveillance systems, and grids using energy resources in distributed pattern [1][2]. However, the IoT's conveniences come with new security dangers and privacy concerns that need to be carefully handled. Hacking IoT devices could have a significant negative influence on the physical environment in addition to causing data leakage. The most prominent IoT attacks are Stuxnet [3] and Mirai DDoS attack [4] and these highlights the devastation caused due to misconfigured IoT devices. With the development of blockchain technology, a new strategy to control distributed transactions in the IoT environment has emerged. The main driving force behind the IoT's adoption of blockchain is to do away with centralization and mechanize a safe real-time transmission of data between IoT devices. This technology transforms the present centralized business models into decentralized ones by deploying distributed, public ledgers to permit unidentified transactions. [5]. Since modification or data tampering necessitates committing a new block, all transactions made on the blockchain network can be tracked, making the public ledger a useful cause of authentic footprints and artefacts. The Blockchain, like any new technology, has drawbacks, particularly when used in crucial IoT infrastructures. For instance, there are still a lot of unresolved problems in supply chain management for IoT sensors and healthcare while protecting patient data. The objectives in this paper can be summarized as follows:

- Discuss the IoT features and present a survey to find recent IoT security and privacy concerns in the literature and how they affect the various layers of an IoT system's architecture.
- Survey the literature and highlight capability of blockchain in IoT systems to overcome security and privacy issues.
- Inspect the challenges along with the security issues imposed by blockchain on blockchain-based IoT ecosystem.
- Recommend a way forward to integrate blockchain into IoT framework to create an efficient and secure system.

The rest of the paper is organized as follows: Section 2 delineates the IoT layered architecture and the challenges pertaining to the security and threats associated with it faced at each layer while discussing the IoT features, Section 3 outlines the characteristics of blockchain technology suitable for reliable and secure IoT systems, Section 4 underlines the difficulties in implementing blockchain in IoT devices in terms of security and privacy. In Section 5 we propose our framework for integration of the two technologies; the Blockchain and IoT and finally conclude the paper is in Section 6.

II. IOT FEATURES : SECURITY & PRIVACY CONCERNS

This section discusses some of the IoT features and the threats associated with them. These features have been identified based on the characteristics and usage of IoT devices.

A. Features

- **Interdependence:** In today's are the machine to human interaction has become easy and requires no human intervention. Needless to say, this has become possible due to the evolution of IoT. These IoT devices are controlled mainly by the environmental conditions and sometimes by other devices. This configuration leads to interdependence among the devices. It may not be possible to directly access and modify the behaviour of the target device but the affecting environment as well as the associated devices may be easily compromised by the attackers. This will affect the target devices too. The attackers can easily make use of this to reduce the difficulty to maliciously influence the target device.
- **Diversity:** The IoT network using heterogeneous devices are designed for defined tasks and require different environment to interact with. These individual requirements make the devices unique. For example, a small temperature sensor might run on a single chip with small flash and RAM, while an automatic industrial machine has higher performance than our smartphone. The communication need and protocol in different applications also differ. This phenomenon leads to an IoT feature; "diversity". The hard-coded key and common Web security vulnerabilities of the IoT devices could easily be used by attackers. Due to lack of practical security experience for new IoT functions such as IoT device bootstrapping [6], the recently developed protocols usually have many potential security problems. For instance, Liu et al. [7] found the attacker could exploit several vulnerabilities of Joy link protocol [8], such as insufficient device authentication. Moreover, different protocols have different semantic definitions, the attackers could also take advantage of this point to find security vulnerabilities like Bad Tunnel [9].
- **Constrained:** With the limitation of cost and physical conditions, many IoT devices are of tiny size; especially industrial sensor, and implantable medical devices, have been designed to be lightweight and small. They have much less computing ability and storage resources than traditional computers or mobile phone. The limitation of the computing/storage resource, power supply and latency of IoT devices is the feature called the "constrained". Attackers could easily intercept communication or launch man-in-the-middle (MITM) attack as many IoT devices even communicate with the server without any encryption.
- **Unattended:** With the rapid growth of wireless sensor, there are smart devices such as home Smart meters, implantable medical devices (IMDs) and sensors in the special industrial, agricultural and military environment that have to operate for a long period of time without being physically attended. The long-time unattended status of IoT devices is an IoT feature named "unattended". In such settings, it is hard to physically connect an external interface to verify the state of these devices. Thus, the remote attacks targeting them are difficult to detect
- **Mobile:** Many IoT devices, such as wearable devices and smart cars are used in the mobile environment. These mobile IoT devices usually hop from one network environment to another and communicate with many unknown new devices. This frequent movement of IoT devices is termed as an IoT feature named "mobile". Because mobile IoT devices usually join more networks, attackers tend to inject the malicious code into mobile IoT devices to accelerate its spread.
- **Ubiquitous:** The IoT devices have pervaded every aspect of our lives. We do not just use them, but also rely more on them. The presence of IoT devices everywhere in our future lives, is an IoT feature named "Ubiquitous". Due to this pervasive nature many a times IoT products are used without paying much attention and may lead to severe vulnerabilities due to lack of inbuilt safety measures.

B. Challenges with IoT Security and Privacy

All IoT system has a few requirements concerning to the security of the system. They are namely, Confidentiality to ensure that any private information can only be viewed and accessed by authorized parties only, Integrity to ensure the any unauthorized person is not able to modify or corrupt the information, Availability such that the information is immediately accessible to the authorized parties when the need be and Authentication to access the information after verification of identity [10]. However, including these elements in an IoT system presents several difficulties [10]. First and foremost, maintaining the security of IoT system entities must be done with minimal impact on their functionality. Any security measures used need to be adaptable enough to protect each of these entities. The potential for security threats grows along with the quantity and variety of IoT entities. The threats associated with IoT are tightly knit to the IoT architecture, influence every layer in the IoT architecture, jeopardizing that layer's security needs. Although there isn't a defined and widely accepted IoT architecture, researchers recently suggested a four-layer architecture. The next section discusses the threats and its influence on the layers of IoT architecture.

C. IoT Layered Architecture

Researchers have defined four layers; the perception layer, the network layer, the processing layer, and the application layer in the IoT layered architectures [11]. The first layer, the Perception Layer is responsible for collecting an enormous data unit through sensors from the surrounding environment. In addition to collecting data from surroundings, it is responsible for successfully transmission of the data for further processing. The major threats faced by IoT system at this layer are in the physical environment. Elements or items in the IoT system can be harmed or abandoned by nature forces and also individuals can damage or steal the items in the IoT setup. Moreover, technologies like RFID, Bluetooth, and Zigbee at the Perception layer are at danger of multiple attacks like This scenario is referred as Selective forwarding attack.The Network Layer reliably transmits the data from the perception layer to the layer above it, i.e., the processing layer using any of the wired or wireless network. This layer is further responsible for analytics, rapid processing, and vast data storage using data centers, edge computing, and cloud computing. All IoT system's security components are at danger due to this.

In the end, at the Application Layer the need is to fulfill end user's request and here the data and information are combined and presented in a required format. This layer is vulnerable to social engineering attack like phishing attack and software attacks like buffer overflow. IoT has been widely employed in a variety of fields, including healthcare, business, transportation, smart homes, and smart grids.

III. BLOCKCHAIN FOR IOT SYSTEMS

The Blockchain technology uses a decentralized approach to data management and storage and distributes shared, secure ledgers to all participants. It removes the use of third-party authority for managing and storing data. Along with providing data exchange in a decentralized manner it maintains a peer-to-peer communication while providing data integrity and transparency. This section presents an overview of blockchain and IoT integration to look into the advancements in security that blockchain augments to IoT security and privacy.

A. Blockchain Fundamentals

With the success of blockchain in Bitcoin researchers have explored its ability to influence other areas also. Blockchain is a regionalized, scattered and immutable record that stores transaction details of P2P network. SHA-256 hashing is used to preserve data authenticity and integrity. Each connected block has a list of transaction details along with the hash of preceding and following block. This makes blockchain unalterable against exploitation and develops a trusted network which is easily retractable. Based on the privileges nodes of the chain have the blockchain platform can further be categorized as Public, Private and Consortium blockchain.

An open-source platform called public blockchain enables anybody to join the network anonymously and grants each node full network capabilities, including the ability to validate transactions and read and write data [12]. Public blockchains have their own security flaws and threats. Private blockchain is a decentralized network that permits data exchange between specified nodes in a particular organization. A consortium blockchain is a partially or semi-private blockchain in which a few companies or individuals oversee validating transactions and committing blocks. Each block is verified using a multi-signature system, which requires the consent and signature of all controlling nodes. They can at any time remove credentials and assign nodes to read or write on the network [13].

B. Blockchain Enabled Privacy and Security for IoT

Blockchain can be utilized in IoT applications to provide improved services to IoT that requires trusted and decentralized services. Blockchain's decentralized structure might help IoT applications avoid serious centralized security problems like single points of failure and ensure the swiftness of IoT controlled services.. To create and assign a large number of addresses that can be regarded as secure and distinctive and also that can be assigned to IoT devices a blockchain uses 160-bit address space as hashed public key. This has been created by ECDSA (Elliptic Curve Digital Signature Algorithm). To ensure data immutability and reliability, transactions made in the network are also irreversible and trackable.

Throughout an IoT device's lifespan, the owner may change, necessitating the use of an effective and secure identity management system. Manufacturer, GPS coordinates, serial number, kind, and other IoT device-related attributes all require secure and reliable management [14]. Additionally, since only the user with the associated private key can decrypt encrypted data, all nodes can store and handle data without jeopardizing its confidentiality.

Blockchain has the potential to reduce the issues over the complete life cycle of an IoT device. With the use of a decentralized and distributed ledger, it can handle connected IoT devices' complicated properties and relationships as well as their authorized and reliable identities.

IV. BLOCKCHAIN INTEGRATION TO OVERCOME IOT SECURITY

This section presents the overview of utilization of blockchain approaches in IoT in recent years and then discusses the limitations still associated with the Blockchain-IoT integration.

A. Blockchain for IoT Paradigm:

Security of Communications: The messaging protocol is crucial for the development of IoT applications, particularly in industries where M2M communications is required for dependable and effective channels for data transmission. MQTT and AMQP are a few examples of developing messaging protocols [15]. Many light-weight cryptographic algorithms [16][17] have been devised in blockchain for proof of authentication. They can be extended very easily to IoT devices.

- **Protection and Security:** To address the issue of security in IoT information sharing, a blockchain framework is defined [18]. It creates data blocks that safeguard data integrity via a consensus technique. The framework was determined to be exceptionally resilient against six attacks, including device injection attacks and DDoS and DoS attacks. Moreover, it was discovered that the framework is both highly and somewhat resistant to attacks like modify attack and consensus cycle attack.
- **Access Control:** By granting and removing user privileges, centralized access control systems guarantee data security while not considering the

drawback of a single point of failure. But blockchain technology can get over this restriction by giving a decentralized access control manager to give or cancel permissions to users of diverse IoT architectures. Authors suggested an access control technique in [19] that makes use of blockchain technology to provide access policies to users who want to share resources.

- **Optimization and Scalability:** The overall response time and transaction throughput is a challenge in IoT world. Blockchain technology can be a help to reduce the overhead associated with transaction auditing. Authors in [20] designed an optimized and adaptable memory to help with the blockchain's astronomical growth in size for IoT applications the permanent category where the transactions are kept permanently and then from those stored certain transactions are selected and summary of that is created to obtain a summarized category [21].

V. BLOCKCHAIN INTEGRATION TO IOT ARCHITECTURE: A FRAMEWORK FOR SECURE SYSTEM

The conventional IoT centric security mechanisms can be combined with blockchain technology to obtain efficient and secure integration. The blockchain integration can be done to IoT layered architecture to obtain the optimized output.

A. Perception layer

Low storage capacity devices, denial of service attacks, and object theft are the difficulties that the perception layer of IoT architecture faces the most. A new device can only become the part of the network with the consent of the network minor, who are needed to first solve a riddle to verify the new device (proof-of-identity). As a result, information produced by IoT devices linked to a network is encrypted, given a specific public and private key, and then sent to the blockchain.

B. Network layer

The IoT gadget can begin communicating its encrypted data by committed blocks as soon as it is connected to the network. By maintaining the ledger on each participant machine and assigning unique privileges to each item when it joins the network, the distributed ledger may meet these two needs.

C. Processing layer

As an alternative to managing data storage on a central cloud architecture, it is suggested that IoT systems use a combination of private and public blockchain networks. Use of a timestamp to record transactions on a public blockchain ensures data immutability, non-repudiation, authenticity, and integrity. Also, sometimes when a request is made to reveal any user's confidential information with a trustworthy third party for analytics, blockchain can act as a reliable communication layer.

D. Application layer

When data is retrieved from processing layer, it is presumed to be authentic and is then visualized by this layer. In the next step the application layer securely access data stored on the blockchain network for analytics and provide immediate replies is the next step. However, since the blockchain network is being used, no servers are needed to view large data sets for analytics, and all genuine IoT devices that have joined the network.

VI. CONCLUSION

With the growth in IoT devices the concern toward its security and privacy has to be increased. With the success of blockchain in Bitcoin, the blockchain has emerged as a potential technology for maintaining the privacy in IoT as well. While combining blockchain in IoT environment, there may be some serious security and applicability difficulties. With the purpose to identify potential security and privacy vulnerabilities and further to reduce these risks through the use of blockchain technology, this paper evaluates the requirements for IoT security based on its 4-tier architecture. Additionally, this research paper identifies recent security issues that have arisen as a result of the adoption of blockchain in IoT systems and identifies further study to identify potential remedies. To guarantee an efficient integration the proposed architecture incorporates few changes for an effective and safe integration of blockchain and IoT.

REFERENCES

[1] F. S. Ali, M. Aloqaily, O. Alfandi, and O. Ozkasap, "Cyberphysical blockchain-enabled peer-to-peer energy trading," Computer, vol. 53, no. 9, pp. 56–65, 2020.

[2] M. Aloqaily, A. Boukerche, O. Bouachir, F. Khalid, and S. Jangsher, "An energy trade framework using smart contracts: Overview and challenges," IEEE Network, vol. 34, no. 4, pp. 119–125, 2020.

[3] D. Kushner, "The real story of stuxnet," IEEE Spectrum. [Online]. Available: https://spectrum.ieee.org/the-real-story-of-stuxnet, 2013.

[4] I. Arghire, "Mirai-based botnet launches massive DDOS attack on streaming service," 2019.

[5] H. Subramanian, "Decentralized blockchain-based electronic marketplaces," Commun. ACM, vol. 61, no. 1, pp. 78–84, 2017.

[6] Network Working Group Internet-Draft, "Secure IoT Bootstrapping: A Survey." [Online]. Available: https://datatracker.ietf.org/doc/draft-irtf-t2trg-secure-bootstrapping/.

[7] H. Liu et al., "Smart solution, poor protection: An empirical study of security and privacy issues in developing and deploying smart home devices," in Proceedings of the 2017 Workshop on Internet of Things Security and Privacy, pp. 13–18. Nov. 2017

[8] JD, "Joylink." [Online]. Available: https://smartdev.jdcloud.com/.

[9] Y. Yang, "BadTunnel: NetBIOS Name Service spoofing over the Internet." [Online]. Available: https://www.blackhat.com/docs/us-16/materials/us-16-Yu-BadTunnel-How-Do-I-Get-Big-Brother-Power.pdf.

[10] H. Liu et al., "Smart solution, poor protection: An empirical study of security and privacy issues in developing and deploying smart home devices," in Proceedings of the 2017 Workshop on Internet of Things Security and Privacy, pp. 13–18, Nov. 2017.

[11] I. Lee, "The Internet of Things for enterprises: An ecosystem, architecture, and IoT service business model," Internet of Things, vol. 7, p. 100078, 2019.

[12] A. C. Jaiswal, S. Sinha, and P. Makkar, "Using TRPO to control quadruped gait behaviors," Journal of Integrated Science and Technology, vol. 11, no. 4, pp. 574-574, 2023.

[13] J. Gu, B. Sun, X. Du, J. Wang, Y. Zhuang, and Z. Wang, "Consortium blockchain-based malware detection in mobile devices," IEEE Access, vol. 6, pp. 12118-12128, 2018.

[14] S. Sinha, A. Agrawal, A. Singh, and P. Raj, "Transforming interactions: mouse-based to voice-based interfaces," Telecommunications and Radio Engineering, vol. 79, no. 14, 2020.

[15] N. Naik, "Choice of effective messaging protocols for IoT systems: MQTT, CoAP, AMQP and HTTP," in 2017 IEEE International Systems Engineering Symposium (ISSE), Oct. 2017, pp. 1-7.

[16] D. Puthal and S. P. Mohanty, "Proof of authentication: IoT-friendly blockchains," IEEE Potentials, vol. 38, no. 1, pp. 26-29, 2018.

[17] S. Sinha and P. Makkar, "Wireless sensor networks: Concepts, components, and challenges," in Security and Privacy Issues in IoT Devices and Sensor Networks. Academic Press, 2021, pp. 1-27.

[18] H. Si, C. Sun, Y. Li, H. Qiao, and L. Shi, "IoT information sharing security mechanism based on blockchain technology," Future Generation Computer Systems, vol. 101, pp. 1028-1040, 2019.

[19] D. Singh, S. Sinha, and V. Thada, "Review of attribute based access control (ABAC) models for cloud computing," in 2021 International Conference on Computational Performance Evaluation (ComPE), Dec. 2021, pp. 710-715.

[20] S. Mehrotra, S. Sinha, and S. K. Sharma, "Overview of the Internet of Things and Ubiquitous Computing," in Blockchain Technology for Data Privacy Management. CRC Press, 2021, pp. 1-19.

[21] A. Dorri, S. S. Kanhere, and R. Jurdak, "MOF-BC: A memory optimized and flexible blockchain for large scale networks," Future Generation Computer Systems, vol. 92, pp. 357-373, 2019.