IoT Privacy and Security: A Blockchain Approach

Rajeev Kumar Chopra
RIMT University, Mandi Gobindgarh, Punjab
Email id- ranjeevk.chopra@rimt.ac.in

ABSTRACT: Blockchain has a lot of potential in the coming years. It is indeed a system that allows you to create and share tamper-proof transactional general ledger. Blockchain applications are growing in quantity and breadth in a variety of fields, including the Internet of Things (IoT), economics, and cybersecurity. Despite the fact that several government and commercial sectors are adopting such system, it remained a source of concern for others owing to a dearth of acquaintance or the fact that it has yet to play a significant part in any large security businesses. This paper describes what a blockchain is, as well as its features, advantages, and distinctions apart from assisting individuals in selecting the appropriate kind to meet the requirements. Afterwards the paper discusses the integrity of blockchain along with its advantages, as well as how it compares to a conventional system. Lastly, we'll look into blockchain security, evaluate it to traditional data protection, and make a comparison in various security situations. Future research will target on establishing what IoT devices are best suited for adopting blockchain-based protection mechanisms on a larger scale, as well as how to efficiently deploy the blockchain or decentralised ledgers that allow IoT.

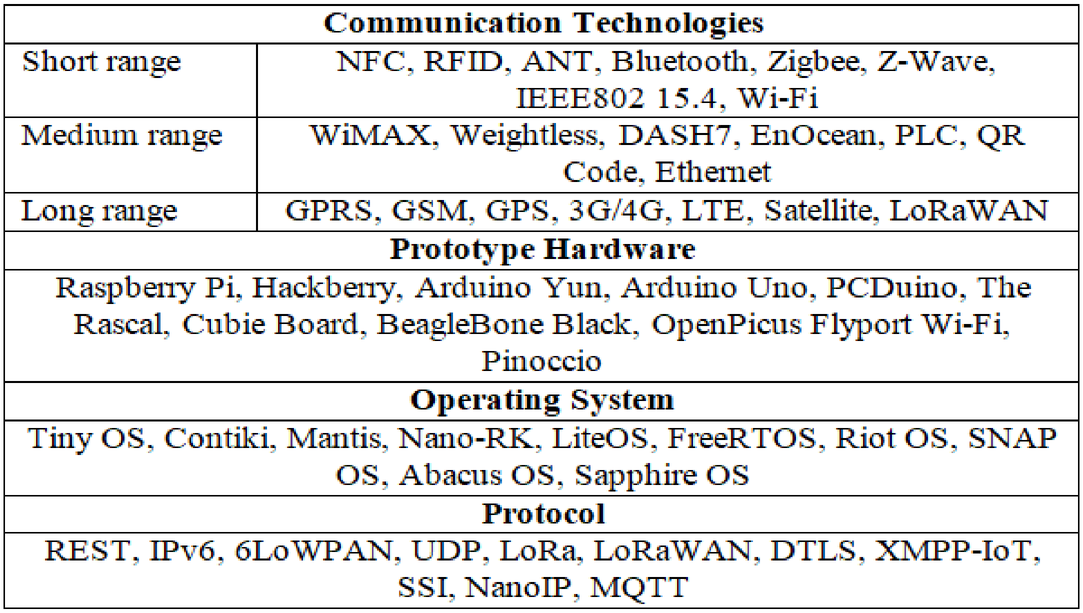
KEYWORDS: Blockchain, Internet of Thing, Privacy, Security, Systems.

1. INTRODUCTION

The Internet of Things (IoT) is gaining popularity as a digital communications revolution which enables continuous, consistent, and automatic device-to-device (D2D) interaction. IoT devices produce, analyse, and share massive quantities of secure as well as confidential data, making them attractive candidates for different cyber assaults [1]. Many of the new gadgets utilized in IoT systems are small and energy efficient. Such gadgets should dedicate the majority of its energy available and processing power in performing essential functions, making it difficult to provide safety and confidentiality in a cost-effective manner. In terms of power usage and computational complexity, conventional protection techniques are sometimes too costly for IoT. Furthermore, owing to the difficulties of scalability, the many-to-one characteristics of the transmission, as well as single point of failure, several frameworks related to security are extremely centralized and therefore are not inevitably well enough for IoT systems. Some of the IoT technologies are illustrated in Table 1.

Blockchain is a distributed, unchangeable record that makes documenting transactions and monitoring resources in a corporate network more easier [3]. It's a data-storage technique that makes it difficult to breach the network or alter the content recorded on it, rendering it safe and unchangeable. It's a computerized system for simultaneously capturing transactions and associated statistics in many locations. To avoid a solitary source of malfunction, every device in a public ledger keeps a record of transactions, and all instances are updated and verified at the same time. A blockchain is a digital ledger that organizes data into units called blocks, each of which contains a collection of data [4]. Blocks have specific storing capacity, and when they're full, they're chained onto the preceding block, creating a data chain. The asset may be physical, such as a home or a vehicle, or intangible, such as inventions or trademarks. On a blockchain network, almost anything of importance may be monitored and exchanged, lowering risk and improving efficiency for all concerned parties. When a block is added to the chain, it is assigned an accurate timestamp which cannot be changed or updated.

Table 1: Illustrates the Internet of Thing (IoT) Technologies [2]**.**



Communication Technologies	
Short range	NFC, RFID, ANT, Bluetooth, Zigbee, Z-Wave, IEEE802 15.4, Wi-Fi
Medium range	WiMAX, Weightless, DASH7, EnOcean, PLC, QR Code, Ethernet
Long range	GPRS, GSM, GPS, 3G/4G, LTE, Satellite, LoRaWAN
Prototype Hardware	
Raspberry Pi, Hackberry, Arduino Yun, Arduino Uno, PCDuino, The Rascal, Cubie Board, BeagleBone Black, OpenPicus Flyport Wi-Fi, Pinoccio	
Operating System	
Tiny OS, Contiki, Mantis, Nano-RK, LiteOS, FreeRTOS, Riot OS, SNAP OS, Abacus OS, Sapphire OS	
Protocol	
REST, IPv6, 6LoWPAN, UDP, LoRa, LoRaWAN, DTLS, XMPP-IoT, SSI, NanoIP, MQTT	

The paper serves as an outline and argumentative piece for the usage of Blockchain technologies in IoT security. Previous approaches for protecting individual confidentiality frequently expose distorted or partial information that could make it difficult for certain IoT systems to provide better experience. As a result, IoT necessitates a safety and confidentiality protection that is compact, flexible, as well as dispersed. Because of its decentralized, secured, and private nature, the Blockchain technology that underlies Bitcoin's, the first crypto currency platform, seems to have the potential to solve the aforesaid problems. Further, the most common uses of blockchain technology have been around for the implementation of monetary operations, intelligent agreements, and crypto-currencies. New prospective uses, on the other hand, are developing.

2. LITRATURE REVIEW

Dorri et al. go into more detail and describe the different basic elements and functionalities of the home automation in a study [5]. Every home-automation comes with a "miner," a device that is constantly online and handles every communication both inside and outside the house. The miner also maintains a safe and highly protected Blockchain, which is utilized for information sharing supervision and inspection. The authors demonstrate the trustworthiness of the suggested Blockchain-based home automation architecture by carefully examining it in terms of the basic security objectives of secrecy, authenticity, and accessibility. Eventually, they provide simulated results showing that the operating costs imposed by their method are negligible in comparison to the privacy and security benefits it provides.

Kshetri assesses the significance of distributed ledger in enhancing data protection in IoT [6]. The fundamental processes underpinning the blockchain-IoT security relation are discussed. In terms of protection, the study demonstrates how ledger technologies may be better in many ways to the existing IoT environment that is built mostly on centralised data centres. The author claims that Blockchain's decentralized structure is expected to yield in minimal susceptibility to modification and falsification by malevolent actors, utilizing real world examples and implementations. The use of blockchain-based authentication and authorization systems to solve a few of the major issues related with IoT security has been granted some special attention. The study goes into the function of blockchain in monitoring the origins of vulnerability in distribution networks including smart nodes in great detail. It is also feasible to contain an IoT security compromise in a tailored manner utilizing blockchain once it has been detected. The study also examines and analyses blockchain-related efforts from enterprises, interdepartmental connections, and businesses.

In this paper, Banerjee et al. survey articles presenting IoT security solutions published in English since January 2016 [7]. They make a number of observations, including the lack of publicly available IoT datasets that can be used by the research and practitioner communities. Given the potentially sensitive nature of IoT datasets, there is a need to develop a standard for sharing IoT datasets among the research and practitioner communities and other relevant stakeholders. Thus, they posit the potential for blockchain technology in facilitating secure sharing of IoT datasets using blockchain to ensure the integrity of shared datasets and securing IoT systems, before presenting two conceptual blockchain-based approaches. They then conclude the paper with nine potential research questions.

3. DISCUSSION

3.1. Security Issues and Internet of Thing (IoT) Framework:

IoT offers a broad range of applications, and its adoption is accelerating. It functions according to how it was built or developed, depending on the many utility areas of the IoT. In a quintessential IoT implementation, diverse gadgets having sensing devices embedded are networked together. IoT devices are easily distinguished by their minimal energy consumption, tiny storage, as well as restricted computing capacity. The gateways are used to link IoT objects to the external environment so that resources and applications may be delivered to IoT consumers remotely. However, it lacks a well-defined functioning framework that is generally adopted. The framework of the IoT is determined by its usefulness and application in various industries. Even yet, the IoT is constructed on a fundamental procedural flow. Thus, in this paper, the authors will describe the 4-Stage IoT design as depicted in Fig. 1, which is the core essential framework of the IoT.

3.1.1. Accounting, Authorisation and Authentication:

Authentication is needed among involved individuals interacting in the IoT to safeguard their conversation. The gadgets should always be authenticated in order to have elevated access to essential resources. Because of the many diversified fundamental frameworks and ecosystems supporting IoT devices, there is a wide range of authentication methods for IoT. These conditions make establishing a uniform worldwide standard for IoT authentication difficult. Similarly, authorisation procedure guarantees that only those who are permitted have information or service accessibility. A trusted environment is created by properly implementing permission and authentication, which provides a robust information network. Furthermore, service utilization accounting, as well as monitoring and reporting, offer a dependable method for network administration security.

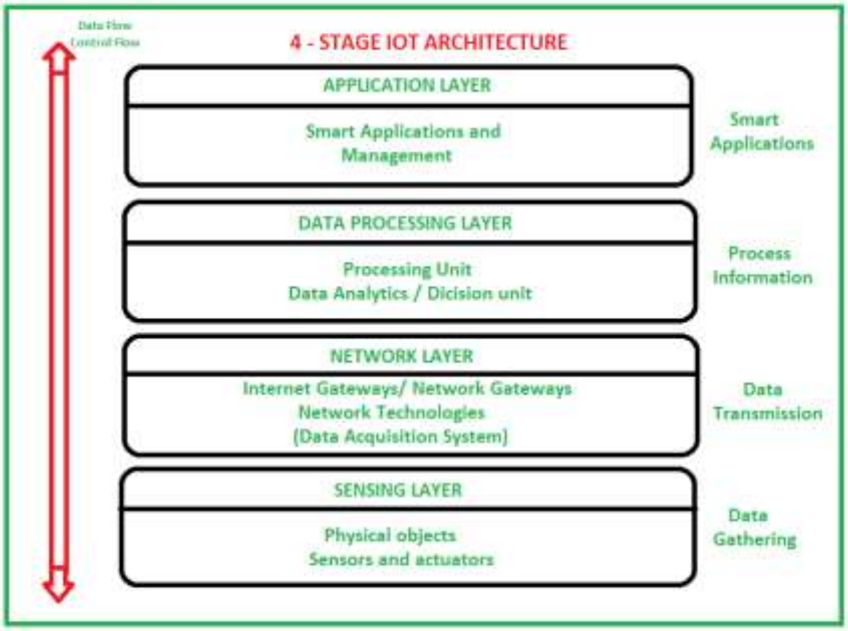


Fig. 1: Illustrates the Internet of Thing Framework [8]**. The first layer consists of physical objects like sensors for gathering data, second layer consists of network gateways for data transmission, third layer consists of processing unit for data processing, and the last layer being application layer for smart application management.**

3.1.2. Efficiency in Terms of Energy:

IoT devices are generally resource-restricted, with minimal energy consumption and limited memory capacity. By overloading the network and depleting IoT resources via repeated or faked service requests, attacks against IoT designs might lead to a surge in energy usage.

3.1.3. Service Accessibility:

Using traditional denial-of-service (DOS) cyber-attacks, breaches against IoT systems may obstruct the supply of services. Several methods, such as sinkhole attacks that occur when a hacked node attempts to capture network traffic by announcing a bogus routing change, jamming adversaries where an attacker sends out a long-range signal to interrupt communication, and playback attacks in which legitimate data transfer is deliberately or fraudulently replayed or delayed, exploit IoT components at various levels to degrade the quality-of-service (QoS) offered to IoT consumers.

3.1.4. Confidentiality, privacy, and integrity of data:

Because IoT data goes via many steps in a system, it necessitates the use of an encryption method to guarantee data security. The data saved on a machine is susceptible to privacy violations by compromised components in an IoT system due to a varied integration of services, equipment, and networks. Because IoT devices are vulnerable to cyber-attacks, an intruder may compromise integrity of data by altering it for nefarious reasons.

3.1.5. Single failure points:

Rapid expansion of diversified systems for IoT-based architecture could potentially expose a substantial proportion of single failure points, resulting in deterioration of IoT-based applications. It requires the creation of a tamper-proof infrastructure for a huge amount of IoT equipments, and also alternate methods for fail-proof network deployment.

3.2. Categories of Security Problems:

Because IoT includes a broad range of gadgets and gears, from tiny embedded processor to huge upscale servers, it must handle security and privacy concerns at many levels. Fig. 2 shows a categorization of IoT security and privacy concerns. The authors classify the security risks in relation to the IoT infrastructure as stated hereunder.

- High-level
- Moderate-level
- Low-level

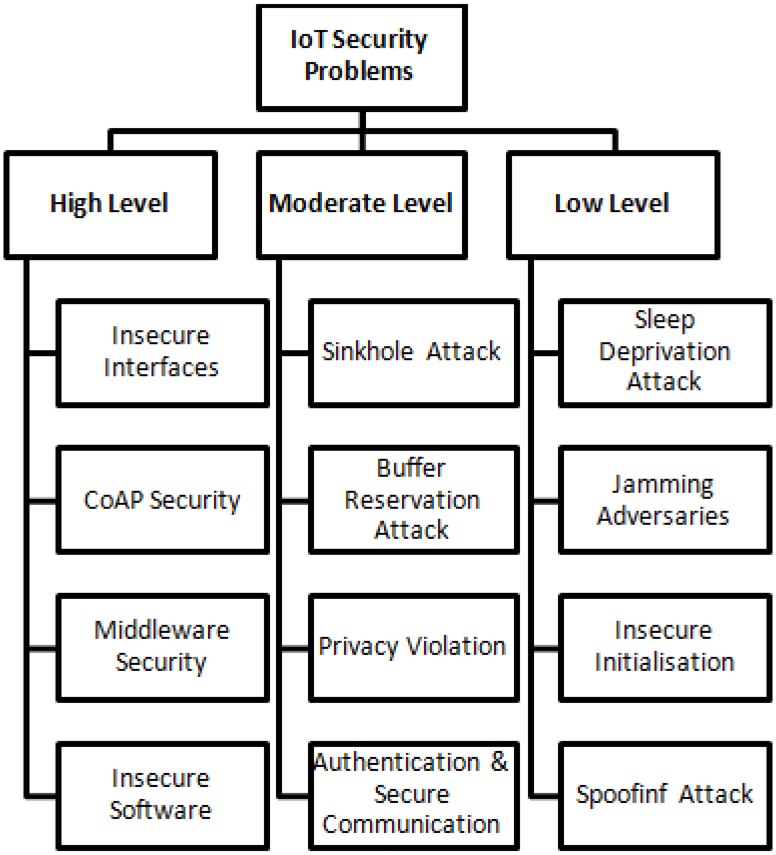


Fig. 2: Illustrates the categories of security problems in Internet of Thing environment [9].

3.3. Blockchain Security:

The blockchain is a system that permits transactions to be confirmed by a number of untrustworthy individuals. It creates a public ledger that is unchangeable, accessible, secured, and verifiable. The blockchain may be examined in an open and comprehensive manner, enabling transparency to all transactions that had already happened from the system's inception, and therefore may be checked and compiled by any party at a certain point. The blockchain system organizes data into a series of chunks, each of which contains a list of Bitcoin transactions completed at a specific point in time. A network is formed when units are chained consecutively with a reference to the preceding unit. Network neighbours need to deliver the essential functions like storage, routing etc. to maintain and administer the blockchain [10]. Various kinds of endpoints might be included within the system depending on the functionality they are capable of providing.

The networking functionality, which comprises transactions and blocks transmission, is expected to undergo in a distributed system. The node's memory mechanism is in charge of maintaining a record of the chain. Users can initiate transaction, or operate using the crypto currencies, using digital certificates provided by digital wallets. Lastly, by completing the proof of work, the mining functionality is in charge of constructing fresh blocks. Miners are endpoints that do proof of work, or mining, so they are rewarded with newly created crypto currencies and service charges. One of the elements to enabling trust free agreement in a public ledger is the concept of proof of work. A complex analytical operation is required for the production of units in the proof of work. This assignment must've been difficult to solve while yet being readily verifiable once finished.

3.4. Integration of Internet of Thing (IoT) and Blockchain:

Primarily, blockchains may be used in the IoT to guarantee the authenticity of transactional data. It's worth noting that the processes described earlier add to the total complexity of an IoT platform, particularly if the peer-to-peer (P2P) infrastructure is developed worldwide. Due to the obvious constraints of edge devices, it could not very well be feasible to have a fully blockchain-secured system in the general IoT sense. However, many such important implementations, including such smart contract, smart grids, digital insurance and e-health, may have reasonable potential to aid the required P2P features. One more option is to create P2P systems with a natively narrow capability rather than a broader system.

Additionally, the amount of blocks to be analysed and saved may be reduced. Based on the available processing and storing power of IoT nodes, the possible limits of incorporating these functions in generalized IoT edge devices to build blockchains may be obvious, and chain abilities therefore ought to be deployed in specific networking components in the network. An IoT node, such as a distant sensing device, is unlikely to vouch for the authenticity of the whole ecosystem's data. Therefore, only a few chosen components might well be poised to bring on that more difficult job. Depending on the functional criteria, one alternative would be to utilize a basic blockchain system wherein transactions are cryptographically signed alongside however a complex consensus mechanism is not really implemented.

3.5. Future of Blockchain:

Blockchain has a plethora of intriguing possible applications. It's a subject which always gets a lot of attention and meets the requirements for a lot of other exciting new developments. IoT, robotics, intelligent gadgets, and driver-less automobiles are just a few examples. It could serve as an enabler for all of the concepts indicated above, along with many others. Consider the concept of an intelligent fridge that records "Need Milk" as soon as it runs out of it. On contemplating such an application, many individuals become uncomfortable and afraid because they are concerned about privacy and how to safeguard it. What guarantees the security and un-traceability of the system's information? One more factor worth mentioning is the ever-decreasing cost of gadgets and the ever-increasing need for computation power.

4. CONCLUSION

IoT devices nowadays are unsafe and are unable to protect itself. This is largely because of lack of secured design of software and hardware, deployment in IoT devices and its implementation, as well as limited resources in IoT devices, maturing standardization etc. From both an academic and an industry standpoint, cyber security, especially IoT security, is receiving a greater focus these days. Due to significant power utilization and computational complexity, conventional security approaches are not always suitable for IoT. We examine and analyse key IoT security problems in this research, and suggest a solution for addressing these issues by utilizing the Blockchain that is an unchangeable record of blocks. One of the most significant benefits of blockchain is its recovery capacity from a variety of attacks and vulnerabilities. It does have a lot of new features too, such as enhanced dependability, failure resistance, processing time, and expandability. We described the many fundamental components of the Internet of Things in this study, as well as the numerous transactions and processes connected with it. Future work will focus on determining which IoT applications are most suitable in implementing blockchain-based protective measures on a broader level, as well as how the blockchain or decentralised ledgers that enable IoT can be deployed effectively. We'll look at how the framework may be used in various IoT-related projects.

REFERENCES

[1] A. H. Ngu, M. Gutierrez, V. Metsis, S. Nepal, and Q. Z. Sheng, “IoT Middleware: A Survey on Issues and Enabling Technologies,” *IEEE Internet Things J.*, 2017, doi: 10.1109/JIOT.2016.2615180.

[2] M. Gloukhovtsev, “IoT Security: Challenges, Solutions & Future Prospects,” pp. 1–44, 2018, [Online]. Available: https://education.dellemc.com/content/dam/dell-emc/documents/en-us/2018KS_Gloukhovtsev-IoT_Security_Challenges_Solutions_and_Future_Prospects.pdf.

[3] T. T. Kuo, H. E. Kim, and L. Ohno-Machado, “Blockchain distributed ledger technologies for biomedical and health care applications,” *Journal of the American Medical Informatics Association*. 2017, doi: 10.1093/jamia/ocx068.

[4] L. Carlozo, “What is blockchain? Here is a primer on the potentially transformative digital ledger technology,” *J. Account.*, 2017.

[5] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, “Blockchain for IoT security and privacy: The case study of a smart home,” 2017, doi: 10.1109/PERCOMW.2017.7917634.

[6] N. Kshetri, “Can Blockchain Strengthen the Internet of Things?,” *IT Prof.*, 2017, doi: 10.1109/MITP.2017.3051335.

[7] M. Banerjee, J. Lee, and K.-K. R. Choo, “A blockchain future for internet of things security: a position paper,” *Digit. Commun. Networks*, vol. 4, no. 3, pp. 149–160, Aug. 2018, doi: 10.1016/j.dcan.2017.10.006.

[8] geeksforgeeks, “Architecture of Internet of Things (IoT).” https://www.geeksforgeeks.org/architecture-of-internet-of-things-iot/ (accessed Aug. 18, 2017).

[9] M. A. Khan and K. Salah, “IoT security: Review, blockchain solutions, and open challenges,” *Futur. Gener. Comput. Syst.*, vol. 82, pp. 395–411, 2018, doi: 10.1016/j.future.2017.11.022.

[10] A. M. Antonopoulos, A. Çarkacıoğlu, and İ. Kırbaş, “Mastering Bitcoin: Unlocking digital cryptocurrencies,” *Sermaye Piyas. Kurulu Araştırma Dairesi*, 2014.