ISSN: 0974-5823 Vol. 7 No. 2 February, 2022

International Journal of Mechanical Engineering

A Review of Challenges to Security in IoT

Srivalli Ch[1], Dr.Vinay Chavan[2]

[1]Faculty, Institute of Insurance and Risk Management, Gachibowli, Hyderabad

[2] Associate Professor, Head, Department of Computer Science, Seth Kesarimal Porwal College, Kamptee, Nagpur

Abstract

As smart devices are increasingly getting deployed in distinct scenarios it is important to examine how the various demands of these practical uses will affect the dynamics of protection. The Internet of Things (IoT) is a long-term technological vision in which items will be able to speak with one another and connect to the internet to create self-configuring, intelligent systems. The majority of IoT apps complete tasks without the involvement of humans or physical objects. Current and future gadgets must be smart, efficient, and capable of providing services to users in order to deploy such a new technology in a secure manner. As a result, researchers are investigating security concerns on a daily basis. As IoT devices are so small and light, they have a number of difficulties, including battery consumption, memory and as they operate over a wide range they have the issues of security also. We have discussed security attacks with reference to several types of IoT layers in this review paper.

Keywords:-IOT, security, privacy, IOT architecture, solutions

Introduction

The internet of things revolutionises how data from the real world is accessed. Thousands to millions of small sensor networks with unique computing and networking capabilities to sense the environment make up the backbone of smart appliances. When these instruments are networked together, they can provide exceptionally dependable and resolved information about the observed phenomenon. There are certain issues that arise during the incorporation process. According to the [1] report, "the expected things that will be connected are 8.4 billion all over the world in 2020 and this number will be approximately increased to 20.4 billion in 2022. Increment in the usage of IoT applications in all the scenarios over the worldwide, the growth of connectivity between the machines is expected from 5.6 billion and will be increased up to 27 billion from 2016 to 2024" [1]. The wide range of IoT Application usage some privacy & security, authentication, and storage issues have been raised and it's a challenging topic, for now, a day between the research communities. Without a secure environment and infrastructure, it's very difficult to use the IoT application with full features and in a trustable manner. According to [2] "in 2017 attacks against IoT devices has been increased by 600 percent. Usually, attackers are not targeting IoT edges directly but use it as a weapon to access other sites."

IoT will be used in practically every field, including industry, government, and consumer sectors, according to a report by International Data Corporation (IDC). Furthermore, 20 percent of IoT companies will leverage Blockchain's basic services. In addition, nearly 75% of all IoT manufacturers will strengthen their security capabilities, making them more appealing to purchasers.

"Blockchain is formed using a linked data structure where the first block is known as the foundation/genesis block and the respective blocks each is linked to the previous block in the chain by storing the digital hash code of the previous block" [3]. With each new transaction, a new block is appended to the chain of blocks.

Blockchain has the following characteristics

- **Decentralization** - Because Blockchain is based on a distributed ledger, each node stores a copy of the transaction. As a result, there is no centralised organisation. This decentralised feature eliminates the possibility of a single point of failure in Blockchain.
- **Transparent** - Because each node in the Blockchain network has a copy of the digital ledger, any effort to add a transaction must be verified by all users. Only with the approval of the majority of users can a block be added to the network. As a result, the network's transparency is preserved.
- **Open Source :** Blockchain code is open source and available on the internet. When the first Blockchain was created, the code was made publicly available so that anyone could download it and tweak it as needed. The Blockchain network's open source development model allows more users to engage in the network, making it considerably more versatile and decentralised, boosting transparency and fostering confidence.
- **Autonomy:** Due to its autonomous architecture, Blockchain may operate without the need for a central authority. As a result, Blockchain technology is decentralised and autonomous, requiring no third-party middlemen to facilitate transactions between nodes. To support the direct transaction of digital currencies, Blockchain employs autonomous smart contracts that are set within the Blockchain.
- **Immutability**: Once a transactional block has been appended to the digital ledger, it cannot be changed. Each block has its own unique hash code, which is combined with the previous block's hash to produce a chain of blocks. Attempting to amend a

transaction would result in the development of an entirely new hash, which would need computing the hash of all prior blocks, which would be computationally infeasible. As a result, the Blockchain network is immutable in nature.

➢ **Anonymity** - In order to preserve and safeguard a Blockchain network's security, it must keep its users' identities disguised to thwart cyber attacks. The users' anonymity is maintained by cryptography, which employs a public key to communicate and share information among users and a private key to conceal the user's identity.

Blockchain Methodology

Blockchain technology works by creating a safe and transparent environment for financial transactions using virtual currencies like Bitcoin. Each block's hash code keeps records secure in the Blockchain. This is because, regardless of the amount of the data or document, the mathematical hash function generates a hash code for each block that is exactly the same length. As a result, changing a block of data would result in an entirely new hash value.

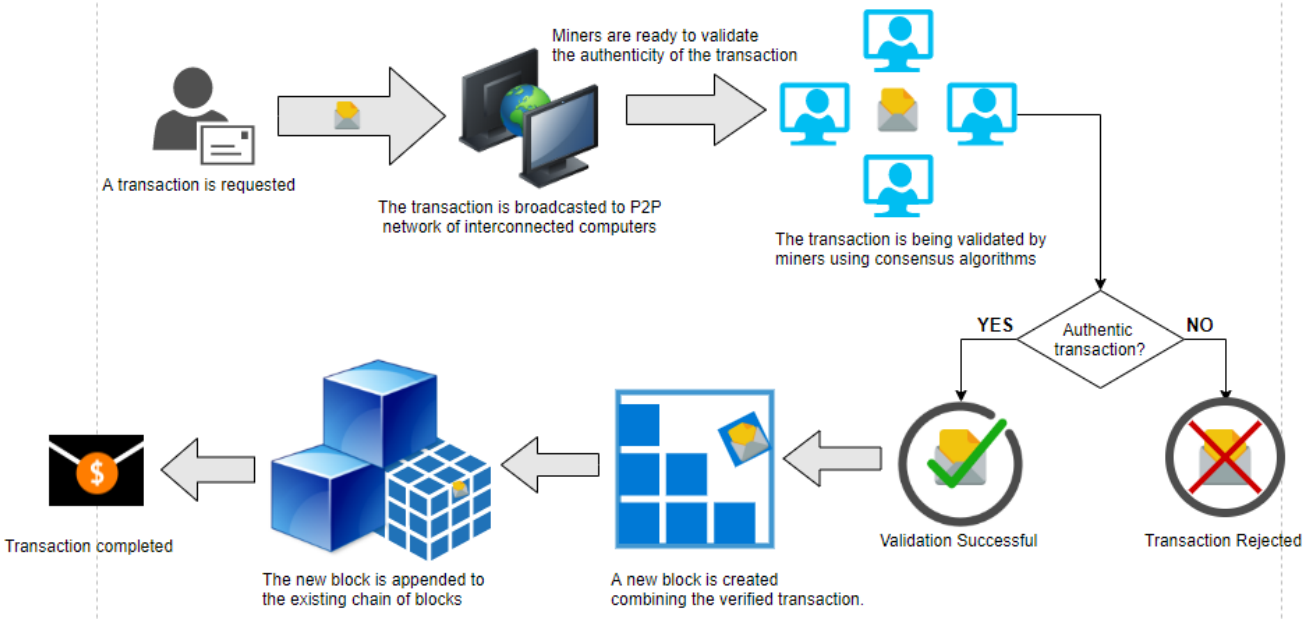

Fig. 1: Transaction in Blockchain

A network that is available to everyone while also maintaining user anonymity raises trust concerns about the participants. As a result, in order to establish confidence, participants must use different consensus techniques, such as Proof of Work and Proof of Stake.

Literature Survey

A research performed by Hewlett Packard [4] "discovered that there are significant limitations in 70% of all the most widely utilized IoT products. Due to their architecture, IoT applications are responsive to safety risks owing to the unavailability of some of these safety measures such as unreliable networking media inadequate specification of encryption and permission. As a result, everybody, either individual people or businesses, would be affected when IoT is accessible. In particular, the functionalization of domains offers different possibilities for impact and trade. This adds to a number of new possible hazards that should be regarded with respect to data safety and information preservation."

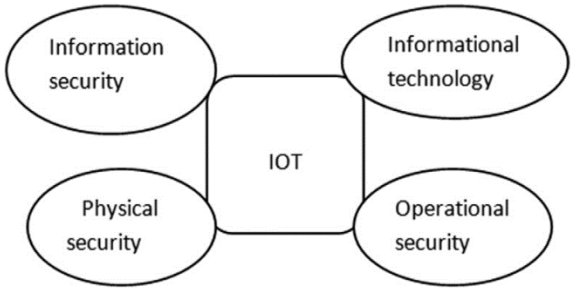

Fig. 2: Data Safety and Information Preservation

"Security concerns and aspects can be remedied by presenting engineers and programmers with sufficient guidance to incorporate safety approaches into IoT applications, thereby enabling consumers to use IoT authentication methods incorporated within the devices" [5].

"In particular specific machines and entire networks, inadequate protection and bad encryption habits now have to be taken into account again through beginning and safety planned. In various places and technologies, billions of external interconnected systems indicate how this IoT environment had expanded the sophistication of systems"[6]. "Security problems are massively increased because as amount of linked Smart devices constantly grows, so most security concerns need to be taken into account as a whole system" [7].

Security Challenges In Iot Devices

Because there are billions of IoT smart devices communicating, IoT security is the most important and difficult challenge for the research community. Because IoT is still in its early stages and demand for smart devices is growing, manufacturers are overlooking security concerns and releasing vulnerable devices into the market. As a result, attackers can easily target these devices and launch a large number of DDoS and other types of attacks to steal user personal information and data from IoT devices.

Fig. 3: Security Challenges In Iot Devices

- Data privacy and integrity(Unauthorized access of devices) : Data privacy and security remain the most pressing concerns in today's interconnected digital world. Because user data continues to flow through numerous integrated channels and is shared, transferred, and processed by several IoT devices, data kept in IoT devices within an integrated network of services is vulnerable to cyber attacks. This can result in attackers gaining unauthorised access to IoT networks, stealing and manipulating sensitive user data, and compromising the privacy and integrity of sensitive user data for malevolent objectives.
- Authentication and Authorization of IoT devices: Authentication of devices is a critical concern for parties communicating securely in an IoT network. Because an IoT network's broad heterogeneity of devices and services necessitates distinct authentication procedures, no standard global security protocols could be created. This makes authentication and authorization of IoT devices problematic. Similarly, device authorization is required to ensure that only authorised users and devices have access to the network's essential resources.
- Insecure Devices : The vast majority of embedded devices in an IoT network are low-cost, low-power devices with limited memory and computing power. As a result, attackers can easily acquire access to such physically vulnerable equipment. Blockchain implementation gives identification credentials in the form of unique key pairs that are registered in the distributed ledger for each connected IoT device, resulting in increased security.

- Node Tampering: In this type of assault, the attackers physically or electronically harm the sensor nodes in order to get access to and manipulate vital information, such as shared crypto keys, which may result in the entire sensor system being damaged.

- Malicious Node Injection: The attackers install the malicious node between two or more nodes and monitor the traffic to and from the nodes in this sort of attack. Man-in-the-Middle-Attacks are another name for this type of attack.

- Phishing attack: This type of assault typically uses emails or websites to steal the user's sensitive information, such as credit card numbers, email passwords, and so on. Adversary creates phishing sites that seem just like the real thing and tracks users. The opponent can utilize emails, websites, and phone calls against you.

- DoS Attack: A denial of service assault occurs when an adversary sends unexpected traffic across a system, rendering the resources unavailable to other users. The attacker can potentially deceive the data and temper it for resending in a denial of service attack.

- RFID Spoofing: RFID tags are not physically reproduced in this type of attack. In a spoofing attack, the adversary uses special devices with additional functionalities that can replicate RFID tags in order to obtain data. The attacker is attempting to gain access

to the original RFID tag, which will require privileges. The adversary gains complete access to data channels as the original tag using this strategy.

- Sinkhole and Wormhole Attack : Sinkhole attack is an active attack in which a compromised node in the network uses enticing phoney routes to get neighbouring nodes to send their data packets to the destination. As a result, data packets are dropped in the middle, resulting in a sinkhole. Wormhole attacks are active attacks in which two compromised nodes purposefully situate themselves at opposite ends of a network to form a tunnel. This tunnel creates the misleading appearance that it is a low-latency active bypass path for data packets to be transported.

Conclusion

The Internet of Things is a cutting-edge technology that has already made significant advancements in software efficiency. IoT has a lot of benefits in terms of industry, professional domains, and for the users themselves. People have concentrated on the considerations of how IoT system protection will be enforced, including some actual means of doing so. Companies are now attempting to strike a careful balance between improving stable IoT while rapidly deploying IoT-based goods across the sector. As the use of sensor networks expands in the real world, it is impossible to ignore the issue of security. While adding access control results in a longer product-to-market time and higher costs, the answer - trustworthy information hacks - puts such measures well within reach. Tech companies must undergo a paradigm shift in their thinking and motivation to implement additional security controls to protect the information of their company and that of the government. Electronic and analogue processes can now be integrated using a variety of new frameworks and methodologies. Transfer electronic sensors to work together for safe information.

However, unless the client only gives the required content at the required time and rejects the majority of the details, the exploitation of client information can be fully avoided, making the technique faster, more effective, and less vulnerable to the security threats discussed in the article.

References

[1]. V.Hassija1, V.Chamola, V.Saxena, D.Jain, P.Goyal & B.Sikdar, "A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures," IEEE, vol. 7, pp. 82721 - 82743, 2019.

[2]. M.Stoyanova, Y.Nikoloudakis, S. Panagiotakis, E.Pallis, & E. K. Markakis, "A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches and Open Issues," IEEE, pp. 1-38, 2020.

[3]. V. P. Mrs. Harsha, G.R. Mrs. Kanchan, V.T. Mrs. Malati , " A Study on Decentralized E-Voting System Using Blockchain Technology" International Research Journal of Engineering and Technology, Volume:5 Issue:11, Nov 2018. Page, 48-53

[4]. S. Kiran, S.B. Sriramoju, A study on the applications of iot, Indian J. Public Health Resear. Develop. 9 (11) (2018) 1173–1175.

[5]. M. Alam, J. Rufino, J. Ferreira, S.H. Ahmed, N. Shah, Y. Chen, Orchestration of microservices for iot using docker and edge computing, IEEE Commun. Mag. 56 (9) (2018) 118–123.

[6]. Thirupathi, V.N.R. Padmanabhuni, Multi-level protection (Mlp) policy implementation using graph database, Intern. J.Advanced Com. Sci. App. (IJACSA) 12 (3) (2021), https://doi.org/10.14569/issn.2156-5570 10.14569/ IJACSA.2021.0120350.

[7]. P.V. Lingala Thirupathi, N. Rao, Developing a multilevel protection framework using EDF, Intern. J. Advanced Research Eng. Technol. (IJARET) 11 (10) (2020) 893–902.