Quest Journals
Journal of Software Engineering and Simulation
Volume 9 ~ Issue 5 (2023) pp: 41-45
ISSN(Online) :2321-3795 ISSN (Print):2321-3809
www.questjournals.org

Research Paper

Security Flaws in Internet of Things (IoT) and their possible solutions

Abhishek Mishra
Department of Computer Science & Engineering
Galgotias University

***R**eceived 08 May, 2023; **R**evised 17 May, 2023; **A**ccepted 19 May, 2023 © The author(s) 2023.*
P**ublished with open access at **www.questjournals.org

Abstract—**This paper provides a comprehensive survey and analysis of the current state and concerns related to the security of the Internet of Things (IoT). The IoT framework aims to establish connections between individuals and entities from any location. Typically, IoT adopts a three-layer architecture composed of Perception, Network, and Application layers. To ensure a secure IoT realization, it is essential to enforce a variety of security principles at each layer. The future of the IoT framework depends on the successful resolution of its associated security issues. In response to these concerns, many researchers have implemented corresponding countermeasures, tailored to address the specific security concerns of IoT layers and devices. The purpose of this paper is to present an overview of security principles, technological and security challenges, proposed countermeasures, and future directions for securing the IoT.**

Keywords*—*Internet of things; IoT

I. Introduction

The Internet of Things (IoT) is a network of interconnected objects, devices, services, and people that can communicate and share data to achieve common goals across various domains and applications, such as transportation, healthcare, energy, and agriculture. To be identified in a collection of similar and heterogeneous devices, IoT devices follow an Identity Management approach. Similarly, each entity within a region defined by an IP address in IoT has a unique identification. The purpose of IoT is to enhance daily life by enabling intelligent devices to perform tasks, such as smart homes, smart cities, and smart transportation. IoT has many application domains, ranging from personal to enterprise environments, such as finance, banking, and marketing, and service and utility monitoring, including agriculture and energy management.

The development of Radio Frequency Identification (RFID) and Wireless Sensor Networks (WSN) has driven the rapid development of IoT applications in recent years. RFID tags or labels every device to serve as the basic identification mechanism in IoT, while WSN makes each "thing" a wireless identifiable object that can communicate among physical, cyber, and digital worlds.

II. IoT Architecture

The architecture of IoT is composed of different layers, each defined by its functions and the devices used in that layer. While there are varying opinions on the number of layers in IoT, most researchers agree that there are three primary layers: the Perception, Network, and Application layers. Each layer of IoT has its unique security issues associated with it. Fig. 1 presents an overview of the three-layer IoT framework and the devices and technologies used in each layer.

A. Perception Layer

The Perception Layer, also known as the "Sensors" layer, serves the purpose of collecting data from the environment with the help of sensors and actuators. This layer detects, collects, and processes information before transmitting it to the Network Layer. The Perception Layer is also responsible for facilitating IoT node collaboration in local and short-range networks.

B. Network Layer

The Network Layer is responsible for data routing and transmission to different IoT hubs and devices over the Internet. Cloud computing platforms, Internet gateways, switching, and routing devices are some of the technologies used in this layer, including WiFi, LTE, Bluetooth, 3G, Zigbee, among others. Network gateways serve as intermediaries between different IoT nodes by aggregating, filtering, and transmitting data to and from various sensors.

C. Application Layer

The Application Layer is responsible for ensuring the authenticity, integrity, and confidentiality of data. This layer is where the purpose of IoT is achieved, and the creation of a smart environment is realized. In other words, the Application Layer enables the development of various IoT applications, such as smart homes, smart cities, smart transportation, and infrastructure.

*Corresponding Author: Abhishek Mishra

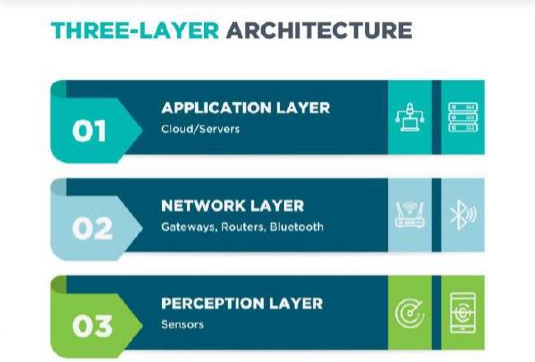

Figure 1. IoT architecture.

II. IoT Security challenges

A. The General Security Threats to IIoT

The security threats to IoT can be categorized into four main categories: data breaches, device hijacking, DoS attacks, and privacy violations.

Data breaches refer to the unauthorized access, theft, or manipulation of data collected by IoT devices. IoT devices often collect sensitive personal data, such as health data, financial data, and location data, which can be used for malicious purposes if not protected properly. For example, in 2018, a fitness app called Strava revealed the locations and routes of military personnel, which could compromise national security.

Device hijacking refers to the unauthorized control or manipulation of IoT devices. Attackers can take control of IoT devices and use them for malicious purposes, such as launching DoS attacks or stealing data. In 2016, a massive DoS attack was launched using IoT devices, causing widespread disruption to Internet services.

DoS attacks refer to the intentional disruption of IoT devices or services by flooding them with traffic. This can cause the devices or services to crash or become unavailable. IoT devices are particularly vulnerable to DoS attacks due to their limited processing power and memory. In 2017, a DoS attack was launched on a DNS provider, which caused widespread disruption to Internet services.

Privacy violations refer to the unauthorized collection, use, or disclosure of personal data collected by IoT devices. IoT devices often collect sensitive personal data, such as health data, financial data, and location data, which can be used for malicious purposes if not protected properly. For example, in 2019, a popular video doorbell company was criticized for sharing personal data with third-party companies without user consent.

1) Lack of Standardization :

The IIoT ecosystem is comprised of various devices and systems from different vendors. Each vendor has their protocols and communication standards, which can make it difficult to integrate and secure the systems. Lack of standardization can create security loopholes that can be exploited by attackers.

2) Insecure Communication :

Communication between IIoT devices can be insecure due to various factors, such as unencrypted communication channels, weak authentication mechanisms, and unsecured data transfer. This can lead to unauthorized access to sensitive information or control of critical systems.

3) Physical Security :

Physical security of IIoT devices is also a concern. Unauthorized access to devices can lead to tampering with the devices or data theft. Theft or destruction of devices can also lead to significant financial losses and disruption of operations.

4) Lack of Security by Design :

Security is often an afterthought in IIoT systems, which can lead to vulnerabilities that can be exploited by attackers. Security by design is a critical aspect of IIoT systems that must be integrated into the design process.

5) Complexity :

The IIoT ecosystem is complex, with multiple devices, systems, and networks communicating with each other. The complexity can make it difficult to identify and address security vulnerabilities.

6) Legacy Systems :

Upgrading legacy systems to newer and more secure versions can help reduce the security risk. Additionally, implementing security patches and updates can help protect legacy systems from new vulnerabilities.

7) Remote Access :

: Implementing secure remote access mechanisms such as two-factor authentication, network segmentation, and remote access policies can help secure IIoT systems.

B. Security Challenges for Every Layer of IIoT

The security of each layer in the Internet of Things (IoT) is vulnerable to both active and passive attacks that may stem from external sources or from within the network due to an insider attack. Active attacks interrupt the service directly, while passive attacks monitor the information within the IoT network without affecting its operation. Denial of Service (DoS) attacks are a threat to IoT devices, resources, and networks at every layer, rendering them inaccessible to authorized users.

1) Perception Layer

The IoT perception layer faces several security issues that need to be addressed. The first issue is the vulnerability of wireless signals used for transmitting data between IoT sensor nodes. The wireless signals are susceptible to interference, which can compromise their efficiency and lead to data loss. Secondly, the physical location of IoT devices makes them vulnerable to physical attacks, which can compromise the sensor node's hardware components. The dynamic nature of the network topology also poses a challenge to securing the perception layer, as IoT devices are often moved around different places.

Thirdly, the limited storage capacity, power consumption, and computation capability of sensors and RFIDs in the perception layer make them susceptible to many types of attacks. Replay attacks, for instance, can exploit the confidentiality of this layer by spoofing, altering, or replaying identity information of IoT devices. Such attacks can lead to unauthorized access to data, compromising the security of the entire IoT network.

To address these security challenges, IoT perception layer security mechanisms must prioritize the use of strong encryption and authentication protocols to protect the wireless signals transmitted between sensor nodes. Additionally, IoT devices in the perception layer should be physically secured, and hardware components should be tamper-resistant. The use of dynamic key management schemes and random number generation algorithms can help prevent replay attacks and ensure data confidentiality in the perception layer. Finally, the implementation of secure boot processes and updates firmware can help protect IoT devices against infections and malware other software-based attacks.

2) Network Layer

The network layer of IoT is vulnerable to a range of attacks that can compromise the confidentiality, privacy, and availability of data. Apart from DoS attacks, adversaries can attack the network layer through traffic analysis, eavesdropping, and passive monitoring, exploiting the remote access mechanisms and data exchange of devices.

One of the most significant threats to the network layer is the Man-in-the-Middle (MITM) attack, which can lead to eavesdropping and the compromise of secure communication channels. The key exchange mechanism in IoT needs to be secure enough to prevent intruders from eavesdropping and committing identity theft. Ensuring secure communication channels and key exchange mechanisms is critical to protecting the confidentiality and privacy of data in the network layer.

The heterogeneity of network components in IoT presents compatibility issues that make it difficult to use current network protocols for efficient protection mechanisms. Attackers can exploit the fact that everything is connected to gain more information about users and use it for future criminal activities. Protecting both the network and objects in the network is crucial in IoT, as objects must have the ability to detect abnormal situations and behaviors that can compromise their security. This requires the development of robust protocols and software that enable objects to respond proactively to potential threats.

3) Application Layer

Furthermore, due to the large number of devices and applications in the IoT ecosystem, there is a risk of malicious applications being developed and deployed. Malicious applications can access sensitive information or even take control of IoT devices. These types of attacks can be prevented by implementing security measures such as application isolation, code signing, and secure software updates.

Another challenge in the application layer is the lack of standardization of communication protocols and data formats. This can lead to interoperability issues and vulnerabilities, as different devices and applications may not be able to communicate with each other securely. To address this, industry-wide standardization efforts such as the Open Connectivity Foundation (OCF) and the Industrial Internet Consortium (IIC) are working towards establishing common standards for IoT communication and data exchange.

Lastly, the application layer is also vulnerable to social engineering attacks, where attackers trick users into revealing sensitive information or granting access to their devices. This can be mitigated by increasing user awareness and providing training on how to identify and avoid social engineering attacks.

IV. IoT Security fixes and patches

Security measures are crucial for IoT at all levels, namely the physical layer for data collection, network layer for routing and transmission, and application layer for ensuring confidentiality, authentication, and integrity. In this section, we will discuss the latest security measures that specifically target the unique characteristics and security objectives of IoT.

A. Methods of Authentication

Authentication is an important security measure in IoT, and there are several methods available to achieve this. One such method is presented by Zhao et al. in 2011, which is a mutual authentication scheme for IoT between platforms and terminal nodes based on hashing and feature extraction. Wen et al. proposed a one-time one cipher method for ID authentication at sensor nodes, which is based on a request-reply mechanism and uses a pre-shared matrix between the communicating parties. Another approach is the Identity Authentication and Capability based Access Control (IACAC) protocol presented by Mahalle et al., which combines both authentication and access control capabilities using a public key approach. It prevents man-in-the-middle attacks by using a timestamp as the Message Authentication Code (MAC) and grants access to resources to only one ID at a time. Finally, researchers introduced a light- weight authentication protocol to secure RFID tags, which ensures mutual authentication between RFID readers and tagged items without introducing large overhead on these devices.

One popular approach to authentication in IoT is the use of digital certificates. Digital certificates can be used to verify the identity of devices in the network, as well as to encrypt and sign data transmissions. However, the use of digital certificates can be challenging in IoT due to the limited processing power and memory of many IoT devices.

Another approach to authentication in IoT is the use of biometric authentication. Biometric authentication relies on physical characteristics such as fingerprints or facial recognition to verify the identity of users or devices. This can be particularly useful in applications such as smart homes, where multiple users may need access to the same devices.

The use of blockchain technology is also being explored for authentication in IoT. Blockchain can be used to create a decentralized, tamper-proof record of device identities and transactions, which can help to prevent unauthorized access and ensure data privacy.

In addition to traditional authentication measures, some researchers are exploring the use of behavioral biometrics for authentication in IoT. Behavioral biometrics use patterns of behavior such as typing speed or mouse movements to identify users, and can be particularly useful for identifying unauthorized access attempts. However, the use of behavioral biometrics can also raise privacy concerns, as it requires the collection of sensitive data about users' behavior.

B. Trust Establishment

In addition to the mutual trust framework, there are several other trust establishment mechanisms that have been proposed for IoT.

One such mechanism is presented where a trust-based access control framework is proposed for IoT. The framework includes three components: a trust management system, a policy engine, and a security module. The trust management system evaluates the trustworthiness of IoT devices based on their behavior and interactions, and assigns trust scores to them. The policy engine defines access control policies based on the trust scores of the devices, and the security module enforces these policies.

Another trust establishment mechanism is proposed, where a reputation-based trust model is used to evaluate the trustworthiness of IoT devices. In this model, each device maintains a reputation score based on its behavior and interactions with other devices. The reputation score is used to determine the level of trust that other devices should have in the device. Devices with high reputation scores are trusted more, while devices with low reputation scores are trusted less or not at all.

A trust management framework is proposed that uses a combination of cryptographic techniques and reputation-based trust models to establish trust between IoT devices. The framework includes four components: a trust evaluation module, a trust update module, a trust propagation module, and a trust aggregation module. The trust evaluation module uses reputation scores to evaluate the trustworthiness of devices, and the trust update module updates the reputation scores based on the feedback received from other devices. The trust propagation module uses cryptographic techniques to propagate trust values between devices, and the trust aggregation module combines the propagated trust values to compute an overall trust score for each device.

C. Federallly structured IIoT

The concept of federated IoT has gained significant attention in recent years, as it provides a way to address the challenges associated with the heterogeneity of devices, software, and protocols in IoT systems. One notable effort in this regard is the Industrial Internet Consortium (IIC), which has developed a reference architecture for federated IoT systems. The IIC's reference architecture defines a set of core components and interfaces that can be used to create interoperable IoT systems, regardless of the underlying technologies.

Another important aspect of federated IoT is access control, which plays a crucial role in ensuring the security and privacy of IoT systems. One approach to access control in federated IoT is to use a delegation model, where a centralized authority delegates access rights to various entities in the system based on their roles and responsibilities. This approach has been studied extensively in the literature, and several delegation models have been proposed for federated IoT systems.

In addition to access control, federated IoT also requires mechanisms for enforcing policies and ensuring compliance with security requirements. One promising approach is to use security toolkits that can be integrated with IoT protocols and middleware to provide end-to-end security.

For example, the MQTT-Security-Kit (MQTT-SecKit) is a security toolkit that provides end-to-end encryption, access control, and integrity protection for MQTT-based IoT systems. This toolkit can be used to enforce policies and ensure compliance with security requirements, although it may introduce some additional latency in the system.

D. Awareness of Security Risks

In addition to the study mentioned, there have been several high-profile incidents that have brought attention to the issue of security awareness in IoT. For example, in 2016, the Mirai botnet was responsible for launching a massive distributed denial-of-service (DDoS) attack that affected a number of high- profile websites, including Twitter, Netflix, and PayPal. The botnet was made up of compromised IoT devices, such as routers and webcams, that were infected with malware due to weak security measures such as default passwords and unpatched vulnerabilities.

Since then, there has been a growing awareness of the need for better security measures in IoT, including stronger authentication mechanisms and regular software updates. Many manufacturers are now including security features such as two- factor authentication and encryption in their IoT devices.

There are also efforts to educate users about the importance of strong passwords and other security measures. For example, the U.S. Federal Trade Commission has published guidelines for IoT security that include recommendations for strong authentication, secure software updates, and privacy protection.

need for new identification, wireless, software, and hardware technologies to resolve the currently open research challenges in IoT.

References

[1] Alexandru RADOVICI; Cristian RUSU; Răzvan ŞERBAN, "A Survey of IoT Security Threats and Solutions" in 2018 17th RoEduNet Conference: Networking in Education and Research (RoEduNet).

[2] Aishah Abdullah; Reem Hamad; Mada Abdulrahman; Hanan Moala; Salim Elkhediri: "A Review of Internet of Things (IoT) Security Issues, Challenges and Techniques" in 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS).

[3] Paul C. van Oorschot; Sean W. Smith, "The Internet of Things: Security Challenges," IEEE Security & Privacy (Volume: 17, Issue: 5, Sept.-Oct. 2019)

[4] Tanishq Varshney; Nikhil Sharma; Ila Kaushik; Bharat Bhushan, "Architectural Model of Security Threats & theirCountermeasures in IoT" in 2019 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS)

[5] Shashi Rekha and Lingala Thirupati, "Study of security issues and solutions in Internet of Things (IoT)" on https://doi.org/10.1016/j.matpr.2021.07.295