Universe Scientific Publishing

Architecture and Solutions For IOT Device Security

Xiaoliang Zhou

James Cook University Singapore, 387380 Singapore.

Abstract: The Internet of Things (IOT) is a prominent technology that enables networked connection and data transfer between physical devices. It has found applications in home automation, healthcare, environmental monitoring, and industry. However, the exponential growth of IOT devices has raised concerns about network security, data leaks, and potential threats. This paper aims to provide an overview of security risks in various IOT areas, improve IOT application architectures, and explore recent security mechanisms and technologies. The conclusion highlights the importance of security attributes and discusses four technologies, namely blockchain, fog computing, edge computing, and machine learning, to enhance IOT security.

Keywords: Internet of Things (IOT); Networked Connection; IOT Application Architectures; Security Mechanisms

1. Introduction

With billions of connected devices globally, the Internet of Things (IOT) has grown quickly. But this growth has led to worries about privacy and security. Users may be required to provide personal information for tailored services, which raises vulnerabilities in the absence of a dependable and interoperable IOT ecosystem. Identity, administration, storage, and network security issues affect IOT devices. It is critical to secure the IOT system architecture and take security issues into account when designing and producing the system. Potential IOT security solutions to mitigate these concerns include edge computing, fog computing, machine learning, and blockchain.

2. Key application areas of IOT security

IOT devices are vulnerable to simple, direct assaults that aim to breach user privacy and information. These gadgets can collect anything from simple ambient readings to extremely sensitive personal data. Attackers may potentially choose to target and control IOT network devices in order to profit financially. In light of this, maintaining security is crucial for the creation of IOT applications. Various types of IOT applications that require security will be covered in this chapter.

2.1 Smart city

Smart cities use cutting-edge technology to improve quality of life, but they also present privacy issues. Payment information may be compromised through smart card services, and smartphone apps may track the whereabouts of users, especially young children. However, if hackers manage to get in, this might be dangerous.

2.2 Smart environment

IOT applications like earthquake detection, pollution monitoring, and others can have a big impact on local communities in a smart environment. However, these applications' shortcomings, including security holes or false results, can have unfavorable effects. For instance, failure to foresee earthquakes can result in the loss of lives and property while wrong earthquake identification might result in financial losses. To avoid such problems, IOT applications must be accurate, secure, and dependable.

2.3 Smart Metering and Smart Grids

Smart metering encompasses various applications for measuring, monitoring, and managing resources such as electricity, water, oil, and gas. While smart meters are widely used in smart grids to track energy usage and prevent power theft[1], they also have vulnerabilities to both offline and online threats. Advanced Metering Infrastructure (AMI) collects data from connected devices, but malicious actors can manipulate this data, resulting in losses for service providers or clients.

3. Sources of security threats in IOT applications

The four tiers of IOT applications are the perceptual layer, network layer, middleware layer, and application layer. Each tier uses different technology, which can lead to security vulnerabilities. This section discusses potential threats in IOT applications across these layers.

3.1 Security issues at the perception layer：

Sensors and actuators form the majority of the sensing layer. Sensors detect physical events in their surroundings, while actuators perform precise actions based on these observations. The main security threats to this layer are as follows:

1.Node capture:

2.Malicious code injection attacks:

3.Fake data injection attacks:

4.Bypass attack (SCA):

3.2 Security issues at the network layer：

The information obtained from the sensor layer is transferred to the processing unit via the network layer as its primary function.

1.Phishing site attacks:

2.Access attacks：

3. DoS and DDos attacks：

3.3 Security issues at the middleware layer：

Middleware provides a layer of abstraction between the network and application layers in IOT. Middleware provides processing and storage capabilities for IOT systems but is vulnerable to various attacks, including program takeovers and security risks in cloud and database components.

1.man-in-the-middle attack

2.SQL Injection attack

3.Signature wrapping attack

3.4 Security issues at the application layer：

The application layer directly processes and provides services to the end user. Smart home, smart meter, smart city, smart grid and other IOT applications.Security problems at the application layer are as follows

1.Data theft

2.Access control attacks

3.Service interruption attack

4. Internet of Things security using blockchain：

IOT's decentralized and scalable nature makes it challenging to apply traditional centralized security strategies. Blockchain offers an appealing alternative by providing robust security against data modification, preventing malicious devices from disrupting operations or spreading false information[2].

4.1 There are several advantages of using blockchain in IOT applications：

There are several benefits of using blockchain in the context of the Internet of Things (IOT):

4.1.1 Storing IOT device data

Blockchain provides a promising solution for storing and securing data generated by IOT devices. Regardless of the layer of an IOT application, blockchain can be used for data storage and transmission, preventing misuse of the data.

4.1.2 Decentralized architecture

The decentralized nature of blockchain eliminates the risk of a single point of failure, which is often present in cloud-based IOT systems. This ensures safe and reliable storage of data produced by IOT devices, regardless of their physical location.

4.1.3 Proxy architecture for limited resource devices

IOT devices often have limited resources, making it challenging to maintain large general ledgers. By using a proxy architecture, where data is stored in encrypted form on a network, IOT devices can leverage blockchain security features. Proxy servers can be set up to facilitate encrypted file downloads by clients.

5. Internet of Things security using fog computing

Fog computing uses a multi-layered architecture to enable local processing of IOT data. It provides two frameworks based on storage and processing capacities: Fog-Device and Fog-Cloud-Device. Both wireless and cable cross-layer communication are possible. When compared to cloud computing, fog computing minimizes data traffic and reaction times. Compared to mobile cloud computing and mobile edge computing, it is different. Applications include real-time video analytics, augmented reality, content delivery, mobile big data analytics, and augmented reality.

5.1 Fog computing provides a solution to overcome the security threats of the Internet of Things

5.1.1 Man-in-the-middle attack

Between the end user and the cloud or Internet of Things system, the Fog serves as a layer of protection. Before being delivered to the system, any threat or assault on an IOT system must travel through a layer of fog that detects anomalous activity and mitigates it.

5.1.2 Data transmission attacks

Data management and storage on a secure fog node are significantly better than on IOT devices. The data is more securely saved on the fog node as opposed to the end-user device. Fog nodes have made user data more easily accessible.

5.1.3 Eavesdropping

Instead of sending information via the whole network when using a fog node, communication only takes place between the end user and the fog node. There are fewer possibilities for attackers to try to eavesdrop when there is less traffic on the network.

6. IOT security using machine learning

The field of machine learning has attracted a lot of attention lately. ML is used in many industries for both development and IOT security. ML appears to be a possible solution for protecting IOT devices from cyberattacks since it provides a distinctive technique for fighting off attacks from other traditional ways.

6.1 ML provides a solution to overcome security threats

6.1.1 DoS attack

DoS attacks from IOT devices are a serious problem. Multi-layer protocols based on MLP can protect against such attacks. Training MLPS using particle swarm optimization and backpropagation improves wireless network security, defending IOT devices and improving inference accuracy.

6.1.2 Eavesdropping

A hacker can intercept internet communications, but nonparametric Bayesian algorithms or Q-learning-based unloading processes can prevent such attacks. Q-learning and Dyna-Q ML technologies can also defend against eavesdropping, as described in through experiments and reinforcement learning.

6.1.3 Privacy breach

Collecting personal information, such as health data or location, puts users' privacy at risk. To prevent privacy disclosure, adopt Scientific Computing for Privacy (PPSC) [3] and the Commodity Integrity Detection Algorithm (CIDA) based on the Chinese Residual Theorem (CRT) to develop IOT application trust.

7. Internet of Things security using edge computing

Edge computing and fog computing are additional layers to cloud computing in IOT applications. They differ in computational power and location intelligence. Edge computing brings processing tasks closer to users through small edge servers, improving security by keeping data off devices and reducing transmission costs.

7.1 Protect and improve the Internet of Things with edge computing

7.1.1 Data leakage

In edge computing, data is processed and stored locally, reducing the likelihood of data theft and leakage. In fog computing, the mobility of data between devices and layers can be exploited by attackers.

7.1.2 Data compliance issues

To prevent data from leaving their borders, several countries have strict rules in place, such as the GDPR established by the EU (General Data Protection Regulation). Edge computing enables businesses to keep data inside their own borders and ensure compliance with data sovereignty regulations.

7.1.3 Bandwidth issues

Edge computing in IOT allows for data cleaning and aggregation tasks to be performed at the edge nodes, reducing the need to transfer raw and insignificant data to the cloud. This minimizes bandwidth costs and security risks.

Conclusion

The network, middleware, gateway, application, and sensor layers, as well as other IOT application layers, are all covered in this paper's examination of security issues. In relation to IOT security, it analyzes the potential of blockchain, fog computing, edge computing, and machine learning. The study also identifies open questions and potential concerns with these solutions. Additionally, it offers a summary of the state of IOT security research at the moment and suggests lines of inquiry for additional research to enhance IOT safety.

References

[1] Xia X, Xiao Y, and Liang W, ‘‘ABSI: An adaptive binary splitting algorithm for malicious meter inspection in smart grid,’’ IEEE Trans. Inf. Forensics Security, vol. 14, no. 2, pp. 445–458, 2019.

[2] Yan Z, Zhang P, and Vasilakos AV, ‘‘A survey on trust management for Internet of Things,’’ J. Netw. Comput. Appl., vol. 42, pp. 120–134, Jun. 2014.

[3] Ni J, Zhang K, Lin X, and Shen XS, ‘‘Securing fog computing for Internet of Things applications: Challenges and solutions,’’ IEEE Commun. Surveys Tuts., vol. 20, no. 1, pp. 601–628, 1st Quart., 2018.