International Journal of
Computer & Software Engineering
Review Article Open Access

The Review of IoT Security Framework Based on Mobile Edge Computing

Fan Yongkai[1,2], Zhao Guanqun[1,2], Sun Xiaofeng[1,2*] and Lin Xiaodong[1,2]
[1]*Beijing Key Lab of Petroleum Data Mining, China University of Petroleum, Beijing, China*
[2]*Departmentt of Computer Science and Technology, China University of Petroleum, Beijing, China*

Abstract

At present, IoT has received extensive attention and has exerted tremendous influence in the life of people and production. The number of actuators and sensors stationed across the world is also growing rapidly. The application of smart devices and smart services has upgraded our lives more refined and more convenient. However, while bringing convenience to our lives, it also brings a series of security and privacy risks. In this article, we have integrated the background knowledge of IoT, including the development process and applications, the mobile edge computing, the security threats, the security requirements and the basic architecture of IoT. On this basis, we focused on the analysis of the mainstream of the academic community. Compared with the IoT security framework adopted by the industry, comparing and evaluating several popular frameworks, we have put forward our own security framework perspectives and possible in-depth research points in the future.

Publication History:

Received: June 10, 2019
Accepted: July 16, 2019
Published: July 18, 2019

Keywords:

IoT, Security, Security framework, Review, Mobile edge computing

Introduction

Basic concept

The IoT, which is the abbreviation of internet of things, is a novel definition in the area of the modern wireless telecommunication systems. The core of this paradigm is the universal existence of sundry objects around us for example, cell phones, sensors, actuators, etc. -have the ability of exchanging to others and realize their common goals mutually [1].

Application

IoT has developed for many years since it was presented, and it has found wide utilization in many areas indeed. In this section, we'll introduce several aspects in which the IoT has an essential influence [2-4]. Besides, we'll explain some of the technologies applying to the IoT. And we also show that how the IoT exchanges the daily life of humanity.

Semantic technologies

Semantic technology is a kind of new technique of computer science. In the area of IoT, semantic technologies can help discover devices and achieve semantic inseparability [5]. With the help of the cloud, semantic technologies will also act as a vital role in validating the sharing of varieties of virtual objects. The semantic concentration of virtual object instructions will realize for IoT. And IoT will assist the users to find the relevant proven virtual objects to polish up their performance.

Networking technology

In recent years, the networking technology has been promoted by a series of information-based service, such as receiving email, chatting with others on the internet, and making calls. It is predicted that over the next couple of years, the devices of IoT which have less communication mode will add in the network, including M2M modules, vehicles, and different types of sensors [6]. Some of these devices need all the time bandwidth; others are required to send out plenty of tiny bits of data every day. The architecture of these kinds of network must meet the requirements for IoT applications. A high-capacity network is essential for the IoT communication.

Smart household

We live with plenty of intelligent devices which own a variety of sensors in home and the owner of network can use their information collected freely. In home, a smartphone served to communicate with several interfaces, such as Bluetooth for interfacing sensors to measure physiological parameters [7]. Also, there are some applications for IOS, Android and Windows Phone operating systems which measure various parameters. What's more, Doctors can use a monitoring system to observe their patients.

Smart grid

In integrating IoT, the smart grid had been able to replace the traditional power grid for better service quality. With the combination of IoT, houses and buildings deploy several of smart meters in smart grid communication. And then smart meters will aggregate massive data, store and process them to support the effective operations in smart grid [8].

Smart transportation

There is a slew of smart vehicles in the smart transportation system, which is also called the intelligent transportation system. A smart vehicle can contact with others and share the important information efficiently with the transportation networks. What's more, the transportation system can produce a better safety and efficiency route for the drivers [9].

Smart cities

Different from smart grid and smart transportation, the smart city maybe is a multivariate comprehensive framework. We can use it to supervise the public affairs through ICT (information and

***Corresponding Author:** Sun Xiaofeng, Beijing Key Lab of Petroleum Data Mining, China University of Petroleum, 18 Fuxue Rd, Changping Qu, Beijing Shi, China; E-mail: 2017011316@student.cup.edu.cn

Citation: Yongkai F, Guanqun Z, Xiaofeng S, Xiaodong L (2019) The Review of IoT Security Framework Based on Mobile Edge Computing. Int J Comput Softw Eng 4: 148. doi: https://doi.org/10.15344/2456-4451/2019/148

communication technology). In a smart city, public resources will be used in more efficient ways. As a comprehensive framework, smart city plays the role of an integration of services and applications, such as the smart transportation, smart buildings, smart grid, smart health, etc. [10].

Enterprise

In this area, people can use sensors which are set in the industry to ensure the security, control or automation, however as the wireless communication system has developed to overcome many disadvantages, it can replace traditional sensors to provide a better flexibility for any kind of requirement whenever and wherever [11,12]. And this is called an IoT sub-net, which devoted to industry or factory maintenance. The information collected can be used or released by the users or owners. One of these instances is the environmental monitoring application, which is used to follow the trail of the state of industrial buildings.

Utilities

In this area, we propose the water network monitoring as an IoT example. The water network monitoring can ensure the quality of drinking water because quantities of sensors are set in the system. The sensors are used to measuring critical water parameters and the data collected is installed at crucial locations to guarantee nigh supply quality. This kind of application can be applied at drinking water, storm water drains and sewerage systems. And by realizing the system, we can extend this to other areas.

IoT Architecture

Generic architecture

Classically, there are three main key levels in IoT architecture [11,12], and here we will give a brief introduction as Figure 1:

Perception Layer: this layer includes various kinds of sensors, for example, temperature sensors, Barcodes, RFID or any other kinds of sensor networks. Identifying objects and obtaining the status information, then storing the data and handling them are the main purposes of perception layer.

Network Layer: this layer answer for transmitting. It can convey the collected data which are from sensors in perception to other information processing systems through such as the Mobile network, the Internet and so on.

Application layer: this layer answer for realizing different kinds of practical applications like Smart Home, Smart Grid, Smart Transportation even Smart City ,etc. Indeed, all of these applications belong to IoT, and the application layer is able to make them come true according to the users' needs.

SoA-based architecture

The IoT architecture based on SoA is an improved frame [13]. In general, SoA is the abbreviation of Service-Oriented Architecture, and it can be seen as a model based on component, and it can make a connecting with diverse services and functional units through interfaces and protocols. SoA can concentrate on designing the workflow of consorted services, and make the hardware and software components reused. So, using the SoA will enhance the feasibility of the IoT architecture.

How to integrate SoA into traditional IoT architecture? A solution is to extract the data services in the application layer and the network layer, and then form a new layer, which is called the service or middle-ware layer. Here we give a brief introduction of it as shown in Figure 2:

Middle-ware layer: this layer is located between the application layer and the network layer, and it includes many kinds of information

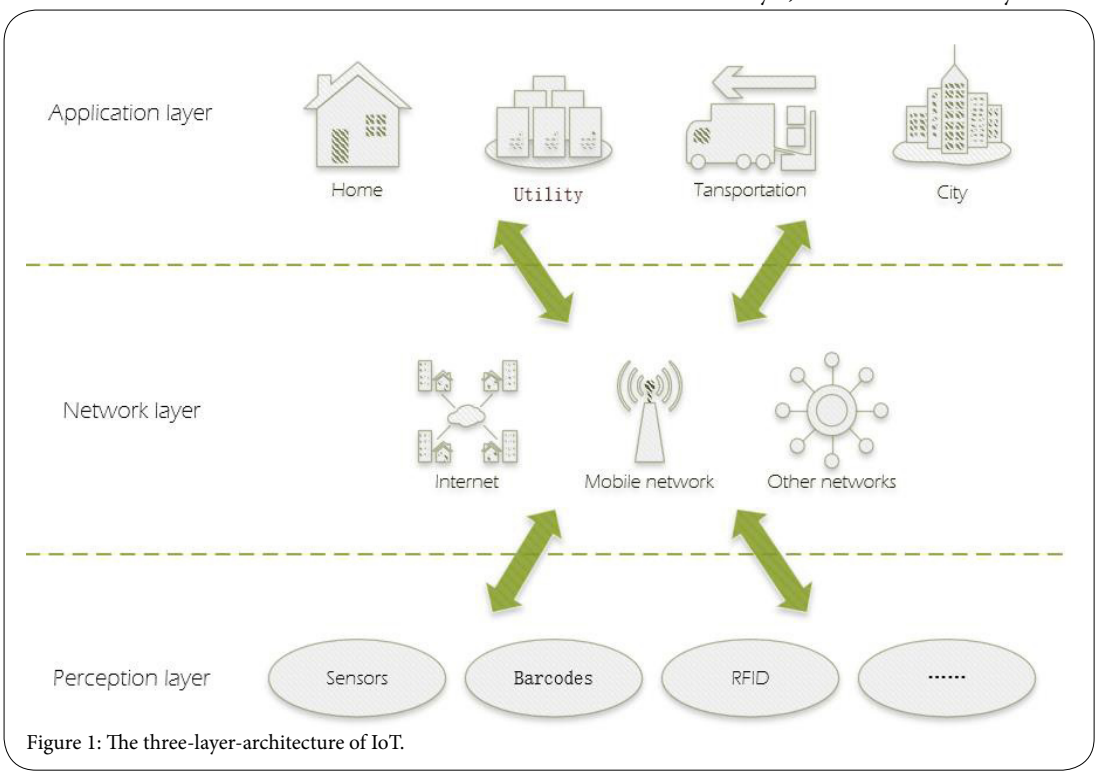

Figure 1: The three-layer-architecture of IoT.

processing systems, which take actions according to the data-processing results. Additionally, it can link the database in which the data storage with the system. What's more, the middle-ware layer is service-oriented that can ensure the same service type among the connected equipment.

The Secure Goals of IoT

When we want to apply applications or service in IoT safely and effectively, the most important thing is to figure out what is the secure goals. Only can we know about the goals to achieve, we can lay emphasis on the feature which to protect from being attack [14].

Confidentiality

This characteristic is created for ensuring that only the authorized consumer can access the information during the whole process. Check measurement devices interconnection in IoT, the confidentiality is a crucial security property. So, making sure the collected data won't disturb or be stolen by other devices is of vital importance. In order to implement the goal, we can employ some security solutions in IoT, such as the secure key management mechanisms or other solutions.

Integrity

During the period of data communication, it is important to prevent the sensitive data from being distorted by different interference, and use integrity to achieve this goal. In IoT, while the applications receive tampered data, wrong operation status can be measured and the system may make a wrong feedback, which can cause the paralysis of IoT applications. So it's important to guarantee the integrity. To protect the integrity, we should develop the integrity mechanisms such as false data filtering schemes.

Availability

Availability is a property which can make sure that the authorized consumer can access the needed data anytime and anywhere. Because of the real-time requirements of IoT, the useful must be transferred in time, unless some services cannot run properly. Thus, availability is a vital security feature for IoT. To this feature, there is a serious attack which is called the DoS attack that can destroy the availability of IoT. To prevent the system from being attacked, security techniques like effective routing protocols should be applied [8].

The Security Challenge in IoT

There are many security challenges we have noticed now. In this section, we will introduce the privacy and security issues in detail, so as to prevent against the probable attacks in the future.

Authentication

Authentication is a critical security issue for IoT and IoT devices. With the authentication, it can ensure that when the legitimate data is delivered in networks, the applications and equipment are legitimate too. However unfortunately, it is difficult to reach the goal because of the lack of memory and CPU power of IoT devices. And it is tough to execute cryptography operations which are required for authentication protocols [15].

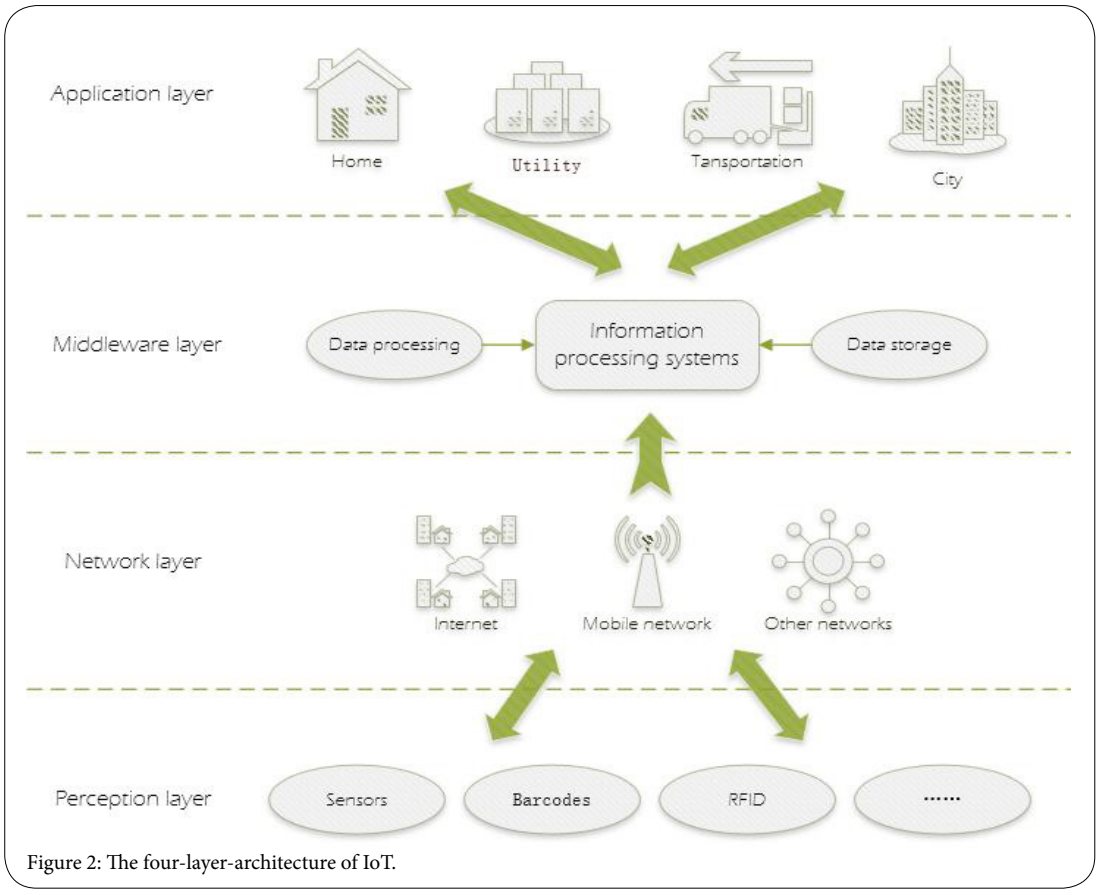

Figure 2: The four-layer-architecture of IoT.

Trust

In IoT, there is no efficient mechanism which can measure how and when to trust an IoT device. And because of the lack of the trust mechanism, it's hard for consumers to know if it's profitable to abstain from a certain IoT service or not. Trust can ensure the security and privacy of the data, and as a result, an effective trust management system is supposed to be set up in IoT.

Access control

Access control is a crucial security technique, which is used to ensure that only authorized users can pay a visit to certain resources, like an IoT device or collected data. In the situation of IoT, we need access control to ensure that only trusted entities can carry on a given action. However, it has present new challenges that we are handling with a number of "things" which have limited resources. What's more, managing access to highly dispersed data is a significant challenge as well.

Intrusion detection

Intrusion detection can find out the malicious IoT devices and behavior, follow the behavior of other devices in the network in order to take appropriate actions [16]. The question is that detecting the insider and outsider attacks will be difficult in such a complicated situation. Besides, how to layout and realize a monitoring system that is able to work in a large-scale, widely GEO distributed, and highly mobile environments is a complex task to achieve.

Rogue node detection

A rogue node in IoT can grab users' data and can send malicious information to other IoT nodes. As a result, users' private information is easy to be stolen, and vicinal nodes or devices can be disturbed by junk information or even be destroyed. Solving this issue can be very difficult, but it is necessary to establish a model based on trust measurement model in IoT environment to detect malicious nodes.

Data protection

The data integrity can be easily destroyed in IoT because of the complex environment [17]. Besides, as the resource limitations exist in IoT devices, the data are usually conveyed to the cloud for dealing with. As a result, these data must be preserved in the processing stage and communication stage. The low capability of IoT devices to encrypt and decrypt makes data's authenticity and integrity become a critical challenge.

Privacy

Privacy can make sure that the data can only be accessed and modified by the specific user. In other words, it ensures that the customer can control some information from the received data and cannot control others. But in IoT, the resource-constrained devices are short of the ability of encrypting or decrypting sensitive data that makes it easy to be attacked by an adversary [18].

Several Security Frameworks or Techniques for IoT

From here on, we are going to introduce some proposed security frameworks or techniques for different fields of IoT. First, we'll give a brief description of each frame and provide readers with structure maps to show the composition. Then, we'll compare all of the frameworks to show the differences and features of them. All of these works will help readers understand better.

A lightweight attribute-based access control system

In IoT, users can access sensors with mobile devices, but they have less ability to track who is using the resources or data. Here some researchers proposed an architecture, which can offer an access control system that protect the security of IoT sensors as well as sensor data [19].

The cloud, the mobile clients, the IoT nodes and the gateway is the four main parts of the proposed framework, which is revealed in Figure 3.

The cloud plays the role of server that receives the request from the mobile clients. It can provide variety kinds of services to clients and transmit web requests to IoT nodes. Whether receiving the request or not depends on the context value and calculated trust value. If the value is lower than the initially setting value, the request will be rejected.

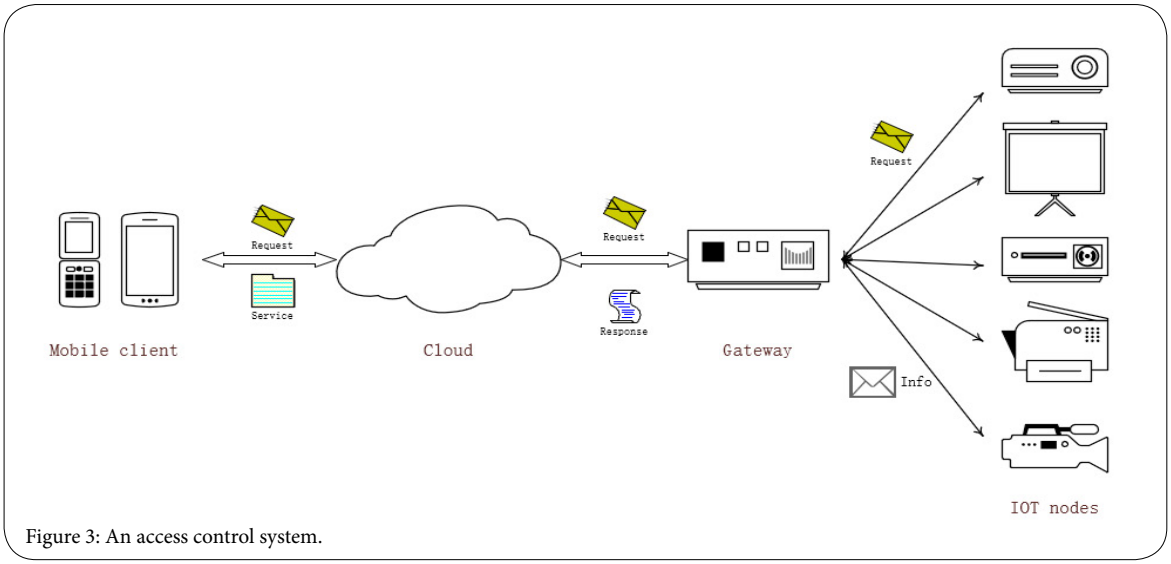

Figure 3: An access control system.

The mobile clients perform the following operations. Once launching to applications, they will register with the sensors; In addition, clients can collect sensor data and initiate authorization requests regularly; what' more, they can send requests as well as the context values through network packages. At last, the mobile clients receive the web response and then present it to users.

Different IoT nodes have different functions. Because the node only trust the gateway server, they can only connect with the gateways. As a consequence, whenever the node receive information from the gateway, they will perform the operations.

The gateway can send connection requests as well as the available sensor lists. The cloud will know which gateway to choose when there is any request passed to the sensor. The cloud transmits request to the specific gateway, and the gateway creates an information after receiving the request. Then the gateway will send the information to IoT nodes.

An IoT security framework for smart cyber infrastructures

Figure 4 shows a security framework for IoT smart infrastructures [20]. The architecture includes four layers, they are IoT End Nodes layer, Networks layer, Services layer and Applications layer.

The first layer is called End nodes layer. There are many IoT devices, and the information (such as environmental conditions, object properties, data, etc.) collected from the real world can be passed to the next layer through them. The actuators and sensors are the most significant components in this layer. The former one is to collect data of the physical world and translate data into digital world, the latter one is to modify the environment to an expected status.

The second layer is called Network layer. It conducts data between the end nodes and the fog or cloud. In this layer there is a secure gateway, it is in charge of controlling access for defending against cyberattacks that might appear. Then the secure data that passed through the gateway can be dispatched to the cloud or fog for further processing, through the internet or other networks.

The third layer is called service layer. It play the role of an interface between the network layer and the application layer. All the required energy and resources are provided as cloud or fog services because there is less memory and computing capacity in IoT devices.

The last layer is called application layer. In this layer, users' requirement can be realized by variety kinds of applications. It can provide needed services to devise and users through applications. Because the most significant aspect of the layer is data sharing, it is seriously important to avoid information leaks and maintain data privacy.

An IoT security framework called SecIoT

The SecIoT framework is responsible for improving the security in IoT. It can provide security for IoT in four steps. Here we'll give an introduction of it as Figure 5 [21].

1. Authentication

The authentication module is in the center of the architecture. Because it connected with data providers and data consumers, the authentication consists of user authentication and device authentication.

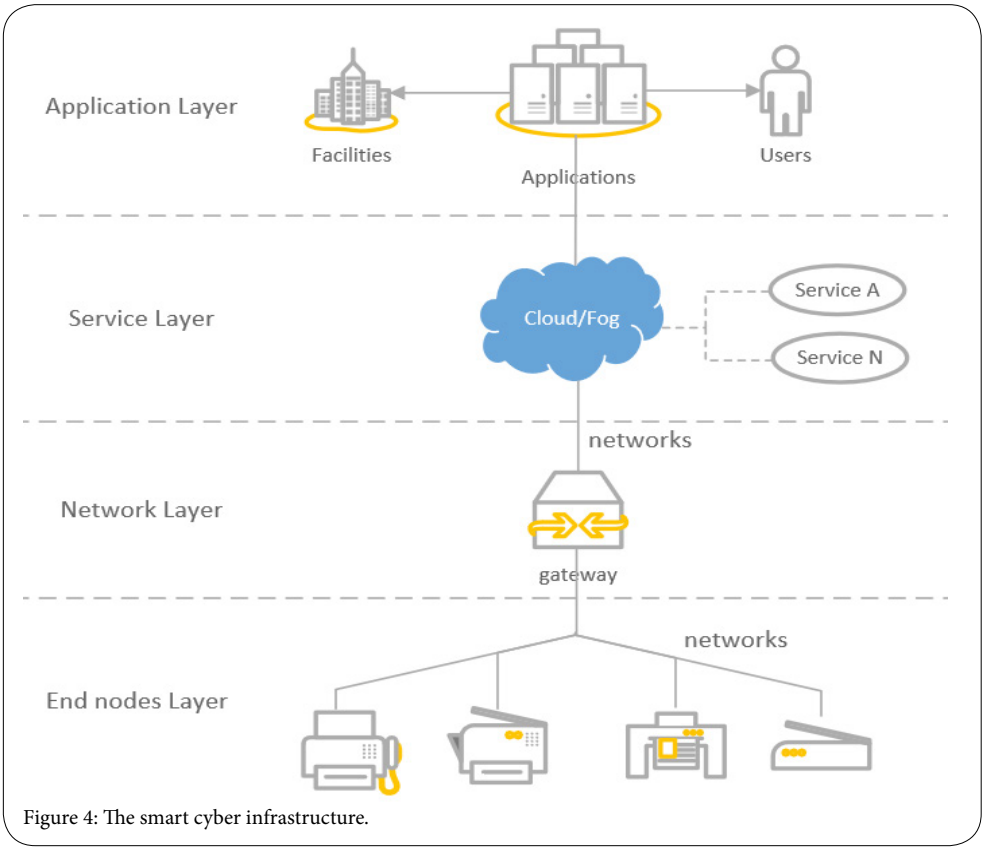

Figure 4: The smart cyber infrastructure.

2. Communication

In fact, the secure communication channel is usually a by-product of successful authentication. The process may use some of the user's credential, for example, public keys and their certificates. Because the IoT exists in the network ecosystem, providing support for security protocols is significant, as the security of IoT depends on the realizing degree in some extent.

3. Authorization

It is very significant for the system to identify whether the users have abilities to access specific data. So, the access control system is a necessary mechanism for protecting security. The role-based access control is a popular mechanism. Different users play different roles, so users with variety kinds of roles can carry out dissimilar jobs. For example, users can access corresponding resource or data, and perform specific operation.

2. Risk indication

A security indicator can indicate the risk degree of current configuration. And it can also help customers to know the security risks better. According to asset identification thread identification and risk evaluation the security indicator is generated. The asset identification can make sure the asset which should be protected, the

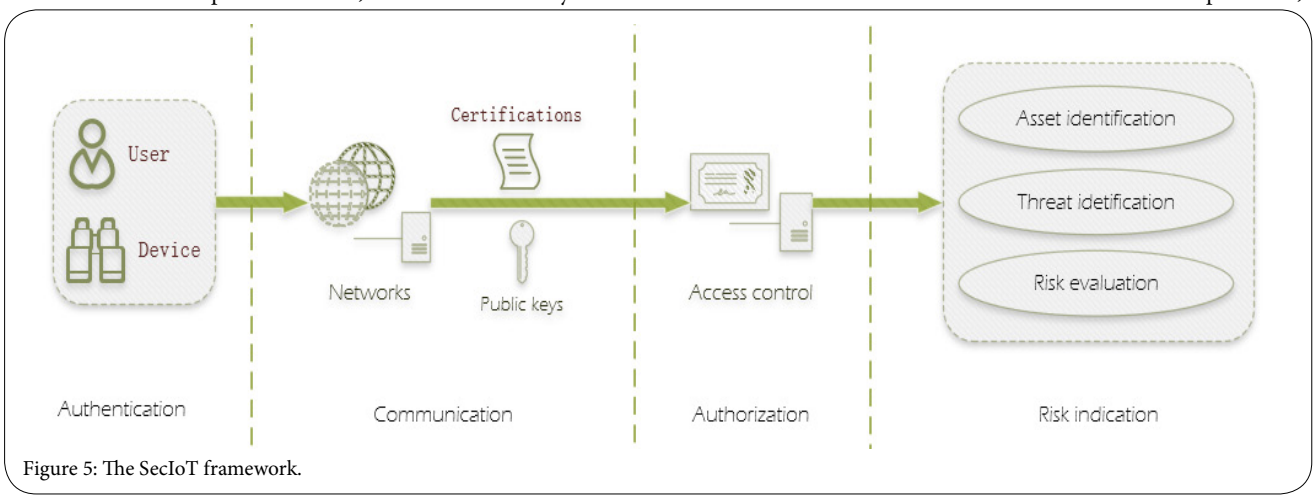

Figure 5: The SecIoT framework.

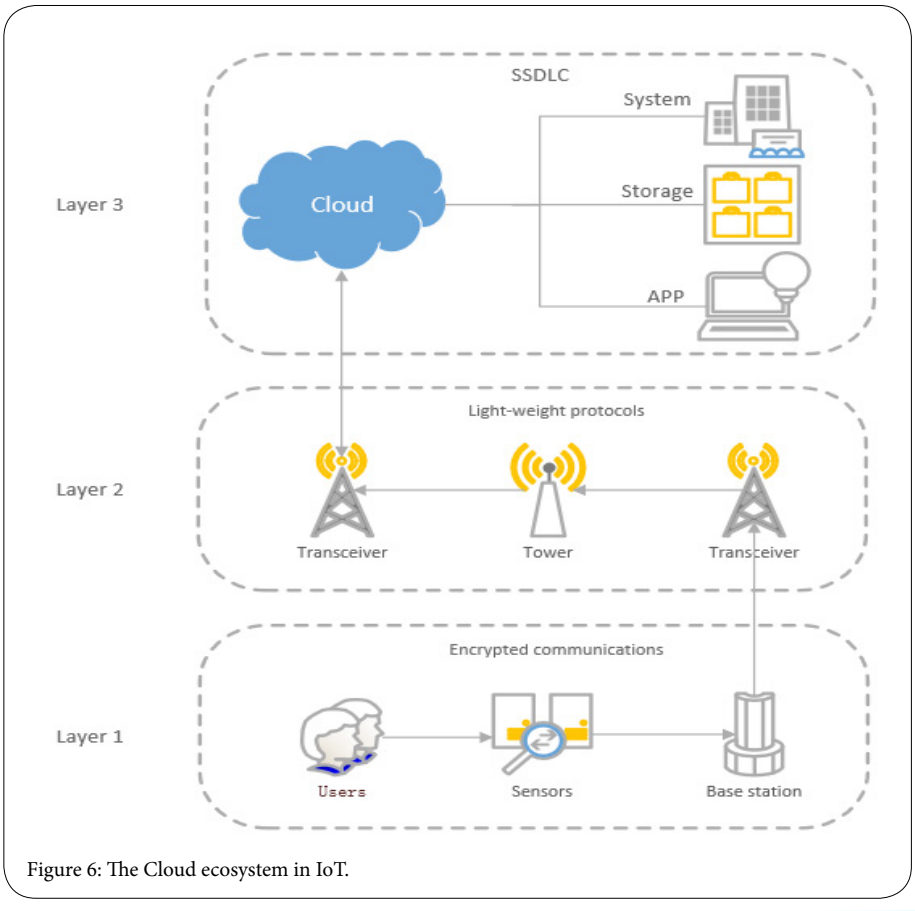

Figure 6: The Cloud ecosystem in IoT.

threat identification is able to identify the probable threat, and the risk evaluation can evaluate the results and influence caused by threat.

An IoT security framework for securing sensor in cloud ecosystem

We all know that sensor is a core part in an IoT system. So in a Cloud Ecosystem, it is without delay to protect sensors from being damaged. In this section, we'll introduce an improved framework on account of the traditional IoT architecture. There are three layers in this framework as is shown in Figure 6 [22].

The first layer is comprised of sensors and base stations. The sensor nodes have secure localization capability, and can sample, process, communicate complicated data and send it to the Base station. All these activities are implemented through encrypted communications. The base station plays a role of a secure gateway. It can guarantee the security of data which are send to the cloud.

The second layer includes Transceiver and Tower. Both of them are in charge of transmitting data between base station and cloud. Besides, preventing eavesdropping is a capacity as well. In this layer, the lightweight wireless protocols as Zigbee and RFID are used to giving an efficient protection.

The third layer consists of a Cloud, which includes applications, systems and the capacity of storage. The cloud can guarantee that only the authorized users have the ability to access and avoid privilege escalation. And SSDLC (Secure System Development Life Cycle) should be included in the cloud.

All above these layers are responsible for guaranteeing the security of the communication between authorized users.

Conclusion

IoT has several advantages such as high efficiency, low cost, and high scalability. Security issues have become extremely serious with the development of IoT. Because people focus on the services provided by the IoT environment, security issues have not received enough attention. This article introduced IoT security-related knowledge and introduced four different security frameworks in IoT. In addition, this paper has received suggestions from different scholars and can help companies, governments, and other agencies choose between existing security frameworks.

Funding

This work was partially supported by CERNET Innovation Project (No. NGII20180406), by Beijing Higher Education Young Elite Teacher Project (No. YETP0683), by Beijing Higher Education Teacher Project (No. 00001149).

Competing Interests

The authors declare that they have no competing interests.

References

1. Luigi A, Lera A, Morabito G (2010) The internet of things: A survey. Computer networks 15: 2787-2805.
2. Gubbi J, Buyya R, Marusic S, Palaniswami M (2013) Internet of Things (IoT): A vision, architectural elements, and future directions. Future generation computer systems 29: 1645-1660.
3. Kulkarni A, Sathe S (2014) Healthcare applications of the Internet of Things: A Review. International Journal of Computer Science and Information Technologies 5: 6229-6232.
4. Madakam S, Ramaswamy R, Tripathi S (2015) Internet of Things (IoT): A literature review. Journal of Computer and Communications 3: 164.
5. Barnaghi P, Wang W, Henson C, Taylor K (2012) Semantics for the Internet of Things: early progress and back to the future. International Journal on Semantic Web and Information Systems (IJSWIS) 8: 1-21.
6. Internet of things based on smart objects: Technology, middleware and applications. Springer Science & Business Media.
7. Jie Y, Pei J Y, Jun L (2013) Smart home system based on iot technologies. International Conference on Computational and Information Sciences. IEEE 2013: 1789-1791.
8. Siano P (2014) Demand response and smart grids-A survey. Renewable and sustainable energy reviews 30: 461-478.
9. Kyriazis D, Varvarigou T, White D, Rossi A, Cooper J, et al. (2013) Sustainable smart city IoT applications: Heat and electricity management & Eco-conscious cruise control for public transportation. IEEE 14th International Symposium on" A World of Wireless, Mobile and Multimedia Networks"(WoWMoM).
10. Li H, Lei X, Yan Z, ChunLi Y (2012) The application and implementation research of smart city in China. International Conference on System Science and Engineering.
11. Maheswari SU, Usha NS, Anita EAM, Devi KR et al. (2016) A novel robust routing protocol RAEED to avoid DoS attacks in WSN. International Conference on Information Communication and Embedded Systems.
12. Staake AT, Fleisch E (2009) Using sensor information to reduce the carbon footprint of perishable goods. IEEE Pervasive Computing 8: 22-29.
13. Xu LD, He W, Li S (2014) Internet of Things in industries: A survey. IEEE Trans Ind Informat 10: 2233-2243.
14. Suo H, Wan J, Zou C, Liu J (2012) Security in the internet of things: a review. International conference on computer science and electronics engineering. IEEE 3: 648-651.
15. Liu J, Xiao Y, Chen CLP (2012) Internet of things' authentication and access control. International Journal of Security and Networks 7: 228-241.
16. Zarpelão BB, Miani RS, Kawakani CT, de Alvarenga SC (2017) A survey of intrusion detection in Internet of Things. Journal of Network and Computer Applications 84: 25-37.
17. Ho HY (2015) Iot security & privacy: threats and challenges. Proceedings of the 1st ACM Workshop on IoT Privacy, Trust, and Security. ACM.
18. Arijit U, Bandyopadhyay S, Pal A (2014) IoT-privacy: To be private or not to be private. IEEE Conference on Computer Communications Workshops.
19. Monir S (2016) A Lightweight Attribute-Based Access Control System for IoT.
20. Pacheco J, Hariri S (2016) IEEE 2016 IEEE 1st International Workshops on Foundations and Applications of Self Systems (FAS*W) - Augsburg, Germany. IEEE 1st International Workshops on Foundations and Applications of Self Systems (FAS*W) - IoT Security Framework for Smart Cyber Infrastructures[C]// Foundations & Applications of Self Systems, IEEE International Workshops 2016: 242-247.
21. Huang X, Craig P, Lin H (2016) SecIo T: a security framework for the Internet of Things. Security and Communication Networks 9: 3083-3094.
22. Rahman AFA, Daud M, Mohamad MZ (2016) Securing sensor to cloud ecosystem using internet of things (iot) security framework. Proceedings of the International Conference on Internet of things and Cloud Computing. ACM.