A Novel Secure Architecture for the Internet of Things

Dong Chen, Guiran Chang, Lizhong Jin, Xiaodong Ren, Jiakia, Li, Fengyun Li
College of Information Science and Engineering
Northeastern University
Shenyang, China
chend.2008@gmail.com, chang@neu.edu.cn, jinlizhongneusoft@yahoo.com.cn, lifengyun@cc.neu.edu.cn

Abstract—With the development of the IoT, different wireless communication technologies and edge network infrastructures are continuously integrated. Therefore, the corresponding communication network environment has become more complex and the security issues involved in the IoT are more complex than any existing network infrastructures. The trust relationship between the heterogeneous entities, security communication, security system and other security issues are more complex and difficult to solve. In order to solve this kind of security problems, this paper gives the system structure, analyzes the security challenges and threats, proposes a novel security architecture for the IoT based on the research of these security demands, and eventually gives details of the designed security verification system.

Keywords—Internet of Things; Cyber Physical System; Secure Framework; WSN

I. INTRODUCTION

The Internet has undergone severe changes since its first launch in the late 1960s. 7 trillion wireless devices will serve 7 billion people in 2017 [1]. In such ambient environment not only user become ubiquitous but also devices and their context become transparent and ubiquitous. The term Internet of Things (IoT) is not well defined and remains difficult to come up with a clear definition [2].

Obviously, the IoT is a concept in which the virtual world of information integrates seamlessly with the real world of things. And the real world becomes more accessible through sensors, sensor embedded devices, computers and smart tiny devices in business as well as everyday scenarios. Different wireless communication technologies and network infrastructures are continuously integrated, including WSN, RFID systems, mobile vehicle network, 3G technology, WiMAX, personal area network (PAN), etc. As the IoT network has expanded rapidly and the corresponding communication network environment has become more complex, the security issues are more complex than any existing network systems.

The remainder of the paper is organized as follows. We give an overview of related influential works in Section II. In Section III, security requirements and challenges of the IoT network are further discussed in details. A novel secure architecture for the IoT based on the research on the architecture and security requirement is proposed in Section IV. In Section V, a security verification system of the proposed secure architecture for the IoT is designed, followed by the conclusion and future work of the paper in Section VI.

II. RELATED WORKS

The IoT as an emerging global Internet-based technical architecture facilitates the exchange of goods and services in global supply chain networks. However, it also has an impact on the security and privacy of the involved stakeholders. In [3], Weber argues that measures ensuring the architecture's resilience to attacks, data authentication, access control and client privacy need to be established. Mattern [4] has pointed out that much of the public debate on whether to accept or reject the IoT involves the conventional dualisms of ‘security versus freedom’ and ‘comfort versus data privacy’. The cloud computing data centers primarily based on personal data which is automatically collected and could be used by third parties without people’s agreement or knowledge for unknown and potentially damaging purposes. In [5], Ukil considers the embedded device security only, assuming that network security is properly in place, and provide the requirements of embedded security, the solutions to resists different attacks and the technology for resisting temper proofing of the embedded devices by the concept of trusted computing. However, existing works usually focus on one aspect of security and do not provide a complete security architecture as our paper does. To solve this issue, we proposed a secure architecture for the IoT.

III. SECURITY REQUIREMENTS

A. The IoT Architecture

As shown in Fig.1, we argue that this architecture is the most suitable model for the IoT which is composed of four layers, including perception layer, heterogeneous network access layer, data management layer and intelligent service layer. Through this architecture, users can easily exchange information between cyber world and physical world by intelligent services.

- **Data Perception Layer.** Trillions of things are connected into the IoT network in order to obtain the real-time ‘sensed’ data from their environment, including RFID Tags, 3G Phones, sensors, RFID sensors, sensor embedded devices and etc.
- **Heterogeneous Network Access Layer.** This layer can help heterogeneous networks to access to Internet/NGI ubiquitously through a widely range
wireless link, including Bluetooth, WiFi, Zigbee, WiMAX, GSM, WCDMA and Satellite.

- **Data Management Layer.** This layer is in charge of data management for the IoT. Therefore, in this layer, there are cloud computing centers, directory management servers, REST [6] based web service servers and etc.

- **Intelligent Service Layer.** The top layer provides various intelligent services towards the IoT users, such as precision agriculture, environment monitoring, intelligent transportation system and so on.

![Illustration of the IoT Architecture](image)

**Figure 1. Illustration of the IoT Architecture**

### B. The IoT Characteristics

The IoT imposes peculiar constraints in terms of connectivity, computational power and energy budget, which make it significantly different from those existing distributed systems. It can be noticed that the existence of tiny computing devices that form ubiquity in IoT domain are very much vulnerable to different security attacks. There are significant different key properties which cause security issues and raise novel security requirements.

- **Smart devices are usually mobile and connected to Internet/NGI via TCP/IP, 6LoWPAN, etc.**

- **Most networks of IoT are wireless networks through which sensors, sensor embedded devices, 3G phones and other smart devices can connect to Internet/NGI ubiquitously. A wide range wireless link can be employed, such as Bluetooth, WiFi, Zigbee, 802.11, WiMAX, GSM, WCDMA and etc.**

- **Heterogeneous smart devices span a range of computational abilities from PCs to RFID tags. Therefore, trust and privacy management mechanisms must accommodate even the simplest device.**

- **The number of devices in IoT is growing rapidly. It means that massive everyday things are increasingly integrated into the global IoT network. Therefore, it is so difficult for us to monitor privacy concerns.**

### C. Security Requirements

However, people may resist the IoT as long as there is no public confidence that it will not cause any serious threats to their privacy. The concept of privacy is deeply rooted into our civilizations and recognized in all legislations of civilized countries. [7]. In IoT, there are several significant different security requirements from any existing networks. The corresponding details have been listed as follows.

- **Data Perception Layer.** The edge network in data perception layer is usually comprised of WSNs which can connect to other networks and Internet through a smart gateway. Devices of this layer normally have limited calculation, communication and storage resources, and cannot meet the demand of traditional security technology. Therefore, design a lightweight key management protocol for data perception layer is a key security issue in the IoT. Furthermore, data perception layer is more vulnerable to an external attack, such as an external DoS attack against WSNs. Establishing effective lightweight intrusion detection and recovery mechanisms in order to improve the system robustness is another important security problem. Meanwhile, establishing trust and reputation model to evaluate suspicious nodes’ behavior can reduce the influence of malicious nodes significantly. This layer may be attacked by the following attacks: Sybil attack, Sinkhole attack, Wormhole attack, Hello Flood attack, Selective Forwarding, etc.

- **Heterogeneous Network Access Layer.** Since the IoT is a dynamic network infrastructure which is comprised of thousands of heterogeneous networks through interconnecting to Internet. Defense capability of the network varies in different networks. Therefore, during the design of a common security architecture for the IoT, we must consider the consistency and compatibility of the proposed security protocols, and ensure that their smooth transitions and seamless connections among different edge networks.

- **Data Management Layer.** The goal of data management mainly is to realize the effective massive data processing and network behavior based intelligent decision-makings. The core of data management is automatic processing technology which can help to implement massive data extraction, classification, filtering, identification and data mining. However, intelligent processing is not enough to detect malicious information. Therefore, designing an effective trust and repudiation management mechanism is an important challenge for data management layer in the IoT. During the collaboration among heterogeneous platforms might leak data owner's privacy, how to implement the separation between information content and information source, is another important challenge. In addition, according to sources of data on the reliability of the timeliness, establishing trust
evaluation mechanisms, realizing efficient mining etc. must also be considered carefully for data security mechanisms.

- **Intelligent Service Layer.** Security demands of the corresponding applications based on the IoT may significantly vary from one application to another one. Therefore, we must provide a suitable security service for a specific user according to its needs. In IoT, the same ‘sensed’ data may be shared by several applications. However, the data precision demands of these applications might be significantly different. Obviously, it will increase the risk of privacy exposure that we only provide the same precision of the corresponding information. How to provide appropriate precision for different application is a key challenge in intelligent service layer. IoT needs to establish security mechanisms to ensure that end users could enjoy convenience intelligent services and prevents any personal security and privacy crisis occurring. Massive things can establish directly communications between them, and this inevitably brings new security and privacy protection problems. Therefore, the IoT must make sure that things and persons will never be marked or tracked by unauthorized things (such as, equipments, services, application, persons, etc.). In order to solve this security issue, deeply research on identification and privacy protection technology is very critical. Meanwhile, the IoT also proposes a big challenge of traditional distributed database technology, since it involves massive data real-time storage and inquiry problems.

IV. A NOVEL SECURITY ARCHITECTURE

In this section, we propose a novel secure architecture for the IoT based on the research on the architecture and security requirement. Similarly, the proposed secure architecture is also comprised of four layers.

A. Secure Architecture

![Figure 2. A Secure Architecture for Internet of Things](image)

It can be noticed that the existence of tiny smart computing devices that form ubiquity in the IoT domain are very much vulnerable to different security attacks. Therefore, in order to circumvent the problem of security domain, we propose a novel security architecture for the IoT in this paper as shown in Fig.2. The security architecture consists of four layers in order to respond to specific security requirements in the corresponding layer in the given architecture in Fig.1.

B. Data Perception Layer

Smart devices in this layer often have limited calculation, communication and storage resources, and cannot meet the demand of traditional security technology. Therefore, it is a key security issue to design a lightweight key management protocol for data perception layer in the IoT. Moreover, this layer is more vulnerable to external attacks malicious nodes significantly. Security precautions mainly included in this layer are as follows,

- Secure routing.
- Key management.
- Intrusion detection.
- Wireless encryption.
- Reputation evaluation.

C. Heterogeneous Network Access Layer

Sensors, sensor embedded devices, 3G phones and other smart devices can connect to Internet/NGI ubiquitously. A wide range wireless link can be employed, such as Bluetooth, WiFi, Zigbee, 802.11, WiMAX, GSM, WCDMA and etc. Heterogeneous smart devices may span a range of computational abilities from PCs to RFID tags. Therefore, trust and privacy management mechanisms must accommodate even the simplest device. Network defense and counter measures involved in this layer mainly include,

- User privacy.
- Data encryption.
- Data integrity.
- Multicast Security.
- Entity authentication.
- Access security.

D. Data Management Layer

In order to realize the effective massive data processing and network behavior based intelligent decision-makings, establishing trust evaluation mechanisms, realizing efficient mining etc. must be considered carefully for data security mechanisms according to the reliability and timeliness of the corresponding data sources. The core technology of data management is automatic processing technology which can help to implement massive data extraction, classification, filtering, identification and data mining. Therefore, the security defense and counter measures involved in this layer mainly include,

- Behavior entities certification
- Data metric
- Key generation and distribution
- Security computation
- Secure communication
- Service multi-party computation

313
E. Intelligent Service Layer

In order to provide a suitable security service for a specific user according to its needs, we must provide appropriate precision for different application in intelligent service layer. The IoT also needs to establish security mechanisms to ensure that end users could enjoy convenience intelligent services and prevents any personal security and privacy crisis occurring. Obviously, the security defense and counter measures involved in this layer mainly include:

- Access control management
- Security management
- Privacy protection strategy

We argue that the proposed four layers secure architecture for the IoT is a unified architecture for the various novel applications.

V. SECURITY VERIFICATION SYSTEM

In this section we design a security verification system towards the precision agriculture of the IoT.

A. System Structure

![Figure 3. The Perception Layer Devices](image)

3G smart terminals can directly visit the restful web service server if passed the user authentication process. Then these smart devices can also query history data sensed from the surroundings. In the system, we allow a smart terminal to access to the WSN edge network in order to query, control, manage, and configure sensor nodes in the underlying perception layer. Web server confirmed recognition, 3G smart devices can access and control resources employ the RESTful service provided by the Web server. The secure communication between a 3G smart object and a Web server can be enhanced by the session key. As shown in Fig.3, the security verification system is comprised of four layers as described in Fig.3.

![Figure 4. The Perception Layer Devices and the Smart Gateway (Restful Web Service)](image)

- The Perception Layer Devices: Sensor Nodes (temperature, moisture, luminance, as shown in Fig.4), CC2530, 2.4GHz. Powered by two AA rechargeable batteries.
- Heterogeneous Network Access Layer Devices: Smart Gateway (shown in Fig.4), OMAP3530, CORTEX-A8 Processor, 1030MHz, 256M DDR. Powered by two AA rechargeable batteries or USB cable.
- Data Management Layer Devices: Data Center, Intel(R) Core (TM) i5, M540 @ 2.53GHz, 4GB RAM, OWB 11g.
- Intelligent Service Layer Devices: Restful Web Server, Intel(R) Core (TM) i5, M540 @ 2.53GHz, 2GB RAM.

VI. CONCLUSION AND FUTURE WORKS

With the development of the IoT, different wireless communication technologies and network infrastructures are continuously integrated, including WSN, RFID systems, mobile vehicle network, 3G technology, WIMAX, PAN, etc. However, the corresponding communication network environment has become more complex and the security issues involved are more complex than any existing network infrastructures. This paper gives a novel system architecture, proposes a novel network secure framework that is to adapt to the future IoT, and finally gives details for the security verification system designed by us.

ACKNOWLEDGMENT

This work is supported by the National Natural Science Foundation of China under Grant No. 60903159 and the Fundamental Research Funds for the Central Universities under Grant No. N100604012.

REFERENCES