IOP Conference Series: Earth and Environmental Science

PAPER • OPEN ACCESS

Research on Defects and Countermeasures of Internet of Things Security Technology

To cite this article: Jie Lin 2019 *IOP Conf. Ser.: Earth Environ. Sci.* **252** 032198

View the article online for updates and enhancements.

This content was downloaded from IP address 220.168.52.245 on 10/10/2019 at 01:10

Research on Defects and Countermeasures of Internet of Things Security Technology

Jie Lin

Xi`an Jiaotong University, Xi`an, 710000, China

Abstract. This paper analyzes the necessity and combination of the two models, proposes the cloud computing-based IoT architecture, and studies the security threats faced by the application layer in the three-tier architecture of the Internet of Things based on the cloud computing platform. The cloud-based IoT security architecture. The method proposed in this paper can effectively improve the security of the Internet of Things application system.

1. Introduction

In the context of the current booming cloud computing and Internet of Things, the cloud computing-based IoT needs such as improving security conditions and technology improvements are properly handled, and the cloud computing-based Internet of Things can be implemented to form an implementation policy in network services. Security architecture. We will conduct a more in-depth study of the above issues and try to come up with more reasonable, effective and innovative solutions and ideas.

2. Security Requirements and Security Analysis of Internet of Things System

The Internet of Things has brought great convenience to people's lives, and people's lifestyle has undergone tremendous changes. However, the Internet of Things is the latest technology, and it is still in the initial stage of development. There are a series of problems in the development process, among which security the problem is most significant. The specific surface is in the following aspects: The security issues faced by the sensing layer mainly include security threats to radio frequency identification technology and security threats to wireless sensor networks. The network layer has the ability to ensure efficient and accurate data transfer. First of all, because the Internet of Things is characterized by huge data nodes and a large amount of data, when a large number of users use the network at the same time, it often causes the system to run slowly and cannot log in to the system smoothly. The application layer provides a wide range of data sharing and data exchange services. It is mainly based on the cloud computing platform. Therefore, the security issue facing this layer is the security issue of the cloud computing platform.

The security requirements of the IoT application layer include: how to configure access rights management massive data in the IoT network; how to protect the personal information of the application system users, and ensure that the information is authentic and reliable when the user authenticates. In response to the above questions, after careful consideration and summary, the author made the following recommendations: (a). Authentication. Identity authentication is the initial link of the Internet of Things, so the IoT system must be designed with an effective identity authentication function. (b). Enhance user information security. In the application process of the Internet of Things, the security issue is a very prominent problem, which is related to the immediate interests of the user.

Content from this work may be used under the terms of the Creative Commons Attribution 3.0 licence. Any further distribution of this work must maintain attribution to the author(s) and the title of the work, journal citation and DOI.
Published under licence by IOP Publishing Ltd

Therefore, the application system must put the security requirements first in the design, and develop a set that allows users to use it with confidence. System. (c). Availability. Usability refers to the combination of large data volumes and other complex factors in the provision of services, authenticated users can still log in and operate the system. (d). privacy. Privacy means ensuring that private data information is not viewed by individuals other than those in the application system. The privacy information contains a lot of content, such as name, occupation, contact information, user location and so on. (e). Controllability. Controllability is a means of regulating the reasonable use of programs by users to ensure the security of the IoT environment and the ability for users to legally execute various programs. (f). Access the application system. Access to the application system refers to the process of interactive transmission of data information between the user and the application system. In the future, the Internet of Things system will be continuously upgraded, and the upgraded system will support unified identity authentication, which is the direction that many program development companies are constantly striving.

3. User data categories in IoT applications

The system mainly provides services for users. Therefore, most of the information in the system is user information. Only users are more complete and more specific, so as to better serve users. User information can be divided into two categories: static information and dynamic information.

Dynamic information, as its name implies, is information that can change automatically over time, such as user login time, login location, etc., which will change accordingly in different time periods. Due to the uncertainty of dynamic information, it cannot be used as data for system user login verification. However, dynamic information can provide a reference for the system to determine whether the user's identity is secure.

Static information is the form of information corresponding to dynamic information. It does not change automatically over time. If no manual changes are made, the static information will remain unchanged. The information that the user enters when registering the system is static information. Static information can be used as valid data for system users during the authentication process.

4. User trust level calculation

The rapid development of the logistics network has a large number of security risks, which also makes many businesses face no small risks in the application of the Internet of Things, so the security issue is an urgent problem to be solved. And an effective trust model can minimize risk. Through the above introduction, we know that user credibility has a correlation with system security, and the trust model can describe the state of user information through specific data conversion.

(a). User dynamic information collection

First, pick a set of dynamic information and define it. The set is represented by U, u1u2, etc. represents the selected dynamic information, and the mathematical formula is: U= $\{u_1, u2\ldots\}$. Taking the user dynamic information listed in the above section as an example, the dynamic information selected here has a login location, a login time, and the like.

(b). Weight set of user dynamic information

Different dynamic information has different security levels, and their importance is different. The letter q is used here to indicate the weight to reflect the importance of the information. The larger the q value, the more important the information is. Here, the letter Q represents the weight set, q_1,q_2… represents the enumerated dynamic information weights, and the weight set of the dynamic information is the weight set of the dynamic information Q=$\{q_1,q_2\ldots\}$.

In order to obtain the weight set, the elements in the dynamic information set are compared, and the corresponding degrees are given according to the importance of the comparison. The specific weight set is shown in formula (1).

$$q_i = \frac{\sum_{j=1}^{n} b_{ij}}{\sum_{j=1}^{n} \sum_{k=1}^{n} b_{kj}} \qquad \text{i=1, 2,} \cdots \text{, n} \tag{1}$$

(c). The credibility of the information stored in a single application system

User credibility can be converted, as shown in the table below. Similarly, specific scoring criteria can also be based on actual application systems. Individual items are deducted from individual scores to obtain a confidence ratio, as shown in equation (2):

$$m_i = {h_i}/{H_i} \tag{2}$$

In equation (2), i is the index of the dynamic information, m is the reliability ratio, h is the single-item score, and h is the single-item score. The confidence ratio m ranges from 0 to 1, which indicates that the credibility of the system user is reflected in a single dynamic message.

The dynamic information credibility scale value set is denoted by M, and m_1, m_2, m_3 represents the specific dynamic credibility scale value, then the credibility scale value set is $M = \{m_1, m_2, m_3\}$.

The set of credibility of dynamic information is represented by F, and $f_1, f_2, \cdots, f_n$ is the specific credibility of dynamic information, then the credibility is determined by vector $F = \{f_1, f_2, \cdots, f_n\}$. The formula for calculating the f value is as shown in the formula (3).

$$f = Q * M = [q_1 \; q_2 \; q_3] * \begin{bmatrix} m_1 \\ m_2 \\ m_3 \end{bmatrix} \tag{3}$$

(d). User credibility in a unified authentication system

Assume that there are n application systems for unified authentication. Here, the letter L indicates its security level set, *l₁,l₂,…,lₙ* respectively indicate the corresponding application system security level, then the application system security level set L={*l₁,l₂,…,lₙ*}. The quantized values of the application security level are normalized according to the application system number and then expressed in the form of a collection. The set of application security levels multiplied by the credibility set of dynamic information is user credibility. Here we use the letter k to indicate the user credibility in the unified authentication system, then:

$$K = L * F = [l_1 \; l_2 \cdots l_n] * \begin{bmatrix} f_1 \\ f_2 \\ \vdots \\ f_n \end{bmatrix} \tag{4}$$

(e). User credibility and user security level

The relationship between the above two can be illustrated by FIG. It should be noted that the user security level here is the security level of the authentication mode selected during the verification process.

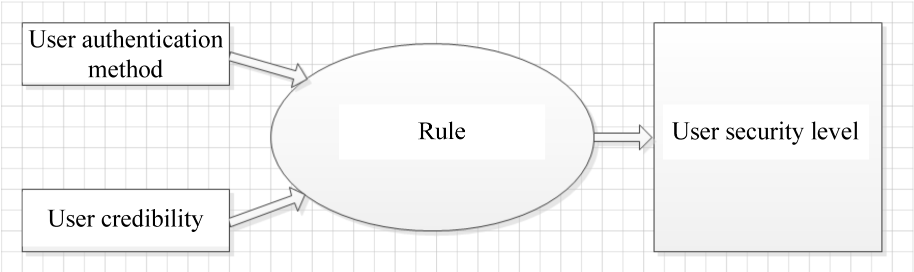

Figure 1. User security level diagram

According to the above algorithm, we can get the credibility of the user. From the above analysis, we can see that the user credibility is derived by the dynamic system through certain conversion, and then summarized, and the user security level is obtained based on the user verification security level. Based on the credibility, the user dynamic information is checked during the user authentication process to ensure the security of the user account.

5. Internet of Things Smart Meter System

A smart meter is a smart meter with microprocessor application and network communication technology as its core. With automatic metering / measurement, data processing, two-way communication, function expansion and other functions. It can realize two-way metering, remote/local communication, real-time data exchange, various types of electricity price billing, remote power-off power supply, power quality monitoring, user interaction and other functions. Smart metering systems based on smart meters can support smart grid requirements for load management, distributed power access, energy efficiency, grid scheduling, electricity market transactions, and energy savings.

The smart meter system consists of three parts: a smart meter node, a gateway node, and a database server. The working principle of the system is shown in Figure 2.

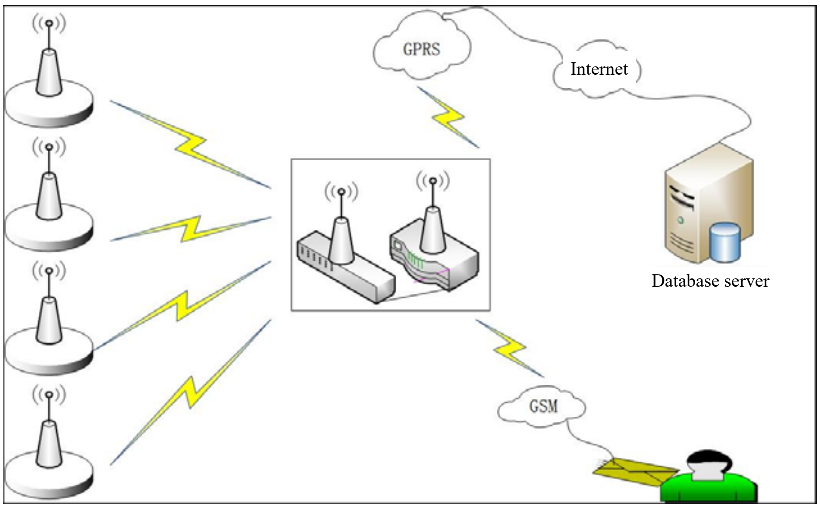

Figure 2. IoT smart meter system working diagram

It is very important to add a unified authentication and authorization system to the smart meter system. Its specific meaning is reflected in the following two points:

(a). The design and development of the unified authentication and authorization system can meet the user's jump in different application systems. Smart meter systems are more complex and variable, and there are many applications with different functions. These applications have different connections. When the IoT smart meter application system is running, smart meter users can access other application systems or access multiple different application system services. If the user invokes each application system, the system user also needs to manually enter user information to perform login verification. This situation violates the transparency of application integration and does not achieve the effect of application integration.

(b). When multiple systems are required to log in, the unified authentication and authorization system provides users with a unified authentication service. It does not require the system user to perform tedious and repeated input authentication information on the user terminal, thus greatly shortening the user operation time. In addition, adding security levels to a unified authentication and authorization system ensures the security of switching access between multiple IoT applications and effectively performs security verification for different application systems and system users.

6. Analysis of the authentication process of the Internet of Things smart meter system

In the layered authentication and authorization method, the hierarchical access policy, as the name implies, has multiple levels of access policies, that is, the user's login verification method can select different levels. Its security level is an important determinant of the security level in a security policy. In this article, login verification methods are divided into three levels, namely low-level, intermediate, and advanced.

If the user passes a high security level of authentication, then the user's security level will determine the security level of a user, which is calculated by the security level. When a user requests access to the smart meter system, only after the security level meets the standards required by the system, the user will successfully pass the security verification and obtain the right to query the account related data within the scope of authority. Give the user the power to query the account-related data within the scope of the permission.

When the user's security level is high, the user's dynamic information changes. For example, if the user's terminal location is changed twice, or if there are two illegal operations, the credibility of the user is lowered. When the system re-measures the user security level, the levels of these users are adjusted to a lower level. At this time, the user sends an access request to the smart meter system. Since the security level does not meet the standard, the security level authentication of the IoT smart meter system cannot pass, and the Internet of Things smart meter system will reject the user's access.

As can be seen from the above description, the steps of the user's authentication process in the unified authentication and authorization system include the following aspects:

(a). In the unified authentication module, the user identifies the user's information by receiving dynamic information;

(b). In the authorization decision module, two forms are used to identify whether the user is safe, one is the security level of the user, and the other is the security level of the system;

(c). In the authorization decision module, how is the unified authorization completed? This is a step of extracting user information from the IoT smart meter system and then assigning roles and user groups to those users.

All in all, this unified authentication security mechanism is very effective, not only provides a secure authorization and authentication method, but also further enhances the security of user login.

7. Conclusion

This paper proposes a multi-level authorization and authentication method based on the analysis of the security requirements of the Internet of Things application system, based on the existing authorization technology and access control algorithm, combined with the idea of effective system integration. At the end of the article, the unified authentication and authorization design of the Internet of Things smart meter application system was carried out.

References

[1] [1] Nie Xiao. Research on Internet of Things Security Based on Cloud Computing [J]. Industrial and Mining Automation, 2013, (4): 47-50.

[2] [2] Sun Hong, Yang Li. Research on security issues of Internet of Things based on cloud computing [J]. Electronic Technology, 2015, (9): 175-179.

[3] [3] Barroso LA, Dean J, Holzle U. Web search for a planet: The Google cluster architecture. IEEE Micro, 2013, 23(2): 22−28.

[4] [4] Zhang Jianxun, Gu Zhimin, Zheng Chao. Summary of research progress in cloud computing