ATLANTIS PRESS

Advances in Engineering Research, volume 173

4th Workshop on Advanced Research and Technology in Industry Applications (WARTIA 2018)

Research on Internet of Things Security Technology Based on Cloud Computing

Wu Junying[1], Zhu Jinhui[2], Li Jingquan[2], Xin Rui[1], Chen Liandong[1], Lu Xin[3]

[1]State Grid HeBei Information & Telecommunication Company, HeBei ShiJiaZhuang 050021, China

[2]State Grid HeBei Company, HeBei ShiJiaZhuang 050021, China

[3]SGIT-GreatPower, Fujian, Fuzhou, 350003, China

Keywords: cloud computing, Internet of Things, security technology, convergence

Abstract: With the all-round development and advancement of information technology, the integration of cloud computing and Internet of Things technology has become an inevitable trend of Internet development. The Internet of Things is the process of connecting the Internet with the sensor network and the overall development is to establish an intelligent management system. Cloud computing is to provide assistance by applying a large-scale computing platform to expand coverage. This paper briefly analyzes the connotation of cloud computing and IoT technology, and explains the integration process of the two, focusing on the cloud computing-based IoT security technology system, for reference only.

1. The Connotation of Cloud Computing and Internet of Things Technology

1.1 Connotation of Cloud Computing

Cloud computing is a systematic processing method, which effectively performs more unified scheduling and processing of network connection computing resources, rationally constructs computing resource modes, and provides corresponding services according to user needs. The resource system and network structure formed by it is the "cloud". It is worth mentioning that for the user, the "cloud" has the infinite expansion nature, which can be obtained at any time, and can be obtained on demand, or paid according to the use process. This infrastructure can carry out activities for people, provide timely and professional guidance. With the help of the centralized management mechanism, the enterprise data center management mechanism and the computer data management and control system can be kept dynamic and consistent. Moreover, in combination with people's needs to access computers and storage systems, data transmission management channels can be established while improving the convenience level [1].

In addition, cloud computing is based on two core technologies: resource virtualization and distributed parallel architecture. At the same time, the Internet also provides more open source software to provide technical support for user application cloud computing, including Xen, KVM, Lighttpd, Memcached, Nginx, Hadoop, Eucalytus and other applications are more extensive. The cloud computing process is more complicated, and the hypothesis function can be used to predict the exponential cluster. The specific formula is $h(\theta) = 11 + e - \theta TX$" role ="presentation"> $h(\theta) = 11 + e\theta TXh(\theta)) = 11 + e\theta TX$.

1.2 Internet of Things Technology Connotation

Internet of Things technology is a key component of the development of Internet technology in the new era. With the Internet of Things technology, a series of intelligent components such as terminal equipment, intelligent facilities, mobile terminals and facility sensors, or intelligent "dust" connections can be realized. The Unicom management system uses wireless and wired to establish a long/short distance IoT architecture system. The cloud-based SaaS integrated operation system has also become an important operational benchmark for network systems such as intranets and private networks [2]. In addition, in the Internet of Things system, individuals can be personalized and real-time monitored and managed by means of information security, and location and trace processing, alarm linkage processing and online upgrade processing are completed to ensure the establishment of efficient, energy-saving and operational management integration joint mechanism. The infrastructure is shown in Figure 1:

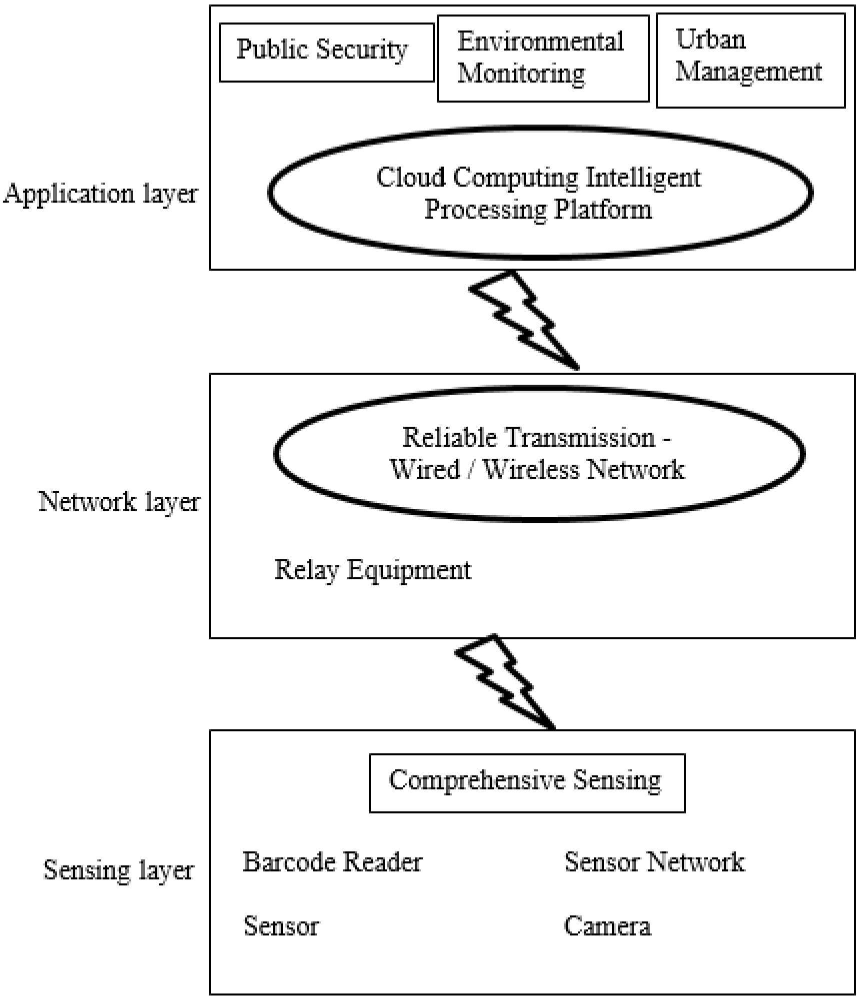

Figure 1: Schematic Diagram of Cloud Computing-Based Iot Architecture

The specific functions of each level are shown in Table 1:

Table 1: List of Functions at All Levels of the Internet of Things

Hierarchy name	Component	Effect
Perceptual layer Sensors	Sensor, sensor gateways, including QR code labels, readers, etc.	The nerve endings equivalent to "eye, ear, nose and throat" can recognize objects and collect information.
Network layer Private network	Private Internet, Internet, wired communication network, wireless communication network, cloud computing platform	This is equivalent to "central nerve" is mainly to transmit information, and process data acquired by the sensing layer
Application layer	Internet of Things and user interface	To meet the needs of the industry, realize the intelligent application of the Internet of Things.

2. The Integration Process of Cloud Computing and Internet of Things Technology

In the process of application of Internet of Things technology, it is necessary to give full play to the spatial characteristics of cloud computing and effectively establish a harmonious interconnection and interoperability processing system. Cloud computing is still in a new type of technology in practical applications, based on distributed computing, parallel computing and virtualization processing. Therefore, the fusion process of cloud computing and Internet of Things provides a massive reference for the Internet of Things. Data and implement the stored process. In the IoT system, the technical structure should connect the basic units such as the radio frequency identification process and the global positioning system according to the basic protocol, effectively realize the communication between the information sensing device and the Internet, and ensure that the information interaction and transmission can meet the real-time requirements, thus perfecting Intelligent identification and tracking of monitoring processes.

It is based on the continuous development and progress of the Internet of Things technology. In order to effectively collect and organize the massive information, it is necessary to use more convenient means and methods to build an effective processing structure. At this time, the cloud computing platform provides it more convenient. The path of using the cloud computing platform to complete information storage and control, and building an IoT linkage structure can improve information computing efficiency and storage capacity while reducing costs, laying a solid foundation for the sustainable development of Internet of Things technology [3].

3. Cloud Computing-Based Iot Security Technology System

In combination with the various hierarchical functions and application environments in the Internet of Things system, in order to improve data and information processing and management and control effects, it is necessary to optimize the technical management path and management and control level, and improve the management process according to the essential attributes of the Internet of Things and the actual application characteristics. The foundation for the comprehensive development of networked control work. In other words, to maintain the level of IoT security technology based on cloud computing, regional security management is required for the perception layer, network layer and application layer [4].

3.1Perceptual Layer Security Technology System

In the cloud computing IoT technology architecture, the sensing layer is the most basic hierarchical structure, and its main responsibility is to collect and summarize information. Therefore, only by maintaining information security from the source, can we rationally improve the security level of the Internet of Things. However, at present, there are still some prominent security risks in the perception layer.

First, local security, especially for some more complicated and dangerous mechanical work, the Internet of Things often replaces the manual work. The practice of some sensory nodes is often unsupervised, which provides convenience for attackers. The attacker can easily search for the corresponding device, destroy it, and even replace the software and hardware with the local operation, resulting in the initial structural change of the data, resulting in serious economic losses.

Second, the energy processing is insufficient. In the process of application and operation of the sensing layer, if the attacker uses the protocol vulnerability to communicate continuously, the energy of the internal nodes of the system sensing layer will be exhausted. Because the basic functions of the IoT layer nodes are relatively simple and the energy carried is limited, the attacker will attack the network with the gaps exhausted by the energy nodes, causing damage to the IoT operation structure and basic operation quality. The integrity of the overall management process.

Third, in the process of IoT operation, because the Internet of Things can connect multiple network media and heterogeneous network structures in real time, it is necessary to apply cross-network authentication mechanism to achieve data connectivity, and this process is relatively fragile. Subject to DOS attacks, the problem of information interaction and processing cannot be carried out in an orderly manner. In addition, the asynchronous attack process, the collusion attack process, etc. will cause some damage.

Fourth, in the era of the continuous development of Internet of Things technology, the protection of private information has become the key. Every item of each person is connected in the network system, and the degree of perception and depth of perception are significantly increased. With real-time supervision and maintenance, there will be problems of misappropriation of business information and theft of personal information. Therefore, in order to achieve comprehensive progress and development of the Internet of Things, security and privacy management is critical.

3.2 Perceptual layer security technology

In response to the threats and problems existing in the Internet of Things, relevant technical departments have developed corresponding technologies, and corresponding technical systems and operational networks have to be established in conjunction with actual needs [5].

First, the secure routing protocol, the RFID security protocol itself is the focus of IoT technology security research, using the Hash function and security protocol to establish the corresponding comparative analysis. The so-called Hash function is to compress a string into an integer by an algorithm. This number is called Hash, for example:

```
unsigned long HashString(char * lpszFileName, unsigned long dwHashType)
{
    unsigned char * key = (unsigned char *)lpszFileName;
    unsigned long seed1 = 0x7FED7FED, seed2 = 0xEEEEEEEE;
    int ch;
    while(*key != 0)
    {
        ch = toupper(*key );
        seed1 = cryptTable[(dwHashType < < 8) ch] ^ (seed1 seed2);
        seed2 = ch seed1 seed2 (seed2 < < 5) 3;
    }
    return seed1;
}
```

The position of the string in the file can be processed to complete the direct reading work.

Second, intrusion detection and prevention. Combined with the requirements of Internet of Things technology, relying on the cryptosystem can still not complete the defense of all attacks. However, the use of intrusion detection technology can provide a better barrier for information transmission, effectively intercepting data or information that violates the security policy behavior. The reporting system ensures that some unauthorized operations are avoided and the impact of exception handling processes on IoT security is reduced.

Third, key management. In the security management of the IoT awareness layer, key technology is widely used, mainly encryption technology and key decryption technology to ensure the degree of synergy of authentication operations, effectively establish a layered sensor network key processing process, and ensure the key. Analyze the rationality of management work [6].

3.3 Network Layer Security Technology System

3.3.1 Network Layer Security Threats

For the Internet of Things (IoT) system, the network layer is a key hierarchical structure for collecting and collecting data from the sensing layer. It can control the data and effectively complete the routing processing operation. It is a complex multi-network overlay open system. Many security risks need to be highly concerned by relevant technical departments.

First, distributed denial of service attacks. In the process of running the network layer structure, outside attackers will use a short time to send and process a large number of requests, which will occupy more network resources while overwriting the network, causing the entire network to operate. The efficiency of the structural operation is limited, and even the normalized flow rate is limited.

Second, in the network information operation system, false network information and man-in-the-middle attacks will also affect it. On the one hand, the false network information is mainly caused by the attacker using the forged communication network for signaling indication, which causes the user to receive the wrong instruction, which seriously restricts the overall operation structure and operation flow. On the other hand, man-in-the-middle attacks rely on MITM attack devices or gateways, which limits the realism of request and response information, and severely restricts the efficiency and authenticity of the entire network.

Third, cross-heterogeneous network attacks, such problems are more serious, and even cause the paralysis of the entire network system, affecting the level of network security management [7].

3.3.2 Network Layer Security Technology

In order to ensure the comprehensive efficiency of network layer security management, it is necessary to actively implement the corresponding authentication mechanism and improve the overall network layer management level with security technology.

First, the authentication mechanism mainly authenticates the identity and information, and centrally checks and verifies the identity of the other party by means of a fixed method, effectively uses the communication parties to complete the basic work, and uses the exchange session key as the basis for communication and authentication. It should be noted that in the exchange session, confidentiality and timeliness are more critical, which not only ensures that the information is transmitted in ciphertext form, but also reduces the loss caused by message retransmission.

Second, the access control mechanism is mainly based on the role access control to ensure the consistency of the role access resources. In the process of the access control work, the user can legally use the resource authentication and control mechanism to ensure that the access policy can be used for resources to protect access rights [8].

3.4Application Layer Security Technology System

3.4.1 Application Layer Security Threats

In the process of data exchange and processing at the application layer, virtualization and data privacy issues pose a threat to its operational security. Because the cloud computing platform relies on virtualization technology, although resource sharing can be realized, because no data is encrypted, some illegal users may cause security problems during the access process. The data privacy issue is the most important topic in the "cloud" technology. After the data is uploaded to the "cloud", most users do not know the specific location of the data storage, and the data owner loses the data completely control, affecting its safety.

3.4.2 Application Layer Security Technology

At present, the application of data isolation technology is extensive. In the process of running the cloud computing platform, in order to avoid the access of different virtual users of the same physical server, the user data is isolated, and a feasible Internet of Things environment is constructed, thereby effectively completing data backup. Improving the scalability and data compatibility of storage devices can effectively improve the security level of data processing [9].

4. Conclusion

All in all, cloud computing and IoT integration have become the development trend of the times. To improve the application level of the grid, it is necessary to establish a more systematic security management mechanism to ensure that network security technology can exert its actual value.

References

[1] Qin Gong. *Research on Internet-based Security Technology Based on Cloud Computing*[J]. Computer Knowledge and Technology,2015,11(25):13-14.

[2] Zhiwei Shen, Yezhou Xin. *Analysis of Cyberspace Security Architecture Based on New Technology*[J]. Internet World, 2015 (10): 20-23.

[3] Xiaoli Lu. *On the New Network Security Technology Under the Background of Cloud Computing*

and Internet of Things [J]. Network Security Technology and Application, 2016(10): 76-77.

[4] Zhihao Huang. *Open Platform and Application Software Development of Mobile Network Cloud System* [D]. Guangdong University of Technology, 2015.

[5] Fu Mo, Jiagang Dai, Yubao Zhou, etc. *Cloud Computing Technology--Inevitable Choice for the Development of Digital Hospitals*[J]. Modern Electronic Technology,2016(5):47-50.

[6] Qun Zhou. *Research on Cloud Data Storage Security and Related Technologies in the Internet of Things Environment* [J]. Electronic World, 2017 (9): 156.

[7] Qiang Wang. *Research on Key Technologies of Big Data Processing Based on Internet of Things*[J]. Computer Knowledge and Technology, 2018, 14(12): 29-31, 39.

[8] Qing Hu, Shichao Lv, Zhiqiang Shi et al. *Advanced Continuous Threat Cloud Detection Game Based on Expert System*[J]. Computer Research and Development, 2017, 54(10): 2344-2355.

[9] Haipeng Ren, Jicai Fang, Jing He et al. *Research on Cloud Data Storage Security Technology in the Internet of Things Environment* [J]. Wireless Internet Technology, 2015, (17): 24-25.