American Journal of Networks and Communications
2020; 9(1): 11-16
http://www.sciencepublishinggroup.com/j/ajnc
doi: 10.11648/j.ajnc.20200901.12
ISSN: 2326-893X (Print); ISSN: 2326-8964 (Online)

Research on Security Evaluation Indicator System of Smart Home

Yan Changshun*, Shao Yong

Faculty of Information Technology, Beijing University of Technology, Beijing, China

Email address:
yuewuxing@bjut.edu.cn (Yan Changshun), shaoyong@bjut.edu.cn (Shao Yong)
*Corresponding author

To cite this article:
Yan Changshun, Shao Yong. Research on Security Evaluation Indicator System of Smart Home. *American Journal of Networks and Communications.* Vol. 9, No. 1, 2020, pp. 11-16. doi: 10.11648/j.ajnc.20200901.12

Received: October 18, 2020; **Accepted**: November 19, 2020; **Published**: November 27, 2020

Abstract: Nowadays, smart home technology is still in continuous development; more and more enterprises and organizations began to enter this industry. However, the security problems and the unknown of emerging technologies make that most people are still in the wait-and-see stage for smart home systems. Under the background that many enterprises have different opinions on the security of smart home systems, this study is committed to forming a set of general evaluation standard index system. The main research work of this paper: the influencing factors of smart home system security are analyzed; according to the characteristics of smart home system equipment, the system security is divided into four aspects: control system, communication technology, intelligent products and cloud services; based on the current national standards, combined with the safety standards of various organizations, safety indicators are selected for each aspect. Finally, the established smart home system security evaluation index system enables users to have a set of relatively general evaluation methods among many different standards to compare and consider the current smart home system with various brands. It is helpful for users to try or further understand the smart home industry to promote the development and progress of the smart home industry.

Keywords: Smart Home, Security Evaluation, Indicator System

1. Introduction

In recent years, more and more companies have launched their own smart home systems, and the safety standards of these systems are varied. Each company will adopt different standards to evaluate their own products, and the evaluation results are undoubtedly confusing and unreadable for ordinary users. After summing up these evaluation results, we will find that due to the different standards adopted, a series of horizontal comparisons can not be carried out at all. This is not conducive to consumers to choose a smart home system that is more suitable for their own but also makes users who use different smart home systems have doubts about security issues.

Today, China does not have a complete set of security standards applicable to the smart home. Each manufacturer uses its own safety indicators for evaluation. Therefore, it lacks universality. In the selection of security standards, the smart home industry can only refer to the existing information security standards and network communication security standards for system security evaluation. Although such organizations as the Internet of things standard GB/T 36468-2018 [1], national standard GB/T 35136-2017 [2], Common Criteria for smart home information security [3], smart home industry alliance [4]and enterprise standard information public service platform(http://www.cpbz.gov.cn) publish Common specifications [5], these standards cannot cover the products of most manufacturers in the market. This paper aims to establish a simple and universal smart home system safety evaluation indicator system.

2. Security Analysis of Smart Home System

Smart home system is essentially a series of interconnected home products that can provide a series of intelligent services. Through the analysis of the existing smart home system, the whole system can be divided into four parts: control system, communication technology, intelligent equipment and cloud

service. The security of the system can be evaluated from these four aspects, as shown in figure 1.

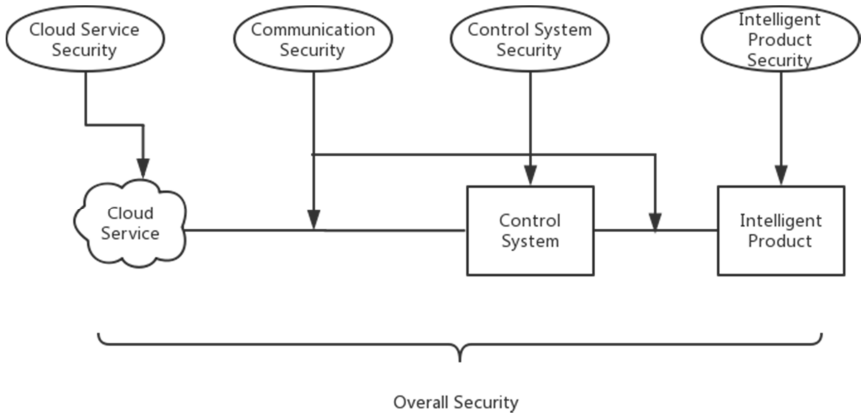

Figure 1. *Distribution of Security Problems in Smart Home System.*

3. Control System Security

The control system includes a gateway and a personal control terminal. Gateway plays a key role in the whole control system, which realizes the interconnection of smart home products and the function of data storage and transmission. The remote management of smart home systems, human-computer interaction, and even docking with cloud services all depend on the smart home gateway. For the smart home control system, its various security issues include gateway access security, access control, device authority management; Control terminal operating system security, firmware security and so on. Specific index design is shown in figure 2.

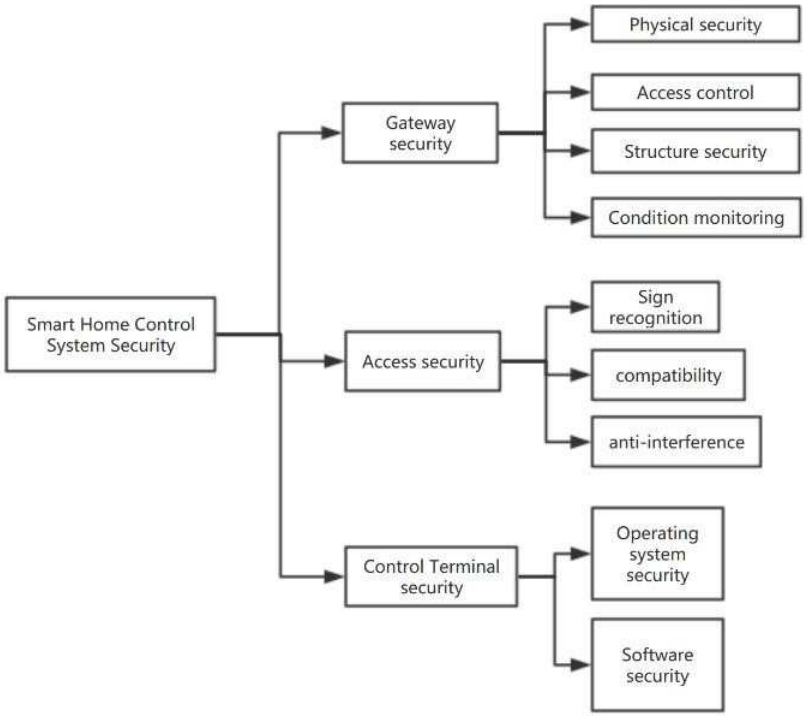

Figure 2. *A. Control System Security.*

3.1. Gateway Security

Physical security: The security problem caused by the gateway when threatened by physical external forces. It can be solved by reasonable wiring, adding protective shell and other methods.

Gateway reliability: The reliability of the gateway itself will affect the execution efficiency of the command transmission of the whole system to the control system. The unreliability of gateway will lead to a series of security problems such as command delay, control signal blocking and leakage. We need indicators that can verify gateway stability and vulnerability. Gateway throughput, number of parallel connections, anti-virus filtering capability and vulnerability repair degree, are the key attributes of gateway reliability.

Access control: Access control includes authentication of

devices, access control policies, and security audits. For certification, not only the degree of accuracy of certification should be considered, but also the certification strategy should be measured in terms of whether it is a two-way certification and whether there is reasonable certification feedback. The access control policy should follow the principle of minimum permission, minimum disclosure and security classification.

Equipment condition monitoring: The smart home control system should play the role of monitoring and supervising each module and each product in the system. For the control system itself, it is necessary to pursue the real-time, stability and accuracy of the device state monitoring to ensure the security and stability of the entire intelligent home system. We can measure it with the maximum frequency of data packets received and recognized by the system and the set frequency. In addition, monitoring algorithm, cloud computing and collaboration technology in the cloud should also be specifically analyzed.

3.2. Access Security

Identity recognition: The control system should have the function of identifying the identity of the device when accessing the device. The accuracy of identification and the number of compatible device types are important standards to measure access security. At the same time, for devices that cannot be identified successfully, there should be measures to restrict or deny access, and the user can be provided with enough information about the unrecognized devices, such as interfaces, required permissions, etc. to assist the user in screening and judgment.

Compatibility: The control system should support the identification of as many device types as possible, and support for more devices can help the system run stably under different device configurations, thus improving the security of the whole system.

Anti-interference performance: The control system should be able to resist external interference as much as possible to ensure that the system can run safely and stably.

3.3. Control Terminal Security

Operating system security: Nowadays, it is common for software programs on mobile devices or computers to act as control terminals, so the operating environment of these programs should be considered first. The classification of operating system security is defined in GB/T17859. These grading systems comprehensively consider the requirements of the operating system for security functions such as identity authentication, access control, data flow control, audit, data security, trusted path and so on, and grade the operating system, which directly reflects whether an operating system is secure or not. In addition, configuration optimization of the operating system can significantly affect the security of the operating system. Common computer operating systems are C2 standard, part of the Unix-like security performance can achieve higher level B. Besides, the use of the modified operating system or abnormal modification of system permissions will lead to the reduction of system security, including various so-called optimized versions of Win, jailbreak operation of IOS or root operation of android system.

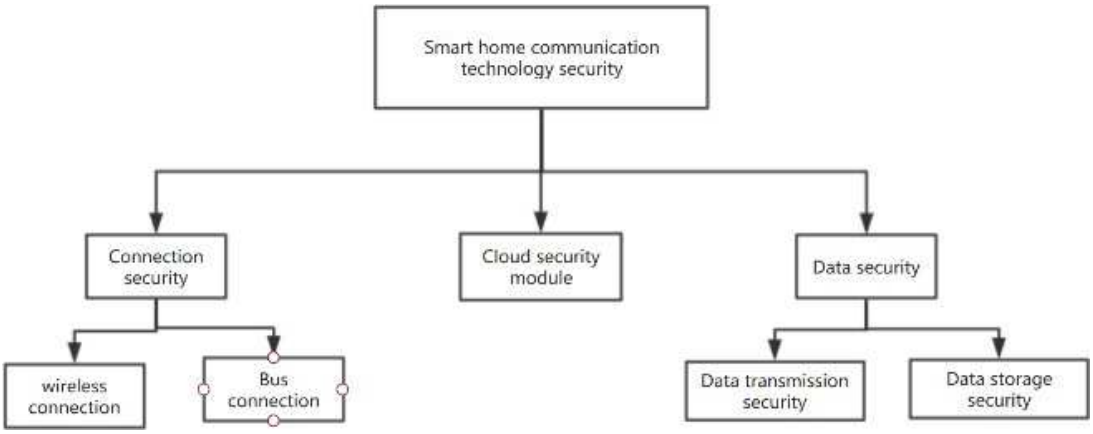

Figure 3. *Communications Security.*

Software security: At present, many smart home devices do not use mutual authentication or strong passwords. Many devices are simply set to a four-digit PIN code. The correct way for users to use a strong password is to use a combination of numbers, special symbols and upper and lower case letters. There is also no strong password in the cloud interface so that hackers can access more cloud data. The control software shall provide two or more forms of user authentication, and shall have an independent authentication method as an insurance measure when opening the lock, accessing the user's personal information and other sensitive operations. The software should provide instant encryption protection for user keyboard input such as password verifications. For example, the use of character - by - character encryption, random key soft keyboard, anti - keyboard eavesdropping technology, MAC code verification and so on. At the same time, the software should prevent the attack of multiple false verifications, and the password strength of the user to make requirements. The software should be started to verify the integrity and version, environment operation, and automatic upgrade or repair to avoid control software is malicious tampering. The software

should be able to maintain its own program log for professionals to debug queries.

4. Communications Security

The main consideration is the security of information transmission and data security between the device and the control system or device. As shown in figure 3.

4.1. Connection Security

For the security of connection mode, we divide the connection mode into bus connection and wireless connection.

Bus system: This type of smart home system is structurally safer and more reliable than the wireless one. For the common bus smart home structure in the market, it has the following characteristics: Rs-485 serial bus adopts balanced sending and differential receiving, which can effectively suppress the common mode interference. Rs-485 serial bus also uses a bus transceiver with high sensitivity, transmission signals can be very timely feedback and recovery. Without specification, but due to technology companies of the RS - 485 product can direct communication each other, and use this bus technology system as a wholeneeds a main contact, between various modules using polling of the connection mode of "hand in hand" type of communication, main contact attack is easy to make the whole system is affected; KNX type system has obvious characteristics in structure: in the whole system, all sensors are connected to the brake through data line, that is to say, each sensor has an independent controller to assist and control the electrical appliances by controlling the power circuit. The command data sent by the sensor will also be directly transmitted to the brake at the corresponding address, and then the brake will control and perform the corresponding function. The structural characteristics of using brakes for control and the high responsiveness of bus information make KNX safer and more general; LonWorks bus technology uses the LonTalk protocol encapsulated in the Neuron chip and implemented. This technique doesn't require a host, and it uses a neural network. For the system connected by the neuron network, each node is a neuron, and when these nodes are connected, they will control each other and work together. Since the master control system is not required for centralized control of all information and control signals, the security and stability are greatly improved compared with other buses. However, due to protocol encapsulation, its complete openness is questioned; Can-bus protocol not only uses CRC test to ensure the security of information, but also provides corresponding error handling function for the test, ensuring the reliability of data communication; Other buses, such as c-bus, a-bus, MODBUS, etc., adopt different structures and main cable types respectively, and have their own characteristics. For example, c-bus that does not rely on computer control, Modbus that is open source and simple, etc.

Wireless system: Wireless transmission has been widely used in smart home systems because of its convenience and cost performance. However, for the security of wireless transmission technology, the technology category should be considered first. According to the current situation, the most common wireless communication protocols are as follows: Zigbee [6], z-wave [7], Wifi [8], and bluetooth [9]. Bluetooth is not suitable for smart home systems because of the transmission distance and the number of connections. Although there are relatively complete encryption technology and verification technology in terms of Wi-Fi technology security, many WI-FI systems do not adopt any kind of security protocol. This kind of connection has poor security in the absence of any security protocol protection or outdated security protocol, which requires the combination of protocols to analyze security performance jointly. The most commonly used Wi-Fi security technologies are WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access), and wpa2-psk (upgraded version of WPA); Some systems use WPA-PSK [TKIP] + WPA2-PSK [AES] -- allowing clients to use WPA-PSK [TKIP] or wpa2-psk [AES] two different encryption protocols and encryption methods to further enhance security. However, these protocols are more or less vulnerable, so the security of Wi-Fi technology is considered at a relatively low level. ZigBee security is recognized as excellent. It uses the AES-128 encryption method, which can carry out multiple rounds of encryption. Cracking this encryption method requires obtaining both the encryption function, the key, and the number of encryption rounds. So brute force cracking is almost impossible. In addition, the ZigBee network has a strong self-organizing network and self-healing ability. Z-wave is an emerging short-distance wireless communication technology that is RF-based, low cost, low power consumption, high reliability and suitable for the network. It is a proprietary wireless standard developed independently and is not as open as other wireless standards, which is a barrier to breaking it down. However, despite the high reliability and security of the paired z-wave device, it is less secure than ZigBee due to the lack of encrypted transmission mode and the risk of degrading attack.

4.2. Cloud Security Technology

Cloud security technology marks the most cutting-edge information security strategy in this era. It integrates parallel processing, grid computing, unknown virus behavior judgment, and other emerging technologies and concepts. Through the data collection of a large number of clients, the cloud composed of multiple servers can easily analyze the abnormal behavior of software in the network and monitor it. The monitored data will be sent back to the cloud further consolidate the behavior identification of the virus Trojan horse. Being connected to the cloud means accessing the latest information and solutions of Trojans and malware on the Internet in real-time. For the smart home system, every smart device is a good information acquisition platform. As long as there is a strong cloud to support, this data can be converted into a smart home system to deal with the threat of prevention measures and improvement methods extremely efficiently.

4.3. Data Security

A large amount of data will inevitably be generated in the

smart home system. The security of storage and transmission of these data also plays a decisive role in the system security.

Security of data transmission: The premise of data transmission security is that both communication parties need mutual authentication or one-way authentication. The data transmission process needs to be secure, complete, and immune to some common data attacks. Data confidentiality is also known as data encryption. During the transmission and exchange of information, one end converts the information into an unrecognized form, and then restores it by the other end which usually uses the AES-CBC encryption algorithm [10]. The transmission of data requires both parties to hold the key. Data transmission is also considered integrity, that is, to ensure that the data in the transmission process is not tampered with. MD5 [11] or SHA [12] algorithms are usually used to determine whether data has been compromised. Malware that can capture a legitimate ciphertext and then resend it or retransmit it multiple times can interfere with the system, known as a replay attack. This attack can be countered with a sequence number or time stamp in the body of the message.

Security of data storage: A complete data storage scheme includes an online redundant storage system and an offline backup system. The most common form of online redundant storage systems is RAID [13]. High-end storage machines such as EMC and NetApp use RAID6, which can withstand two disks out of a group (approximately 12-16 disks). The disadvantage is that it is very expensive. The other is represented by Google FS, which USES 3 times redundancy. Hadoop's [14] HDFS [15] follows a similar principle. Offline backup systems are most commonly operated by tape *drives using robotic arms to physically retain data and eliminate the possibility of data theft.*

5. Security of Cloud Services

Most smart home systems have applied cloud computing technology. But this mode of distributed storage computing undoubtedly adds security risks to the whole system. For the smart home system that adopts cloud computing, we need to consider the security of cloud computing into the system security. As shown in figure 4:

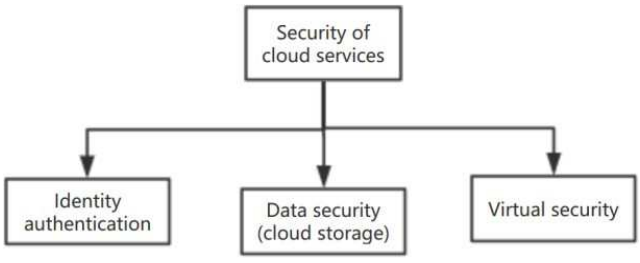

Figure 4. *Security of Cloud Services.*

5.1. Identity Management and Authentication

In order to ensure the isolation and secure access of data in the interaction of users' cloud space, it is necessary to establish user identity management and access control in the cloud computing system shared by multiple users, which is also one of the key technologies of cloud computing security. The single sign-on protocol allows users to register and log in only once when using cloud services, which can reduce the burden on users. Federated identity, which means that users can use one account to log into different cloud service platforms that trust each other, is based on single sign-on technology.

5.2. Data Security

Data security is the core of cloud computing security, including static storage data protection and dynamic data isolation protection. In addition to the general characteristics of data security, recoverability is the key to cloud computing security. Federated storage can make it more likely for data to be recovered and restored through backup in other locations after a loss.

5.3. Virtual Security

Virtualization is a process that breaks the rigid connection between physical hardware and the operating system and the applications running on it. Virtualization can be applied to computers, operating systems, storage devices, applications, or networks. Under the virtualization platform, the resources of the server are integrated so that the utilization rate of resources is greatly improved. Simultaneously, the virtualization platform itself provides the convenience of fault recovery, business deployment, migration, transformation, update, maintenance, and other aspects, which reduces the IT cost and improves the use efficiency and flexibility. Virtualization technology is the basis of developing SaaS cloud services. Therefore, the security issues of server virtualization, storage virtualization, and network virtualization are crucial to the security of cloud computing system [16].

6. Smart Home Product Security

For the security of smart products, this paper focuses on sensors related to the Internet of things. As shown in figure 5:

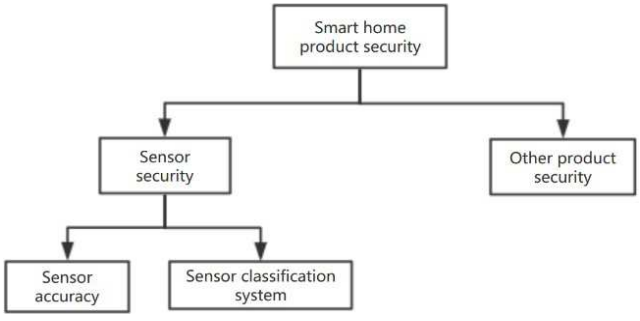

Figure 5. *Security of Smart Home Product.*

6.1. Sensor Security

Sensor accuracy includes indicators of the range measurement, error value, and deviation which aim to measure the quality of the sensor. The high-precision sensor

helps the Induction identification of the target efficiently, which can accurately obtain data and reduce the error of system analysis and control.

The sensor classification system classifies sensors according to basic safety indicators, fault tolerance of components, self-inspection and mutual-inspection, and other security measures.

6.2. Other Security Features of Smart Home Products

Smart home products as the security of the product itself, such as the physical security of the door lock, anti-skid index, and so on. It is not related to this paper's content, and it is recommended to adopt professional test indicators.

7. Conclusion

This paper introduces a set of standard index systems based on the nationally recommended standard, and comprehensively considers the standards implemented by various manufacturers. Its main purpose is to be able to make the user in a lot of different standards in a set of relatively general evaluation methods to the current brand variety of smart home systems. Be able to truly understand the safety features and shortcomings of various smart home systems. However, the index system described in this paper only provides a kind of general evaluation of smart home systems; the selected index and reference value may not be the best evaluation idea. I hope to be able to provide some help for organizations or individuals to carry out relevant research.

Acknowledgements

My thesis would like to thank the Beijing software product quality inspection center and Beijing Key Laboratory of testing technology for their help. They have given us a lot of financial support through the new generation of information testing technology and research projects(40025001201838). They also provide an experimental and testing environment for our research process. At the same time, I would like to thank the authors of the references and relevant researchers, whose research has provided me with important reference and help, and provided me with a good reference completing my paper.

References

[1] Wei Liu, Wei Li, Yao-chen Hu, Analysis of the standard protocol requirements of home Internet of things. Technology Innovation and Application, Vol 23, 2018, pp.74-75.

[2] Pei Zhao, Peng Tao, Chong Li, Lin-qing Liu, Meng-yu Li, Research and interpretation of Internet of things information security technology standards. Hebei electric poewer, Vol 38, 2019, pp.1-3.

[3] Hai-yan Li, The status quo of smart city standardization in China and its challenges and Countermeasures. China Standardization, Vol 6, 2019, pp.193-197.

[4] Yong-shu Xiao, Construction and development analysis of smart home standardization system. Technology Innovation and Application, Vol 15, 2018, pp.40-42.

[5] Yan Zhang, Practical application of enterprise standard information public service platform. Machinery Industry Standardization & Quality, Vol 15, 2018, pp.40-42.

[6] Rong-hua Ri, Yang, Yue Zhao, Intelligent transportation system based on ZigBee. Internet of Things Technologies, Vol 10, 2019, pp.107-109.

[7] Ping Yang, Yang-yang Peng, Chao Hu, Intelligent classroom system design based on IPv6 and: Z-Wave intelligent gateway. Computing Technology and Automation, Vol 38, 2019, pp.96-101.

[8] Jia-hong Liu, Bao-Lu li, Lan Yang, Shuo-bing Qiu, Yue Li, GPS / Wi Fi Indoor and Outdoor Fusion Positioning Method Based on Grey Prediction Model. Computer Engineering, Vol 45, 2019, pp.264-269.

[9] Xiang Shen, Design of Internet of things gateway based on hardware TCP / IP protocol. Internet of Things Technologies, Vol 10, 2019, pp.35-37.

[10] Hua Chen, Jin-xin Xie, Li-huang Chen, CNN-based Encrypted C & C Communication Traffic Identification Method. Computer Engineering, Vol 45, 2018, pp.31-34.

[11] Yun-long Miao, Yan-hui Lu, Feng Yin, Shou-yi Yang, Research on Wi-Fi indoor location algorithm based on MD5-KNN. Computer Applied Research, Vol 36, 2018, pp.2746-2749.

[12] Jun Ma, Hui Huang, Chuan-fu Xia, Li-li Zhang, Beidou terminal access authentication negotiation protocol based on identity authentication and SM2 algorithm. Electronic Design Engineering, Vol 28, 2020, pp.67-70.

[13] Zhu Yuan, Ping Xie, Sheng-ling Geng, Summary of Research for RAID System Scaling Schemes. Acta Electronica Sinica, Vol 47, 2019, pp.2420-2431.

[14] Ka Feng, Research on Big Data Platform Risk Monitoring System Based on Hadoop, Vol 39, 2020, pp.135-138.

[15] Guo-dong Jin, Hao-qiong Bian, Yue-guo Chen, X iao-yong Du, Survey on Storage and Optimization Techniques of HDFS. Journal of Software, Vol 31, 2020, pp.137-161.

[16] Song Yang, Hongshan Liu, Yan Cheng, Overview of design and implementation of cloud computing security system. Journal of Chongqing University of Posts and Telecommunications (Natural Science Edition), Vol 32, 2020, pp. 816-824.