Research on the Security of Internet of Things Based on Cloud Computing

Haonan ZHANG, Yunqiu SHI
University of Science and Technology Liaoning, Anshan, 114051, China

Abstract: The IOT (Internet of Things) based on cloud computing is facing with more complex information security situation, and this security issue becomes an important obstacle of its development. This paper analyzes the main security issues of IOT, and proposes the system architecture and security model of IOT based on cloud computing. It gives one unified cloud security management solution on IOT. In addition, the security weaknesses of Internet of Things based on cloud computing are discussed.

Keywords: cloud computing, Internet of Things, Information Security, cloud security, Internet of Things security

1. Introduction

In order to achieve intelligent identification, positioning, tracking, monitoring and management of network, IOT uses the agreement agreed to connect anything with the Internet connection to complete information exchange and communication through radio frequency identification (RFID) devices, infrared sensors, global positioning systems, laser scanners, sensor nodes and other information sensing device. Its core is to make object information sensible, knowable, transitive and controllable. With the implementation of cloud computing, the combined application of IOT and cloud computing is imperative. Large-scale development of IOT is inseparable from the cloud computing platform support, and comprehensive cloud computing platform and large-scale applications require the development of IOT to provide maximum user. Compared with traditional Internet, the Internet of Things is facing more serious security challenges. It includes three factors: the sensor node security, sensor network security and operational security. IOT security features reflect the diversity of sensory information, the network environment and the application requirements. This paper analyzes the main security issues of Internet of Things, and proposes the system architecture and security model of Internet of Things based on cloud computing. It gives one unified cloud security management solution on Internet of Things. In addition, the security weaknesses of Internet of Things based on cloud computing are discussed. The research on the security of Internet of Things based on cloud computing will provide the most reliable protection to for the development of cloud computing and IOT, and it also is the booming necessary conditions of both development.

2. The System Architecture of IOT based on Cloud Computing

IOT construction involves three aspects: the physical world perception, the construction of a large number of independent single IOT applications, many single-depth IOT applications interconnection and cross-domain collaboration. The system architecture of Internet of Things based on cloud computing is shown in Fig. 1. It consists of four layers: the sensing layer, network layer, cloud service platform and application layers.

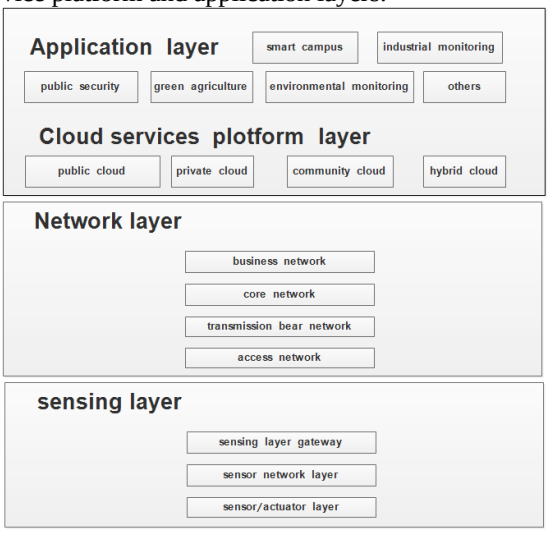

Figure 1. The system architecture of Internet of Things based on cloud computing

Where the sensing layer emphasis on real-time and accurate perception of the surrounding environment, information summarized and data transmission, it is the core technology of the base layer, and Communicate through the RFID tag and reader, sensors and sensor networks and other technical equipment to complete. Network Layer emphasized data gathering, processing and transmission through WiMAX, GSM, 3G communication

networks, satellite networks, and Internet. Cloud services platform is an efficient and reliable technical support cloud computing platform for the upper layer's application service, it provides cloud computing services through parallel processing and data mining , shields the underlying network, information heterogeneity. Application layer is to establish the corresponding cloud-based business models according to the needs of users, and runs the appropriate applications.

3. The Security Model of IOT based on Cloud Computing

3.1. The general safety indicators of internet of things based on cloud computing

Cloud computing security and safety of IOT both include commonality of network security technology. As a network of multi-network integration, IOT security involves various different levels, including mobile communications network, the Internet and perception networks. The general security indicators of Internet of Things based on cloud computing are as follows: ©Reliability: Three Measure Standards (survivability, survival, effective). © usability: Metricing with the ratio of the normal working time and the overall measure. © Confidentiality: Require that information is not disclosed to unauthorized persons, commonly used encryption technologies are anti-interception, radiation protection, encryption and physical security. © Integrity: The information cannot be changed without authorization; integrity requires that information can withstand a variety of cause's destruction. © Non-repudiation: Participants cannot deny the operation has been completed and commitment features.© controllability: The control features for information dissemination and content. The integrity and availability of the Internet of Things runs through data stream of the whole process. Network intrusions, denial service attacks, Sybil attacks, routing attacks can damage the integrity and availability of IOT information. While the perception of IOT interactive process also requires a network with a high degree of stability and reliability.

The Security Model of Internet of Things Based on Cloud Computing

Compared to the traditional network, most of IOT sensor nodes are deployed in unattended environment, with the ability fragile, limited resources, etc., and because IOT extends aware network and application platform based on the existing network, traditional network security measures are not enough to provide reliable security, make IOT show with special security issues. Fig. 2 shows the composition structure of IOT based on cloud computing.

The wireless sensor network of sensing layer uses a wireless channel for networking and data transmission, and wireless channel is very susceptible to interference, eavesdropping and attacked. Attacking the wireless sensor networks means is more. There are some security threats for RFID, wireless sensor networks against security threats and for mobile intelligent terminal security threats.

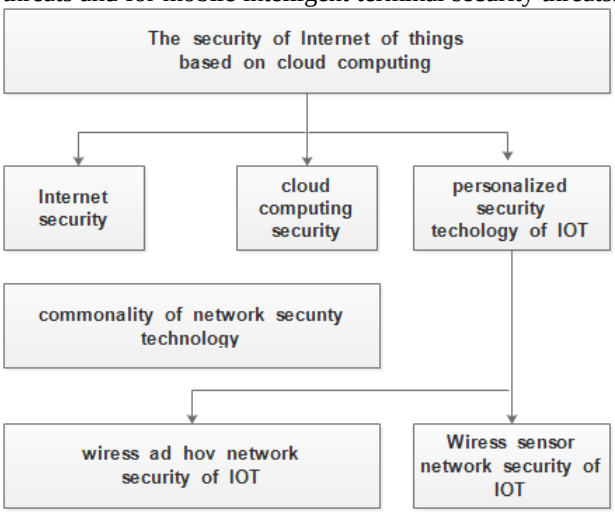

Figure 2. the composition structure of IOT based on cloud computing.

With cloud-based networking system architecture, cloud-based security model of IOT is shown in Fig. 3, which involves four security levels: ©information application security: Information Application Security.© cloud computing security: Cloud architecture, governance / management of cloud (IT governance and enterprise risk management, legal and e-discovery, compliance and audit, information lifecycle management, portability and interactivity), cloud Run / cloud operations (traditional security, business continuity and disaster recovery, data center operations, incident response and remediation notice, application security, encryption and key management, identity and access management, virtualization)© information transmission security: Firewall / IPS, security domain classification and security isolation, secure transmission (VPN, SSL) Network Access Control, DDOS defense, zombie / worm attack source, virtual firewalls, traffic analysis and control, content monitoring and filtering, security reinforcement, endpoint security, penetration testing, security audits, vulnerability analysis, emergency response © Information security of awareness, perception nodes safety: RFID security (physical attacks, channel blocking, forgery attacks, impersonation attacks, copy attacks, replay attacks, information tampering), wireless sensor network security (gateway node capture, sensor information eavesdropping, DOS attacks, replay attacks, complete sexual assault, false routing information, selective forwarding, Sinkhole attack, Sybil attack, Wormholes attack, HELLO flood, confirmed cheating), mobile intelligent terminal security (malware, botnets, operating systems, and privacy leaks and other defects)

3.2. The Unified Cloud Security Management Solution of IOT

Several layers of IOT are combined one of the large system, many security problems derived from systems integration. The platform supporting networking activities have different security policies, such as cloud computing, distributed systems, massive information processing, etc. These services support platform to the upper management and large-scale industrial applications may establish an efficient, reliable and trusted system, the large-scale, multi-platform, multi-service type make IOT business-level security face new challenges, applications for different industries to establish appropriate security policies, or the establishment of an independent security architecture is the existence of an IOT security controversy. Different IOT applications have different sensitivity; the "tailored" security strategy can effectively reduce the redundant configuration with excess energy consumption. In this paper, according to the user's demand needs, we give the unified cloud security management solution of IOT, which combines traditional network management and security management, technical architecture, functional modules and the operation and maintenance methods. As is shown in Fig.4, the unified cloud security management platform of IOT includes three parts: cloud security management layer, cloud security function layer and cloud security functional layer. In the cloud security function layer, the cloud security function adapter may select the appropriate type safety according to user demand security needs.

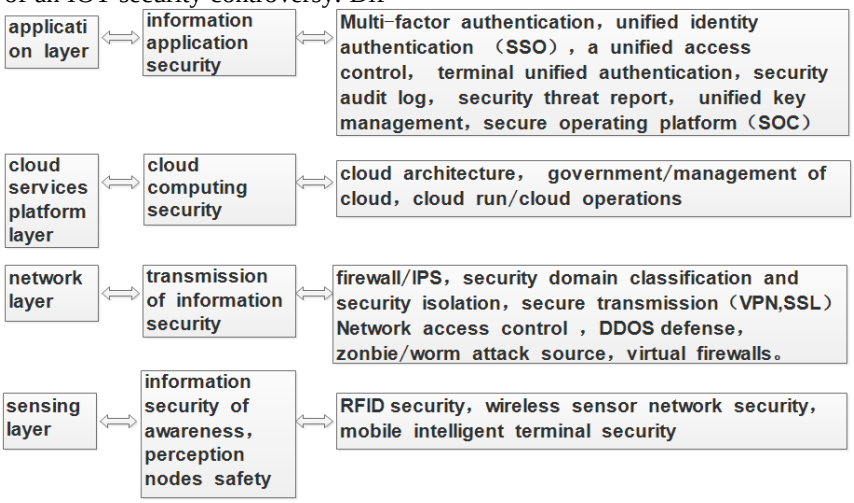

Figure 3. the security model of Internet of Things based on cloud computing

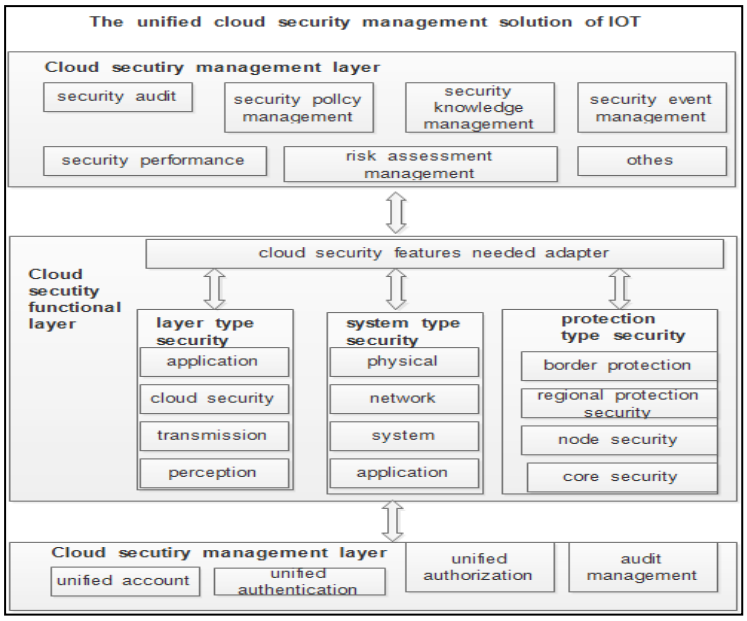

Figure 4. The unified cloud security management solution of IOT

Through the unified cloud security management solution of IOT, we can manage all kinds of IT resources for network performance monitoring and security event management. This may avoid the fragment between network management platform and security management platform in the traditional mode, and integrates effectively network management and security management routine operation and maintenance work.

4. The Security Weaknesses of IOT based on Cloud Computing

Currently, the security weaknesses of IOT manifested in many ways, the protection mechanisms of comprehensive information security perception layer is serious lack, and need lightweight cryptographic algorithms / lightweight security protocol, and its variability is strong, standardization is low. For the reliable transport layer, its information security protection mechanism is relatively perfect, but need to be strengthened, requiring high strength cryptographic algorithms / High-strength security protocols. and its standardization is high, and with the expansion of the scale of IOT , it should be constantly strengthened. Cloud services platform layer is lack of information security protection mechanisms, and need industrial default standardization needs. Mainly in: © Hadoop platform security. © cloud computing environment authentication services. Achieve the user to authenticate identity, issuing licenses to access etc. © cloud computing environment data security services. Provides data encryption, integrity, and accuracy data verification, and fault-tolerant storage of mass data management. ® cloud computing environment access control authorization services. According to the access control list, it giver access authorization to an authenticated user.© cloud computing environment system security. The system of cloud services should continue to provide users with reliable service at any time in response to user requests. Even if the server malfunctions or site failure, but also in a short time to return to normal state, and will not affect the services requested by the user. © cloud computing environment application security. Run the application in the cloud to ensure continuous and reliable access, one common method is the use of partitioning and memory segmentation method against viruses and harmful small program, making the system in case of failure to restore the minimum required operating to ensure application security.® cloud computing transmission security. Data transmission services provide a unified transit transport services and security mechanisms for data transfer between the modules. © Virtualization Security, in order to solve the security problems of virtualization platform, the original security technologies must support a virtualized environment and be able to accompany the virtual platform migration. In addition, the security needs of integrated application layer between different applications, security mechanisms are quite different, privacy protection research and technology industry is the largest short board, safety management as a security risk, non-technical factors also need to be strengthened.

5. Summary

There would be no its wide application without the security of IOT. At present, China's Internet of Things cloud-based security development is still in its infancy. Generally speaking, a cloud-based networking security research focuses on cloud-based security system of IOT, IOT individual privacy protection mode for cloud computing environment, endpoint security functions and security-related law of IOT. In contrast, the sensor network security research is still in its infancy, and there is not a complete solution for it. Since the sensor network resource limitations, it is difficult to study security issues, so sensor network security research will be an important part of IOT security. At the same time, how to create an effective multi-network integration of cloud security architecture, the establishment of a unified network across multiple cloud security model, the formation of an effective cloud security jointly coordinate defense system will be the next important research direction.

Acknowledgement

University of Science and Technology Liaoning 2016 provincial college student innovation and entrepreneurship training program number 201610146048

References

[1] Jing X, Jian-Jun Z. A brief survey on the security model of cloud computing[C]//Distributed Computing and Applications to Business Engineering and Science (DCABES), 2010 Ninth International Symposium on. IEEE, 2015: 475-478.

[2] Alliance C S. Security guidance for critical areas of focus in cloud computing v3.0[J]. Cloud Security Alliance, 2015.

[3] Liuyanbing, Huwenping. Security model and key Technologies of Internet of Things [J]. Digital Communication, 2015 (004): 28-33.

[4] Yanggeng, Xujian, Chenwei ,et. Security characteristic and Technology in the Internet of Things [J]. Journal of Nanjing University of Posts and Telecommunications, 2015, 30(004): 20-29.

[5] Yangguang, Diguining, Doujing et. security threats and measures for Internet of Things [J]. Journal of Tsinghua University (Science and Technology) , 2015, 51(10): 1335-1340.

[6] Liwei, Fenggang, Liudong. IOT System Safety and Reliability Testing Technology Research [J]. Computer Technology and Development, 2016, 23(4): 139-143.

[7] Ren Wei, Song Jun , Ye Min, Liu Yuliang. Autonomous Security Adaptive Layer for IOT and T2T Anonymous Authentication Protocols in T2ToI [J]. Journal of Computer Research and Development, 2015, 2.

[8] SUN Zhi-xin, LUO Bing-qing, LUO Sheng-mei, ZHU Hong-bo. Security Model of Internet of Things Based on Hierarchy [J]. COMPUTER ENGINEERING , 2015, 37(10): 1-7.

[9] Li Zhiqing. Security architecture and technology in the Internet of things [J]. MICROCOMPUTER & ITS APPLICATIONS, 2015, 30(9): 54-56.