Application of Hierarchical Protection in Data Security of Internet of Things

Liangyan Chu1,*
1Water conservancy of Shandong Technician College, Shandong, China

*Corresponding author e-mail: liangyan@sdcw.net

Abstract. The traditional Internet of things data security focuses on the application of various security protection technologies, but this protection method is difficult to effectively cope with the growing protection needs and changing product forms. It needs to be constructed from two aspects of technology and management combined with the hierarchical protection system. Based on this, this paper first analyses the concept of Internet of things data security protection measures and level protection, and then studies the specific application process of hierarchical protection in computer Internet of things data security.

Keywords: Hierarchical Protection, Data Security, Internet of Things

1. Introduction

With the iterative progress and maturity of information tech represented by the IoT, it has been widely and deeply studied and applied in many fields, and has achieved remarkable application results [1]. The popularity of IoT not only greatly facilitates people's travel and life, but also brings some hidden dangers to data security and privacy protection. In this context, how to ensure the security of data data has become an important prerequisite for the healthy and sustainable development of IoT tech. In recent years, the IoT has been widely used in many fields as shown in Figure 1, which greatly promotes the development of data industry through intelligent perception, recognition and computing.

Once the IoT system is attacked, the security and privacy will be violated, which will lead to more serious consequences [2]. Ensuring the data security of the IoT is an important basis for further development and application of the IoT, and also an important symbol of the maturity of the large-scale application of the IoT. The security threats brought by uncontrollable factors of the IoT need to be judged from the specific security needs and characteristics to determine whether its security can meet the real threats. The research of computer IoT data security based on hierarchical protection is to divide the security level of the IoT system, and realize the specific application of level protection in the data security of the IoT.
At present, the data security threats faced by the IoT mainly include the lack of computing resources of the IoT sensing devices, the lack and disunity of the identity identification of the sensing devices, and the integration of the sensor network and the traditional data system, which bring great uncertainty to the data of the IoT. According to the requirements of the hierarchical protection system of network data, the obligation of security protection shall be fulfilled, and the security protection shall be carried out according to the requirements of the national hierarchical protection system.

In addition, the traditional IoT data security focuses on the application of various security protection technologies, but this protection method is difficult to effectively cope with the growing protection needs and changing product forms [3]. Therefore, it is necessary to establish a complete data security protection system of the IoT, and integrate the data security protection tech and data security management organically, so as to ensure the whole process management of the IoT data in terms of integrity, reliability, security, availability and controllability. Therefore, it is of great practical value to carry out the application research of hierarchical protection in data security of IoT.

2. IoT data security protection measures and level protection

2.1. The meaning of IoT data security level protection
The system security level protection of IoT data refers to the classification of data and data system into five security protections and supervision levels, including independent protection, guidance protection, supervision protection, compulsory protection and special control protection[4]. According to the importance of the application business of the IoT data system and its actual security requirements, it is necessary to implement protection at different levels, categories and stages, so as to ensure the normal operation of data security and system security, and to safeguard the national, industrial, enterprise and public interests and social stability.

In addition, the core of hierarchical protection is to classify, manage and supervise the security of data system, especially business application system. At the government level, the IoT data security level protection work using laws and technical specifications to strengthen supervision. Highlight the key points and ensure the security of important data resources and important data systems.

2.2. Grading dimension and stage of classified protection
The classification dimension of hierarchical protection is mainly aimed at the object that is infringed when the object of data security of IoT is damaged, and the degree of infringement to the object is determined [5]. The conditions of grading objects include having a unique security responsibility unit, meeting the basic elements of data system and carrying relatively independent business applications. In addition, in the level of identification and division of classification objects, it mainly includes the system that may make the rating elements assign different factors, the system running in different network environment and the system that cannot be separated, according to the high-level protection.
2.3. Grading process of grade protection
First of all, it is necessary to identify the basic data of the unit and determine the macro positioning of the main data system of the unit. Secondly, it is necessary to identify business types, processes and services, and understand the specific ways and degrees of services provided by different business systems in the data system of rating objects in terms of influencing the performance of unit functions [6]. In addition, at the level of identification data, we investigate and understand the data processed by the classification object data system, and understand the requirements of the unit for data security attributes. At the level of identifying network structure and boundary, the characteristics of internal and external network environment of data system are mastered. By identifying the main hardware and software equipment, the sharing degree of different data systems in the use of equipment is found. By identifying the type and distribution of users, the scope and degree of system service interruption or system data destruction can be judged. Finally, the result of grading is formed, which takes the higher of all kinds of data and services.

2.4. Relationship between grading elements and safety protection level
When the objects of hierarchical protection are damaged, the objects infringed include the legitimate rights and interests of citizens, legal persons and other organizations, social order, public interests and national security. The three degrees of harm to different objects mainly include general damage at the first level, serious damage at the second level and especially serious damage at the third level. The relationship between grading elements and safety protection level is shown in Table 1.

| Intruded object                      | The degree of infringement on the object |
|--------------------------------------|-----------------------------------------|
|                                      | General | Serious | Particularly serious |
| Citizens, legal persons, organizations | Primary | Secondary | Secondary           |
| Social order and public interest     | Secondary | Tertiary | Quaternary          |
| National security                    | Tertiary | Quaternary | Fifth degree       |

2.5. Grading method and process
According to the object that the business data security is damaged and the degree of infringement to the corresponding object, according to the business data security protection level matrix table shown in Table 1, the business data security protection level can be obtained. Secondly, the main factors such as system type, business data category, system service scope and business dependence determine the classification, as shown in Figure 2 below. In addition, during the operation of the IOT data system, the security protection level should be appropriately changed with the change of the data and business status processed by the data system. When the state change may lead to a great change in the infringed object and the degree of infringement after the business data security or system service is damaged, which may affect the security protection level of the system, it should be regraded according to the grading method given by the grading standard.
3. Application of hierarchical protection in data security of IoT

3.1. Basic requirements for security level protection of IoT data system
The basic requirement of security level protection of IoT data system is the benchmark of system security protection and grade evaluation. The system of the same level should be measured by unified benchmark to ensure the authority. At the same time, after the data system of each level is protected according to the basic requirements, the data system has the corresponding level of basic security protection ability and achieves the basic security state. The security protection of each level of data system can be supplemented by requirement analysis and other standards related to level protection or security can be referred to.

3.2. Relationship between data security protection and system grading in IoT
According to the requirements of business data and system services, the security protection level of the whole system is determined, and the protection requirements of the IoT data system are reflected in the grading process. In addition, the importance of different levels of IoT data system is different, so it has the ability to deal with different threats. In this context, different security protection capabilities correspond to different basic requirements. The relationship between the elements is shown in Figure 3 below.

3.3. Implementation and evaluation of classified protection in data security of IoT
The implementation of grade protection should be carried out according to the principles of independent protection, key protection, synchronous construction and dynamic adjustment. According
to the IoT data system grading, overall security planning, security design and implementation, safe operation and maintenance, grade change, local adjustment and data system termination process to carry out specific implementation. In addition, in the implementation level of classified protection evaluation, including physical security evaluation, network security evaluation, host system security evaluation, application security evaluation and security management, the specific implementation is carried out according to the evaluation standards.

4. Conclusion
In summary, the establishment of complete data security protection system of IoT represented by hierarchical protection, organically integrate data security protection tech and data security management, so as to ensure the whole process management of data integrity, reliability, security, availability and controllability. Based on the analysis of data security protection measures and grade protection of IoT, this paper studies the grading process, grading elements and the relationship between security protection levels. Through the research on the application of classified protection in the data security of the IoT, this paper analyzes the basic requirements of the security level protection of the data system of the IoT, the relationship between the data security protection of the IoT and the system grading, and the implementation and evaluation process of the hierarchical protection in the data security of the computer IoT.

References
[1] Li Guoqin. Research on Application of hierarchical protection in data security of IoT [J]. 28th National Conference on computer security, 2013 (39): 14-20.
[2] Liu Yanbing, Hu Wenping. Security model and key tech of IoT II]. Digital communication, 2010, 4:28-33.
[3] Ma Li, Bi maning, Ren Weihong. Research on the relationship between security protection model and security requirements of hierarchical protection [J]. Data network security, 2011 (06): 1-4.
[4] Wang Huibo, Wu Du. Research on data security tech system of IoT [J]. Data security and communication confidentiality, 2013. (5): 60-61.
[5] Wang Ning, Liu Zhijun. Research on Hierarchical Protection in IoT security [J]. Network data security, 2011 (06): 5-6.10.
[6] Zhao Liang. Research on the impact of IoT and cloud computing on rating evaluation [J]. Data security and tech, 2013. (8): 28-29.