Research on Information Security of E-government based on Internet of Things

Ping Du [1], Yucai Luo [2]

[1]Xi'an Peihua University, Xi'an 710100 China

[2]Xi'an Huawei Technology Co., LTD., Xi'an 710100 China

Keywords: Internet of Things, E-Government, Information, Security.

Abstract: Due to the low security level of traditional research methods, research on Internet of things-based e-government information security is proposed. At the level of network system security research, the Internet of things e-government information level protection system is established. In this system, corresponding security service information needs to be configured to ensure that each security service can be implemented by one or more security mechanisms.In order to improve the confusion in the management of e-government, the system of information security level protection is optimized, the legal system of information security is perfected, the legal regulation of the comprehensive coverage of the central government to the local departments is formed, the information security system is planned and constructed, and the information of e-government is formulated and perfected. The security management system should be strengthened, and the sense of security and secrecy should be strengthened, so as to realize the research of Internet of things e-government information security. According to the experimental results, the Internet of things based research method has a higher security level, which can ensure the effective transmission of e-government information in safe mode.

1. Introduction

With the rise of computer network and modern communication technology, information and networking have become an important feature of the present era. We are all enjoying the convenience brought by the information age, and the information network has been extended to almost every field of social life. At the same time, the rapid development of information technology also provides technical support for the promotion of government reform, and many governments and scholars are also committed to the research and development of e-government. Under the background of such an era, the vast majority of the countries, including the developing countries, are actively promoting the e-government construction of their own governments under the influence of the trend of e-government information in the developed countries. Due to the transmission of e-government through the network system, the data, data and files involved in the transmission process have a certain level of confidentiality, and most of the materials can copy the shellfish through the hardware channels [1]. Therefore, there is a risk coefficient of artificial operation factors in the E-government work system. In addition, because of the defects of the network system, the defects of the program, the attack of hacker and so on, the non-control risk factors in the network transmission process are formed, and the information security is threatened. From the point of view of national security and long-term development, it is imperative to carry out classified protection for e-government information security.

From the view of the existing information security system in China, the risk and hidden danger have always existed, and the examination and approval system between the administrative decision-making level of our country is more tedious, and the leakage crisis in the process of document transmission has increased greatly. In the process of collecting, collecting and communicating government information, there is a lack of effective system support. The current legal regulation, technical level, management level and other aspects of construction are lagging behind, which are not compatible with the current economic development situation and the national macro strategic planning. Therefore, the construction of a perfect information security level

protection system is an important step to ensure the national information security, economic stability and stable social progress in the construction of the e-government platform in China. It is the objective requirement of the socialist Scientific Outlook on Development [2]. Therefore, a comprehensive e-government information security architecture is proposed to promote the healthy and sustainable development of E-government in China.

2. Research on Information Security of Internet of Things E - government

In the research direction of network security access setting, the security performance of the electronic government network system is greatly enhanced by controlling the unsafe factors in the system through the early warning mechanism and controlling the access by automation technology. In the technology, the related technologies related to information security are discussed, especially for the prevention and filtering technology and recognition. The technology, the prevention of hacker invasion and key management and other related technologies, the security risks in the E-government internal network and the external network system are discussed and detailed. And from the professional angle, the information security is studied as a professional subject in the aspects of technical research and development, personnel training and professional grade assessment. In the end, the corresponding protection means is put forward [3].

The design level of network system security is shown in Fig.1.

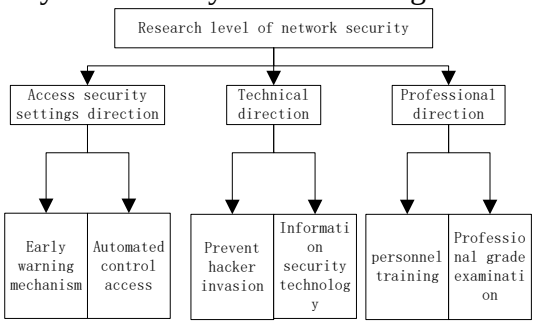

Fig. 1 Research level of network system security

2.1 Construction of Internet of Things E-government Information Classification Protection System

The security level protection system of e-government information is composed of physical security, network security, information security, application security and management security. Different levels of security bodies are derived at all levels, such as physical security and operating environment, equipment and media, and other aspects, and the content involves the establishment of the machine room. Plan, site security, site technology and power management, line management, anti-physical interference management, data security and media security; network security is related to system and operation and subnetwork status. Details relate to the anti-virus capabilities, self-detection, analysis and anti-intrusion capabilities of the host and server, and information storage. Line backup, recovery and emergency state recovery, firewall security detection management; application security and application software, data collected, related to web services and key applications; management security involves equipment management and system management, technology, personnel management, and other aspects, system management is the guarantee of management security. Personnel management is the key to safety management, which is directly related to the entity security vulnerability factor in the operation of government affairs [5]. Therefore, in the e-government information security management system, safety management is still the top priority.

The coordinate points of e-government information are given by formula (1):

$$For = \{compute\ average\ of\ \ cluster\} \tag{1}$$

The average Euclidean distance from each information point in the cluster to the center of mass is calculated.

$$If\left(d\left(x_i,m\right)\right)=d_{avg} \tag{2}$$

In the upper form, $d\left(x_i,m\right)$ represents the distance between the information point and the center of mass of the cluster, d_{avg} represents distance variance.

Categorize information points into suspected e-government information points:

$$If\left(d\left(x_i,m\right)\right)d_{avg}=Consider^{n}\ x_i \tag{3}$$

In the upper form, n represents the sample size of the information.

The calculated sensing information is compared according to the standard deviation from the selected information point to the centroid of mass. If the information is less than the latter, the information is normal, whereas the other is e-government information, that is:

$$If\left(d\left(x_i,m\right)\right)d_{avg}\geq 1.67\times sqrt\left(v_d\right) \tag{4}$$

In the upper form, $sqrt\left(v_d\right)$ represents the standard deviation.

In the face of an actual e-government application, it is necessary to implement the security technical measures based on these dimensions, and use this technology to ensure the security of the e-government application. In this architecture, corresponding security services need to be configured, and each kind of security service can be implemented by one or more security mechanisms [6].

2.2 Optimization of E-government Information Security Classification Protection System Plan

The e-government system belongs to the state administrative system and plays the management function of the state machine. Its information security is equivalent to the national security in a sense. It is closely related to the policy resolution, implementation, supervision, quality of service and national credibility. State leadership is to make unified goals and unified steps by the state. Administrative organs at all levels implement information security grade construction according to unified principles and requirements, improve the chaos in e-government management, and improve the communication, work and safety efficiency of the downlink units in the unified system, and introduce social evaluation institutions and implement the letter. The construction of interest safety system is necessary for operation training and certification [7].

2.2.1 Perfecting the Legal System of Information Security

In laws and regulations, the legal regulation should be formed to the overall coverage of the central government and the local departments, and the rules and regulations of the national legislature should be set up in the general direction, the local regulations are supplemented and the department rules and regulations are detailed. The local laws and regulations should be based on the national law, adhere to the policy and guidance of the national information security, integrate the information security needs in the local government system, supplement and refine the relevant laws and regulations. The legal regulations between local governments at all levels should not be inconsistent with each other and should be responsible for each other. The function of the rule of law should be coordinated, standardized and controlled [8]. The construction of a complete legal system for information security is illustrated in Fig. 2.

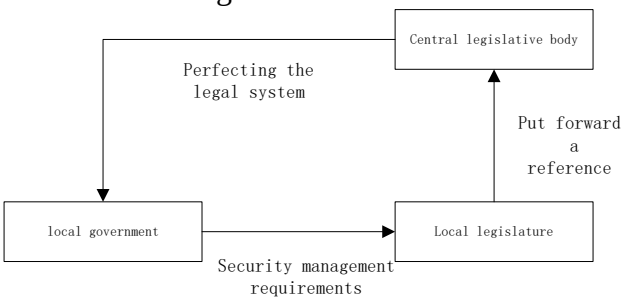

Fig. 2 Building a complete legal system of information security

From Fig. 2, it can be seen that the computer technology relying on E-government has developed rapidly, and the information technology also shows a rapid development trend. Compared with the dynamic information security external environment, the legal system is often in a relatively static state. Therefore, for the legislative system, the relevant legal regulation of the information security level protection needs to look around the world, look at the overall situation, based on the great vision of the human social development, and strengthen the legal timeliness higher than the present situation [9].

2.2.2 Unified Planning and Construction of Information Security System

In order to avoid duplication of construction and ensure safety, in the early stage of information construction, we should conscientiously comply with the overall planning and unified deployment formulated by the state information leadership group, plan information security work as a whole, unify the safety standards and standards, and strictly implement it. The relationship between development and security should be handled well, and the cost and effectiveness of security should be comprehensively compared. It emphasizes the establishment of information security management system of stratified defense, which allows the qualified information security institutions to provide information security planning and implementation scheme. From the overall and overall nature of the information security, the security management defense can be carried out from the system level of information flow. The construction stage and the operation and maintenance stage are the two stages of the life of the E - government information security system, and from the perspective of management, the information security management of E - government includes two types of management - project management and operation management. In the Internet of things environment, the construction of information security system is prior to the maintenance of the system. Therefore, the construction of the system directly affects the robustness of the system and the operation and maintenance after the application of the system. Therefore, the planning of E-government security projects plays an important role in the security level of the entire e-government system [10].

2.2.3 Strengthening the Consciousness of Safety and Secrecy of Personnel

The objective guarantee of e-government information security is the establishment of institutions and institutions, but in order to ensure information security, subjective safety awareness should also be enhanced. In the Internet of things environment, to grasp the security and security management of e-government information under the information condition, we should strengthen the security consciousness, the consciousness of security and the training and education about the safety technology of the staff, especially the chief executive of the e-government, the system management personnel, the personnel of the system, and enhance the consciousness of security and secrecy from the subjective.

First, strengthen publicity and education on information security and confidentiality. We should make great efforts to make innovations in overall planning, content method and channel way, and promote the systematization, effectiveness and normalization of secrecy education. Through security analysis, expert lecture and technical stealth demonstration, we can help the related personnel to understand the severity and the means of secrecy management of the electronic government information security under the information conditions. The concealment and conscientiously do well in the management of information security and confidentiality in e-government.

Second, we should establish a responsibility system for implementing information security work at different levels. Clarify the safety responsibilities of users of e-government information system, and sign responsibility letters, implement them and responsibilities to people. Establish a safety performance appraisal mechanism, and use rewards and punishments to urge safety responsibilities.

Third, strengthen the study of law and regulation system. Through the publicity and learning of information security and confidentiality management knowledge, we should enhance the sense and regulation consciousness of leading cadres' compliance with discipline and discipline.

Last, strengthen the learning of confidential knowledge. E-government personnel are the backbone of information security management. We must understand the theory and dynamics of

secrecy frontier, keep the basic knowledge of secrecy, and master the basic skills of prevention. Extensive publicity should be carried out in various forms to help the relevant personnel master basic protection skills, enhance their ability to prevent and ensure network security.

3. Experiment

In view of the reliability of Internet of things-based e-government information security, the following experimental analysis is carried out. The traditional methods and Internet of things-based research methods are compared and analyzed in two aspects of legal system construction and personnel security awareness training. The results are as follows.

（1） The construction of the legal system

In order to verify that under the influence of the legal system, the security of using the Internet of things research method is better than the traditional method, and the comparative analysis is carried out, as shown in Fig. 3.

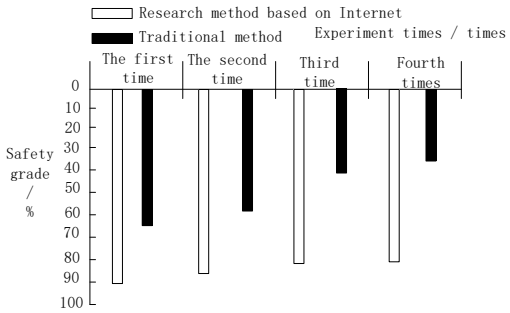

Fig.3 Comparison of the two methods under the influence of the legal system

As shown in Figure 3, when the number of experiments is 1, the traditional method security level is 64%, and the security level of the Internet of things research method is 89%; when the number of experiments is 2, the traditional method is 57%, and the Internet of things research method is 86%. When the number of experiments is 3, the traditional method is 41%, and based on the security level of the traditional method. The security level of the Internet of things research method is 82%; when the number of experiments is 4, the traditional method is 37%, and the safety grade of the Internet of things research method is 86%. Through the analysis results, we can see that under the legal system, the security level of the Internet of things research method is higher than that of the traditional method.

（2）Training of people's consciousness of safety and secrecy

The comparison between the traditional method security level and the security level based on the Internet of things research method in the training of people's security awareness is compared. The comparison results are shown in Fig. 4.

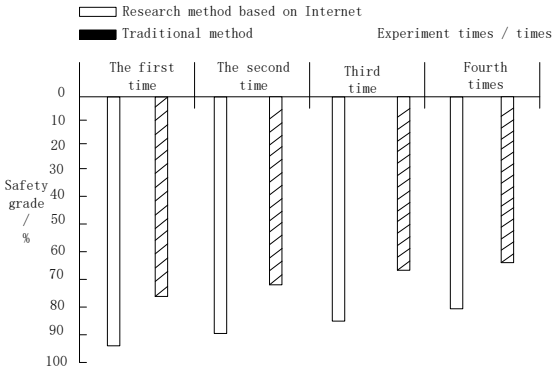

Fig.4 Comparison of two methods in safety awareness training

As shown in Figure 4, when the number of experiments is 1, the security level of the traditional method is 78%, while the security level of the Internet of things research method is 95%; when the number of experiments is 2, the traditional method is 73%, and the Internet of things based research method is 90%. When the number of experiments is 3, the traditional method is 68%, and the basis of the traditional method is 68%, and the basis of the traditional method. The security level of the Internet of things research method is 86%; when the number of experiments is 4, the security level of the traditional method is 64%, and the safety grade of the Internet of things research method is 82%. According to the analysis results, the safety level of Internet of things research method is higher than that of traditional methods under the cultivation of personnel safety and confidentiality consciousness.

To sum up, the research of e-government information security based on Internet of things is reliable.

4. Conclusion

The security protection of e-government involves many factors, many aspects, not a certain factor and one aspect can be completed independently. It is necessary to establish an electronic government security system with various protection forces in the internet of things environment, and take security measures at many levels to ensure the acceptable level of E-government security to be acceptable. The degree. In order to maintain the national interests and the interests of the people, we should build a domestic technology system to fully safeguard the information security of the E-government activities, promote the transformation of the government's work functions, and use the service oriented government system to safeguard the national interests and the people.

Acknowledgements

Xi 'an social science planning project for 2018 (Research on the Construction Path of Xi 'an Mobile Government New Media Cloud Platform) (Project no. 18X76).

References

[1] LI Junwei, JIANG Xuedong. Comprehensive evaluation model for information security risk of e-government system[J]. Modern Electronics Technique, 2017, 40(7):74-77.

[2] WANG Lianfeng, SONG Gang, ZHANG Nan. The Five Core Elements of Smart City Management and the Interaction among Them: An Innovation 2.0 Perspective[J]. Urban Development Studies, 2017, 24(3):67-73.

[3] WEN Qianyu, HU Guangwei. Research on the Mechanism of E-government Service Value Co-creation Based on the Value Net[J]. Journal of Intelligence, 2017, 20 (12):152-158.

[4] LONG Yi, LI Guoqiu. Research on the cooperative game of information sharing in G2C e-government under the view of "Internet + government"[J].Information Science, 2017, V35(5):34-41.

[5] ZHANG Huiping, GUO Ning, YANG Guofu, et. al. A Study on Cybersecurity Mechanisms of Internet Plus Government Services Using Socio-technical Framework[J]. Journal of Intelligence, 2017, 15 (12):16-21.

[6] LI Yan, ZHU Chunkui. How does e-government affect trust in government? An empirical study based on survey data from Wuhan, Tianjin and Chongqing[J]. Social Sciences in Nanjing, 2017, 12 (5):65-73.

[7] DING Yi, LIU Binfang, LIU Yuenan. Assessment of Government Online Services Development in China---An Empirical Study of 338 Cities in China[J]. Journal of Intelligence, 2017, 36(1):136-141.

[8] LI Yongzhong, CAI Jia. Theme Evolvement and Visual Analysis of Domestic E-government Research Based on LDA[J]. Modern Information, 2017, 37(4):158-164.

[9] ZHANG Yanlin, XIE Weihong, WU Xueyan. Citizen Trust in E-Government: An Empirical Analysis Based on Attribution Theory[J]. Chinese Journal of Management, 2017, 14(7):1088-1094.

[10] WANG Yu, WU Weixin. Simulation of Precision Monitoring for Data Transmission of Communication Information in Internet Users[J].Computer Simulation,2018,35(03):373-376.