Research and Design of Information Security Framework in Smart City

HongBin Pan

Kunming Metallurgy College, Kunming, Yunnan 650033, China

bestphb@21cn.com

Keywords: Smart city, Information security, Framework research, Design approach

Abstract: The emergence of smart city can not only bring more convenience to people’s work and life, but also fully demonstrate the comprehensive strength of our society. Strengthening the in-depth research and scientific design of the information security framework in the smart city can ensure that the role and value of the smart city can be brought into full play. Therefore, this paper makes a detailed analysis on the research contents and design approaches of information security architecture in smart cities, so as to lay a solid foundation for further promoting the development of Chinese cities towards intelligence and modernization.

1. Introduction

The establishment of smart city is an important measure to comprehensively promote the completion of a well-off society and the development of urbanization in China. Especially with the full popularization of Internet technology, cloud computing technology, Internet of things technology and big data technology, the full integration of relevant technologies with the construction of smart city can not only further improve the efficiency and response speed of public services in the city, ensure a richer industrial structure in the city, bring comfortable life experience to city residents, but also solve problems such as lack of initiative and advanced city management, lack of timeliness of information communication and lack of effectiveness of evaluation mechanism. This paper takes the information security framework of smart city as the core, sets the public model based on PKI / CA information security framework at the top-level planning stage, and establishes a set of smart city security system and security audit system with high feasibility and rationality, so as to provide positive support for the effective operation of different smart application security factor measurement strategies and the overall smart city information security factor measurement index system. As a result, it can ensure that the goal of further expansion of three-dimensional safe space is effectively realized, and can safely expand in combination with the characteristics of different smart cities.

2. Security System Framework Design

First, based on KPI / CA security system and PMI authorization management system, establish trust and authorization service platform layer, and provide service authentication, data encryption service, data integrity service, non-repudiation service, notarization service and other functions.

Second, use information security technology to establish a trusted support platform and provide trusted WSDL, trusted UDDI, trusted SOAP, trusted ceg-MXL, trusted Web Service and other support services.

Thirdly, based on the secure operation management workflow engine of security strategy and risk assessment, establish a security service platform to provide general web middleware services, platform integrated security services, business logic interface of smart applications, security audit services, etc.

The three-level security information framework can not only provide good services for the effective development of security work and audit work at all levels, but also ensure the high integrity of security mechanism and security services, and provide guarantee for the security of application, platform, data, system, transmission and equipment of smart city.

DOI: 10.25236/icited.2022.033

3. Safe Operation Design

In the process of designing the safe operation of smart city, we always follow the idea of "harmony but not sameness" and take resource-sharing as the principle to ensure that the urban safety management command center and emergency center share the workplace and relevant work equipment under the scientific guidance, realize joint office, and ensure the orderly operation of office, computer room, large screen and other working environments. Combined with the effective application of separate video monitoring system, we can carry out safety setting detection to avoid mutual interference between the safe operation and working environment of different departments.

We can fully connect the smart city network system with the public security video monitoring signal, make full use of the existing service hotline resources, and ensure that the built smart city information management platform has high unity characteristics. By fully combining urban components, cell grid management and event management, and in accordance with the division of security responsibilities and workflow standards, we can ensure that the information behind each component and event in the grid can be accurately sent to the security command center under the action of the information collector. On this basis, a series of effective supervision means such as video inspection, media exposure and leadership supervision are used to fully realize the safe operation and management objectives of the smart city [1].

4. Smart Application Security Design

Smart city is composed of diversified factors, and the smart application systems involved also have diversified characteristics. In the process of designing the smart city information security system, the security level and comprehensive performance must be fully considered. The overall performance of urban information security application system includes data exchange response ability, data exchange flexibility, dynamic geographic location query performance, strong stability, good concurrent response ability, data storage and management ability, etc. Based on the security policy and role authority definition, it provides guarantee for the identification and access authority of different users. Users only need to log in once to facilitate operation in the authorized application of the system, and there is no need to switch and log in again in the subsequent application process. When smart application types are different, the provided security policy interface and security policy indicators will inevitably change, and all these changes can ensure the seamless connection between plug and play mode and smart city public security strategy [2].

5. Security Design of Data Acquisition Terminal

Based on IOS and Android smart phone operating system, the terminal equipment of smart city is automatically expanded. It not only sets GPS inside, but also provides a platform for secondary development to support the effective development of basic functions such as data storage, image acquisition, WiFi connection, voice call, SMS message and recording function. Moreover, a camera is set inside, which can clearly shoot static objects within 30 meters, so as to ensure that the terminal equipment can work safely in the outdoor environment. In addition, all devices are equipped with password function, which can ensure the safe use of the system [3].

6. System Integration Security Design

The smart city management system is a collection of multiple systems and platforms. At the level of system integration security, we should attach great importance to the design of data security verification mechanism, data fusion security attribute control, reliability design and evaluation. Through the strict control of system access rights, it can ensure that the different needs of different users for security levels are fully met, and can effectively respond to all kinds of emergencies and system attacks, so as to further improve the security protection ability of urban network.

In the process of designing the data security verification mechanism, the staff should sort out the data before verification fusion and the data after fusion to ensure that they have highly consistent security and standardization. By improving system reliability, network reliability, interface reliability, storage system reliability, data backup reliability and data recovery reliability, the reliability of system integration security design is further strengthened [4].

7. Hardware Platform Security Design

In the process of designing the hardware security system of smart city, we should comprehensively consider the security of terminal equipment, storage equipment, network equipment and service cluster, mainly including terminal equipment, intrusion detection server, firewall, load balancing router, aggregation switch, storage array, audit server, access authorization server, network security server, mobile network server, Web server, GIS server, database server cluster, etc., and focus on the security of each link. On the basis of ensuring the hardware safety of smart city, we should improve the ability of performance analysis, operation monitoring and comprehensive platform safety evaluation of key hardware equipment of smart city [5].

8. Software Platform Security Design

In the process of designing smart city software security system, we should comprehensively consider middleware security, geographic information platform security, database platform security and operating system security, mainly including database operating system, mobile device operating system, network operating system, system recovery ability, data recovery ability, etc. Combined with the actual analysis, we can know that although almost all software platforms will provide corresponding security application services, but in the process of designing the smart city software system, we should conduct comprehensive audit and evaluation on the security of all software platforms again [6].

9. Design Audit Information Security

First, the automatic response function is designed to ensure that audit events can respond in time when potential security attacks are found. Specific functions include real-time alarm, real-time early warning, termination of violation process, invalidation of user account, etc.

Second, the log generation function is designed to ensure that security related events can be recorded. The specific contents include listing the types of audit events, identifying audit levels, and distinguishing the set of audit information provided by various audit records.

Thirdly, the operation analysis function is designed to find the possible security violations through the analysis of system activities and audit data, so as to automatically respond to security violations and intrusion detection. The specific contents include anomaly detection, anomaly exploration, potential attack analysis, etc. [7].

10. Conclusion

For the information security framework design of smart city, it is the basis and standard to judge the successful construction of smart city. Based on the specific construction objectives and application ways of smart city, it is necessary to build a security system that integrates the functions of information security public service, monitoring, audit, evaluation, emergency response, command and dispatching, highlighting the characteristics of “harmony but not sameness” of the system. We can regard information security as an independent system and design the overall framework. Starting from the diversified aspects of information security, information fusion, big data mining and key technologies of security evaluation, this paper makes a comprehensive exploration on the feasibility of the designed information security system framework of the smart city, and effectively manages the safe operation of the smart city step by step, level by level and stage by stage, so as to promote the smart city to give full play to its role, improve China’s comprehensive urban development capacity.

References

[1] Wang Fang, Zhang Yunyong, Fang Bingyi, et al. Building smart city information system with Internet of things and cloud computing [J]. Mobile Communication, vol.35, no.15, pp.49-53, 2019.

[2] Chen Hongsong, Han Zhi, Deng Shuning. Analysis and research on big data security in smart city [J]. Information Network Security, no.7, pp.1-6, 2018.

[3] WILLIAMS. Cryptography and network security theory and practice [M]. Translated by Wang Zhangyi, Yang Min, Du Ruiying, et al. Version 5. Beijing: Electronic Industry Press, no.12, pp.72, 2020.

[4] Zhao Yang, Chen Yang, Xiong Hu, et al. A data ownership proof scheme with revocable authorization in cloud environment [J]. Information Network Security, no.8, pp.1-7, 2019.

[5] Bian Chen, Yu Xingyan, Xiu Weirong, et al. Analysis and design of network monitoring system based on MPLS VPN Technology [J]. Information Network Security, no.5, pp.28-33, 2019.

[6] Zhang Xiaohui, Lin Baigang. Research on Internet of things security based on balanced binary decision tree SVM algorithm [J]. Information Network Security, no.8, pp.20-25, 2019.

[7] Zhang Haitao, Zhang Yongkui. Internet of things architecture and core technology [J]. Journal of Changchun University of Technology: Natural Science Edition, vol.33, no.2, pp.176-181, 2021.