Research on Information Security System of Smart City Based on Information Security Requirements

Na Dong¹, Junsan Zhao¹*, Lei Yuan² and Yun Kong¹

¹Faculty of Land and Resources Engineering, Kunming University of Science and Technology, Kunming, China.
²School of Information Science and Technology, Yunnan Normal University, Kunming, China.
Email: 40439968@qq.com   *Corresponding author, Email: 1429620189@qq.com

Abstract. In the process of smart city construction, information security is an important factor to ensure the sustainable development of smart city. The paper focuses on information security problems in the construction of smart city, and explores the overall framework and construction contents of information security system. First of all, the paper summarizes the characteristics of smart city information system, and analyzes the requirements for information security. Then, combined with the relevant standards and norms of information security, the paper puts forward construction ideas of information security system. On this basis, the overall framework of information security system is constructed with a global perspective, which includes three systems: management system, technology system, construction and operation system. At the same time, the construction contents and guarantee strategies of each system are put forward. The establishment of information security system helps to ensure safe management and operation of smart city. This research provides a reference for the related research of information security in smart city.

1. Introduction
The slogan of "Smart City" was put forward by IBM in 2009, hoping to lead the world city to prosperity and sustainable development through the construction of smart city. In recent years, there has been an upsurge in building smart cities both at home and abroad. As for the definition of smart city, there is no authoritative conclusion in the world. The paper quotes IBM's definition of smart city: "It can make full use of information and communication technology to measure, analyze and integrate the key information of the core urban operation system, so as to respond intelligently to the various needs, including people's livelihood, environmental protection, public safety, urban services, industrial and commercial activities to make a better city life accordingly" [1].

As a new city form, smart city is highly integrated with information resources. The new generation of information technology, such as Internet of things, cloud computing, big data and so on, is widely used in urban management, which makes the threat of information security deep into every corner of the city. The big data of urban operation and management will easily become a significant target of network attack, which leads to leakage of urban management information. When the urban operation system is attacked, the data is destroyed and the information is lost, it will cause a great blow to the operation and management of the city and it is difficult to recover. These factors will lead to paralysis of daily life or major economic losses [2]. In addition, due to the lack of safety experience in smart city's construction and the existence of loopholes in the security system, it will also increase the vulnerability of operation and management. The security threat of personal information and privacy protection is multiplied and even poses a threat to national information security. Therefore, the
information security has become a new challenge in the construction and development of smart city [3]. How to give full play to the huge role of information sharing, coordination and integration, meanwhile, keeping the stability of information security at a certain limit, which has become a practical problem that smart city has to solve. In 2016, Chinese government issued The People’s Republic of China network security law and The national cyberspace security strategy, which embodies the importance of building information security system and carrying out the construction of information security in smart city.

Based on the requirements analysis of information security, this paper constructs the overall framework of information security system for smart city. It puts forward the corresponding construction contents and safeguard strategies from technology level, management level, construction and operation level.

2. Characteristics of Information System and Analysis of Information Security Requirements for Smart City

2.1. The Characteristics of Information System

Compared with the conventional information system, information system of smart city has different characteristics, which are reflected in the following aspects:

2.1.1 Extensive internet of things technology. The extensive internet of things technology connects the public service resources, such as water, electricity, oil, gas and traffic in the city with the various facilities and articles of individuals and families through the internet to achieve a comprehensive physical connection, forming a more thorough perception and more in-depth intelligence [4].

2.1.2 Cloud technology. The use of cloud technology makes network resources, computing resources and storage resources readily available, and provides all the technical capabilities for people to achieve their goals on the internet [5].

2.1.3 Communication technology of the new generation. The use of the communication technology in a new generation aprovides internet access capability at any time, any place and any device [6].

2.1.4 Big data technology. Because information system of smart city has kept all the data of internet of things, application access, user information, city management information and so on. These data can provide more valuable urban management information through large data processing and data mining [7].

According to the characteristics of information system, with the application and development of high and new technologies such as the internet of things, cloud computing and large data, the network environment in smart city will become more complex. The security problems of information and network and even the application terminal will be more than the conventional information security problems.

2.2. Analysis of Information Security Requirements in Smart City

Information security refers to the protection of information systems (including hardware, software, data, people, physical environment and their infrastructure). The information system will not be damaged, changed, and leaked by accidental or malicious reasons. The system runs continuously, reliably and normally, the information service is not interrupted, and the business continuity is finally realized [8].

The information security of smart city needs to ensure the stability and reliability of the city's key information infrastructure system and network operation, to ensure the confidentiality, integrity and authenticity of the government, enterprises, institutions, social groups and individual information, and to ensure the availability and reliability of the integration and sharing of resources and services in smart city. So as to realize the safe and effective operation of smart city [9]. Because smart city is composed of network, communication equipment, hardware, software, information resources,
information users, rules and regulations, different parts and different environments have different security risks and requirements. Therefore, about information security requirements, it can be analyzed from three aspects of management, technology, construction and operation. The paper draws the table on the analysis of information security requirements in smart city, as shown in table 1, which shows the corresponding management requirements, technology requirements, construction and operation requirements.

2.2.1 Management requirements. The information security of smart city is not only a technical problem, but also needs to be taken by combining management system, assessment system, information security products and service certification access mechanism[10], personnel and network information security technology training[11] to improve the ability of risk protection accordingly.

2.2.2 Technology requirements. In view of the information security problems that smart city may encounter, the technology requirements can be divided into physical security, network security, host security, data security, application security and cloud computing security [12].

2.2.3 Construction and operation requirements. Information security construction needs to ensure the implement security of smart city engineering [13]. Information security operation needs to be able to understand the overall operating state of smart city, to monitor and warn the risk of information security in an all-round way, and to make emergency plans for the network information security events.
Table 1. A table on the analysis of information security requirements in smart city

| Management Requirements                                           | Technology Requirements                                                                 | Construction and Operation Requirements                          |
|-------------------------------------------------------------------|----------------------------------------------------------------------------------------|------------------------------------------------------------------|
| Clearing the goal of safety protection.                          | Physical and environmental information security of the sensing layer device.            | Implementation safety of information security engineering.      |
| Establishing the information security management system of smart city. | Establishing a unified identity identification and identity authentication mechanism.   | Comprehensive monitoring and early warning of information security risk. |
| Improving the organization and post responsibility.              | Information security detection and special protection.                                 | Establishing and improving the emergency mechanism.              |
| Establishing information security mechanism.                      | Information security protection for network hardware and network communication lines.   | Formulating emergency preparedness plan for network information security events. |
| Training of personnel information security awareness and network information security technical knowledge. | Preventing illegal access and malicious attacks.                                      | Timely repair and event tracing.                                 |
| Improving the system of urban information security assessment, inspection and acceptance. | Ensure the confidentiality and integrity of data transmission in network communication layer. |                                                                     |
|                                                                   | Security in data storage and processing.                                               |                                                                     |
|                                                                   | Information security of basic software such as operating system.                      |                                                                     |
|                                                                   | The security of the basic service interface.                                           |                                                                     |
|                                                                   | Life cycle safety of data acquisition, aggregation, storage, use, sharing and so on.   |                                                                     |
|                                                                   | Security of application software system, intelligent terminal, portal website and user account. |                                                                     |
|                                                                   | Virtualization security.                                                               | Taking technical measures to eliminate the hidden dangers of security. |
|                                                                   | Avoid cloud platforms being attacked.                                                 |                                                                     |
| Establishing a unified access mechanism for smart city information security products and service certification. | | |

3. Construction of Information Security System

3.1. Construction Ideas of Information Security System
To build the information security system of smart city, we can follow the following train of thought: Firstly, the necessity and feasibility of information security system construction are analyzed, the information security requirements and the characteristics of the business system are studied. Secondly, the general logic model of the information security system is designed, combined with the relevant standards and specifications of information security. Thirdly, the overall framework and construction plan of information security system are established through comprehensive analysis. Finally, the construction of information security system is completed, which needs to be examined and perfected gradually through safety inspection and emergency rehearsal. Figure 1 shows the construction ideas. It can be seen that through systematic analysis, a set of interconnected and complementary information security system is formed step by step.
3.2. The Overall Framework of Information Security System

Based on the analysis of information security requirements, for future construction and development, a relatively unified information security system should be built in a global perspective. Follow the relevant safety system construction reference standards and specifications [14], the overall framework of information security system in smart city are established, as shown in figure 2.

As shown in figure 2, the construction of information security system begins with the information security of the urban business system, taking international standards, domestic standards and industry regulations as the basic guiding ideology to complete the system construction. The information security system is mainly composed of three systems, which are management system, technology system, and construction and operation system. The three systems are both organic and mutually supporting. The relationship between them is "security organization and personnel follow safety management system, and security technology is used to ensure the safe operation of the system" [15]. By building a unified information security system, the risk of physical layer, network layer, data layer, application layer, management and operation can be covered more comprehensively, so as to guarantee the information security of smart city effectively.

![Diagram](image-url)
3.3. The Main Construction Contents and Guarantee Strategies of Each System

3.3.1 Management system. The construction management system is based on the international and domestic related standards. It makes clear requirements in the aspects of security management organization, security management system, product specification, security risk assessment, personnel information security training and other factors [16]. Finally, a set of systems and regulations for effective management of information security in smart cities is formed.

3.3.2 Technology system. The technology system mainly uses a series of information security technology to realize the security protection of the physical environment, network transmission, host system, data resources and application services.

   • Physical environment security
      The goal is to prevent physical devices from being accessed or damaged under unauthorized conditions, so as to ensure the absolute security of hardware[17]. The security strategy used mainly in the following aspects. Using of intrusion detection system to prevent the theft of sensing network information behavior, this way can enhance information transmission of sensor network and radio communication security. An access control mechanism is established to realize the security authentication and control of the sensing nodes and the base stations, so as to prevent illegal users from controlling the sensing devices. By using situation analysis technology to prevent malicious code attacks, it can control the risk of sensor equipment failure to ensure physical security. At present, the
The key technology of smart city perception layer is RFID (Radio Frequency Identification) technology. Because RFID carries electronic information, its data content can be protected by passwords, so that its contents are not easily forged and altered.

- **Network transmission security**
  The network structure of a smart city is usually made up of a new generation of cable networks, mobile networks, WIFI networks and satellite communication networks. The network is the most vulnerable place to be attacked and may be illegally hijacked and stolen in the data transmission process [18]. Network security technology mainly through the establishment of cross network authentication mechanism between heterogeneous transmission networks, to prevent the security risks of cross isomerism network and enhance the transmission efficiency of information across the network. At the same time, data encryption technology is applied to prevent leakage in the network transmission process and enhance the integrity and credibility of data information.

- **Host system security**
  The challenge of host security technology in smart city refers to the host security technology challenge in cloud computing environment. Because of the unique virtual computing environment of cloud computing, the security problem is more difficult to handle [19]. Therefore, we must study the new protection solution of host security, and remould the security mechanism of the host system from the aspects of identity authentication, sensitive marking, access control, security audit, intrusion prevention, malicious code prevention and so on.

- **Data resources security**
  Data security and privacy protection is a major challenge in big data environment. Through a large amount of collection, filtering and integration of business data and meticulous business analysis and association rules mining, enterprises or related data management departments can perceive their own network security situation. In addition, using security baseline and large data analysis technology and so on, it can detect and discover all kinds of abnormal behavior and security threats in the network in time, so as to take corresponding security measures. In the future, by using the strategy of building large data security institutions and open design services, we can deploy the overall security solutions from many angles and ensure the security of the large data computing process, data form and application value.

- **Application services security**
  The security of application services is mainly to consider the security increase, reinforcement and transformation of the application systems, and to provide a unified support platform for the security protection functions of the cloud computing center and the region. The main protection strategies are as follows, for example, building a security application support platform, establishing a system security audit system to improve the quality of development, using digital watermarking technology to ensure data and system code security, using secure encapsulation to achieve access control to application services [20].

### 3.3.3 Construction and operation system

The construction and operation system mainly contains two layers of meaning: Firstly, it means to locate, protect and eliminate security events such as virus or hacker attack on network or system during operation and maintenance, so as to ensure that the system is not infringed by internal and external. Secondly, safety operation and maintenance services such as monitoring, warning, response, assessment, emergency and disaster recovery should be carried out during operation and maintenance. Through the construction of the construction and operation system, we can improve the response speed of emergency and service by means of intelligent analysis and prediction, so as to improve the level of urban management and service.

Furthermore, considering the dynamics, relativity and integrity of information security, the information security system of smart city is not invariable. We should accumulate experience in the implementation of information security system, so that the information security system can be continuously improved.
4. Summary
In the process of smart city construction, information security can not be ignored. The information security system should be implemented simultaneously. In this paper, the overall framework of information security system for smart city is set up from three aspects of management, technology, construction and operation. It is helpful to realize the security construction and operation for smart city in the future.

In the future, the focus of information-technology industry in a new generation is network and intelligence. It emphasizes the integration of information technology into various sectors of social and economic development, and the data is more open and shared. Therefore, it is necessary to improve the information security regulatory mechanism and relevant information security standards as soon as possible. We believe that through continuous efforts, the lack of information security standards in smart city will eventually be solved. It will bring the information security level of smart city to a new level.

5. Acknowledgments
This study was supported by the project of national natural science foundation (No.41761081). The authors express gratitude to laboratory colleagues for their help in the research.

6. References
[1] Paroutis S, Bennett M and Heracleous L 2014 J. Technological Forecasting and Social Change. Vol 89 pp 262-272.
[2] Zuhadar L, Thrasher E, Marklin S and de Pablos PO 2017 J. Computers In Human Behavior. 66 pp 273-281
[3] Liu SF, Peng L, Chi TH and Wang XM. 2016 Proc. Ieee International Geoscience and Remote Sensing Symposium (Igrass) pp 623 - 625.
[4] Ziegler S, Rolim J and Nikoletsea S 2016 Proc. Ieee 30th International Conference on Advanced Information Networking And Applications Workshops (Waina 2016). pp 611-616.
[5] Hu M and Li C 2012 J. Internet of Things. vol312:466-4+.
[6] Yaqoob I, Hashem IAT, Mehmood Y, Gani A, Mokhtar S and Guizani S 2017J. Ieee communications Magazine. Vol 55 (1) pp 112-20.
[7] Hashem IAT, Chang V, Anuar NB, Adewole K, Yaqoob I and Gani A, et al 2016 J. International Journal Of Information Management. Vol 36 (5) pp 748-58.
[8] Liu Z, Seo H, Sun HM, Huang CT 2017J. Journal of Information Science and Engineering. Vol 33 (4).
[9] Zhu N.N and Zhao H.Y 2018 J. Computers & Electrical Engineering. Vol 65 pp 34-43.
[10] Yuan Fan 2014J. China Information Security. 10 p 119.
[11] Guguloth, R, Kumar and T.K.S 2018 J. Computers & Electrical Engineering. Vol 65 pp 79-89.
[12] Dajiang Zhang, Xiaoyu Bi, Xin Lu and Xiaolu Han 2017J. Reasearch of Information Security.Vol3 (8) pp 710-717.
[13] Mazza, D, Tarchi, D and Corazza, G. E 2017J. Ieee Communications Magazine. Vol 55 (3) pp 30-37.
[14] GB/T 34678-2017, 2017 S. China National Standardization Management Committee.
[15] Cilliers, L and Flowerday, S 2014 J. 2014 World Congress on Internet Security (Worldcis) pp 36-41.
[16] Bharat V, Shubham S, Jagdish D, Amol P, Renuka K 2017 Proc.Proceedings Of the 2017 International Conference on Big Data Analytics And Computational Intelligence (Icbdac) pp 267-71.
[17] Cassandras CG 2016 J.Engineering.Vol2 (2) pp 156-158.
[18] Zou X, Cao JH, Guo Q, Wen T. 2018J. Computers & Electrical Engineering. Vol 65 pp 67-78.
[19] Klonari V, Toubeau JF, Lobry J, Vallee F. 2016 Proc. Smart greens: Proceedings of the 5th International Conference on Smart Cities and Green Ict Systems. pp 166-178.
[20] Zhang K, Ni JB, Yang K, Liang XH, Ren J, Shen XM. 2017 J. Ieee Communications Magazine.vol 55 (1) pp 122-129.