Research on the Construction of an Information Security Assurance System for Smart Cities in the Big Data Environment (Postprint)

Authors: Zou Kai, Guo Yihang, Xiang Shang, Wan Zhen

Date: 2023-10-08T00:00:00+00:00

Abstract

[Purpose / Significance] Under the big data environment, information security issues faced by smart cities are becoming increasingly prominent. Accordingly, constructing a smart city information security assurance system characterized by comprehensive perception, systematic operation, and collaborative integration in the big data environment, optimizing smart city information security management under such environment, and improving current smart city information security construction possess certain theoretical significance and practical value. [Method / Process] This study applies total quality management theory to research on smart city information security assurance systems. Grounded in the four fundamental connotations of information security, it constructs the basic architecture of a smart city information security assurance system under the big data environment through the four stages of the PDCA cycle. [Results / Conclusion] Addressing smart city information security assurance issues through the PDCA cycle aligns with the characteristic that urban construction and development processes require continuous dynamic adjustment. This approach provides a reference for the whole-process implementation of smart city information security assurance under the big data environment, encompassing: in the planning stage "direction + objectives, norms + constraints, plans + indicators" ; in the implementation stage organizational structure, infrastructure, and technical systems; in the control stage situational awareness, emergency response, and risk management; and in the improvement stage multi-stakeholder collaboration among government, operators, and the public.

Full Text

1 Introduction

With the widespread adoption of Web 2.0, Internet of Things, and cloud computing technologies, information exchange and sharing among governments, enterprises, and society have become increasingly frequent during smart city construction and operation. While generating massive data resources, this trend has also introduced many non-traditional information security problems. Privacy leakage incidents caused by the interweaving and superposition of these problems are growing exponentially, easily leading to adverse economic and social impacts. China' s 14th Five-Year Plan outlines the need to "ensure national data security while promoting the deep integration of new-generation information technologies with various industries, and advance the construction of big data centers." As a key technology driving the rapid development of smart cities, big data integrates critical information from urban public infrastructure operation systems, tracks urban operation status, coordinates management of information resources from all parties, monitors and handles various emergencies, and facilitates the evolution of traditional data centers toward new types that are high-performance and highly efficient, thereby ensuring favorable conditions for urban operation.

Current research on smart city information security by domestic and international scholars is relatively abundant. Shen Minghuan [1] first emphasized the need to strengthen strategic-level management of smart city information security. Chen Z Y [2] first mentioned information security protection during visual data processing for smart cities. Against this backdrop, scholars gradually began research on smart city information security. In the initial stage, most studies were qualitative and macro-level, exploring basic connotations [3], current dilemmas [4-7], risk assessment [8], key technologies [9], and assurance strategies [10-11]. As research expanded, scholars began conducting quantitative analyses, innovative technology integration, and specific practical applications, examining risk prediction [12-13], assessment models [14-15], risk factor identification [16-17], and risk supervision [18] in smart city information security risk management. They also constructed smart city information security systems from different dimensions [19] and levels [20] to address operational risks, with further improvements made by relevant scholars [21-22]. Research has also investigated the deep integration of new-generation information technologies [23-26] in smart city construction and explored specific practices for security and privacy protection in different smart application scenarios [27].

In summary, while research on many aspects of smart city information security is relatively mature, studies on assurance systems remain limited and lack systematic planning and mature theoretical guidance. Particularly under the big data environment, data in information security is presenting a new form characterized by multi-dimensional fusion, multi-stakeholder open sharing, cross-domain interconnection of all things, overlapping penetration of software and hardware,

and convergence through coordination and integration. This greatly increases the complexity, interweaving, dynamism, and comprehensiveness of information security management [28]. Information security is not merely a technical issue but a collaborative management problem across all aspects [29]. Therefore, constructing a comprehensive smart city information security assurance system is imperative. From a top-level design perspective, this paper first analyzes the inherent connection between the challenges facing smart city information security and its basic connotations under the big data environment. It then applies the PDCA cycle from total quality management theory to implement comprehensive dynamic quality management across different stages of smart city information security work. Finally, it constructs an information security assurance system that emphasizes business requirements and continuous improvement to meet the needs of smart city information security construction, aiming to provide recommendations for specific practices.

2 Formation of Smart City Information Security Assurance System under Big Data Environment

2.1 Challenges Facing Smart City Information Security under Big Data Environment

The construction of smart cities and the development and application of big data technologies have opened a new chapter of large-scale, real-time, online, multi-party collaborative social governance. Leveraging big data can provide powerful decision-making support for urban planning, management, security and disaster prevention, and public opinion monitoring, thereby optimizing administrative resources, reducing management costs, improving efficiency, and enhancing emergency response capabilities. However, while driving urban intelligence upgrades, big data also brings more severe information security challenges, mainly in three aspects:

First, traditional protection methods have become complex and difficult. Under the big data environment, conventional data protection methods such as data isolation, encryption, access control, and disaster backup require further innovation. Risks of data leakage, tampering, and destruction exist throughout data transmission, processing, and storage stages, differing from traditional threats.

Second, data fusion and sharing have complicated management tasks. The high degree of data fusion and development presents unprecedented challenges for information security management. At the macro level, smart city information security assurance systems, relevant laws and regulations, and supervision mechanisms remain incomplete, with capability building still in its infancy. At the micro level, information security workers must design different security strategies and prevention schemes for different operating environments, system architectures, database systems, and data formats across various smart city information systems, further increasing operational management and monitoring audit difficulties.

Third, personal privacy protection and data security have become more urgent. The concept that "information is value" is deeply rooted in the big data era. Relevant enterprises collect large amounts of unnecessary personal information and disclose or disseminate it without authorization, exacerbating personal information abuse. More seriously, the practice of profiting from selling personal information is common, as exposed in cases such as "illegal theft of facial information" and "illegal sale of resume platform personal information" on the "315" Evening Gala. The incident of "Didi platform being removed from app stores due to information exposure" even threatened national security. Additionally, cyber hackers exploit technical vulnerabilities and inadequate supervision to steal personal information from multiple dimensions, subsequently conducting telecom fraud and other illegal activities. In today' s ubiquitous network era, criminals can use big data analysis technologies to launch multi-dimensional, simultaneous cyber attacks with fewer resources, making information security threats more precise and damaging.

2.2 Basic Connotation of Smart City Information Security under Big Data Environment

Based on the national "Regulations on the Security Protection of Computer Information Systems," the basic connotation of smart city information security can be divided into four aspects: physical security, data security, operational security, and management security. Physical security refers to physical security design conducted through hardware facilities and environmental construction of smart city information system entities to build a secure physical network. Data security establishes security protection for data processing systems to ensure the availability, integrity, and confidentiality of network data. Operational security focuses on the operational characteristics of smart cities, using security technologies and measures to protect security during information processing, analysis, and usage. Management security involves formulating corresponding standards, norms, and institutional rules to manage and constrain the daily work and behavior of smart city information security personnel. Comprehensive dynamic management of these four aspects helps address the enormous challenges of smart city information security under the big data environment.

2.3 Architecture of Smart City Information Security Assurance System under Big Data Environment

Total quality management theory was proposed in the late 1950s by Feigenbaum of General Electric and quality management expert Juran. It is a management system that achieves pre-control and comprehensive control to realize comprehensive management of objects, processes, personnel, and scope. Dr. Deming summarized the total quality management work process as a four-phase cycle of "Plan-Do-Check-Act," abbreviated as the Deming Cycle (PDCA). It is a cyclical system that repeats endlessly, with large cycles containing small cycles, small cycles driving large cycles, and stepwise improvement [30]. Currently, the Dem-

ing Cycle (PDCA) has been widely studied and applied in information security across different industries [31-33] and organizations [34-36].

Smart city information security construction is a long-term, quality-centered endeavor based on the participation of government, enterprises, and the public to achieve benefits for all and ensure success. Drawing on the ISO/IEC 27001:2005 standard, this paper constructs an information security assurance system for smart cities under the big data environment, as shown in Figure 1 [Figure 1: see original paper]. By adopting the PDCA cycle control concept, the smart city information security assurance system is divided into four phases: "Planning-Implementation-Control-Improvement."In the planning phase, overall objectives are established based on strategic planning characteristics of smart city information security assurance. In the implementation phase, according to the four basic elements of total quality management— "structure, technology, personnel, and change drivers"—the smart city information security implementation process is divided into three components: organizational structure, infrastructure, and technical system to protect physical and data security. In the control phase, based on the characteristics of smart city information security under the big data environment and in conjunction with the national standard GB/T 20282-2006 "Information Security Technology—Information System Security Engineering Management Requirements," strong control is exercised over data operations and business processes from three aspects—situational awareness, emergency response, and risk management—to protect operational and management security. In the improvement phase, different improvement requirements and suggestions for smart city information security are proposed from the perspectives of the state, smart city service providers, and the public, forming a complete architecture for the smart city information security assurance system.

3 Whole Process of Smart City Information Security Assurance under Big Data Environment

3.1 Planning of Smart City Information Security Assurance under Big Data Environment

The primary task in smart city information security planning is to determine the overall direction and macro objectives. After collecting suggestions from the public and various organizations, the government utilizes big data analysis and mining technologies and information security protection characteristics to establish construction goals for information security work, providing guiding opinions for the implementation and control processes. Second, the government must plan the basic elements of risk management under the top-level framework while coordinating the balance among opportunities, environment, and organizational resources from all parties. Under the guidance of laws and regulations such as the Data Security Law and the Personal Information Protection Law implemented on November 1, 2021, and corresponding policies, information security organizational activities and work are standardized and constrained.

Finally, information security authorities must formulate corresponding detailed plans and indicators, design quality assessment models, develop data quality technologies, strengthen the construction of management regulations and means, and implement security management measures.

3.2 Implementation of Smart City Information Security Assurance under Big Data Environment

During smart city information security implementation, based on the four basic elements of total quality management– "structure, technology, personnel, and change drivers" –the smart city information security implementation process is divided into three components: organizational structure, infrastructure, and technical system to protect physical and data security.

3.2.1 Establishment of Smart City Information Security Organizational Structure In the implementation phase of smart city information security assurance, to achieve information security construction for different application projects, it is necessary to establish a professional, departmentalized, and formalized information security organizational structure that coordinates the division of labor, grouping, and collaborative cooperation among various information organizations at different levels. Smart city information security organizational structure construction should connect various resources into corresponding modules according to the objectives and work plans of smart city information systems, establish business and administrative departments at different levels, stipulate internal staffing and authority division, and define mutual subordination relationships, making the smart city information security organization an organic whole with reasonable structure and complete functions. Combining the characteristics of specific practices in smart city information security and starting from the actual needs of smart city information security, this paper establishes a "pyramid" structure for smart city information security organizations, as shown in Figure 2 [Figure 2: see original paper].

The Information Security Leadership Group is the decision-making body for smart city information security, mainly responsible for determining information security strategy and direction from a global perspective, deploying information security management work, and exercising effective control over smart city information security projects. The Information Security Supervision Agency supervises the work of the Information Security Management Committee and implementation agencies, reports review results to the Smart City Information Security Leadership Group, and provides improvement suggestions for information security work in various departments and business systems. The Information Security Management Committee provides decision support for the decision-making body, formulates relevant rules for information security work, conducts reviews and quality control of information security projects, manages information security implementation agencies, and regularly reports information security conditions to the smart city information security supervision agency.

For example, relevant cloud service and supply chain providers must sign information security assurance agreements, forming effective information security assurance plans and evaluation indicators within the company and strictly following national standards and industry norms for management and operation.

The Information Security Implementation Agencies include the information security operations team and the information security incident response team, responsible for implementing and executing the policies and work requirements of higher-level departments and timely responding to and handling information security emergencies within eight major application projects such as smart public services and smart city integration [37].

3.2.2 Construction of Smart City Information Security Infrastructure

Smart city information security infrastructure construction is the material foundation for smart city information security assurance. Through information security infrastructure construction, functions such as information security data sharing, information content monitoring, and harmful information filtering can be achieved, which is beneficial for network security assurance and cyberspace governance of relevant smart city application projects. Guomai Internet [38] divides smart city infrastructure into three components, as shown in Table 1 :

Table 1 Smart City Information Security Infrastructure

Information Security Infrastructure	Information Security Infrastructure Content
Information Network Facilities	Wired broadband, wireless broadband, urban IoT, triple network convergence, etc.
Information Sharing Facilities	Cloud computing platforms, information security service platforms, testing centers, etc.
Intelligent Traditional Facilities	Water, electricity, gas, heating pipeline networks, roads, bridges, stations, airports, etc.

Based on the newly issued "Regulations on the Security Protection of Critical Information Infrastructure" by the State Council, the advancement of smart city information security infrastructure construction should mainly include three aspects: First, overall planning and systematic management of information security infrastructure construction, stipulating that information obtained during work can only be used for maintaining network security. Second, closely tracking and studying international development trends and technological advances, and enhancing infrastructure capabilities in combination with the technical characteristics of smart city information security under the big data environment, such as upgrading infrastructure, expanding bandwidth, and improving intrusion detection technology. Third, strengthening communication and connection among

various network command centers, integrating the work capabilities of different units, enhancing cooperation in online monitoring and situational awareness of smart city information security through coordination and analysis, and establishing a network security information sharing mechanism.

3.2.3 Construction of Smart City Information Security Technical System The core objectives of information security technology generally include confidentiality, integrity, availability, controllability, and non-repudiation. Following principles of security isolation, dynamic protection, and deep protection, a relatively comprehensive and complete smart city information security technical system is established from three dimensions: hierarchy, space, and level, as shown in Figure 3 [Figure 3: see original paper].

In the hierarchy dimension, various smart city information systems integrate infrastructure such as computer hardware, software, networks, and communication devices to process internal business information flows, which can be divided into four aspects: perception layer, network layer, data layer, and application layer [39]. The four layers of smart city information systems progress layer by layer, with security deficiencies in lower-layer facilities affecting the operational security of higher layers, creating intertwined information security threats that impact overall system security. During information security environment construction, security products should be built layer by layer while paying attention to compatibility and complementarity among security products at different layers to avoid contradictions between security strategies and factors.

In the space dimension, networks are connected into numerous distributed network systems of varying sizes. Protection strategies and technical means will differ for different security objectives in different network regions, requiring domain-specific protection measures based on regional characteristics. Based on the existing computer network system composition standard GB/T 20282-2006, smart city network information systems can be divided into four types: local computing environment, network boundary, network transmission, and network infrastructure [40]. Identity verification, physical isolation, intrusion detection, and other security technologies and related security products are used in each region to ensure information security within each security domain.

In the level dimension, different smart city application projects and business departments have different requirements and importance levels for information security, and the costs and prices paid for information security protection will also differ. Therefore, combining the classification and grading protection concept for data in the Data Security Law, smart city information security protection is divided into five levels [41]. Key information related to smart city construction and operation and urban residents' privacy receives focused protection, while secondary information receives appropriate protection. Additionally, during the construction of the smart city information security technical system, prevention and protection in all aspects of information systems should be continuously strengthened in synchronization with the continuous improvement of

information security theories and methods and technological advancement.

3.3 Control of Smart City Information Security Assurance under Big Data Environment

In the smart city information security control process, based on the characteristics of smart city information security under the big data environment and on the foundation of establishing basic elements of smart city information security, and in combination with national standards and specific practices of information security engineering, strong control is exercised over data operations and business processes from three aspects—situational awareness, emergency response, and risk management—to protect operational and management security of smart cities.

3.3.1 Smart City Information Security Situational Awareness The focus of smart city information security situational awareness is to protect the security, stability, and continuous operation of core applications in the urban network environment. It involves identifying and reporting all information security violations during smart city construction and operation, detecting and tracking relevant events, and handling changes in urban information security situations according to security objectives and strategies. Urban network core applications involve the supervision of various assets within smart city application projects. Therefore, situational awareness must closely follow the main line of "asset-data-situation" to identify, analyze, and respond to potential security threats in asset structure, management, and service status.

In the asset layer, after preprocessing such as data reduction and fusion, asset information and monitoring data are represented and stored using corresponding asset databases and event databases to provide data support for the data layer. In the data layer, through the application of network feature extraction technology, correlation analysis technology, and other related intelligent algorithms and security models under the big data environment, stored data is deeply mined and processed to identify security events affecting the operational situation of smart city information systems. In the situation layer, during security event handling, data visualization technology should be used to supervise system security situation changes based on real-time data feedback, predict system security status and security event development trends, make forward-looking judgments, and provide early warnings for information security.

3.3.2 Smart City Information Security Emergency Response Smart city information security emergency response refers to the preparatory work done before and emergency measures taken after the occurrence of various information security events in smart city systems [42]. Smart city information security emergency response can be divided into four parts: emergency preparation, incident warning, emergency handling, and incident evaluation. Due to the timeliness and effectiveness requirements of information security event

handling, incident warning and emergency handling often occur simultaneously. Incident evaluation runs throughout the entire emergency response process, assessing the smart city information security emergency response process, various institutions, and personnel behavior.

In emergency preparation, information security management agencies refer to the "Information Security Incident Classification and Grading Guide" to classify incidents into different categories and levels based on three factors—information system importance, system loss, and social impact—and formulate corresponding information security emergency plans to enable rapid response when security events occur.

In incident warning and emergency handling, when an information security event occurs in a smart city business system, if the security event is under control, the information security implementation agency immediately activates the corresponding information security plan, makes adequate information preparation, and records all activities for subsequent review. Conversely, if the security event is not under control, an incident warning should be issued promptly, an information security situation and event report form should be completed as required, and it should be reported to the Information Security Incident Response Team (ISIRT). Additionally, if the incident is determined to be a major information security event, it should be immediately reported to ISIRT management and senior management.

In incident evaluation, the Information Security Management Committee and Information Security Supervision Agency should collect and securely preserve relevant electronic evidence during the emergency response process to support subsequent legal prosecution or internal personnel rewards and punishments. After the security event is resolved, the Information Security Management Committee should conduct incident evaluation based on detailed emergency records in the report, learn lessons from security events and their protective measures, and modify existing emergency plans when necessary to prevent similar security events from recurring.

3.3.3 Smart City Information Security Risk Management During smart city operation, the diversification of software and hardware systems, system integration, and network connections inevitably create defects and potential weak links, thereby causing information security risks of varying degrees. Drawing on previous research foundations [43-46], this paper argues that smart city information security risk management should adopt a target-driven management model, conduct smart city information security risk management modeling, and strengthen the construction of risk libraries, as shown in Figure 4 [Figure 4: see original paper].

First, massive information security raw data is obtained through big data collection technology to analyze the characteristics of internal business needs in smart cities, set information security control points for business requirements, define

important boundaries of processes, and determine the objectives of smart city information security risk management to complete risk management preparation under target drive.

Second, corresponding risk management business processes are established according to the business objectives and security needs of information systems. When conducting smart city information security risk management work, various data features and security attributes in the system are analyzed and identified to determine lists of assets, threats, vulnerabilities, and control measures. For various known risks in smart city information systems, corresponding intelligent algorithms and mathematical models under the big data environment are selected from the risk model library to analyze information security risk threat indices, classify corresponding risk levels, predict the likelihood of risk occurrence and social impact, and extract information security risk patterns and store relevant characteristic data into the risk database. Based on the obtained risk patterns and characteristic data, relevant rules and response measures in terms of systems, technology, and management for handling such risks are obtained from the risk knowledge base, and risk resolution results are evaluated, reviewed, and stored for the record.

Finally, for newly discovered information security risks or new changes in existing risks, the risk database, risk model library, and risk knowledge base are updated in a timely manner.

3.4 Improvement of Smart City Information Security Assurance under Big Data Environment

The improvement of smart city information security assurance under the big data environment is an important module built upon planning, implementation, and control. Through the PDCA cycle approach, it can drive problem-solving in smart city information security assurance and promote continuous improvement of assurance capabilities. The improvement phase involves the joint participation of multiple stakeholders, who propose corresponding improvement requirements for smart city information security based on business needs at different stakeholder levels.

Integration of resources under national macro leadership. During smart city planning, big data technology is used to comprehensively analyze information security events. While ensuring overall direction unity, local target adjustments and new work plan deployments are made to drive the optimization and upgrading of smart city information security organizational structure, infrastructure, and technical systems. While leveraging its own leadership advantages, attention should be paid to information resource sharing among different management organizations, coordinating information security needs and work tasks across various organizations.

Increased technology investment to promote spatial governance. During smart city construction, smart city information infrastructure and service

providers should accelerate the development and application of information security technologies under the big data environment, use big data perception technology to protect critical network applications in smart cities, and actively promote real-time monitoring based on big data. Meanwhile, during the process of improving new-generation information security protection technologies that integrate big data and cloud computing, cyberspace census tools composed of multiple systems such as situational awareness, asset detection, and operation centers should be established to continuously enhance cloud security protection technologies based on machine learning.

Promotion of public participation and security awareness. During smart city operation, the field of smart city governance continues to exhibit characteristics of diversified stakeholders and deepened participation, which requires more and more public participation in smart city governance work. Information and communication technologies in smart cities can disseminate public information anytime and anywhere, ensuring efficient and smooth channels for information exchange and feedback, and enabling citizens' electronic participation (e-participation) in urban governance. Additionally, massive data generated during citizens' electronic participation in smart city information security construction should be stored and deeply mined to provide improvement suggestions for smart city information security assurance planning.

4 Conclusion

This paper has analyzed the severe challenges facing smart city information security under the big data environment, combined with the basic connotations of smart city information security, applied total quality management theory to smart city information security assurance research, and constructed a smart city information security assurance system under the big data environment using the four phases of the Deming Cycle (PDCA). The aim is to provide reference ideas for smart city information security management research and related work. While this paper represents an innovative attempt at the theoretical level, due to varying conditions, characteristics, and resources across different cities, the construction of smart city information security assurance systems should not follow a one-size-fits-all approach. The specific focus directions, application planning, and design requirements of each city' s information security construction should be considered, requiring further exploration and verification in practical application.

Smart city construction and operation are dynamic processes, representing a large-scale, comprehensive systems engineering project involving multiple stakeholders. Therefore, the smart city information security assurance system should be continuously adjusted in conjunction with the dynamic process of urban construction and development. Big data technology provides a new solution for smart city information security assurance. Future efforts should accelerate the further deep integration of key big data technologies with smart city information security assurance, promote paradigm changes in information security manage-

ment and the establishment of intelligent decision-making systems in the big data era, and facilitate the sustained and healthy development of smart cities.

References

[1] Shen Minghuan. "Smart City" Assists the Transformation of China' s Urban Development Model [J]. Urban Observation, 2010(3): 140-146.
[2] CHEN Z Y, FAN W, XIONG Z, et al. Visual data security and management for smart cities[J]. Frontiers of computer science in China, 2010, 4(3): 386-393.
[3] Li Yong. Analysis of the Strengthening and Impact of Smart City Construction on Urban Information Security[J]. Library and Information Service, 2012, 56(6): 20-24.
[4] Deng Xianfeng. Risk Analysis of "Smart City" Construction[J]. Finance World, 2011(1): 106-109.
[5] ELMAGHRABY A S, LOSAVIO M M. Cyber security challenges in smart cities: safety, security and privacy[J]. Journal of advanced research, 2014, 5(4): 491-497.
[6] ZHANG K, NI J B, YANG K, et al. Security and privacy in smart city applications: challenges and solutions[J]. IEEE communications magazine, 2017, 55(1): 122-129.
[7] ALDAIRI A, TAWALBEH L. Cyber security attacks on smart cities and associated mobile technologies[J]. Procedia computer science, 2017, 109(3): 1086-1091.
[8] ABBAS H, MAGNUSSON C, YNGSTROM L, et al. Addressing dynamic issues in information security management[J]. Information management & computer security, 2011, 19(1): 5-24.
[9] Lu Xiaofeng, Li Haijun. Supporting Technology for Smart Cities—Information Security Technology[J]. Intelligent Building & City Information, 2013(2): 90-98.
[10] FERRAZ F S, FERRAZ C. Smart city security issues: depicting information security issues in the role of an urban environment[C]// IEEE/ACM 7th International Conference on Utility and Cloud Computing. London: IEEE, 2014: 842-847.
[11] Song Jing, Li Bin, Ban Xiaofang, et al. Current Status and Reflections on Smart City Information Security in China[J]. China Information Security, 2016(2): 107-111.
[12] Xiang Shang, Zou Kai, Jiang Zhiyi, et al. Smart City Information Security Risk Prediction Based on Random Forest[J]. Chinese Journal of Management Science, 2016, 24(S1): 75-81.
[13] QI L, HU C, ZHANG X, et al. Privacy-aware data fusion and prediction with spatial-temporal context for smart city industrial environment[J]. IEEE transactions on industrial informatics, 2020, 17(6): 1.
[14] Zou Kai, Xiang Shang, Zhang Zhongqingyang, et al. Construction and Empirical Research on Smart City Information Security Risk Assessment Model[J]. Library and Information Service, 2016, 60(7): 49-56.
[15] Mao Zijun, Mei Hong, Xiao Yiming, et al. Research on Smart City In-

formation Security Risk Assessment Based on Bayesian Networks[J]. Modern Intelligence, 2020, 40(5): 19-26, 40.
[16] Mao Zijun, Huang Yingxu, Xu Xiaolin. Research on Smart City Information Security Risk Analysis and Response Strategies from an Information Ecology Perspective[J]. Chinese Public Administration, 2019(9): 123-129.
[17] Zhang Yanfeng, Wang Yuxi, Zou Kai, et al. Research on Smart City Information Security Risk Factor Identification and Management Strategies Based on Fuzzy DANP[J]. Information Theory and Practice, 2020, 43(10): 144-150.
[18] Zou Kai, Wan Zhen, Cao Dan, et al. Evolutionary Game Analysis of Smart City Information Security Supervision Strategies[J]. Modern Intelligence, 2021, 41(3): 3-14.
[19] Li Yang, Xie Qing, Qiu Jingping, et al. Research on Smart City Information Security Assurance System[J]. Information Technology and Network Security, 2018, 37(7): 18-21.
[20] Zhang Dajiang, Bi Xiaoyu, Lü Xin, et al. Research on Smart City Information Security System[J]. Information Security Research, 2017, 3(8): 710-717.
[21] Wang Qing' e, Chai Xuanxuan, Zhang Xuan. Smart City Information Security Risks and Assurance System Construction[J]. Science & Technology Progress and Policy, 2018, 35(24): 20-23.
[22] Yang Tiankai, Lu Jie. Analysis of Information Security System Architecture in New Smart City Environment[J]. China Management Informationization, 2019, 22(19): 140-142.
[23] DAGHER G G, MOHLER J, MILOJKOVIC M, et al. Ancile: privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology[J]. Sustainable cities & society, 2018, 39(2): 283-297.
[24] MEMOS V A, PSANNIS K E, ISHIBASHI Y, et al. An efficient algorithm for media-based surveillance system (EAMSuS) in IoT smart city framework[J]. Future generation computer systems, 2018, 83(6): 619-628.
[25] WAZID M, DAS A K, VIVEKANANDA B K, et al. LAM-CIoT: lightweight authentication mechanism in cloud-based IoT environment[J]. Journal of network and computer applications, 2020, 150(1): 102496.
[26] ULLAH Z, Al-TURJMAN F, MOSTARDA L, et al. Applications of artificial intelligence and machine learning in smart cities[J]. Computer communications, 2020, 154(3): 313-323.
[27] ZHANG K, NI J B, YANG K, et al. Security and privacy in smart city applications: challenges and solutions[J]. IEEE communications magazine: articles, news, and events of interest to communications engineers, 2017, 55(1): 122-129.
[28] Wang Shiwei. On the New Characteristics and Requirements of Information Security in the Big Data Era[J]. Library and Information Service, 2016, 60(6): 5-14.
[29] Guo Hua, Su Xinning. Research on the Environment, Challenges, and Models of Smart City Information Security Management[J]. Library and Information Service, 2016, 60(19): 49-58.
[30] Huang Shuiqing. Process Approach to Digital Library Information Security

Management[J]. Library and Information Service, 2013, 57(11): 5-11.
[31] Zhao Hai, Chen Fang. Research and Practice of Electronic Payment Information Security Management System[J]. Information Security Research, 2019, 5(6): 534-541.
[32] Liu Shan, Yang Hua, Yue Keming. Research on Big Data in Power Information Security[J]. Shanxi Electric Power, 2018(4): 45-47.
[33] Wu Xuan. Application of PDCA in Hospital Information System Security Supervision[J]. Network Security Technology & Application, 2018(3): 114-115.
[34] Zeng Zhiqiu, Cheng Guanghuan, Yang Mengke. Research on Information Security Risk Management System for Telecom Operators[J]. Science and Technology Management Research, 2016, 36(18): 160-165.
[35] Hu Changping, Wan Li. Construction of a Comprehensive Security Assurance System for National Academic Information Resources in Cloud Environment[J]. Journal of Intelligence, 2017, 36(5): 124-128.
[36] Gao Donghuai, Shen Xiajuan, Ning Yuwen, et al. Research on University Informatization Management Service System—A Case Study of the Practice of the Fourth Military Medical University[J]. Wuhan University Journal (Natural Science Edition), 2012, 58(S1): 65-69.
[37] Hu Xin. Smart City[J]. Telecommunications Technology, 2016(9): 46-47, 51.
[38] Jiang Defeng, Qi Ruirui. Construction and Evaluation of Smart City Infrastructure[J]. Video Engineering, 2013(14): 4-5.
[39] Fan Yuan. Smart City and Information Security in the Big Data Era[M]. Beijing: Publishing House of Electronics Industry, 2018: 96.
[40] Wang Binjun, Ji Zengrui. Research on Information Security Technology System[J]. Computer Applications, 2009, 29(S1): 59-62.
[41] GB/T 22240-2020, Guidelines for Grading of Cybersecurity Protection Levels[S]. Beijing, Standardization Administration of China, 2020.
[42] Wang Xiang. Research on the Hierarchical Structure and Linkage of Network and Information Security Incident Emergency Response System[J]. Network Security Technology & Application, 2015(5): 177, 179.
[43] Zeng Zhilian, Huang Danfeng. Design of Information Security Risk Assessment Integrated Management System[J]. Education Teaching Forum, 2016(23): 249-250.
[44] Wu Bin, Zhang Yuqing, Mao Jian. Design and Implementation of Information Security Risk Management System[J]. Computer Engineering, 2007(21): 134-136, 139.
[45] Guan Haibin, Xie Zongxiao, Wang Xingqi. Crisk: A Knowledge Base-Based Information Security Risk Assessment Method and Its Tool Implementation[J]. Journal of Qingdao University (Natural Science Edition), 2013, 26(1): 66-70.
[46] Wang Zhenzhen, Xie Yongqiang, Wu Xiaoyue, et al. Research on Information Security Risk Management[J]. Information Security and Communications Privacy, 2007(8): 162-164, 167.

Author Contributions

Zou Kai: Proposed research ideas, drafted and revised the paper;
Guo Yihang: Designed research framework, drafted and revised the paper;
Xiang Shang: Drafted and revised the paper;
Wan Zhen: Collected relevant literature and revised the paper.

Note: Figure translations are in progress. See original paper for figures.