Research on Influencing Factors of Information Security Risks in Smart Cities

Lei Chen[a]*, Xinyi Zhang[b]

Chengdu University of Information Technology, Chengdu 610103, China

[a]* 834669328@qq.com, [b] 2902869455@qq.com

Abstract. This study investigates the influencing factors of information security in smart cities, aiming to address the complex risks arising from the integration of technologies such as the Internet of Things, big data, and cloud computing. Based on a three-dimensional framework encompassing environmental, logical, and organizational dimensions, the research identifies key risk factors through questionnaires and the DEMATEL method. Findings reveal that mobile internet security access (B3), data leakage (B5), security vulnerabilities (B6), and data distortion (B10) are among the most critical factors affecting information security. The study further proposes strategies to enhance risk management, including strengthening institutional systems, promoting technological innovation, and raising public awareness. By providing a structured approach to risk identification and mitigation, this research offers theoretical and practical insights for ensuring the secure and sustainable development of smart cities.

Keywords: Smart City, Information Security, Influencing Factors, DEMATEL, Risk Management.

1 Introduction

A smart city represents an advanced urban paradigm that integrates cutting-edge technologies, including the Internet of Things, big data analytics, cloud computing, and artificial intelligence, to optimize urban governance, streamline public services, and elevate the overall quality of life for residents[1]. Through the interconnectivity of infrastructure, data-driven decision-making, and intelligent automation, smart cities enhance efficiency in transportation, energy management, environmental monitoring, healthcare, and public safety[2].

Nevertheless, the rapid evolution of smart cities introduces significant information security challenges. The extensive data flows, pervasive network connectivity, and increased reliance on digital systems—particularly in critical infrastructure—amplify vulnerabilities to cyber threats. These risks encompass potential breaches of personal privacy, exposure of sensitive business or commercial data, compromise of intellectual property, and threats to national security arising from attacks on essential services such as power grids, water supply, and communication networks[3].

D. Magni et al. (eds.), *Proceedings of the 2026 3rd International Conference on Applied Economics, Management Science and Social Development (AEMSS 2026)*, Advances in Economics, Business and Management Research 389,

https://doi.org/10.2991/978-94-6239-672-2_3

To foster the sustainable and secure development of smart cities, it is imperative to conduct systematic and in-depth research on information security issues. This involves not only identifying and analyzing emerging risks but also developing robust frameworks for risk prevention and mitigation. The present study seeks to contribute to this effort by constructing a comprehensive system of impact factors for information security risks. By doing so, it aims to offer theoretical insights and methodological tools that can strengthen China's capacity to assess, manage, and respond to information security challenges in the context of smart urban development.

2 Body Paragraphs

2.1 Construction of Influencing Factors System

The development of a smart city information security risk framework is a systematic process based on three core dimensions: environmental, logical, and organizational. The environmental dimension covers policy, physical infrastructure, technology, and management systems.[4] The logical dimension focuses on the entire data lifecycle, from collection and storage to processing and use. The organizational dimension involves governance structures, staffing, and operational workflows for security management.[5]

Table 1. Influencing Factors System

Primary factor	Subfactor
Smart infrastructure security risk (A1)	B1 IoT infrastructure deployment
	B2 core equipment is independently controllable
	B3 Mobile Internet Secure Access
	B4 Virtualization resource pool stability
Data service security risk (A2)	B5 Data Leak
	B6 Security Vulnerability
	B7 Data Encryption and Audit
	B8 Data Backup and Recovery
Information content security risk (A3)	B9 Data source
	B10 Data Distortion
	B11 Information Content Controllability
	B12 Supply Chain Security
Information Management Security Risk (A4)	B13 Information Security Protection Policy
	B14 Operation error
	B15 Security Management System
	B16 Security Operations Management
	B17 Safety Training
	B18 Public Information Security Awareness
	B19 Information Security Ethics

As shown in Table 1, after clarifying the core components of the three dimensions, it is essential to further refine the specific influencing factors within each dimension.[6]

2.2 Identification of Information Security Risk Factors in Smart Cities

Data Collection. This study investigates the relationships among factors affecting information security in smart cities through a questionnaire survey. Questionnaires were distributed to 50 scholars and experts from relevant disciplines in universities, who rated the correlation strength of 19 sub-elements in the influence system outlined in Table 1. The scoring criteria are as follows: 0 points indicate no correlation, 1 point indicates weak correlation, 2 points indicate moderate correlation, and 3 points indicate strong correlation.[7]

Data Analysis. The paper analyzes the collected survey data using SPSS 24.0 to evaluate the questionnaire design. All Cronbach's alpha coefficients exceed 0.700, indicating high reliability.

2.3 Construction of the DEMATEL-Based Influencing Factors Analysis Model

Build the direct impact matrix. Based on the questionnaire survey, the results were processed as the mean (retaining the integer). At the same time, different weights were assigned to the respondents with different educational levels, with 1 for bachelor's degree, 2 for master's degree and 3 for doctor's degree.[5]

Table 2. Direct Effect Matrix G

	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12	B13	B14	B15	B16	B17	B18	B19
B1	0	2	1	1	3	2	2	3	1	1	1	2	2	3	2	1	3	1	3
B2	2	0	2	3	1	2	3	2	3	1	2	1	3	2	1	2	2	2	3
B3	3	2	0	2	1	1	3	3	3	3	2	3	3	3	3	2	1	3	3
B4	1	1	2	0	1	3	2	2	2	1	3	2	1	3	3	1	1	1	1
B5	1	2	2	1	0	3	3	3	2	3	3	1	1	1	3	3	3	1	2
B6	2	3	3	2	3	0	2	2	2	3	2	3	3	2	1	3	3	3	2
B7	3	2	1	3	2	3	0	3	3	2	1	3	2	3	3	2	1	3	1
B8	1	3	3	2	1	2	1	0	1	2	1	2	3	1	2	3	2	1	1
B9	2	1	2	3	2	1	3	2	0	2	3	1	1	3	1	1	3	2	3
B10	2	3	2	3	3	2	3	1	3	0	3	3	3	2	3	3	2	3	1
B11	3	1	3	1	1	3	2	3	2	3	0	1	3	1	3	3	3	2	3
B12	2	1	1	3	2	1	1	3	3	3	1	0	2	3	1	1	3	3	1
B13	3	3	3	2	3	2	3	3	2	1	3	2	0	1	2	3	1	2	3
B14	2	2	3	2	2	2	2	2	2	1	2	2	2	0	2	2	2	2	2
B15	2	2	2	2	2	2	2	2	2	1	2	2	2	2	0	2	2	2	2

B16	2	2	2	2	2	2	2	2	2	1	2	2	2	3	2	0	2	2	2
B17	2	2	3	2	3	2	2	2	2	2	2	2	1	2	2	3	0	2	2
B18	2	1	2	1	2	2	2	2	2	3	2	2	1	2	2	2	2	0	2
B19	2	1	2	2	2	2	2	2	2	3	2	2	2	2	2	2	2	2	0

As shown in Table 2, standardize the direct influence matrix to obtain the normalized elements. The sum of the direct influence matrix and the indirect influence matrix yields the comprehensive influence matrix T.

Calculation of Influencing Factors. Calculate the influence degree D and the affected degree R, then calculate the centrality and the cause degree.

Table 3 provides a detailed breakdown of the indices and rankings for the sub-factors of information security risks in smart cities, including their impact, vulnerability, centrality, and causality. These metrics reveal the relative importance and interrelationships among the sub-factors within the risk framework.

Table 3. Subfactor Index and Ranking

Subfactor	Impact D	arrange Name	Impact R	arrange Name	centrad D+R	arrange Name	Reason D-R	arrange Name
B1	3.74	15	3.95	18	7.69	18	-0.21	11
B2	3.98	10	3.75	19	7.73	16	0.23	7
B3	5.02	3	4.35	5	9.37	1	0.67	4
B4	3.46	19	4.08	11	7.54	19	-0.62	17
B5	4.40	7	3.97	16	8.37	7	0.43	6
B6	5.02	2	4.03	15	9.05	3	0.99	2
B7	4.58	6	4.41	2	8.99	4	0.17	8
B8	3.57	18	4.67	1	8.24	10	-1.1	19
B9	4.02	9	4.27	6	8.29	8	-0.25	12
B10	5.17	1	4.07	13	9.24	2	1.1	1
B11	4.78	4	4.07	14	8.85	6	0.71	3
B12	3.92	11	3.95	17	7.87	14	-0.03	9
B13	4.77	5	4.14	9	8.91	5	0.63	5
B14	3.79	13	4.38	4	8.17	11	-0.59	15
B15	3.62	17	4.24	7	7.86	15	-0.62	16
B16	3.75	14	4.39	3	8.14	12	-0.64	18
B17	4.09	8	4.20	8	8.29	9	-0.11	10
B18	3.62	16	4.08	12	7.7	17	-0.46	14
B19	3.82	12	4.11	10	7.93	13	0.23	7

2.4 Result Analysis

Cause analysis of influencing factors. Based on causality analysis, factors are classified as causes (values >0) or results (values <0). Key causal factors with significant influence (causality >0.6) include data distortion (B10) and security vulnerabilities (B6) – both exceeding 0.8 and identified as most critical by Pareto's principle – along with controllable information content (B11), secure mobile internet access (B3), and protection strategies (B13). In contrast, basic information resources (B1) is the primary result factor, showing the highest susceptibility and requiring comprehensive protective measures across all smart city development aspects to prevent leakage.

Centrality Analysis of Influencing Factors. Through factor importance analysis, we propose a centrality-based measurement method. The identified factors include data leakage (B5), mobile internet security access (B3), data distortion (B10), data encryption and audit (B7), and security vulnerabilities (B6). Among these, data leakage (B5) demonstrates the highest centrality, exerting the most significant impact on information security risks in smart cities. Notably, data leakage (B5) is also the most vulnerable factor, indicating its heightened susceptibility to influence from other elements.

3 Conclusion

To effectively implement information security management systems, address system vulnerabilities, and prevent malicious data breaches, establishing a robust smart city data protection framework necessitates a comprehensive, multi-pronged strategy. This involves: refining and standardizing data management protocols to clearly define responsibilities and processes across the entire data lifecycle—from collection and storage to processing, sharing, and disposal; integrating a suite of advanced technological safeguards, including end-to-end encryption, dynamic and role-based access controls, and resilient backup and disaster recovery systems, to ensure data confidentiality, integrity, and availability; enhancing personnel competency through regular, role-specific security awareness training and realistic drills to bolster emergency response capabilities; strengthening governmental oversight, policy enforcement, and interdepartmental coordination to create a unified regulatory and operational front; and instituting a proactive regime for continuously identifying, assessing, and patching vulnerabilities in both software systems and management protocols, thereby constructing a systematic, layered defense mechanism.

Ensuring secure mobile internet access constitutes a critical pillar of smart city information security, given the proliferation of mobile devices and applications. A robust, multi-layered defense system must be established, with core technical measures including: implementing strict, multi-factor identity authentication and granular, context-aware access control policies; adopting universally encrypted communication protocols (e.g., TLS/SSL) for all data transmissions; and rigorously maintaining systems through regular updates and prompt patching of identified vulnerabilities. This technical foundation must be supplemented by key managerial and behavioral controls, such as continuous network traffic monitoring and intrusion detection, comprehensive user secu-

rity education programs, and periodic third-party security audits and penetration testing. This integrated approach synergizes technical safeguards with stringent management protocols to create a comprehensive, adaptive defense framework against evolving mobile threats.

Preventing data distortion and ensuring data integrity are paramount for credible smart city operations. To combat data tampering, inaccuracies, and corruption, a closed-loop data governance and integrity management system should be established. Key steps include: developing and enforcing unified data quality standards, validation rules, and verification mechanisms while standardizing all data collection and processing workflows; leveraging big data analytics and AI technologies, such as machine learning algorithms, for automated data cleansing, consistency checks, and real-time anomaly detection; enhancing staff training on data handling ethics and implementing clear accountability assessments to foster a culture of data stewardship; implementing cryptographic techniques (e.g., digital signatures, hashing) and strict access controls to prevent and detect unauthorized tampering; and achieving sustainable data quality management through continuous monitoring, periodic audits, and a feedback loop for evaluation and systematic improvement.

References

1. Hong, W. X., & Jia, W. J. (2022). Research on influencing factors of smart city information security. Journal of Hangzhou Dianzi University (Social Sciences), 18(3), 17–23+31. (In Chinese)
2. Lom M, Pribyl O. Smart city model based on systems theory[J].International Journal of Information Management,2020:102092.
3. Canhoto A I, Quinton S, Pera R, et al. Digital strategy aligning in SMEs: A dynamiccapabilities perspective [J]. The journal of Strategic Information Systems, 2021,30(3):1-17.
4. AlDairi A,Tawalbeh L.Cyber Security Attacks on Smart Cities and Associated Mobile Technologies!l.Procedia Computer Science,2017(109):1086-1091.
5. Hou, L. (2020). Research on influencing factors of information security risk in smart cities[Doctoral dissertation, Xiangtan University]. (In Chinese)
6. Jiang D. The construction of smart city information system based on the Internet of Things and cloud computing[J]. Computer Communications, 2020, 150: 158-166.
7. Liu, R., Duan, H., & Wu, X. (2021). Research on forest fire influencing factors based on DEMATEL. Journal of Anhui Agricultural Sciences, 49(4), 115–118.(In Chinese)