ISSN 1330-3651 (Print), ISSN 1848-6339 (Online) https://doi.org/10.17559/TV-20210816043215
Original scientific paper

Influencing Factors of Smart Government Information Security: Experience from China

Fengke WANG, Juzheng ZHANG, Panke ZHANG*

Abstract: Based on information technology, smart government processes information data to help improve the efficiency of government operations. Information security has become the key to the transformation of government wisdom and improvement of government service efficiency and transparency. To explore the influencing factors of government information security, 27 influencing factors from 6 dimensions of personnel, facilities, information, personnel management, system, and environment were extracted. The decision-making trial and evaluation laboratory (DEMATEL)-interpretative structural modeling (ISM) composite model was used to determine the importance of each factor, the mechanism between the influencing factors was analyzed, and a smart government information security interpretation structure model was constructed. Results show that policies and regulations are the root factors affecting the information security of the smart government. The international environment is a deep-layer influencing factor on government information security. Infrastructure, moral training, and other factors are middle-layer influencing factors that are influenced by the superior factors. Psychological factors, platform construction, and others are surface-layer influencing factors that play a connecting role. Security awareness, behavior security, moral level, and others are directly influencing factors and determine the level of smart government information security. Results of this study also show the feasibility of DEMATEL-ISM model in identifying the relevant factors and analyzing their influencing mechanism on smart government information security. A novel modeling method and its analysis approach are provided for the government to improve the level of information security.

Keywords: DEMATEL-ISM; influencing factor; information security; smart government

1 INTRODUCTION

As a new version of the traditional government governance model, smart government can help officials to more efficiently deal with work and provide new information services for the masses through data processing and other forms based on the application of new information technology. Smart government can effectively reduce the workload of officials, reduce administrative costs, and improve the public image of the government. In addition, as the "brain" of the city, the intelligent transformation of the government can also help them rebuild the network platform and drive intelligent construction in the fields of economy, health care, and education. In recent years, with the successful development and application of artificial intelligence, 5G and other information and communications technology (ICT) [1], the construction of smart government in the world has reached certain achievements. However, the realization of urban fine governance also brings unprecedented information security challenges [2]. In March 2019, Venezuela's electric power system and state-owned power lines were attacked, resulting in blackouts in 21 states and lasted for six days. In July 2019, the information of the Capital One Financial of the United States was illegally stolen and the personal information of nearly 100 million American citizens was leaked. In November of the same year, the government website of Nunavut in Canada was attacked and all local electronic information services were paralyzed. As a new government management mode, the information security level of smart government is affected by technology research and development, information processing methods, infrastructure, and other factors [3, 4], which are complex and interact with each other. Therefore, identifying these influencing factors is the basis of improving the level of government information security.

However, current studies related to government information security focus more on the analysis of information technology [5], open data [6], and physical measures [7]. Attention to the internal management mechanism of the government and the psychological content of civil servants is limited, and researches related to the comprehensive mechanism and interaction of the influencing factors remain lacking. Therefore, this study has the following aims: to extract the factors that affect the information security of smart government from the facilities, system, environment, and other dimensions; analyze the importance degree and interaction of each factor; and to divide the factors into the root, deep-layer, middle-layer, surface-layer, and direct-layer based on their influence degree. This study also constructs an interpretation structure model of smart government information security and extracts impact paths. On this basis, this study analyzes the effective paths to improve the information security of government and corresponding management suggestions from the central and local aspects are put forward to improve the level of government information security and contribute to the construction and improvement of smart government, which has a very practical significance.

2 STATE OF THE ART

The perfection of laws lies in its development and reform under current conditions, and its evolution in the change of social environment [8]. Elmaghraby and Losavio [9] believed that, to a certain extent, legislation can alleviate the problems of public information security and personal privacy produced by the development of the Internet of Things (IoT). Hwang and Choi [10] illustrated the organizational reform pressure of e-government information security innovation through the evolution of laws and system. Ki et al. [11] found that the development and access performance of government digital services are in direct proportion to the development of relevant government documents and policies while also helping keep government information open.

New communication technology is an important part of the digital industry. The rapid network development is inseparable from the protection of information security, which needs not only legal protection but also technical support. Chesla [12] believed that urban information

security ensures the confidentiality, integrity, availability, and controllability of information in its usage from the technical level, and emphasized the important guarantee role of communication information technology and confidentiality technology. Liu et al. [13] believed that information security is the core issue to ensure the smooth implementation of e-government, and considered cloud computing to discuss the construction of information security of e-government cloud computing from three aspects of technology, management, and law. With the progress of technology, most government public service processes can be automated [14]. Guenduez et al. [15] believed that the success of smart government depends on the effective use of the automation technologies and put forward three key factors, namely, the quality of systems, information, and service. Dečman [16] studied the technology acceptance of government employees using the Unified Theory of Acceptance and Use of Technology (UTAUT), and proposed that expected performance, social environment, employee age, experience difference, and other factors affect the technology acceptance of government employees.

Government information security needs not only internal supervision, but also public supervision and social participation [17]. Geiger and Von Lucke [18] defined open government data (OGD) as "all data stored in the public sector, which can be accessed by the public according to the will of the public without any restrictions on use and dissemination". Data is an important resource for national and government governance, which has become an international consensus. Scholars and government officials believe that the conflict between government and private data can affect the security of government information, and the disclosure of non-confidential data can effectively alleviate the contradiction between the two. Barns [19] believed that to provide high-quality digital services, the government needs to ensure that data is open and machine-readable by default. At the same time, the data opening policy can help obtain effective supervision and improve the security of government information. Attard et al. [20] studied the government data disclosure from the perspective of stakeholders, and believed that moderate level of disclosure is helpful to promote social development.

In summary, the related studies mainly focus on the direct influencing factors such as law, technology, and data openness, while less on the factors such as management mechanism and civil servants' psychology. Research related to the comprehensive mechanism and influencing factors of information security under the background of smart government is lacking, and the main reasons for the frequent government information security incidents are not revealed.

Therefore, based on the practical experience of China, this study constructs the DEMATEL-ISM model. The main influencing factors are extracted by Delphi and literature methods, and the centrality and cause degree of each factor are calculated to determine the importance of influencing factors. The interpretative structure model was constructed to clarify the mechanism and influence paths among the factors.

The rest of this study is structured as follows. Section 3 introduces the extraction idea and modeling method of influencing factors of smart government information security. Section 4 analyzes the key factors and the impact paths based on ISM and DEMATEL Model. Section 5 further discusses the results. Finally, Section 6 presents the conclusions.

3 METHODOLOGY

3.1 Extractionof Influencing Factors

Government information security is a multi-dimensional and complex model that is affected by numerous factors. The influence mechanism among the factors can be examined by first determining the main influencing factors of government information security. In this study, the government information security impact dimension is divided as follows: personnel, facility, information, personnel management, system, and environment. Finally, after repeated communication with the expert group, the influencing factors were determined by using Delphi and literature methods. Given that technology research and development is not the main responsibility of the government, this study excludes simple technical factors. Tab. 1 shows the 6 primary dimensions and 27 secondary indicators.

Table 1 Influencing factors of smart government information security

Personnel [21]	A1 safety consciousness [22] A2 behavioral safety A3 psychological factors A4 moral level A5 operation specification
Facility	B1 infrastructure B2 platform construction, B3 technical reference [23] B4 firewall construction
Information	C1 information acquisition [24] C2 information transfer [3] C3 information storage C4 information logic
Personnel management	D1 moral cultivation D2 technical training D3 safety education and training [22]
System	E1 leadership mechanism E2 evaluation mechanism [25] E3 feedback mechanism [26] E4 emergency mechanism E5 regulatory mechanism E6 anti leakage mechanism [26]
Environment	F1 policies and regulations [27] F2 network propaganda F3 third-party supervision [28] F4 public supervision F5 international environment

3.2 Modeling Method for Influencing Factors

(1) Modeling method and process:

DEMATEL model is mainly used to determine the degree of the direct relationship between the influencing factors, calculate the influence of each factor on others and the degree of effect, distinguish the causal and the result factors. ISM model can divide a complex model into several subsystems to further clarify the influence relationships and paths among factors. The combination of the two models, namely, DEMATEL-ISM, can more comprehensively and concretely analyze the levels of influencing factors [29, 30].

(2) Establishment of direct impact matrix:

In this study, 13 government information professionals were invited to form an expert group to evaluate the influencing factors. These experts use ratings based on a five-point Likert scale according to the following criteria: very strong (4 points), strong (3 points), average (2 points), weak (1 point), no impact (0 point). After scoring, the mean value method is used to process the data (the results were retained in integers) and the influence strength of each factor was determined. Then, the direct impact matrix X was constructed.

(3) Establishment of total impact matrix:
Organize the original data by normalizing the direct impact matrix X and obtaining the normalized impact matrix D. The formula is as follows.

$$D = \left(1 / \max_{i=1}^{n} \sum_{j=1}^{n} a_{ij} \right) \cdot X \tag{1}$$

Obtain the total impact matrix T by processing the normalized impact matrix D. The formula is as follows.

$$T = D \cdot \left(I - D \right)^{-1} \tag{2}$$

(4) Identification of centrality and cause:
The sum of each row of factors in the total impact matrix is the influence degree of this factor affected by other elements, which is called influence degree R. The sum of each column of factors in the total impact matrix is the influence degree of this factor on others, which is called the influenced degree C. The centrality F ($F = R + C$) of an element refers to its importance in the model. The cause degree J ($J = R - C$) of an element refers to its contribution to the formation of the entire model.

(5) Establishment of reachable matrix:
Set the threshold value λ, filtering out the relatively weak influence relationship through the following formula, and transform the total impact matrix T into the adjacency matrix K to get a clearer interaction.

$$t_{ij} \geq \lambda \left(i, j = 1, 2, ..., n \right), \; k_{ij} = 1 \tag{3}$$

$$t_{ij} \leq \lambda \left(i, j = 1, 2, ..., n \right), \; k_{ij} = 0 \tag{4}$$

(6) Establishment of interpretative structural model:
The reachable set R_i, antecedent set S_i, and the intersection set Y_i were determined by the reachable matrix U.

Reachable set R_i: set of column elements that contain element 1 in the row corresponding to element U_{ij} in reachable matrix U.

Antecedent set S_i: set of row elements that contain element 1 in the column corresponding to element U_{ij} in reachable matrix U.

Intersection set Y_i: intersection of reachable set R_i and antecedent set S_i.

If $R_i = Y_i$ is true, then the corresponding element is the underlying influence factor. Delete the row and column corresponding to this element, and continue to repeat this step until the influence level and relationship of all elements are determined.

4 RESULT ANALYSIS

4.1 Identification of Key Factors Based on DEMATEL Model

After the professionals scored, the mean value method was used to sort out the data, and the direct impact matrix X was obtained. Convert the direct impact matrix X into the total impact matrix T according to the formulas 1 and 2. The calculation results of each factor are obtained through matrix T, as shown in Tab. 2.

Table 2 Calculation results of influencing factors

	R	C	J	F
A1	0.81	2.00	−1.20	2.81
A2	0.62	1.75	−1.13	2.36
A3	0.67	0.96	−0.29	1.63
A4	0.37	0.29	0.08	0.66
A5	0.99	1.83	−0.84	2.81
B1	1.04	0.66	0.38	1.70
B2	1.15	0.77	0.38	1.92
B3	0.80	0.89	−0.09	1.70
B4	0.88	1.28	−0.40	2.16
C1	0.91	0.49	0.42	1.39
C2	1.34	0.90	0.44	2.24
C3	1.46	1.21	0.26	2.67
C4	0.83	1.15	−0.32	1.97
D1	0.54	0.32	0.22	0.86
D2	0.52	0.57	−0.05	1.09
D3	0.89	1.12	−0.23	2.02
E1	2.04	0.95	1.09	2.99
E2	1.11	1.17	−0.06	2.28
E3	0.80	1.27	−0.47	2.07
E4	0.69	1.11	−0.42	1.80
E5	1.17	2.21	−1.03	3.38
E6	1.65	2.80	−1.15	4.45
F1	1.97	0.41	1.55	2.38
F2	1.12	0.95	0.17	2.07
F3	1.50	0.94	0.56	2.44
F4	1.60	0.94	0.66	2.55
F5	1.69	0.23	1.46	1.91

The results of cause degree were further visualized using a causality diagram of influencing factors of smart government information security, as shown in Fig. 1.

The centrality represents the degree of association between the factors. From Tab. 2, the factors with high centrality include E6 anti-leakage mechanism, E5 regulatory mechanism, among others, which are highly correlated with others. The factors with low centrality include A4 moral level, D1 moral cultivation, and other factors, which therefore are highly independent.

The factors with positive cause are causal factors and are located in the upper part of the coordinate axis in Fig. 1. According to numerical order, these are F1 policies and regulations, F5 international environment, E1 leadership mechanism, among others. Among these, the cause degree of F1 policies and regulations is the largest, which therefore have the greatest impact on others and belong to the root influencing factor.

The elements with negative cause degree J are result factors and are located in the area below the coordinate axis of Fig. 1. According to numerical order, they are A1 safety consciousness, E6 anti-leakage mechanism, A2 behavioral safety, among others. Among these, A1 safety consciousness and E6 anti-leakage mechanism are the direct factors to determine the level of government information security.

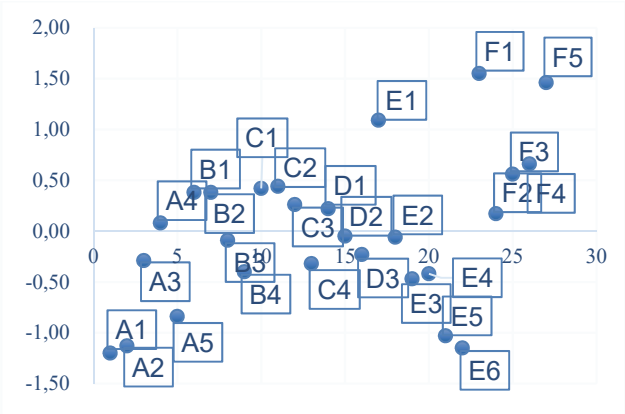

Figure 1 Causality diagram of influencing factors

In this study, the key influencing factors were determined according to the centrality F and cause J. According to the contents in Tab. 2 and the above analysis, several factors have high centrality and cause degree, such as E1 leadership mechanism and F1 policies and regulations. According to their centrality and cause degree, the top 8 factors in these two groups were selected. With a total of 13 key factors, the order of centrality is E6 anti-leakage mechanism, E5 regulatory mechanism, E1 leadership mechanism, A1 safety consciousness, A5 operation specification, C3 information storage, F4 public supervision, F3 third-party supervision, F1 policies and regulations, C2 information transfer, B2 platform construction, F5 international environment, and C1 information acquisition.

4.2 Impact Paths Analysis Based on ISM Model

(1) Establishment of interpretative structural model:
After the key influencing factors were determined, the threshold λ was obtained according to the total impact matrix T. In this matrix, the median of each value is calculated as 0.075. For ensuring the consistency of subsequent calculation results, the threshold λ is determined as 0.08. After calculation, the influencing factors were divided into five levels.

Among these factors, F1 (fifth layer) is a root influencing factor, which is the most important guarantee and means to promote the information security of the smart government. F5 (fourth layer) and B1, D1, E1, F3, F4 (third layer) are important influencing factors. F5 is a deep influencing factor, while the others are middle influencing factors. A3, B2, B3, C1, D2, F2 (second layer) are surface influencing factors and play an important role in the relationship model. A1, A2, A4, A5, B4, C2, C3, C4, D3, E2, E3, E4, E5, E6 (first layer) are direct influencing factors, which determine the information security level of smart government. According to the influence level division and reachable matrix U, the ISM model was established, as shown in Fig. 2.

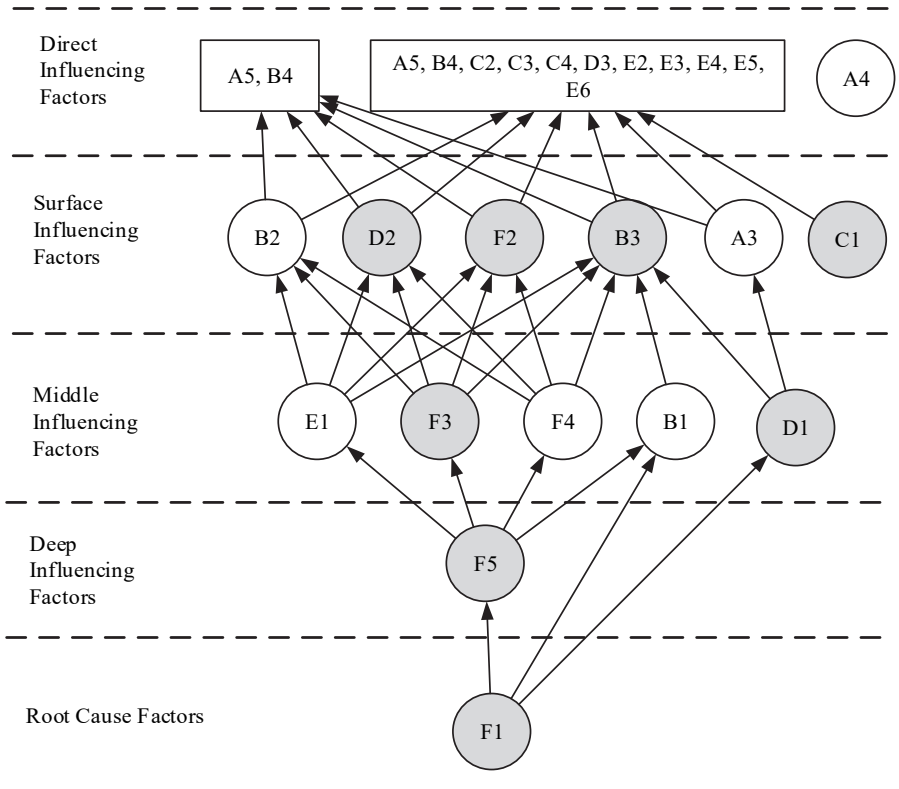

Figure 2 Interpretative structural model of influencing factors

(2) Hierarchical analysis of influencing factors:
F1 policies and regulations are in the fifth layer of the ISM model, which is the root factor, in line with the development status of China and the world's mainstream countries. Therefore, to fundamentally improve the level of government information security, the government should carry out the following: continue to strengthen information security legislation, law enforcement, and other activities; further enhance the authority of the legal system; emphasize the importance of information security in the government and society and promote information security to the height of development strategy.

F5 international environment is in the fourth layer, which is the deep influencing factor. In recent years, with the increase of uncertainty in the international development environment, considerable changes have occurred in the relations among countries. Hacker attacks, information theft, and other acts have increased dramatically, severely threatening government information security. Therefore, only by continuing to strive to maintain a peaceful and stable international development environment can the threat to the information security of governments be effectively reduced.

B1 infrastructure, D1 moral cultivation, E1 leadership mechanism, F3 third-party supervision, and F4 public supervision are in the third level and belong to the middle level influencing factors. F3 third-party supervision and F4 public supervision are the main supplementary forms of Chinese government supervision, which can effectively promote the improvement of government information security management systems and facilities construction. B1 infrastructure, D1 moral cultivation, and E1 leadership mechanism can influence civil servants.

A3 psychological factors, B2 platform construction, B3 technology reference, C1 information acquisition, D2 technical training, and F2 network propaganda are in the second layer of the ISM model and belong to the surface influencing factors. Among them, A3 psychological factors are mainly affected by D1 moral cultivation. C1 information acquisition has no relationship with high-level influencing factors, which is therefore relatively independent.

A1 safety consciousness, A2 behavioral safety, and other factors are located in the first layer of the ISM model. This layer involves the direct influencing factors of government information security and directly determines the level of government information security. Among them, A1 safety consciousness, A2 behavioral safety, A4 moral level, and A5 operation specification belong to the personnel dimension. These factors are subjective and difficult to quantify, and thus motivating civil servants to promote their development has always been difficult. B4 firewall construction, C2 information transfer, C3 information storage, and C4 information logic mainly ensure information security by controlling information flow. D3 safety education and training is the main form of training for Chinese government civil servants. E2 evaluation mechanism, E3 feedback mechanism, E4 emergency mechanism, E5 regulatory mechanism, and E6 anti-leakage mechanism belong to the system dimension. As seen in Fig. 2, the system dimension is affected by multiple factors, which is of great significance to the level of government information security.

(3) Impact paths analysis

The ISM model (Fig. 2) shows several influence paths, among which the dominant path is F1 → F5 → (B1, E1, F3, F4) → (B2, B3, D2, F2) →(A1, A2) → government information security. By further improving the laws and regulations of various countries, improving the international environment, promoting the optimization of management mechanism and the renewal of facilities construction, further strengthening the leadership training of relevant civil servants within the government, and improving the level of government information security through the personnel progress, this path is the most important and effective way to improve the information security of the smart government.

In addition to the dominant path, other improvement paths are identified. For example, F1 → (B1, D1) → (A3, B3) → (C2, C3, C4). Control and supervision of the information processing methods of public servants ensure the advanced nature of information equipment in the form of laws and regulations, enhance the moral level of public servants, and improve the level of government information security. In addition, F1 → (B1, D1) → (A3, B3) → (E2, E3, E4, E5, E6) mainly indicates the standardization of management systems to improve the level of government information security.

The improvement path of specific factors can also be found in the interpretative structural model in Fig. 2. For example, tracing the arrow in Fig. 2, the construction of B2 platform can be improved through its connections with E1 leadership mechanism, F3 third-party supervision, and F4 public supervision. The new type of leadership (information leadership) focuses on data management, and emphasizes the construction of data processing and management platforms. The main supervision content of the third-party institutions and the public on government information security is the level of platform construction and maintenance. The improvement of these influencing factors directly promotes the government to increase investment and maintenance on platform construction. Through further tracing, E1 leadership mechanism, F3 third-party supervision, and F4 public supervision are all connected with F1 policies and regulations and F5 international environment. The improvement of relevant legal system can determine the minimum standard of platform construction and provide legal protection for the orderly use of the platform. The change of international environment also affects the focus of platform construction.

5 DISCUSSION

This study considers the influencing factors and paths of government information security level under the background of smart government as the research object. Through literature review and repeated discussions with the expert group, 6 dimensions and 27 influencing factors were obtained (Tab. 1). Through the DEMATEL model, the cause degree and centrality of each factor were calculated (Tab. 2), and finally, 13 key influencing factors were determined. According to the numerical order of centrality, the top three factors are E6 anti-leakage mechanism, E5 supervision mechanism, and E1 leadership mechanism. Thus, the system dimension factor is not only the core of ensuring the government's information security but also an important means for its improvement.

In addition, based on the ISM model, the interpretive structure model of influencing factors of smart government information security was constructed (Fig. 2), and the influencing factors were divided into five levels. Among them, F1 policies and regulations is the root influencing factor, the improvement of the relevant laws and regulations is the most important way to improve the level of government information security. One of the most important characteristics of smart government is the application of new ICT technology [31]. The local government should continue to promote the improvement

of laws and regulations to help the combination of new ICT technology and government. F5 international environment is the deep influencing factor of government information security. Because this factor belongs to the external environment and cannot be effectively controlled, the increase of its uncertainty will increase the risk of government information security and threaten the effective use of government information resources [32]. The middle and surface influencing factors play a connecting role in the model. On the one hand, they are controlled by the upper influence factors, on the other hand, they directly control the direct influence factors. The direct influencing factors directly determine the level of government information security. It should be pointed out that due to the complexity of its influence relationship, the improvement of a single direct influence factor cannot greatly improve the information security level of smart government [33]. In addition, from the content of Fig. 2, A4 moral level is not related to other influencing factors, indicating that this factor is highly independent and not easily affected by other factors. According to the communication with the expert group, this study believes that in the environment of relatively perfect legal system, rule of law plays a greater role in the field of information security than rule of virtue.

At the national core leading departments level, the following actions are suggested: further build and improve the laws and regulations in the field of government information security; accelerate the reform of its information security management system; continue to break the information barriers between different regions, institutions, and departments; and promote the full use of information resources on the premise of ensuring information security. According to the findings of this study, the following suggestions are put forward:

(1) Establish or clarify the government information security department in the national system, and promote the government information security and information sharing around the country. Those responsible for the improvement of national and local government information security policies, suggestions, standards, and opinions can clarify the standards for the construction and maintenance of government information network platform, clarify and emphasize the supervision role of all sectors of society on government information security, and highlight the role of the government's smart transformation.

(2) Improve laws, regulations, and systems. Government information security should be guaranteed in the form of laws, and the boundary between government and public information should be clarified in the form of legislation. The specific functions and powers of smart government information management department, supervision department, and accountability department should be clarified. Various measures can also speed up the establishment of legal systems and standards for the government to use the IoT, 5G, artificial intelligence, and other ICT [34].

(3) Give full play to the strength of all sectors of society, encourage the masses, consulting companies, and other non-governmental organizations to enter the government supervision system consciously, orderly, and legally. New development momentum can also be injected into the government information supervision system.

At the local government level, attention should focus on the 13 key factors extracted in this study to improve the internal management mechanism and information supervision structure of the government, further strengthen the business training and safety education of civil servants within the government, and determine standards of information usage. This study suggests that:

(1) The local government should first solve the problems of leadership and supervision mechanism. Due to the professionalism of knowledge, the administrative system of local government inevitably has fragmentations, which ensures the professionalism of business but also inevitably leads to the obstruction of communication between departments. In addition to the problems of poor information circulation and low utilization rate of information resources, information barriers also have a potential impact on information security. Therefore, before the introduction of new ICT or smart transformation, the government should prioritize the establishment of data management departments or special groups, which are fully responsible for the information security and usage within their departments.

(2) Pay attention to the quality training of government information workers. As the upgraded version of the traditional government governance model, the upgrading of hardware and software equipment leads to higher requirements for civil servants. Therefore, the government should regularly organize information security law popularization, service standards, business training, anti-disclosure, and other learnings. The focus is on government officials to learn the relevant knowledge of new ICT introduced by their departments and strengthen the business processing level and improve their information processing ability. Similarly, attention is necessary on the cultivation of public servants' awareness of information security, anti-leakage, and handling work in strict accordance with information security standards.

(3) Improve the platform construction and maintenance. According to the local actual development and department, a smart cloud platform that meets requirements must be established. Monitoring of the information update, timely feedback, and regular maintenance of the network platforms are also necessary.

6 CONCLUSIONS

Given its advantages in business, decision-making, supervision, service, and other fields, the smart government has been widely discussed around the world. However, due to the high risk in information security, achieve the desired effect in the actual construction is difficult. To accurately evaluate the information security of smart government, this study constructs the integrated DEMATEL-ISM model and, combined with the relevant research basis and the actual construction experience of China examines the influencing factors and paths of the information security of the smart government. The conclusions are as follows.

(1) Based on the DEMATEL-ISM model, this study distinguishes the causal and result factors of smart government information security. The causal factors include policies and regulations, international environment, leadership mechanism, and public supervision, among

others. The result factors include safety consciousness, anti-leakage mechanism, behavioral safety, and supervision mechanism, among others. The causal factors affect the result factors.

(2) Based on the DEMATEL-ISM model, 13 key influencing factors of smart government information security were determined as follows: anti-leakage mechanism, supervision mechanism, leadership mechanism, safety consciousness, operation specification, information storage, public supervision, third-party supervision, policies and regulations, information transfer, platform construction, international environment, and information acquisition.

(3) Based on the DEMATEL-ISM model, the importance and influence level of influencing factors were distinguished. Policies and regulations are the roots influencing factor that affects the information security level of smart government. The international environment is the deep influencing factor. Infrastructure, moral cultivation, leadership mechanism, third-party supervision, and public supervision are the middle-level influencing factors. Psychological factors, platform construction, technology reference, information acquisition, technical training, and network propaganda are the surface-level factors. Safety consciousness and behavioral safety, among others, are the direct influencing factors.

(4) The DEMATEL-ISM model can more accurately reflect the relationship and comprehensive mechanism among the influencing factors of smart government information security. A simple and reliable model and analysis ideas are provided for objectively evaluating and improving the level of smart government information security.

This study distinguishes the importance of the influencing factors of smart government information security and distinguishes the causal and result factors. The interpretative structure model was constructed to better express the mechanism of influencing factors. However, this study does not consider the improvement path and priority of specific factors, which need further research in the future.

7 REFERENCES

[1] Pastor-Lopez, I., Sanz Urquijo, B., Tellaeche, A., Bringaso, P. G. (2021). Current trends and barriers of applied artificial intelligence. *DYNA*, 96(2), 123-125. https://doi.org/10.6036/9866

[2] Miloslavskaya, N. & Tolstoy, A. (2019). Internet of Things: information security challenges and solutions. *Cluster Computing*, *22*(1), 103-119. https://doi.org/10.1007/s10586-018-2823-6

[3] Kankanhalli, A., Charalabidis, Y., & Mellouli, S. (2019). IoT and AI for smart government: A research agenda. *Government Information Quarterly*, *36*(2), 304-309. https://doi.org/10.1016/j.giq.2019.02.003

[4] Kumar, R., Kumar, R., Sachan, A., & Piyush, G. (2021). An examination of the e-government service value chain. *Information Technology & People*, 34(3), 889-911. https://doi.org/10.1108/ITP-09-2018-0438

[5] Zhao, J. J. & Zhao, S. Y. (2010). Opportunities and threats: A security assessment of state e-government websites. *Government Information Quarterly*, *27*(1), 49-56. https://doi.org/10.1016/j.giq.2009.07.004

[6] Dawes, S. S., Vidiasova, L., & Parkhimovich, O. (2016). Planning and designing open government data programs: An ecosystem approach. *Government Information Quarterly*, *33*(1), 15-27. https://doi.org/10.1016/j.giq.2016.01.003

[7] Kim, S. H., Lee, G. S. (2016). An Empirical Study on Influencing Factors of Using Information Security Technology. *Journal of Society for e-Business Studies*, *20*(4), 151-175. https://doi.org/10.7838/jsebs.2015.20.4.151

[8] Workman, S., Jones, B. D., & Jochim, A. E. (2009). Information processing and policy dynamics. *Policy Studies Journal*, *37*(1), 75-92. https://doi.org/10.1111/j.1541-0072.2008.00296.x

[9] Elmaghraby, A. S. & Losavio, M. M. (2014). Cyber security challenges in Smart Cities: Safety, security and privacy. *Journal of Advanced Research*, *5*(4), 491-497. https://doi.org/10.1016/j.jare.2014.02.006

[10] Hwang, K. & Choi, M. (2017). Effects of innovation-supportive culture and organizational citizenship behavior on e-government information system security stemming from mimetic isomorphism. *Government Information Quarterly*, *34*(2), 183-198. https://doi.org/10.1016/j.giq.2017.02.001

[11] Ki, N., Kwak, C. G., & Song, M. (2020). Strength of strong ties in intercity government information sharing and county jurisdictional boundaries. *Public Administration Review*, *80*(1), 23-35. https://doi.org/10.1111/puar.13135

[12] Chesla, A. (2004). Information security: A defensive battle. *Information System Security*, *12*(6), 24-32. https://doi.org/10.1201/1086/44022.12.6.20040101/79783.5

[13] Liu, B. F., Zhong, H. H., & Wang, M. (2014). How to Design the Cloud Computing Used in E-government's Information Security. *Applied Mechanics and Materials*, *536-537*, 616-619. https://doi.org/10.4028/www.scientific.net/AMM.536-537.616

[14] Wirtz, B. W., Weyerer, J. C., & Sturm, B. J. (2020). The dark sides of artificial intelligence: An integrated AI governance framework for public administration. *International Journal of Public Administration*, *43*(9), 818-829. https://doi.org/10.1080/01900692.2020.1749851

[15] Guenduez, A. A., Singler, S., Tomczak, T., Schedler, K., & Oberli, M. (2018). Smart government success factors. *Yearbook of Swiss Administrative Sciences*, *9*(1), 96-110. https://doi.org/10.5334/ssas.124

[16] Dečman, M. (2015). Understanding technology acceptance of government information systems from employees' perspective. *International Journal of Electronic Government Research*, *11*(4), 69-88. https://doi.org/10.4018/IJEGR.2015100104

[17] Martin, C. (2014). Barriers to the open government data agenda: Taking a multi-level perspective. *Policy & Internet*, *6*(3), 217-240. https://doi.org/10.1002/1944-2866.POI367

[18] Geiger, C. P. & Lucke, J. V. (2012). Open government and (linked) (open) (government) (data). *JeDEM-eJournal of eDemocracy and open Government*, *4*(2), 265-278. https://doi.org/10.29379/jedem.v4i2.143

[19] Barns, S. (2018). Smart cities and urban data platforms: Designing interfaces for smart governance. *City, Culture and Society*, *12*, 5-12. https://doi.org/10.1016/j.ccs.2017.09.006

[20] Attard, J., Orlandi, F., Scerri, S., & Auer, S. (2015). A systematic review of open government data initiatives. *Government Information Quarterly*, *32*(4), 399-418. https://doi.org/10.1016/j.giq.2015.07.006

[21] Liu, C. R. & Wang, C. (2020). The status and guidance countermeasures of civil servants' information security behavior. *Journal of Beijing Electronic Science and Technology Institute*., *28*(3), 49-55.

[22] Grassegger, T. & Nedbal, D. (2021). The Role of employees' information security awareness on the intention to resist social engineering. *Procedia Computer Science*, *181*, 59-66. https://doi.org/10.1016/j.procs.2021.01.103

[23] Gil-García, J. R. & Pardo, T. A. (2005). E-government success factors: Mapping practical tools to theoretical

foundations. *Government Information Quarterly*, *22*(2), 187-216. https://doi.org/10.1016/j.giq.2005.02.001
[24] Yuan, T, W. & Chen, P. (2012). Data mining applications in E-government information security.*Procedia Engineering*, 29, 235-240. https://doi.org/10.1016/j.proeng.2011.12.700
[25] Alharbi, A. S., Halikias, G., Rajarajan, M., & Mohammad, Y. (2021). A review of effectiveness of Saudi E-government data security management. *International Journal of Information Technology*, *13*, 573-579. https://doi.org/10.1007/s41870-021-00611-3
[26] Qi, Q. (2020). Analysis of the measures taken by the government to strengthen the network information security in the era of big data. *Digital Technology & Application*, *38*(5), 172-173.
[27] Wu, W. C. (2021). Research on the government-led model of UK cybersecurity: achievements and problems. *Journal of Intelligence*, *40*(3), 98-103.
[28] Zhao, Y. & Cao, Y. W. (2020). Path choice of smart government construction: an analysis based on the reform of "one network, all can be handled". *The Journal of Shanghai Administration Institute*, *21*(5), 63-70.
[29] Yue, R. T. & Han, Y. X. (2020). On the DEMATEL-ISM model for analyzing the safety risk-involving factors of the airline companies. *Journal of Safety and Environment*, *20*(6), 2091-2097.
[30] Chen, W. G., Zhang, N., Zhang, Y. S., et al. (2021). Study on influencing factors of urban disaster resilience based on DEMATEL-ISM. *Journal of Catastrophology*, *36*(1), 1-6.
[31] Wang, D., Zhou, T., & Wang, M. (2021). Information and communication technology (ICT), digital divide and urbanization: Evidence from Chinese cities. *Technology in Society*, *64*, 101516. https://doi.org/10.1016/j.techsoc.2020.101516
[32] DeLuca, L. (2020). Searching FOIA Libraries for government information. *Government Information Quarterly*, *37*(1), 101417. https://doi.org/10.1016/j.giq.2019.101417
[33] Chatfield, A. T. & Reddick, C. G. (2019). A framework for Internet of Things-enabled smart government: A case of IoT cybersecurity policies and use cases in US federal government. *Government Information Quarterly*, *36*(2), 346-357.https://doi.org/10.1016/j.giq.2018.09.007
[34] Aveleira-Mata, J., Munoz-Castaneda, A. L., Garcia-Ordas, M. T., Cuellar, C. B., Andrades, J. A. B., & Moreton, H. A. (2021). IDS prototype for intrusion detection with machine learning models in IoT systems of the Industry 4.0. *DYNA*, *96*(3), 270-275. https://doi.org/10.6036/10011

Contact information:

Fengke WANG, Associate Professor
Henan University of Science and Technology,
No.263, Kaiyuan Avenue, Luolong District, Luoyang, Henan, 471000, China
E-mail: fengkewang@126.com

Juzheng ZHANG, Graduate Student
Henan University of Science and Technology,
No.263, Kaiyuan Avenue, Luolong District, Luoyang, Henan, 471000, China
E-mail: 2489684930@qq.com

Panke ZHANG, PhD
(Corresponding author)
Henan University of Science and Technology,
No.263, Kaiyuan Avenue, Luolong District, Luoyang, Henan, 471000, China
E-mail: cnzpk@163.com