ISSN 1330-3651 (Print), ISSN 1848-6339 (Online) https://doi.org/10.17559/TV-20190104101416
Original scientific paper

Research on Personal Information Risk Assessment Model in Smart Cities

Xuebo YAN*, Yuemin FAN*, Hyun-Hyo LEE, Rongguo QIU

Abstract: Personal information security plays fundamental and critical role in promotion of smart cities. By taking personal information, vulnerability and threat as basic elements for risk assessment, this article proposes a Markov method-based personal information security risk assessment model in smart cities with the core of threats (Li Hetian, 2007). Based on threat probability, threat consequence attribute and attribute value acquired through the Markov method, threat analysis, the multi-attribute decision-making theory and the expert grading method, this article calculates the objective threat indexes, which is then utilized for risk ranking, so as to provide scientific basis for formulating targeted personal information security risk management and control strategies.

Keywords: consequence attribute weight; risk assessment model; smart cities; threat index

1 INTRODUCTION

Smart cities mean a new mode promoting smart construction, management and service of cities by utilizing the new generation of information technologies such as the Internet of Things, the cloud computing and the big data. Smart cities are constructed to adapt to the trend of global society information-oriented development and the demands on reforms and upgrading of cities, which are the strategies to realize intensive, smart, green and low-carbon development of cities.

Smart cities also mean a complex integrated system that integrates the natural society. Containing geographic information, GPS data, 3D building data, statistical data collection, camera images and multi class data, it has core ideas of perception, control, transmission and intelligence, so as to form a larger and more complex network system based on Internet, mobile communication network, wireless sensor network. Therefore, information sharing is the basis for the application of intelligent cities, and the protection of personal information becomes the prerequisite for the development of intelligent cities. Because of the high transparency of information in the operation of a smart city, it may lead to a large number of personal information security vulnerabilities. Therefore, it is particularly urgent to evaluate personal information risks under the environment of smart cities.

Personal information security in smart cities is faced with numerous new challenges at present. Large amount of personal information is registered and recorded in various platforms including online shopping (smart logistics), seeking for medical services in hospitals (smart medical services), transportation (smart traffic), education and training (smart education) and business activities (smart government affairs); some of the information can be disclosed and some shall be protected as privacies. Besides, there are some inevitable defects and system loopholes in software and hardware design of various systems (including the personal information management) supporting the operation of smart cities, which lead to personal information disclosure and illegal use, giving rise to risks and obstructions to the promotion of smart cities. Personal information security risk assessment is a scientific assessment process on security features of information and the information system such as authenticity, completeness, security and availability according to related international information security technology standards by utilizing qualitative and quantitative scientific analysis methods and technical means on the aspects of risk control and management [1].

In order to conduct assessment on personal information security risks in an accurate way, it is needed to establish the personal information security risk assessment model in smart city environment, to conduct quantitative comparison on risks of the information system in smart cities, so as to acquire objective and reasonable risk threat index and rank the severity of risks. Among all the existing risk assessment methods for security assessment, there is no risk assessment model established specially aiming at the personal information management system in smart cities. Therefore, by taking existing risk assessment research findings as references, this article proposes a new, general, easy and feasible personal information security risk assessment model in smart cities by taking the characteristics of the personal information system of smart cities into consideration [2].

2 AN ASSESSMENT METHOD FOR PERSONAL INFORMATION RISKS IN SMART CITIES

Risk assessment methods include qualitative methods, quantitative methods and combined methods. Typical qualitative methods include factor analysis method, logical analysis method, historical comparative method and Delphi method. Qualitative methods can avoid the disadvantages of quantitative methods and explore deep thoughts, achieving more overall and profound assessment conclusions; however, such methods have strong subjectivity, with very high requirements on assessors. Typical quantitative analysis methods include clustering analysis method, factor analysis method, decision tree method, timing sequence model and regression model. In some conditions, the problem which can be explained by only a data cannot be illustrated by a large paragraph of text. However, it is necessary to complicate and fuzzify the simple thing in order to quantize it; in addition, some risk factors may be misunderstood and misinterpreted after quantization. As a complicated process, it is necessary to take a lot of factors into consideration of information security risk assessment. Some risks are easy to be quantized but some are not; therefore, in a large number of conditions, it is necessary to utilize methods combined

with qualitative and quantitative methods [3].

A lot of scholars research on risk assessment models on information system security by utilizing multiple methods such as the Markov method, the neural network, the grey theory, the analytic hierarchy method, the Bayesian network, the fuzzy mathematics and the decision tree method, acquiring numerous research findings. Some of the methods are objective and accurate with disadvantages such as complicated computing, difficult implementation and time-consuming assessment, and cannot be popularized. A personal information risk assessment model based on threat, sensitivity and vulnerability is proposed in this paper, i.e., the TSV-PITA risk assessment model. This model is also applicable to personal information security risk assessment in smart cities. By taking threat analysis as the core, it utilizes the Markov method, the expert scoring method, the fuzzy mathematical theory and the multi-objective decision theory to analyze the attribute of the threat consequence and calculate the weight of the consequence attribute, so as to give reasonable assessment results. By utilizing unique professional knowledge and experience of experts, the TSV-PITA model conducts quantitative processing to related information and ranks the risks as per their severities, so as to provide objective reference for the formulation of personal information protective strategies in smart cities [1].

3 TSV-PITA RISK ASSESSMENT MODEL

Sensitivity, vulnerability and threat of personal information constitute the three basic elements of information security risk assessment, with the relationship as shown in Fig. 1, in which personal information is the object to be protected; principally, higher information sensitivity means larger risk. Threat is the potential reason for possible incidents to systems or organizations; more threats for personal information mean larger risk, which may lead to security incidents. Vulnerability means personal information and sensitive information which may be utilized by the threat, which leads to disclosure of sensitive personal information. More unprotected sensitive information means higher possibility on security incident induced by utilizing the vulnerability of the information system [4].

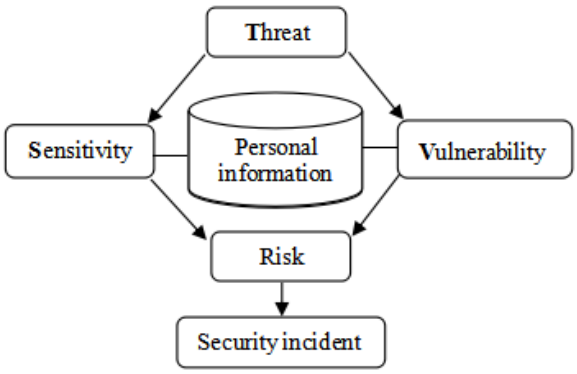

Figure 1 Relationship among Sensitivity, Vulnerability and Threats

As for a specific information system, not all the sensitive information will be disclosed, nor will all the vulnerabilities be attacked by threats. On this basis, this article proposes the personal information risk assessment model (TSV-PITA model) which takes threats as the core (as shown in Fig. 2).

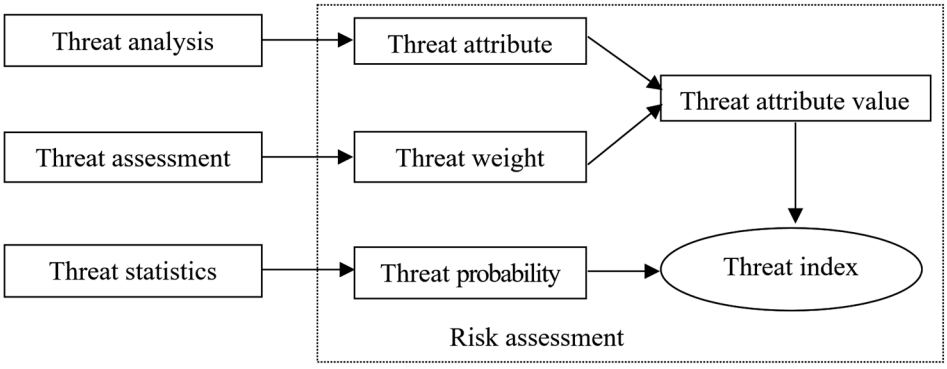

Figure 2 TSV-PITA Risk Assessment Model

The formula of TSV-PITA risk assessment model is:

$$R = f(S, V, T) = f\left[T_{\mathrm{p}}(V, T), C\right] \tag{1}$$

In which: R - risk, V - vulnerability, T - threat, T_{P} - threat probability, C - threat consequence, S - sensitivity. In fact, T_{P}, C and V, T are all related, so we only need to take T_{P} and C into consideration. That is to say, the possibility and threat of risk and threat will directly affect the impact of the system. The risk assessment is to assess the consequences and the threat probability, based on vulnerability and threat assessment only, as the risk assessment model of data source evaluation is as a consequence and the possibility of reference. So the actual risk should be calculated as shown in Eq. (2).

$$R = f(T_{\mathrm{p}}, C) \tag{2}$$

The TSV-PITA risk assessment model is established based on the risk assessment principle and takes threat analysis as the core. Firstly, it conducts assessment on the three basic elements of risk assessments including sensitivity, vulnerability and threat and conducts statistics on security incidents. It then acquires the threat probability, the threat consequence attribute and corresponding weight by utilizing the Markov method as well as threat analysis and assessment. After that, by utilizing the acquired threat consequence attribute and weight, it calculates the threat

consequence attribute value. Finally, it calculates the threat index according to threat probability and threat consequence attribute value. Threat index means the severity of the threat, and larger threat index means larger severity caused by the security index; therefore, it can be utilized to measure the size of risks. Based on the above analysis, sequences of threat can be ranked according to threat indexes, to formulate threat preventive strategies with prominent emphasis and priority control, so as to establish targeted security guarantee systems.

4 RISK ASSESSMENT METHOD

The analysis on the threat consequence is the key part of the TSV-PITA risk assessment model. Considering that the damages caused to the information system by threats are generally multi-dimensional ones but not a single one, if the damage caused by threats to certain layer is defined as the threat consequence attribute, the threat consequence has multi-attribute characteristics. The threat consequence attribute value refers to the damage severity of the threat, and it is available to conduct objective and comprehensive assessment on the threat to the information system according to quantized consequence attribute values [2].

3.1 Considering that the TSV-PITA risk assessment model is established based on the three basic elements of sensitivity, vulnerability and threat, various threats of the personal information security system shall be clarified before the risk assessment by utilizing the model (threat set M: $\{m_i | i = 1, 2, \ldots, n\}$, in which m_i is the i^{th} category of threat, and n is the number of the categories of threats of the information system). Considering that personal information security protection is a long term systematic complicated work, it is essential to calculate the probability of the threat to attack the personal information system. At the premise of threat recognition, this model utilizes the long term records of personal information disclosure and the Markov method to calculate the probability of various threats within certain time period in the future (p: $\{p_i | i = 1, 2, \ldots, n\}$, in which p_i means the probability of the threat m_i) [5].

Table 1 Classification of threats

No.	Category of the threat	Description of the threat
m_1	Management specification	The management system of personal information management department is not standard, and the storage, confidentiality and use of personal information are not standard. Management techniques and methods are not appropriate.
m_2	Personal consciousness	The sensitive information is disclosed unconsciously by individuals due to weak information security awareness and insufficient attention to privacies.
m_3	policies and regulations	The legal system is not perfect, the information acquisition and use standard is missing, the punishment measures of information disclosure are not strict, and the responsibility of personal information security is unknown.
m_4	Illegal acquisition	The information is disclosed due to malicious code, back door, illegal invasion, installation of supervisory control devices, interception of network information, malicious cheating of information and illegal data mining.
m_5	Safety technology	The personal information is disclosed due to imperfect personal information protection technologies, improper safety protection measures, as well as improper management such as disaster backup and data recovery.
m_6	Unforeseen factors	The sensitive data and personal information disclosure caused by safety equipment failure, lack of safety personnel, natural disaster factors.

Before information security risk assessment, this article concludes threats of personal information security into six categories according to collective discussion and analysis of experts, and Tab. 1 shows the classification of threats after conclusion.

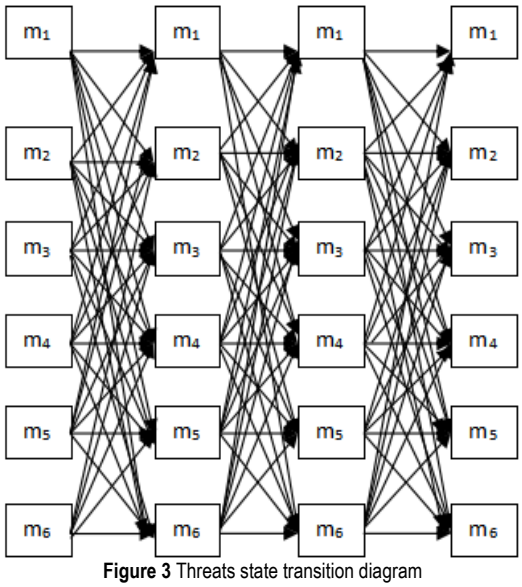

Figure 3 Threats state transition diagram

Considering that it is difficult to determine the threat attacking conditions during certain time in the future, it is needed to acquire the probability of threats to personal information through certain mode, and the Markov process is the effective method solving this problem. During the incident development process, if each state transition is only related to the state of the previous moment, and is not related to the past state; i.e., the state transition has no after-effect, such a state transition process is known as the Markov process. By utilizing the Markov process, this article calculates the probability of threats during a certain period in the future, to record the statistical information of threats of the e-governmental affair information system during various periods through the threat state transition diagram. Fig. 3 is a schematic state transition diagram for threats of personal information.

It is assumed that Tab. 2 shows the statistical condition of threats of certain information system at different time during a period.

The initial probability vector of various threats is defined as $\Pi = \{P_1(i)\}$; according to Tab. 2, $\Pi = \{0, 0, 1, 0, 0, 0\}$. During the development and change process of the incident, the probability of transition to another state after starting from certain state is known as the state transition probability. In the same way, according to Tab. 2, it is available to calculate the matrix of transition probability of threat state by adopting the ideology of frequency approximate probability, with the following calculation process: There are 11 states transited from threat m_1, in which the transition of $m_1 - m_1$ (indicating the

threat m_1 appearing in the previous time period information system and the m_2 appearing in the follow-up time period) occurs during T_{39}—T_{40}; therefore, $p(m_1 - m_1) = p_{11}$; the transition of $m_1 - m_2$ occurs during T_{21}—T_{22} and T_{40}—T_{41}; therefore, $p(m_1 - m_2) = p_{12}$. In the same way, it is available to calculate the transition probability of other threat states, and the threat state transfer probability matrix composed by these probabilities is shown as follows:

$$\begin{array}{c} \\ m_1 \\ m_2 \\ m_3 \\ m_4 \\ m_5 \\ m_6 \\ m_7 \end{array} \begin{array}{c} \begin{array}{ccccccc} m_1 & m_2 & m_3 & m_4 & m_5 & m_6 & m_7 \end{array} \\ \begin{bmatrix} \frac{1}{11} & \frac{2}{11} & \frac{2}{11} & \frac{2}{11} & \frac{1}{11} & \frac{2}{11} & \frac{1}{11} \\ \frac{3}{11} & \frac{1}{11} & \frac{2}{11} & 0 & \frac{1}{11} & \frac{3}{11} & \frac{1}{11} \\ \frac{1}{11} & \frac{1}{11} & \frac{2}{11} & \frac{1}{11} & \frac{3}{11} & \frac{1}{11} & \frac{1}{11} \\ \frac{2}{9} & \frac{2}{9} & \frac{2}{9} & \frac{2}{9} & 0 & \frac{1}{9} & 0 \\ \frac{2}{7} & \frac{2}{7} & 0 & \frac{2}{7} & \frac{1}{7} & \frac{1}{7} & 0 \\ \frac{2}{8} & \frac{1}{8} & \frac{1}{8} & \frac{2}{8} & \frac{1}{8} & 0 & \frac{1}{8} \\ \frac{2}{3} & \frac{2}{3} & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \end{array}$$

$p_t(j)$ is defined as the probability of threat m_j during the time period t of the information system, and it is available to calculate $p_t(j)$ as per the thought of recursion; i.e., $p_t(j) = \sum_{i=1}^{n} [p_{t-1}(i) * m_{ij}]$ (all $p_{t-1}(i)$ have been calculated before $p_t(j)$). Calculate $p_3(2)$, the probability of threat m_2 during the time period of T_3, as shown in Fig. 3, with the following process:

$$p_2(1) = \sum_{i=1}^{6} [p_1(i) \cdot m_{ij}] = m_{31} = \frac{1}{10}.$$

In a similar way, $p_2(2) = \frac{1}{10}$, $p_2(3) = \frac{2}{10}$, $p_2(4) = \frac{1}{10}$, $p_2(5) = \frac{3}{10}$, $p_2(6) = \frac{1}{10}$.

$$= p_2(1) \cdot m_{12} + p_2(2) \cdot m_{22} + p_2(3) \cdot m_{32} + p_2(4) \cdot m_{42} +$$
$$+ p_2(5) \cdot m_{52} + p_2(6) \cdot m_{62} = 0.127$$

The Markov method can be utilized to calculate the probability of the dynamic real-time information system threat probability. Considering that the threat probability has staged characteristics; i.e., it may have high threat frequency during certain time periods (caused by multiple factors such as various configurations of the information system, the development of information technology, the spreading of hacker tools, viruses and Trojans, the operating habits of internal personnel, a major promotion activity, etc.), in condition of inconsistency between the calculated result of threat probability and the practical condition, it is available to re-calculate the state transition probability matrix for threat occurrence according to threat records of recent time periods.

Table 2 Statistics on occurrence of threats

Time period	T_1	T_2	T_3	T_4	T_5	T_6	T_7	T_8	T_9	T_{10}
Threats	m_1	m_2	m_3	m_6	m_4	m_3	m_3	m_5	m_6	m_2
Time period	T_{11}	T_{12}	T_{13}	T_{14}	T_{15}	T_{16}	T_{17}	T_{18}	T_{19}	T_{20}
Threats	m_6	m_4	m_3	m_3	m_5	m_4	m_4	m_2	m_6	---
Time period	T_{21}	T_{22}	T_{23}	T_{24}	T_{25}	T_{26}	T_{27}	T_{28}	T_{29}	T_{30}
Threats	m_3	m_5	m_2	---	m_2	m_4	m_4	m_6	m_2	m_3
Time period	T_{31}	T_{32}	T_{33}	T_{34}	T_{35}	T_{36}	T_{37}	T_{38}	T_{39}	T_{40}
Threats	m_2	m_3	m_1	m_5	m_4	m_1	---	m_2	m_2	m_1
Time period	T_{41}	T_{42}	T_{43}	T_{44}	T_{45}	T_{46}	T_{47}	T_{48}	T_{49}	T_{50}
Threats	m_1	m_6	m_5	m_2	m_6	m_2	m_3	m_4	m_2	m_1
Time period	T_{51}	T_{52}	T_{53}	T_{54}	T_{55}	T_{56}	T_{57}	T_{58}	T_{59}	T_{60}
Threats	---	m_2	m_6	m_3	m_2	m_1	m_4	m_2	m_5	m_5

3.2 Threat analysis and assessment: Considering that threats lead to diversified influences and consequences on personal information, threat analysis involves the multi-objective decision theory based on the premise of threat recognition and long term recording of security incidents in the information system. Threat analysis and assessment is conducted in order to acquire various threat consequence attribute values according to the analysis of internal personnel, internal statistic experts and related professional and authorized personnel, i.e., the damages of threats to personal information on different layers. Common threat consequence attributes include "endangering personal security", "disturbing personal life", "damaging personal fame", "property loss", etc. Different governmental departments have varied concern emphasis and degrees on different threat consequence attributes. It is necessary to assess by selecting significant threat consequence attributes according to practical demands, and adopt objective and scientific method to give corresponding weight, so as to acquire the risk assessment results suitable for the assessed objects. The types of the threat consequence attribute values are expressed as $X: \{x_{ij} | i = 1, 2, \ldots, n, j = 1, 2, \ldots, m\}$, in which x_{ij} is the j^{th} attribute value of the i^{th} category of threat m_i.

The threat assessment in this article is a calculation process for the threat consequence attribute weight. As a relative concept, weight is corresponding to certain index (the index here refers to the threat consequence attribute). The weight of certain index refers to the relative importance of the index in the whole assessment. Weight coefficient selection methods mainly include the expert consultation weight method (the Delphi method), the factor analysis weight method, the information amount weight

method, the independence weight method, the principal component analysis method, the analytic hierarchy process method (AHP method), the superiority chart, the entropy weight method, the standard deviation method, the CRITIC method, the non-fuzzy number judgment matrix method and some other methods. The weight method adopted in this article is described as follows: firstly, grade the weight of various indexes according to expert opinions (original weight), to make the sum of the original weight of all the indexes 1. This method takes the thought of Wang Yuliang, a Chinese scholar, as reference. As a method integrated with qualitative and quantitative methods, with both advantages of the two, this method has easy and feasible calculation, more objective than other methods. The specific operation method is described as follows [7]:

a. Invite professional internal personnel, internal statistic experts and related professional and authorized personnel to analyze and confirm the original weight of the threat consequence attribute, w_{hj}, means the weight of the j^{th} consequence attribute x_j endowed by the h^{th} expert ($\sum_{j=1}^{m} w_{hj} = 1$; i.e., the sum of the original weight of all the attribute consequences of certain threat consequence must be 1).

b. Calculate the average each threat consequence attribute weight. $\overline{w}_j = (\sum_{h=1}^{k} w_{hj}) / k$ (k is the total number of experts participating in grading)

c. Calculate the offset of the weight of the original consequence attribute.

$$w_{hj}^* = \left| w_{hj} - \overline{w}_j \right| \tag{3}$$

d. Calculate the new consequence attribute weight (smaller offset means larger proportion in actual weight).

It is set that

$$w_{hj}^* = \frac{\max w_{hj}^* - w_{hj}^*}{\max w_{hj}^* - \min w_{hj}^*} \tag{4}$$

$$w_{j0} = \frac{\sum_{h=1}^{k} w_{hj}^* \overline{w}_{hj}^*}{\sum_{h=1}^{k} \overline{w}_{hj}^*} \tag{5}$$

Conduct normalization processing to

$w_{j0} = [w_{10}, w_{20}, ..., w_{30}]$,

i.e., $w_j = \frac{w_{j0}}{\sum_{j=1}^{m} w_{j0}}$

w_j - the new weight of the threat consequence attribute x_j

Table 3 Grading of threat consequence attribute by experts

	Damages to physical and mental health	Damages to personal reputation	Loss of property	Discriminatory treatment
Expert 1	0.15	0.15	0.35	0.35
Expert 2	0.2	0.2	0.4	0.2
Expert 3	0.1	0.2	0.4	0.3
Expert 4	0.15	0.25	0.3	0.3
Average value	0.15	0.2	0.3625	0.2875
Attribute weight	**0.15**	**0.2**	**0.36**	**0.29**

The attribute weight is a group of values calculated as per the above method according to expert scoring, and this article aims to provide a scientific and simple weight calculating method. More precise or convenient method can be adopted in practical personal information security risk assessment process.

3.3 Calculate the threat consequence attribute value and threat index: Considering that threat consequence attribute values (endangering personal security, damaging personal fame, property loss and disturbing personal life) have different dimensions, in order to achieve unified measurement, this article adopts a simple linearization technique to nondimensionalize them [7], to acquire the relative value influenced by the consequence attribute.

$$V^* : \left\{ v_{ij}^* \mid i = 1,\ 2, \ldots, m \right\}, \tag{6}$$

v_{ij}^* - the relative influence value of threat m_i on the aspect of the consequence attribute x_j,

$$v_{ij}^* = \frac{v_{ij} - \min v_{ij}}{\max v_{ij} - \min v_{ij}} \tag{7}$$

max v_{ij} and min v_{ij} mean the maximum value and the minimum value of the consequence influences of all the threats in the consequence attribute threat set M.

Table 4 Threat probability and consequence attribute value

Threat	Probability	Endangering personal security $W = 0.15$		Damages to personal fame $W = 0.20$		Property loss $W = 0.36$		Discriminatory treatment $W = 0.29$	
		C_1/ level	C_1^*	C_2/ level	C_2^*	V_3/10 thousand yuan	C_3^*	C_4/level	C_4^*
m_1	0.10	6	0.33	8	1	200	1	15	1
m_2	0.12	12	1	2	0	60	0.26	10	0.64
m_3	0.14	10	0.78	5	0.5	30	0.11	5	0.29
m_4	0.16	8	0.56	3	0.17	10	0	5	0.29
m_5	0.15	3	0	5	0.5	20	0.05	1	0
m_6	0.20	4	0.11	3	0.17	70	0.32	3	0.14

The threat probability in Tab. 4 is the probability of threats during certain time period by utilizing the Markov method. By utilizing the multi-attribute decision-making theory, the TSV-PITA risk assessment mode combines the threat consequence attribute and the weight to acquire the threat consequence attribute value, and then acquires the threat index (*MI*) of various risks by combining the threat consequence attribute value and the threat probability. *MI* is utilized to show the severity of the security incident may be caused by specific risk threat [8].

The threat index corresponding to threat m_i can be defined as:

$$MI_i = p_i \cdot \sum_{j=1}^{m} (c_{ij} \cdot w_j) \tag{8}$$

In which: mp_i means the occurrence probability of m_i; x_{ij} means the j^{th} consequence attribute value of m_i; w_i means the j^{th} consequence attribute weight. Information security risk assessment is conducted to measure the relative severity of various threats and rank them; therefore, in order to achieve direct and easy comparison on the assessment result, it is needed to re-use another linearization technique to conduct normalization process to MI_i and calculate relative threat index (expressed with RMI_i - relative threat index). That is:

$$RMI_i = \frac{MI_i}{\sum_{1}^{n} MI_i} \cdot 100 \tag{9}$$

Tab. 5 is the calculation consequence of Tab. 4 based on the above method.

Table 5 Relative threat index

No. of threat	Type of threat	Relative threat index *MI*, %
m_1	Management specification	26.0
m_2	Personal awareness	21.9
m_3	Policies and regulations	17.4
m_4	Illegal stealing	14.5
m_5	Safety technologies	10.9
m_6	Accidental factors	9.3

5 RISK ASSESSMENT PROCEDURES BASED ON THE TSV-PITA RISK ASSESSMENT MODEL

According to the above analysis and calculation process, the risk assessment on personal information security by utilizing the TSV-PITA assessment model is objective and effective, which can predict the probability of various threats in future periods as well as corresponding damage degree in a favorable way. In order to give full play to its roles in practical utilization, the risk assessment procedures based on the model are given as follows:

a. The period of business investigation and assessment range determination. By investigating personal information system and personal information related business in smart cities, it determines potential risks and objects to be protected, so as to determine the range of personal information security risk assessment.

b. The period of personal sensitive information identification and evaluation. Personal information is the object of information security protection, and it is necessary to recognize and assess the personal information collected in the information system of smart cities and the network, to understand the vulnerability of personal information sensitivity which may be utilized by threats.

c. The period of threat analysis. The working contents during the threat analysis period include: threat recognition and source investigation, threat attacking probability calculation, threat consequence analysis and threat severity ranking. The TSV-PITA risk assessment model is utilized to calculate the threat index of various threats and rank according to the risks caused by the threat indexes.

d. Countermeasures and suggestions. In order to reduce the danger caused by information leakage, it is available to rank as per the threat indexes acquired from risk analysis, so as to formulate demand-oriented personal information security guarantee and prevention strategies with prominent emphasis.

6 CONCLUSIONS

The TSV-PITA risk assessment model has multiple advantages due to the general utilization of multiple methods: it can calculate the dynamic probability of risks of the personal information system with the Markov process. It is available to analyze the threat consequence attribute and estimate the consequence weight by utilizing the unique professional knowledge and experience of experts. It is available to calculate the threat consequence attribute value by utilizing the multi-attribute decision-making theory and some quantized methods, so as to conduct scientific, objective and reasonable ranking to various threats. However, information security risk assessment is involved in a very complicated and difficult work, and the TSV-PITA risk assessment model has its using limitation, and continuous perfection is needed on technical and management layers during the practical using process. For example, in condition of too many threat categories, the threat state transition diagram will be very huge, and it is needed to record the statistical information of various threats in a detailed and accurate way, and it is very troublesome to calculate the probability. In this condition, it is available to establish a more suitable risk assessment model by taking or combining other methods.

Acknowledgements

This paper is from Yan Xuebo's doctoral thesis: A Study on Risk Assessment Model based Personal Information Protection in Smart Cities

The authors acknowledge the Ministry of education of Humanities and Social Science Project (Grant: 17YJC630115), Foundation of Ministry of Education of China (Grant: 15YJC880013), Jiangsu Natural Science Foundation Project (Grant: BK20170876).

7 REFERENCES

[1] Yan, X. (2018). *A Study on Risk Assessment Model based Personal Information Protection in Smart Cities*, Wonkwang University.

[2] Chen, X., Wang, X., & Huang, H. (2009). Research on Methods for Multi-attribute Information Security Risk

Assessment based on Menace Analysis. *Computer Engineering and Design*.
[3] Li, S. & Liu, J. (2010). Dynamic Network Risk Assessment based on Hidden Markov Model. *Science & Technology Information*.
[4] Chen, T., Feng, P., & Zhu, D. (2011). Risk Assessment Model of E-government Affair Information Security based on Threat Analysis. *Journal of Engineering Information*.
[5] Yang, Y. & Yao, S. (2009). A Method for Information Security Risk Assessment based on Menace Analysis. *Computer Engineering and Application*.
[6] Wang, Y. (2005). Bridge Type Scheme Comparison Model based on Fuzzy Mathematic Theory. *Engineering Design and Implementation*.
[7] Li, H., Liu, Y., & He, D. (2007). Information Security Risk Assessment Model based on the Markov Chain. *Journal of Railway*.
[8] Feng, P. (2012). Threat Analysis based Comprehensive Assessment Model for E-governmental Information Security Risks, Huazhong University of Science and Technology, *Master's Thesis*.
[9] Zhang, Y. et al. (2009). Risk Assessment on Emergency Platform Information Security based on AHP. *Journal of Beijing Normal University: Natural Science Edition*.
[10] Zhang, J., Ren, X., & Wang, R. (2010). Risk Assessment on Multi-attribute Information Security based on Bayesian Network. *Computer Security*.
[11] Zhao, J. & Du, Z. (2009). Research on Credit Risk Assessment Model Based on Neural Network and Decision-making Tree. *Journal of Beijing Institute of Technology*.
[12] Qian, P. & Wu, M. (2012). Research and Method Review on Privacy Protection of Internet of Things, Computer Application and Research.
[13] Liu, J. (2015). Research on Information Security Guarantee in Smart City Construction, South China University of Technology, *Master's Thesis*.
[14] Jiang, S. (2016). Research on Security and Privacy Protection in Information Sharing of Internet of Things, Xi'an University of Electronic Science and Technology, *Doctoral Thesis*.
[15] Liu, F. (2005). Information System Security Assessment Theory and Research on Key Technologies, National University of Defense Technology, *Doctoral Thesis*.
[16] (2012). Information Security Technologies, Public and Commercial Service Information System and Personal Information Protection Guide, GB/Z 28828-2012.

Contact information:

Xuebo YAN, Associate professor
(Corresponding author)
School of Management, Fujian University of Technology,
No. 3 Xueyuan Road, University Town,
Minhou, Fuzhou 510320, Fujian, P. R. China
E-mail: abc@fjut.edu.cn

Yuemin FAN, Dr
(Corresponding author)
College of Entrepreneurship Education,
Guangdong University of Finance and Economics,
21 Luntou Road, Guangzhou 510320, Guangdong, P. R. China
E-mail: 124141548@qq.com

Hyun-Hyo LEE, Professor
Dept. of Computer Engineering and Software, Wonkwang University,
460 Iksandae-ro, Iksan, Jeonbuk, Republic of Korea

Rong-guo QIU, Associate Professor
School of Public Administration, Yancheng Teachers University,
No. 2 South Hope Avenue, Yancheng 224007, Jiangsu P. R. China