Risk evaluation model for tourism mobile payment

Cai-Xia Chen*, Li-Hua Wu and Chun Shi
School of Information Science and Technology, Hainnan Normal University, Haikou, P.R.China.
E-mail: 914922505@qq.com
**Corresponding author*

The rapid rise of the mobile payment in China has brought a new round of opportunities and challenges. During this process, the safety problem becomes an important issue of the payment power in the future in China. Based on the general definition of risk, the paper considers the special need of tourism mobile payment, building mobile payment risk evaluation model through the Analytic Hierarchy Process (AHP) and the fuzzy comprehensive evaluation (FCE) and conducting positive analysis. The model not only could evaluate the tourism mobile payment risk, but also could guide the risk control and compare the results of different risk defense strategies.

Keywords: Tourism Mobile Payment; Risk Evaluation; Model.

1. Introduction

With the development of the internet finance, traditional tourism starts to transfer to electrical and digital tourism. More and more online tourism companies provide the customers with one-stop services, including transportation, hotel booking and ticket, which make mobile payment a critical matter for the tourists’ user experience. However, the risk is also rising, a safe and convenient mobile payment market is in need.

So far, no research raises a complete evaluation system for the mobile payment risk. This paper only focuses on the tourism industry, combines the theory and the practice together, and uses the risk management theory to comprehensively recognize and analyze the possible risk in the tourism mobile payment process. The paper also uses the comprehensive Analytic Hierarchy Process (AHP) and the fuzzy comprehensive evaluation (FCE) to build risk evaluation system, build risk evaluation model, and conduct positive analysis to lay the foundation of mobile payment security problem in a quantitative way, meanwhile proposes risk control method and improvement measure.

Copyright © 2017, the Authors. Published by Atlantis Press.
This is an open access article under the CC BY-NC license (http://creativecommons.org/licenses/by-nc/4.0/).

2. Basic Theory of the System Building

2.1 *Concept of risk*

Risk is the probability of security problem and the influence of the problem generated by human or nature. Risk is the combination of risk factor, risk accident, and risk losses.

2.2 *.Risk evaluation*

Risk evaluation is the process in which researcher uses the qualitative and quantitative analysis method to evaluate the potential or actual thread to the subject and recognize, analyze, and put forward solutions from the risk management aspect.

2.3 *Risk evaluation method*

Risk evaluation method, including qualitative and quantitative model and method, will determine the risk level, risk probability, and the order of risk control of the data asset, and then take action and reduce the losses.

Generally, different institution will adopt different evaluation method. Risk of different payment methods on the same device of the same person could be different. In the paper, the evaluation subject is the tourism mobile payment application, and the evaluated subject is the tourism service provider.

3. Tourism Mobile Payment Evaluation Index System

3.1. *Tourism Mobile Payment Concept Model*

For the tourism mobile payment, the risk concept model has three aspects.

(1)Risk Factor: virus invasion, hackers' invasion, packet sniff, service decline, wireless internet safety, malicious scanning, password cracking, and data tampering.

(2)Risk Event: informal website visiting, risky downloading, QR code scanning, and unknown Wi-Fi connecting.

(3)Risk Losses: private information leakage and property losses. The lawbreakers will obtain private information in direct or indirect way. The direct way is to use technical method, for example the Trojans virus or the phishing site, to invade the mobile phone and therefore lure the user to input private information or steal the information directly. The indirect method is to buy huge amount of information or use packet sniffing on the internet, and finally leads to users' property losses.

3.2. *The Content of Risk Recognition and Evaluation*

To analysis the condition of the tourism mobile payment, the author design 30 questions about the tourism mobile payment and conduct research in the tourism market in Hainan. Through the analysis of the valid questionnaire, the classification and summary of 11 major questions, and the interview with the experts, the paper build a model of risk factor assessment, risk event assessment, and the safety vulnerabilities in the mobile payment risk system. Figure 1 shows the result.

To comprehensively and objectively evaluate the mobile payment security risk(Table 1), based on figure 1, the paper design a mobile payment security payment system.

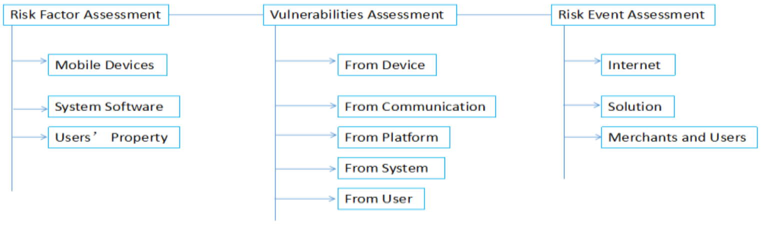
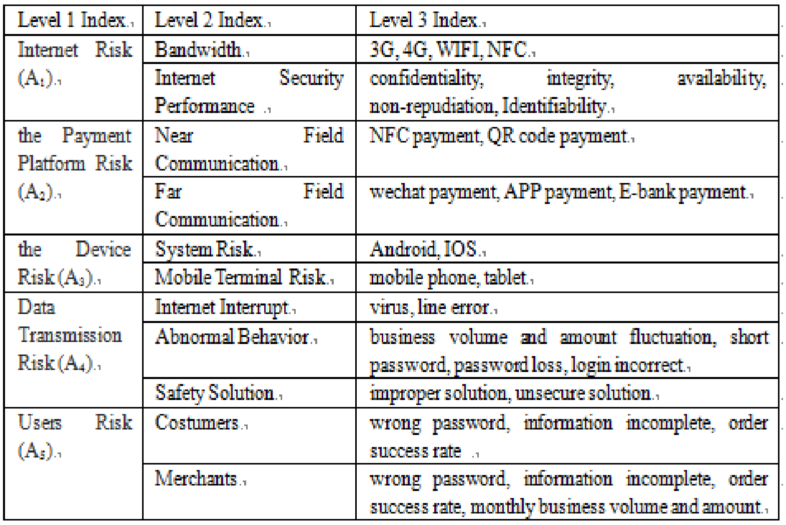


Fig. 1 Mobile payment risk evaluation index system

4. Calculation of Weight of Indexes in the Index System

Tab. 1 Mobile payment risk evaluation index system



Level 1 Index	Level 2 Index	Level 3 Index
Internet Risk (A_1)	Bandwidth	3G, 4G, WIFI, NFC
	Internet Security Performance	confidentiality, integrity, availability, non-repudiation, Identifiability
the Payment Platform Risk (A_2)	Near Field Communication	NFC payment, QR code payment
	Far Field Communication	wechat payment, APP payment, E-bank payment
the Device Risk (A_3)	System Risk	Android, IOS
	Mobile Terminal Risk	mobile phone, tablet
Data Transmission Risk (A_4)	Internet Interrupt	virus, line error
	Abnormal Behavior	business volume and amount fluctuation, short password, password loss, login incorrect
	Safety Solution	improper solution, unsecure solution
Users Risk (A_5)	Costumers	wrong password, information incomplete, order success rate
	Merchants	wrong password, information incomplete, order success rate, monthly business volume and amount

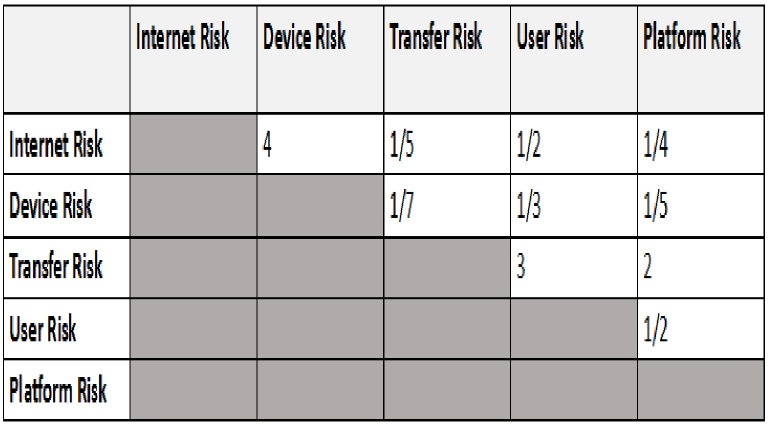
The paper interviews 8 experts by questionnaire, and calculates the weight of indexes (including level 1 and level 2 index) in the system based on the grade from the experts by the AHP method. Table 2 and Table 3 show the result.

Tab. 2 Mobile payment risk evaluation indexes and weights

Level 1 Index	Weights	Level 2 Index	Weights
Internet Risk (A_1)	0.3600	Bandwidth	0.0100
		Internet Security Performance	0.0300
the Payment Platform Risk (A_2)	0.2800	Near Field Communication	0.1500
		Far Field Communication	0.0500
the Device Risk (A_3)	0.2000	System Risk	0.0900
		Mobile Terminal Risk	0.0300
Data Transmission Risk (A_4)	0.1200	Internet Interrupt	0.1326
		Abnormal Behavior	0.1705
		Safety Solution	0.0568
Users Risk (A_5)	0.0400	Costumers	0.2100
		Merchants	0.0700

4.1. *Structure of the judgment matrix*

The judgment matrix reflects the relevant importance of factors in current level with previous level. Based on the interview and the questionnaire, the level 2 risk matrix is showed as the following(Figure 2).



	Internet Risk	Device Risk	Transfer Risk	User Risk	Platform Risk
Internet Risk		4	1/5	1/2	1/4
Device Risk			1/7	1/3	1/5
Transfer Risk				3	2
User Risk					1/2
Platform Risk					

Fig. 2 Level 2 Risk Matrix

Assume that factor C_k in level C is relevant with factor A_1, A_2, …, A_i in the next level, C_I of the judgment matrix equals 0.0367, which is less than 0.1 and therefore meet the consistency requirement.

Tab. 3 Mobile payment risk evaluation level 3 indexes weights and ranks

Project	Weights and Ranks	Project	Weights and Ranks
Virus	0.1199	Integrity	0.0216
SIM	0.0957	Confidentiality	0.0216
Login Incorrect	0.0771	Identifiability	0.0168
Password	0.0695	Wi-Fi	0.0108
Wechat	0.0683	Android	0.0103
Password Loss	0.0599	NFC	0.0085
QR Code	0.0598	Monthly Business Amount	0.0084
Short Password	0.0428	Monthly Business Volume	0.0084
APP	0.0410	3G	0.0077
Bandwidth	0.0400	Non-repudiation	0.0072
Order Success Rate	0.0386	Availability	0.0072
Improper Security Solution	0.0385	Tablet	0.0072
Unsafe Security Solution	0.0300	4G	0.0046
Business Volume Fluctuation	0.0257	Mobile Phone	0.0043
IOS	0.0240	NFC	0.0015
Information Completeness	0.0232		

4.2. *Risk index value set up*

Each condition node has a fixed security value Y_{kj} and an actual value X_{kj}, then the risk index value of the nodes will be $Z_{kj} = X_{kj} / Y_{kj}$. For example, for a certain condition node, user set the password length to 8 digits, but the safe value of length of password is 16 digits, then $Z_{kj} = X_{kj} / Y_{kj} = 0.5$.

4.3. *Node value calculation*

The value of the risk node R,$R = W \times Z$, is a matrix, which represents the product of the weight and the probability of the transfer node under different target nodes, as in Eq. (1).

$$R_i = \sum_{j=1}^{n} W_{ij} Z_{ij} \tag{1}$$

When the value of the risk node exceeds expectation, the plan node will drive the condition node to change, and create a new risk node value. The difference of the new risk node value and the old risk node value is value node value, which would reflect if the risk is under efficient control, or, if the strategy is workable.

Tab. 4 Setting of security level of condition nodes of ctrip.com

	Risk Level Low	Risk Level Middle-Low	Risk Level Middle	Risk Level Middle-High	Risk Level High
password length(C_4)	>12(0.1)		7-12(0.7)		<6(0.2)
bandwidth /KB(C_4)	>500 (0.05)	300-500 (0.1)	200-300 (0.05)	100-200 (0.6)	1-100 (0.2)
order success rate %(C_4)	>80 (0.28)	60-80 (0.4)	40-60 (0.19)	20-40 (0.08)	<20 (0.05)
business volume fluctuation %(C_4)	<20 (0.4)	20-40 (0.2)	40-60 (0.18)	60-70 (0.12)	>70 (0.1)
information completeness %(C_4)	100(0.1)	80(0.23)	60(0.41)	40(0.22)	<10(0.04)
internet security level(C_4)	0.25	0.35	0.25	0.1	0.05
monthly business volume(C_4)	>1000 (0.1)	800-1000 (0.235)	400-800 (0.395)	100-400 (0.22)	<100 (0.05)
payment platform(C_4)	NFC (0.1)	APP (0.2)	SIM (0.2)	Wechat (0.25)	QR Code(0.25)
system device(C_4)	IOS(0.1)	IPhone (0.15)	Brand (0.2)	Android (0.3)	Other (0.25)

5. Positive Analysis

Based on the questionnaire and the data from the Ctrip.com, the paper analyses the risk of 9 elements of Ctrip.com, including password length, bandwidth, order success rate, information completeness, business volume fluctuation, internet security level, monthly business volume, payment platform, and the system device. The setting of the condition nodes is showed on Table 4.

Merchant Risk Node Value Calculation. Finally, R=1.08.

The calculation above is the maximum value of the condition node of Ctrip.com.

During practical application, one could use real condition node data to judge the scale of the risk. For example, assume that the real condition is the one with the minimum risk, then similarly: R=0.23, which is the minimum value of the condition node of Ctrip.com.

6. Conclusion

According to the model,

(1)When the user tries to log on a specific tourism website, he can compare his own risk node with the risk node of the website. If the risk is too high or exceed the expectation, the user could change the mobile payment environment to increase the risk control ability, or choose to use other website with higher risk control ability.

(2)The tourism website can also change its own environment data, for example, increase the password length requirement to 16 digits, to increase the risk control ability of the website and reduce the maximum risk node value.

(3)Conduct mobile payment risk control is important. The paper uses the Analytic Hierarchy Process (AHP) and the fuzzy comprehensive evaluation (FCE) and gathers mobile payment data by expert interview and questionnaire to set up the risk node value. Furthermore, the paper also calculates the entropy weight of the node's influence to the risk through the data analysis and calculation. The data is objective, and can indicate the risk value. Users can take essential action to improve the factors with high risk, and generate risk control strategy.

Acknowledgments

Thanks to the support by NSFC (No.61362016), Education Science Planning Office of Hainan Province (Hjjg2013-18).

References

1. Yin Li, Min Tian, The Construction of Third-Party Payment Risk Evaluation Index System, Xi'An University of Finance and Economics Journal, 2013 (9).
2. National Information Security Standardization Technical Committee.GB/T 20984-2007 Security Risk Assessment Standard of Information Technology,Beijing: Standards Press of China,2007.
3. Dengguo Fen, Yang Zhang, Yuqing Zhang, Information Technology Safety Assessment Overview,Communication Journal, 2004,25 (7): 10-18.
4. Dan Wang, Tao Zhou, Yi Wu, Trusted Platform Control Module Risk Evaluation Model based on Bayes Network,Computer Application,

2011, 31 (3): 767-789.

5. Chunzi Wang, Guangqiu Huang, Anlysis of Internet Thread based on Vulnerability Relation Model,Computer Application, 2010, 30 (11):3046-3050.
6. Sun Wangquan, The risk analysis and safety strategy on remote mobile payment//Proceedings of 2012 IEEE Symposium on Digital Object Identifier, 2012:400-402.
7. Zhang Juncai, Zhao Jinhui, Qian Xun, Risk assessment of mobile payment system security based on extension theory//Proceedings of 2012 International Conference on Computer Science and Service System,2012:880-883.
8. Zhou yu,Chai hongfeng,He shuo,Liao jian. Research on Method of Security Compliance Detection and Analysis for Mobile Payment System[J]. Compute A pplication and Software. 2012(10).
9. Zhang Juncai,Zhao Jinhui,Qian Xun.Risk assessment of mobile payment system security based on extension theory. Proceedings of 2012 International Conference on Computer Science and Service System. 2012.
10. Sun Wangquan.The risk analysis and safety strategy on remote mobile payment. Proceedings of 2012 IEEE Symposium on Robotics and Applications. 2012.