User Acceptance of a Community-Based Healthcare Information System Preserving User Privacy

Chien-Lung Hsu[1] and Ming-Ren Lee[2]

[1] Department of Information Management, Chang Gung University, Taiwan, R.O.C.
clhsu@mail.cgu.edu.tw
[2] Department of Information Management,
Taoyuan Innovation Institute of Technology, Taiwan, R.O.C.
D9009207@mail.ntust.edu.tw

Abstract. Community-based healthcare information systems (HIS) are developed to cope with the demand for home healthcare. However, the issue of privacy protection in HIS adoption has not been given sufficient attention. This study is to propose a privacy-enhanced framework and to investigate the role of privacy protection in HIS adoption. Our research model extends the unified theory of acceptance and use of technology by considering perceived security and information security literacy. Our experimental HIS is implemented according to our proposed privacy-enhanced framework which integrates healthcare applications and privacy protection mechanisms. The former includes health management, physiological monitoring, healthcare education, and healthcare consulting modules. The latter contains secure transmission, privacy protection and access control modules. Analyses indicate that user adoption of HIS is directly affected by social influence, performance expectancy, facilitating conditions, and perceived security. Perceived security has a mediating effect between information security literacy and user adoption.

Keywords: privacy protection, healthcare information system, UTAUT, perceived security, information security literacy.

1 Introduction

Population ageing has become a global trend because of rising life expectancy and declining birth rates. An American study in 2009[1] indicated that people older than 65 years old represent 12.9 percent of the U.S. population. In parts of Asia, elder persons accounted for 10.74 percent in Taiwan in 2010[2]. Japan, one of the most rapidly ageing countries, had the 20.8 percent of elderly population in 2006, and it will increase to 40 percent by 2050[3]. As predicted by the United Nations, the proportion of elders in the

Data source:

[1] Administration on Aging, U.S.A.
(http://www.aoa.gov/aoaroot/aging_statistics/index.aspx)

[2] Department of Statistics, Ministry of the Interior, Taiwan.
(http://www.moi.gov.tw/stat/)

[3] National Institute of Population and Social Security Research, Japan
(http://www.ipss.go.jp)

C. Stephanidis and M. Antona (Eds.): UAHCI/HCII 2013, Part III, LNCS 8011, pp. 453–462, 2013.

world will reach 21 percent in 2050. The ageing phenomenon has caused rapid increase of the demand for health promotion and related services. In a report by the American Association of Retired Persons (AARP), approximately 85 percent of older people prefer to stay in their home when needing medical care [1]. This leads to a growing interest in using information systems to facilitate in-home healthcare and health management.

Research about healthcare information systems (HISs) usually addresses on the outcomes and benefit, but little attention has been given to privacy protection. For instant, several studies aimed to examine the impacts [2], time efficiency [3], benefit and contributions [4] of electronic health records (EHRs) on HISs. Vishwanath, Singh [5] also investigate whether EHRs could improve outpatient workflows. However, unlike other information systems, a HIS accesses a lot of sensitive data such as personal information, physiological parameters and health records. The end-users of a HIS nowadays have been extended from physicians in hospitals to patients (or their family) in home. Thus, challenge in a HIS is the transition from the stand-alone systems to the networked ones [6], but the issue of privacy protection has not been given the attention it needs.

This essay has two purposes. Firstly, for the networked HISs, the mechanisms of privacy protection are not in widespread implementation. One of our purposes is to propose a privacy enhanced framework for networked HIS. Secondly, whether a system is secure or not is related to human psychological cognition. A well-implemented IT system is not the guarantee of keeping a sense of safety because users' feeling of security does not completely reflect the technical security level [7]. Providers will work in vain if users are not aware of the precautions for their privacy. The second purpose is to investigate how users' psychological perception of privacy protection affects their adoption of HISs. To complete these purposes, we firstly design and develop a privacy-enhanced HIS as experimental platform to investigate user behavior. The essay would conclude with implications for research and practice. The proposed framework of experimental platform could provide insides for practitioners interested in HIS development; and the results of empirical survey would provide understanding of privacy protection in HISs adoption.

2 Theory and Hypotheses

To investigate user behavior toward health-related systems, we quoted the unified theory of acceptance and use of technology (UTAUT) [8] in support of our research model. UTAUT is one of the most influential models that have been used to evaluate the acceptance of a new technology. This theory posits that four major variables namely performance expectancy, effort expectancy, social influence, and facilitating conditions are of primary relevance in explaining the user intention to adopt an emerging innovation. Particularly, this study puts attentions on the users' psychological perception of privacy protection. Thus, we proposed perceived security and information security literacy as key indicators of using healthcare system. Figure 1 presents the model and its constructs.

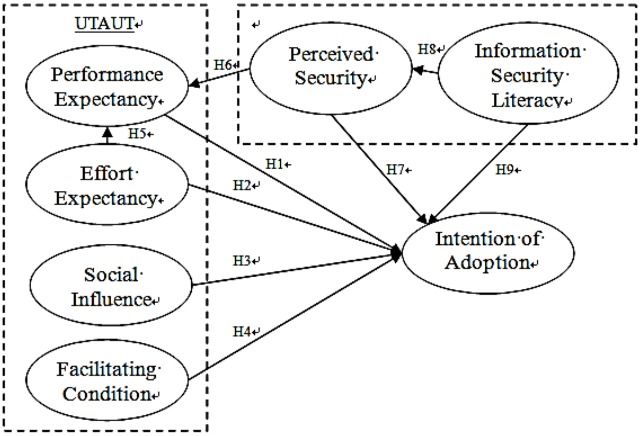

Fig. 1. Research model

2.1 Hypotheses on UTAUT

Modifying the definition given by Venkatesh, Morris [8], we defines performance expectancy (PE) as the degree of which an individual believes that using the privacy-enhanced HIS will help him or her to improves the performance of health management. When coming up with a technology innovation, one of the major concerns for individuals is whether they can benefit by using it. In prior research, PE was shown to possess strong influences on behavioral intention of adopting a new IT [9-11]. Healthcare information systems would advantage users to control over the determinants of their health and thereby improve their health. Especially for patients with chronic disease, the system let users be aware of physiological symptoms such as heartbeats, blood sugar, blood pressure, blood oxygen, and body temperature. Patients can perform regular examinations of self-health management at home or community center instead of going to a clinic. Besides, the health tracking functionality gives assistance to the control of health risk factors. Therefore, we proposed the hypothesis:

***H1**: Performance expectancy positively affects the intention of using privacy-enhanced healthcare information system.*

Effort expectancy (EE) refers to the degree of an individual believes that using the privacy-enhanced HIS is free of effort [8]. Ease-to-use is considered as the essential element during the first time usage [10]. The less effort is required, the more willing users are to adopt a new IT. For example, Zhou and Lu [9] found that users will have more intention to adopt mobile banking system if its interface is easy to learn. Similarly, it takes time and efforts for a newbie to understand how to process healthcare related systems and to get familiar with them. In addition, the amount of effort needed will affect users' evaluation of whether a new IT can improve their job performances [12]. Therefore, we proposed the hypotheses:

***H2**: Effort expectancy positively affects the intention of using privacy-enhanced healthcare information system.*

***H5**: Effort expectancy positively affects users' perception of performance expectancy.*

Social influence (SI) means the degree of which an individual perceives that important others believes he or she should use the privacy-enhanced HIS [8]. Since human cannot live alone, the influence coming family, relatives, or friends would generate powerful impacts on changing their behavior [13]. Prior research has provided empirical support for the effects of social influence on user's behavior of using IT [14, 15]. In terms of health promotion, patients need patience and perseverance to perform the examinations every day. The support of important others in the surroundings is indispensable. Therefore, we proposed the hypothesis:

***H3**: Social influence positively affects the intention of using privacy-enhanced healthcare information system.*

Facilitating condition (FC) is defined to the degree of which an individual believes that resources or knowledge exists to support use of the privacy-enhanced HIS [8]. The conduction of a new IT usually tends to run into many bottlenecks; it needs technological or organizational supports that help to remove barriers to use. Besides, the domain knowledge and skills are necessary for the operation of new IT. For a health-related system, basic healthy knowledge and skills will be required, such as the operation of a sphygmomanometer and the meaning of measured value. The amount of resources one has is considered as a key determinant of IT adoption [9, 16].

***H4**: Facilitating condition positively affects the intention of using privacy-enhanced healthcare information system.*

2.2 Perceived Security and Information Security Literacy

Perceived security (PSY) refers to the degree of which an individual believes that using the privacy-enhanced HIS will be secure [7]. Rather than traditional systems, healthcare information systems cope with private and sensitive data which are directly related to identifiable persons [6]. A general situation is that people would refuse to give authorization of the electronic health records (EHRs) because of privacy concerns [17]. Hence, from the legal perspective, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) emphasizes the necessity to establish the standards for use of electronic data interchange and confidentiality of health-related data.

However, Shin [7] noted that users' feeling of security does not completely reflect the technical security measures. A system with well secure protection will make a futile effort if users do not perceive the sense of precautions. Thus, previous research has indicated that security in cyberspace is subjectively related to human perception such as the image of risk affinity [18]. In e-commerce context, PSY has been considered as the key antecedence of shopping behavior [19]. In addition, PSY will prevent users from using an IT that copes with sensitive transaction such as a mobile wallet system [20]. Since a healthcare information system would conduct the transaction of EHRs, it is importance to investigate the role of PSY in health context. The proposed hypotheses aim to determine how PSY affects the intention to use HISs, directly or indirectly through performance expectancy.

***H6**: Perceived security positively affects users' perception of performance expectancy.*

***H7**: Perceived security positively affects the intention of using privacy-enhanced healthcare information system.*

The other privacy-related factor discussed is Information security literacy (ISL), which refers the ability and knowledge an individual possesses enabling him or her to protect information and systems [21]. Of the same physical security levels, the users' perceptions of security would be different because of their security literacy. Although a secure IT has given users the indication of precautions, individuals with higher ISL, rather than lower ISL, tends to be aware of the security awareness [21]. In addition, the degree of ISL is related to users' behavior of using the secure application [22]. As such, we thus propose relation between ISL, PSY, and the intention of using privacy-enhanced healthcare system.

***H8**: Information security literacy positively affects perceived security.*

***H9**: Information security literacy positively affects the intention of using privacy-enhanced health promotion system.*

3 The Development of Proposed Privacy-Enhanced HIS

The proposed framework has four logical phases: EHRs phase, privacy protection phase, healthcare application phase and multi-roles phase. Firstly, EHRs phase consists of databases storing sensitive information. Secondly, privacy protection phase contains three main modules, namely secure transmission module, privacy protection module and access control module. Thirdly, healthcare application phase includes individual health management module, physiological monitoring module, healthcare education module, and healthcare consulting module. Lastly, multi-roles phase means the users and devices. As shown in Figure 2, when a user performs the healthcare applications by using a PC or physiological testing equipment, all data access should be done through the privacy protection modules.

In healthcare application phase, the individual health management module enables users to manage personal long-term health record in a graphical layout. The physiological monitoring module provides immediate warning of users' physiological data if it does not meet the reasonable ranges. The healthcare education module recommends appropriate health education information to users. The healthcare consulting module enables users to leave an asynchronous message or consult a doctor via video phone synchronously.

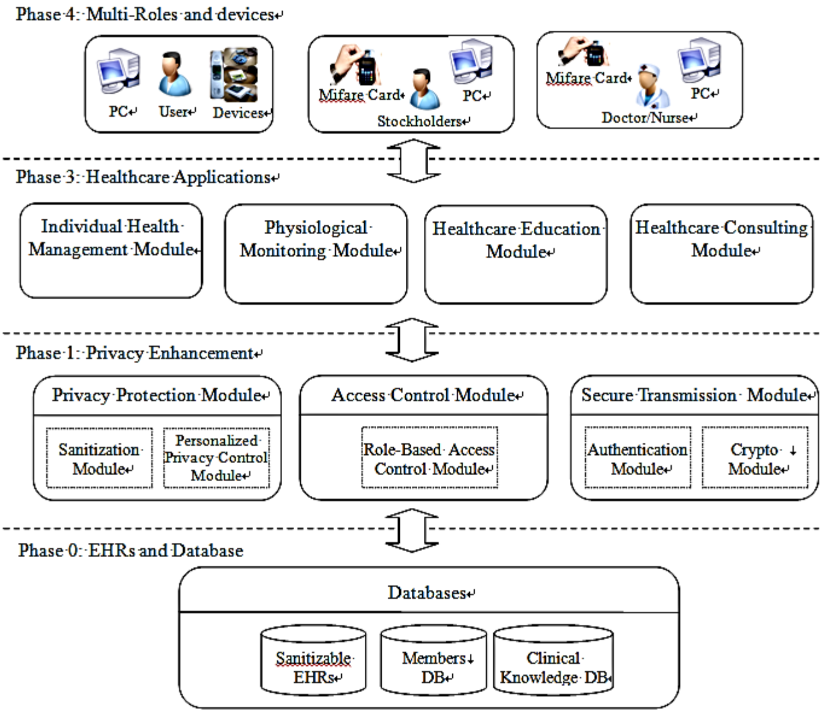
Phase 4: Multi-Roles and devices
PC
User
Devices
Mifare Card
PC
Stockholders
Mifare Card
PC
Doctor/Nurse
Phase 3: Healthcare Applications
Individual Health Management Module
Physiological Monitoring Module
Healthcare Education Module
Healthcare Consulting Module
Phase 1: Privacy Enhancement
Privacy Protection Module
Sanitization Module
Personalized Privacy Control Module
Access Control Module
Role-Based Access Control Module
Secure Transmission Module
Authentication Module
Crypto Module
Phase 0: EHRs and Database
Databases
Sanitizable EHRs
Members DB
Clinical Knowledge DB

Fig. 2. The framework of proposed privacy-enhanced HIS

This study pays attention on privacy-enhanced functionality. Firstly, the secure transmission module prevents physiological information from being eavesdropped by malicious persons. Secondly, the privacy protection module protects user privacy by applying a sanitizable signature scheme. Lastly, the access control module ensures that only authorized users can access system resources, including community information, personal health records and knowledge bases. Secure transmission module is designed to provide a secure wireless transmission between server and physiological monitoring equipment such as body weight machine, blood pressure meter, blood glucose meter, and blood oxygen meter. As EHRs contain sensitive patient information, this study builds a crypto module and applies the Authentication Protocol in ISO standard [23] to identify the legitimacy of these devices as well as user identity. Besides, we encrypt users' physiological data by Advanced Encryption Standard (AES) algorithm to ensure the safety. Privacy protection module is to preserve the confidentiality, integrity, and availability. EHRs, which are mostly private records of patients, should not be leaked out to any third party unless the patients personally agreed to disclose the medical records. This module quotes the conception of sanitizable scheme [24] to shade private information before EHRs is shared within authorized users and in the meantime original digital certificate remains valid. Access control module assures system resources such as EHRs and knowledge bases are only accessed by authorized users. There are multi-roles in HIS system and each role has his own specific security permission. This module applies the Role-Based Access Control mechanism [25] that access permissions are determined by the level of user identity and access control policy.

4 Results and Discussions

The proposed privacy-enhanced HIS and devices were set up in the experimental classroom and totally 315 undergraduates were invited to participate in the experiment. Of the 315 participants, after removing incomplete or invalid questionnaires, we receive 280 usable samples and response rate is 88.9 percent. The participants' ages range from 18 to 29. In terms of gender, 62.9 percent are male and 37.1 percent are female. As for the frequency of going to a clinic for medical treatment, 18.9 percent of participants say they do so about once a week; 18.2 percent go once a month; 33.9 percent are about once a quarter; 17.5 percent only go once annually; 11.4 percent are less than once a year.

The examinations of constructs reliability and validity include factor loading, composite reliability, convergent validity, and discriminant validity. The results are shown in Table 1. Factor loadings, ranging from 0.71 to 0.95, were greater than the threshold value of 0.5. The minimum standard of composite reliability (CR) is 0.7 [26], and our values are between 0.88 and 0.96. The values of average variance extracted from each construct (AVE) were greater than the lowest bound of 0.5 [27]. These results imply that our constructs exhibited acceptable convergent validity. The square root of AVE is greater than any correlation among the constructs, implying that our constructs had acceptable discriminant validity.

The analysis of hypothesis test could give an understanding of what drives users to adopt a privacy-enhanced HIS like ours. Figure 3 presents the results of model testing. In short, all of our hypotheses are statistically supported except H2 (β = -0.02, $p >$ 0.01) and H9 (β = 0.10, $p >$ 0.01). This shows that there exists no direct effect of effort expectancy and information security literacy on the intention of adopting. However, the indirect effect analysis estimated by LISREL discovers interesting findings (see Table 3). First, the effort expectancy has indirect effect on behavioral intention (β = 0.15, $p <$ 0.001). Second, the indirect influence of information security literacy on adoption is also significant (β = 0.09, $p <$ 0.001). Our proposed model explains 65 percent of observed variance in the adoption of the privacy-enhanced HIS.

The study seeks to explore the role of privacy concerns on user willingness to use a healthcare information system. To achieve this purpose, we integrate several secure schemes and implement a privacy-enhanced HIS as our experimental platform. After the experiment about a week we receive 315 usable responses. The analysis results exhibits several findings. First of all, user intention toward using a privacy-enhanced HIS is directly driven by, in order of importance, social influence, perceived expectancy, facilitating conditions, and perceived security. This indicates that users attach great importance to others' suggestions while making a decision on HIS adoption. Thus, the strategy of word-of-mouth marketing would be effective for promotion. For example, providers should pay close attention to what is being said about their HISs in a social network service (SNSs) like Facebook and Twitter, especially negative comments. Meanwhile, they should consider facilitating conditions such as whether there exist sufficient resources supporting their HISs. In other words, the systems should be compatible with existing devices and follow existing international standard like Health Level Seven (HL7). Secondly, the impact of cost-effect on the privacy-enhanced HIS is different from traditional systems; ease of use has no directly impacts on user intention, but affects it indirectly by increasing perceived usefulness. The means performance expectancy might be the mediator variable between effort expectancy and user adoption; the user-friendly interface is not the guarantee of user adoption unless this HIS can improve their healthcare efficiency.

This study addresses on users' information security literacy (ISL) and users' perception of system security (PSY). The mean value of PSY is about 4.23, showing that our experimental HIS receives positive belief of security protection. Our system structure modules could give practitioners insides for developing similar privacy-enhanced HISs. The path analyses show that the increase of PSY could directly enhance intention of HIS adoption; ISL has no direct effects on adoption, but affects it indirectly through PSY, showing that PSY builds the relation between ISL and adoption. That means people with higher ISL would not generate more intention toward adopting HISs unless they are aware of well security protection. Besides, PSY also facilitates the belief of performance expectancy, which is one of the key factors for HIS adoption. In short, providers should endeavor to increase PSY and then make significant enhancement of performance expectancy and user adoption.

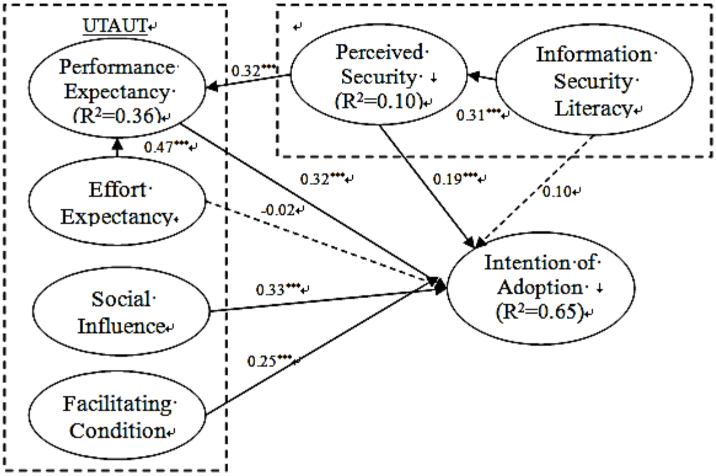
UTAUT
Performance Expectancy (R²=0.36)
Effort Expectancy
Social Influence
Facilitating Condition
Perceived Security (R²=0.10)
Information Security Literacy
Intention of Adoption (R²=0.65)
0.32***
0.31***
0.47***
0.32***
0.19***
0.10
-0.02
0.33***
0.25***

Fig. 3. Analysis results (Note: *:p<0.05; **:p<0.01; ***:p<0.001)

5 Conclusions

This study proposes several implications for research and practice. For academic researchers, this article extends UTAUT to user adoption of privacy-enhanced HISs by integrating the perspectives of perceived security and information security literacy, and the proposed model explains 65 percent of observed variance. Secondly, we find performance expectancy is a key moderator between effort expectancy and user adoption of privacy-enhanced HISs. Besides, perceived security plays an important role that could encourage user adoption as well as increase performance expectancy; security literacy affects user adoption indirectly by increasing the awareness of perceived security. For service providers, this article proposes a framework for a privacy-enhanced HIS and receives positive reactions in the experiment. The functionality of privacy protection, i.e. secure transmission module, privacy protection module, and access control module could give a reference for practitioners to design privacy-enhanced health systems. In practice, practitioners should take account of word-of-mouth effects and whether their systems are compatible with mostly medical testing equipment. There still exists a few limitations should be noted. The implications are suggested on the basis of an experimental study, so caution must be taken while generalizing to other types of systems. The suggestion is based on the 315 participants in the experiment, who are youths with well computer-skill and health-related knowledge; it needs further research if the decision maker of IT in a family is not a young man. Lastly, we take a short-term experiment for convenient and long-term observation can be reserved for further study.

References

1. McKelvey, V.: Spending More on In-Home Care (2010), `http://www.aarp.org/relationships/caregiving/info-01-2010/spending-more-on-in-home-care.html`
2. Häyrinen, K., Saranto, K., Nykänen, P.: Definition, structure, content, use and impacts of electronic health records: A review of the research literature. International Journal of Medical Informatics 77(5), 291–304 (2008)
3. Poissant, L., et al.: The Impact of Electronic Health Records on Time Efficiency of Physicians and Nurses: A Systematic Review. Journal of the American Medical Informatics Association 12(5), 505–516 (2005)
4. Williams, F., Boren, S.A.: The role of electronic medical record in care delivery in developing countries. International Journal of Information Management 28(6), 503–507 (2008)
5. Vishwanath, A., Singh, S.R., Winkelstein, P.: The impact of electronic medical record systems on outpatient workflows: A longitudinal evaluation of its workflow effects. International Journal of Medical Informatics 79(11), 778–791 (2010)
6. Sokratis, K.: Health care management and information systems security: awareness, training or education. International Journal of Medical Informatics 60(2), 129–135 (2000)
7. Shin, D.: Understanding purchasing behaviors in virtual economy: Consumer behavior of virtual currency in Web2.0 communities. Interacting with Computers 20(4), 433–446 (2008)
8. Venkatesh, V., et al.: User acceptance of information technology: Toward a unified view. MIS Quarterly 27(3), 425–478 (2003)
9. Zhou, T., Lu, Y., Wang, B.: Integrating TTF and UTAUT to explain mobile banking user adoption. Computers in Human Behavior 26(4), 760–767 (2010)

10. Davis, F.D.: Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly 13(3), 319–339 (1989)
11. Pai, J.C., Tu, F.M.: The acceptance and use of customer relationship management (CRM) systems: An empirical study of distribution service industry in Taiwan. Expert Systems with Applications 38(1), 579–584 (2011)
12. Premkumar, G., Bhattacherjee, A.: Explaining information technology usage: a test of competing models. Omega: International Journal of Management Science 36, 64–75 (2008)
13. Park, C.W., Lessing, V.P.: Students and housewives: differences in susceptibility to reference group influence. Journal of Consumer Research 4(2), 102–110 (1977)
14. Karahanna, E., Straub, D.W., Chervany, N.L.: Information technology adoption across time: across-sectional comparison of pre-adoption and post-adoption beliefs. MIS Quarterly 23(2), 183–213 (1999)
15. Lewis, W., Agarwal, R., Sambamurthy, V.: Sources of influence on beliefs about information technology use: An empirical study of knowledge workers. MIS Quarterly 27(4), 657–678 (2003)
16. Taylor, S., Todd, P.A.: Understanding information technology usage: A test of competing models. Information Systems Research 6(2), 144–176 (1995)
17. Corey, M.A., Agarwal, R.: Adoption of Electronic Health Records in the Presence of Privacy Concerns: The Elaboration Likelihood Model and Individual Persuation. MIS Quarterly 33(2), 339–370 (2009)
18. Dewan, S., Chen, L.: Mobile payment adoption in the US: A cross-industry cross-platform solution. Journal of Information Privacy and Security 1(2), 4–28 (2005)
19. Lwin, M., Wirtz, J., Williams, J.D.: Consumer online privacy concerns and responses: a power-responsibility equilibrium perspective. Journal of the Academy of Marketing Science 35(4), 572–585 (2007)
20. Shin, D.: Towards an understanding of the consumer acceptance of mobile wallet. Computers in Human Behavior 25(6), 1343–1354 (2009)
21. Wilson, M., Stine, K., Bowen, P.: National Institute of Standards and Technology (NIST) Special Publication 800-16: "Information Technology Security Training Requirements: A Role- and Performance-Based Model (Draft)" (2009), http://csrc.nist.gov/publications/drafts/800-16-rev1/Draft-SP800-16-Rev1.pdf
22. Lin, I.L., Liu, M.D.: An Investigation of High School Teachers' Cyber Security Literacy in Taiwan. In: Taiwan Academic Network Conference (TANET 2007) (2007)
23. ISO/IEC-9798-3, Information technology—Security techniques—Entity authentication mechanisms; Part 3; Entity authentication using a public key algorithm in International Organization for Standardization (1993)
24. Ming, Y., Shen, X., Peng, Y.: Identity-Based Sanitizable Signature Scheme in the Standard Model. Communications in Computer and Information Science 105, 9–16 (2010)
25. Ferraiolo, D.F., Kuhn, D.R.: Role Based Access Control. In: 15th National Computer Security Conference, pp. 554–563 (1992)
26. Nunnally, J.C.: Psychometric Theory, 2nd edn. McGrawHill, New York (1978)
27. Fornell, C., Larcker, D.F.: Evaluating structural equation models with unobservable variables and measurement error. Journal of Marketing Research 18(1), 39–50 (1981)