A Security-Trust based Model for Identity Management Systems Adoption

Ali Alkhalifah

Information Technology Department, Computer College

Qassim University, Qassim, Saudi Arabia

Email: a.alkhalifah@qu.edu.sa

Suleiman Al-Amro

Computer Science Department, Computer College

Qassim University, Qassim, Saudi Arabia

Email: samro@qu.edu.sa

Abstract:

Identity Management Systems (IdMS) aim to support development, productivity and security while lowering costs related to managing users and their identities, credentials and attributes. Users may desire many of the benefits that well-designed IdMS' could potentially offer, such as increased privacy and security. However, users have demonstrated that they are unwilling to spend money or time on security enhancements. This provides the opportunity for a set of end-user requirements to be determined for the adoption of IdMS. Security, trust and privacy are major concerns to consumers and obstacle to the adoption of any innovative technology. This study examines user's intended behavior toward security and trust and how these beliefs could affect their behavioral intention toward using IdMS .The study introduces a security-trust based model for IdMS adoption. This study also suggests positive- mixed methods research to explore and predict a causal model and validate the results. The conclusion of this paper outlines the implications and suggests further directions for future research in this area.

Keywords : *Identity Management Systems(IdMS), adoption, behavior, trust,security.*

I . Introduction

With the advent of Web 2.0 and Web 3.0, online services have emerged that have contributed to the growth of online identities which contain a great deal of information about the user including their personal attributes and behavioral preferences as well as access related metadata. For instance, social networking sites such as Facebook encourage users to create detailed user profiles, and to replicate and develop real world social networks on its site. This represents not only a shift from a technical development perspective, but also the security oriented concept of identity has been shifted to one that is socio-technically driven toward facilitating social interactions and services [1]. The growing use of ICTs in numerous contexts has increased the need to examine closely how we represent ourselves online and who we are actually interacting with. Threatening behaviors in the online world are also on the rise especially those associated with identity theft. Identity affects in a very significant way, the economic decisions that people make [2], and poses security risks targeting both organizations and individuals [3,4]. Nevertheless, whereas proving claims of theft in the normal offline (brick-and-mortar) world is obvious, online identity management seems to be less obvious to consumers [5].

From the user's perspective, IdMS is often not a target in itself but involves a means to facilitate other tasks such as obtaining access to specific services. This means that the adoption of an IdMS by users may often follow the path of least resistance [6]. Users will not likely put much money and effort into the management and control of their identities. Hence, IdMS must consider the need to promote the adoption of IdMS by end-users. In the case of commercial use of IdMS, it is likely that the value of an IdMS will increases as more users adopt it [5]. However, the adoption of IdMS has been slow. For example; the Federated Identity Management (FIM) adoption rate was less than 5% in the U.S. and still lower in other countries [7]. Exploring factors that influence acceptance may increase user adoption. Hence, developing a model that captures salient aspects of IdMS along with factors promoting its adoption is needed particularly from the end-user perspective [8, 9].

IdMS have three major stakeholders: the user, identity provider (IdP) and the relying parties (RP) [10]. Previous IdMS studies have addressed the importance of usability, privacy and security in IdMS. Most of these studies have focused on the more technical issues that deal with the underlying security technologies and on designing privacy protection solutions [11, 12] or providing guidelines about how to design a decentralized web IdMS [6]. IdMS use and the user behavior of IdMS are not well examined in the published literature which is sparse in regard to the topic of directly examining IdMS [9]. Digital identity schemes have been well documented from the providers' perspective and have been examined much less in relation to the perception of IdMS from the user's perspective [13]. Although a few studies have identified and suggested some factors and metrics aimed towards the adoption of IdMS [5,9], to the best of our knowledge, there is no study that empirically explores and measures factors that may impact the user adoption and acceptance of them. This study is an attempt to fill this important gap and to contribute to the literature by conducting research in IdMS adoption in the context of focusing on the security perspective of the end-users behavior.

Therefore, a model of adoption must consider the different aspects of human behavior in such an online environment and provide solutions that are independent of the user's experience. This study aims to examine users' attitudes toward security and trust as well as how the role of these perceptions influences users' behavior.

This paper will address the following questions:

- Q1: How do perceived security and trust affect users' behavioural intention to adopt IdMS?
- Q2: What are the antecedents of trust in the IdMS context?

The rest of the paper is organized as follows. Section 2 introduces and defines some identity related concepts and provides an overview of IdMS. In addition, it discusses security as it relates to IdMS from the user perspective. Section 3 describes the security-trust model proposed in this study. The final section provides a conclusion and discusses future directions of study.

II . related work

A. Identity related concepts

Identity is responsible for determining access rights to sensitive resources for users. An identity describes an *entity* (a person, a computer, an organization, etc.) within a particular *domain*. An identity domain is a scope where each identity is unique [15]. Formally, the identity of an entity within a domain consists of the set of all characteristics (unique or non-unique identifiers) that have been attributed to this entity within the particular domain.

A digital identity is a digital representation of one or more principals that are unique to that principal (or group), and that act as a reference to that principal (or group). In terms of its content, most scholars refer to digital identity as related a set of identity information i.e. data relating to a person. Roussos *et al.* [16] declare that digital identity is the electronic representation of personal information of an individual or organization (name, phone numbers, address, etc.). It refers to how people are identified on computer systems and over the internet [15]. An individual's digital identity may include many different identities, issued by many different providers, and these will be used as well as trusted by the organization that issued them.

Identity 3.0 is a tool of new world identity. Identity 1.0 was the world of physical documentation such as ID cards, signatures and fingerprints. Identity 2.0 was user names and passwords used on diverse websites and for accessing a myriad of services. Identity 3.0 tools encompass more global identifiers such as OpenID, i-names, and Information Cards or InfoCards. According to Sigel [17], some basic principles of Identity 3.0 include:

- Online, the user is in the center; web sites and services cluster around the user, and he/she is always logged in.
- Fewer passwords are better, but the user can have as many passwords as he/she likes.
- Third-party brokers will assist the users in connecting with others with the understanding that this will occur without the broker giving away sensitive information.
- The users authorize third parties to do only those things that they want them to do on their behalf and nothing else.
- The user can create as many identities as he/she wants; each identity gives access to its own services and communities.
- Identity 3.0 tools help prevent phishing, fraud, identity theft, and other common cyber-crimes.

B. Identity Management Systems

IdMS is a confusing concept, because the different stakeholder's concerned (users, service providers, and relying parties) have different requirements and different perspectives. IdMS have also been defined as; the integration of important personal information from multiple systems into one collaborative and unique identity [18]. We define IdMS as the process of using emerging technologies to manage information about the identity of users and control access to business resources [3]. The goal of identity management is to foster productivity and security while lowering the costs related to managing users and their identities, credentials and attributes.

Diverse parties participate in IdMS in different ways. Their participation can be classified by roles, taking into consideration that any individual participant or set of participants can play multiple roles (both at the same time and at different times) [10]. These roles within the IdMS are:

- **Subjects:** are users of digital services. Subjects may act on their own behalf (as individual citizens, customers), or in roles within organizations, companies or government departments.
- **Identity Providers (IdP):** issue identities. For example, individuals might use self-issued identities in contexts such as signing on to Web sites, credit-card providers might issue identities that enable payment, businesses might issue identities to their customers, governments might issue identities to citizens.
- **Relying Parties (RP):** an individual, organization or service that depends on claims issued by a claims provider about a user to control access to and personalization of services.

C. Security from the user perspective

Security of IdMS is one of IdMS aspects that is of great importance to both organizations and individual users. However, advantages and motives for having secure IdMS vary both within and between these two groups. Personal information that is stored in IdMS needs to be secured so that it cannot be obtained by unauthorized persons. Loss of identity information could have a wide range of consequences for users and undermines the user's trust [5]. The number of identity theft complaints, and the number of data breaches, has been increasing [4]. These two issues are main concerns for customers who interact online regularly. Identity affects, in a significant way, the economic decisions that people make [2], because some digital identities are used to retrieve money from bank and credit card accounts. Although a significant amount of the economic loss resulting from identity fraud is carried by businesses [19], the costs in the end always carries over to the customers themselves in the form of increased cost for goods and/or fees for services. The Federal Trade Commission (FTC) estimates that identity theft costs customers about fifty- billion dollars annually [20]. Loss of identity information can also lead to damage to the individual's reputation. In 2008, for example, about 9.9 million Americans were reportedly victims of identity theft. This is an increase of 22% over the estimated 8.1 million who were victimized in 2007[4].Sherman [21] argues that while data breaches continue, user acceptance of new business tools will remain slow. Therefore, the security issues have a negative effect on end-users that may generally affect their intention to adopt new Information Technology (IT) and in particular the use of IdMS.

Conversely, the potential to provide increased security that could be offered by IdMS might increase the general trust in electronic services, and consequently improve the possibilities for making use of ICTs for communication and transactions [5]. Therefore, users have a concern in the security of IdMS. Loss of personal data because of insecure IdMS would have a negative effect on the use and supply of electronic services, whereas trusted and secure systems could lead the way for the acceptance of more efficient and effective services for the end-users.

III . research model

In particular, trust and security are integrated into the comprehensive framework as shown in Fig.1. The conceptual model states that the behavioral intention to use IdMS is a function of some constructs which include security and trust. We consider security variable as a source of trust The model does not illustrate each hypothesis with a specific linkage, but provides a means to organize the primary constructs and relations in this study.

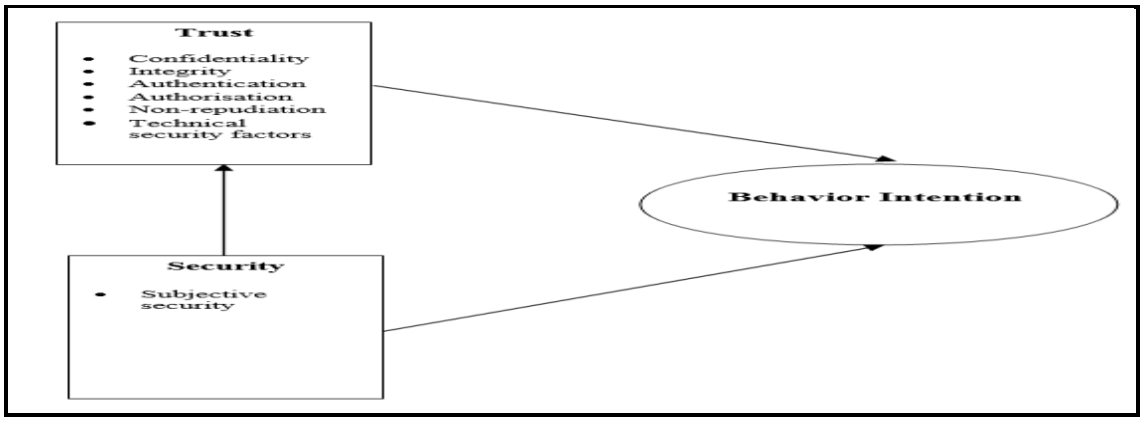

Figure1. Security Trust based model for IdMS adoption.

Behavioral Intention

In the proposed model the behavioral intention to use is taken as the output variable. Behavioral intention to use is defined as 'a user's intent to use an IdMS'. We have chosen to use behavioral intention as a substitute for actual behavior, and have set the importance of the intention to use variable as a determinant of the user's adoption of technology [22]. Intention has been noted to be a good predictor of systems usage [23]. In addition, some researchers argued that intention has a main impact on behavior in mediating the effect of other determinants on behavior [24].

Security

The security concern has been raised in the context of IT. Customers are not able to evaluate the technicalities of objective security [25]. Hence; this study adopts *subjective security* which is defined as "the degree of the perceived sensation of the procedures' security from the viewpoint of the customer." [25]. Thus, subjective security can be seen as the mirror image of risk affinity. Security does not depend on technical security measures alone [26]. Hence, this study approaches perceived security from a broader viewpoint that consists of not only technical issues , such as confidentiality, integrity, encryption, authorization and authentication but also users' complete sense of security and well-being. Although security is a technical commodity based on knowledge, risk assessment and competent delivery of viable solutions to problems, it is the users' perceptions of security that impact trust and intention to adopt [25]. Some researches argue that users refuse to use a particular system because of the lack of subjective security [27, 28]. Therefore, when IdMS are known to have implemented security mechanisms, users tend to believe that these systems are safe. Many studies have examined the role of security and its relation with intention to use in variety IT contexts such as e-commerce, internet banking [29] and mobile commerce [30]. Shin [14] examined the effect of security, trust

and privacy on the adoption of social networks. The results of his study reveal that perceived security moderates the effect of perceived privacy on trust and showed that security is positively related to trust. Therefore, we propose that security has an impact on users' trust and on their intention to use an IdMS.

Trust

Gaining a user's trust is crucial for the success of any innovative IT. Users' perceptions of security influence trust in online transactions [31]. The perception of risk affects trust. Trust is linked to increased risk-taking behavior and a reduction in opportunistic behavior [32]. Trust is defined as "*the belief that allows individuals to be willing to react after having taken the characteristics of the providers and the underlying Internet infrastructure into consideration*" [32, p: 505]

Trust in IdMS is a behavioral belief related to the perception of security in using a particular IdMS. This may be guaranteed by a security IdP and SP by using specific mechanisms such as encryption or digital signatures. Trust is a significant belief of IdMS; and participants need to be educated on security features so that they will understand that they are in place and trust can be established. Moreover, due to the reliability of IdMS and its measurements against risks, information and education needs to be provided to the users in order to gain their trust [5]. In this study, trust is realized by means of the standard user interface and consistent representation of digital identities for all IdMS [5].

Moreover, trust depends on a consistent user experience and social setting which engenders confidence in the user regarding the ability of the system designers [32]. For the users, trust factors that relate to the technical security of IdMS are important .These factors include reputation, previous experiences, security seals, and external audits. Trust is particularly important with regard to accessing or requesting the user's personal data. Theoretically, confidentiality and integrity can be realized by the user himself applying cryptographic mechanisms. However, the confidentiality, integrity and availability of authentication data once it is being stored by the identity provider might still put the user's information at risk [5].

Trust is often viewed as a three-dimensional construct of competence, integrity, and benevolence [32]. In the area of IdMS, trust has some additional factors including confidentiality, integrity, authentication, authorization, non-repudiation and technical security concerns involving such things as protection of reputation, previous IT security experiences, security seals, and external audits [5, 33] (see table1).

Recent information systems studies point out that trust is an important predictor in the acceptance and use of new technology [34, 32, 35]. In addition; trust help to understand the perception of risk [36, 32]. Hence, we propose that trust has a positive influence on the end-user and increases the individuals' intentions to use IdMS.

TABLE 1. DIMENTIONS OF TRUST IN IdMS (Source: [49] and [5]).

Trust Construct	Definition
Confidentiality	Ensures that transaction information cannot be viewed by unauthorized persons.

Authentication	The transaction information actually originates from the presumed transaction partner.
Integrity	The transaction information remains intact during transmission and cannot be altered.
Authorization	Parties involved must be able to verify if everyone involved in a transaction is allowed to make the transaction.
Non-repudiation	No one should be able to claim that the transaction on his/her behalf was made without their knowledge.
Technical security	Reputation, previous experiences, security seals, and external audits.

IV . Methodology

This study will use one of the most popular mixed methods designs in different research: Sequential Transformative design [37]. This model has two distinct data collection phases (qualitative and quantitative) one following the other, and priority could be given to any phase [37]. Creswell [37] states that "By using two phases, a sequential transformative researcher may able to give voice to diverse perspective, to better advocate for participants, or to better understand a phenomenon or process that is changing as a result of being studied" (p.213). Under this view, this study will employ this design (see figure 2) to help developing the framework as well as identify the indicators and measures. In this study, the Sequential Transformative is categorized by the collection of qualitative data followed by the collection and analysis of quantitative data. The priority in this design is given to the qualitative phase, because the qualitative research presents the major aspect of data collection and analysis in the study, focusing on in-depth explorations of the phenomenon. In addition, the qualitative element helps in developing the research model and forming hypotheses (Creswell, 2003).

In the first phase, a qualitative interview and focus groups methods will be used to collect data. The goal of the qualitative phase is to an empirically devise set of dimensions, categories and aspects which is suitable to develop the research model and serve as a basis for the selection of appropriate indicators and measures for the next phase.

In the second phase, the quantitative numeric data will be collected using a survey method. The survey method will be used to test the research model because it allows replicability, provides the basis for establishing generalizability, and has statistical power [38]. The quantitative data and its analysis will be measured and described by representing and testing the hypotheses and exploring participants views in more depth.

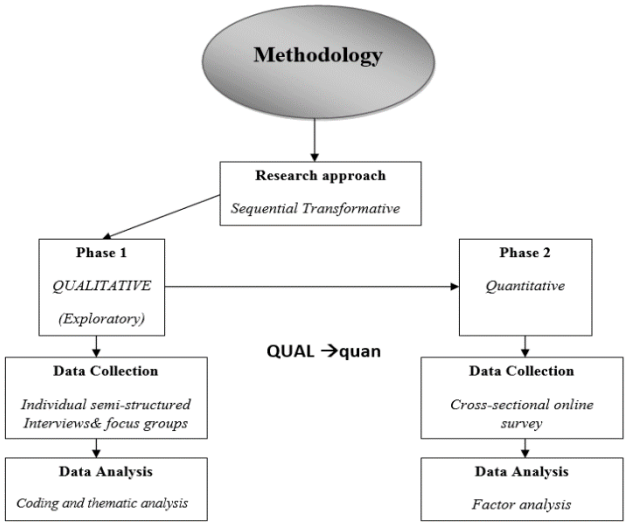

Figure2. Research Methodology.

V . Conclusion and Future Work

This paper proposes a security-trust based model for IdMS adoption from the end-user perspective. Using the proposed model and methodology, this study will develop and validate a road map to measure security and trust perceptions related to the end-users' behavior and potential for IdMS adoption. We have examined these security issues from the academic perspective and will provide general guidance for IT practitioners and particularly for IdMS designers and providers. From a theoretical viewpoint, this study contributes specifically to IdMS and the adoption of IdMS through IT design in several ways. It provides a new framework for the adoption of IdMS by identifying antecedents of user behavioral intention. Furthermore, recently, there has been research done which attempts to establish the relationship between security-related factors such as security and trust by clarifying slight differences between these very similar variables. Therefore, this study contributes to the literature by establishing the relationship and correlation between these security-related factors. From a practical viewpoint, the current study would provide valuable insights for IdMS providers and designers. IdMS providers and designers face the challenge of creating security and privacy polices [33, 9] in an environment which faces resistance to adoption especially at the individual level [8, 9]. The proposed framework offers an increased understanding of user's concerns (security and trust) which in turn will provide designers a tool that can be used to develop trust-building mechanisms and risk-reducing strategies which will encourage IdMS adoption.

Future work would collect and analyze the qualitative data. After that, it will start the second phase to revise and validate the framework by measuring the causal network of relations in the model through an empirical investigation using survey instruments that will be developed in the qualitative phase.

REFERENCES

[1] M. McLaughlin, G.Briscoe and P.Malone,(2010,Oct) ,*Digital Identity in The Absence of Authorities: A New Socio-Technical Approach*[online]. Available: http://arxiv.org/abs/1011.0192

[2] G. A. Akerolof and R. E. Kranton, "Economics and Identity," *The Quarterly Journal of Economics*, vol. 115,no.3, 2000, pp. 715-753.

[3] S. C.Lee,"An Introduction to Identity Management," SANS Institute InfoSec Reading Room, 2003.

[4] K. M. Finklea, ''Identity Theft: Trends and Issues,'' Congressional Research Service, 2010.

[5] WP3, S.Poetzsch, B.Priem, R.Leenes and R.Husseiki," D3.12: Federated Identity Management – what's in it for the citizen/customer?," Future of Identity in the Information Society (FIDIS),2009.

[6] R. Dhamija and L. Dusseault, "The Seven Flaws of Identity Management: Usability and Security Challenges," *IEEE Security & Privacy*, 2008, pp.24-29.

[7] A.Cser and J. Penn ," Identity Management Market Forecast: 2007 To 2014 Provisioning Will Extend Its Dominance Of Market Revenues," Forrester Research ,Feb.2008.

[8] P.Seltsikas and R.M. O'Keefe, R. M,''Expectations and outcomes in electronic identity management: the role of trust and public value,''*European Journal of Information Systems*, vol. 19, 2010, pp. 93–103.

[9] K.Ivy, S.Conger and B.J.Landry , "30P. Federated Identity Management: Why is Adoption so Low?," *Proc . Int.Conf.on Information Resources Management*, 2010.

[10] K.. Cameron, R.Posch and K.Rannenberg, "Proposal for a Common Identity Framework:A User-Centric Identity Metasystem ,''2008.

[11] A.Jøsang,M. AlZomai and S.Suriadi, "Usability and Privacy in Identity Management Architectures," *Proc . the 5th. Australasian sym. on ACSW frontiers*, Ballarat, Australia ,2007,pp. 143 - 152 .

[12] A. M.Rossudowski, H.S.Venter, J.P.Eloff and D.G.Kourie,''A security privacy aware architecture and protocol for a single smart card used for multiple services,''*computers & security*,vol. 29,2010,pp. 393 – 409.

[13] C.Satchella,G. Shanksa, S. Howardab and J.Murphy,''Identity crisis: user perspectives on multiplicity and control in federated identity management,*''Behavior & Information Technology*,vol.30.no.1.2009,pp. 1-12.

[14] D.H.Shin, "The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption," *Interacting with Computers*, vol. 22, 2010. pp. 428–438.

[15] A.Josang and S.Pope,'' User centric identity management,'' *Proc. AusCERT Conf.*, Gold Coast, Australia, 2005, pp. 77–89.

[16] G.Roussos, D.Peterson and U.Patel," Mobile identity management: an enacted view," *International Journal of Electronic Commerce*, vol.8, 2003, pp. 81-100.

[17] M.Siegel,Pull: The Power of the Semantic Web to Transform Your Business, Portfolio, 2009.

[18] M. E.Meints, (2009), *D3.17: Identity management systems – recent developments*, FIDIS, [online] Available: http://www.fidis.net/fileadmin/fidis/deliverables/new_deliverables3/fidis-wp3del3.17_Identity_Management_Systems-recent_developments-final.pdf

[19] R. G. Brody, E. Mulig, and V. Kimball, "Phishing, pharming and identity theft," *Academy of Accounting and Financial Studies Journal*, vol.11, no.3, 2007.

[20] Federal Trade Commission (FTC)," Consumer Sentinel Network Data Book for January – December, 2010", March.2011.

[21] E. Sherman, (2010, July), *Apple and Other Tech Firms Must Fix Customer Security Glitches* [online].Available: http://www.bnet.com/blog/technology-business/apple-and-other-tech-firms-must-fix-customer-security-glitches/4382

[22] P. Legris,J. Ingham and P. Collerette, "Why do people use information technology? A critical review of the technology acceptance model,'' Information *& Management,* vol. 40, no.3,2003, pp. 191-204.

[23] V.Venkatesh, M.G. Morris, G.B.Davis and F.D,"User Acceptance of Information Technology: Toward a Unified View," *MIS Quarterly,* vol. 27, no. 3, 2003, pp. 425-478.

[24] I. Ajzen and M. Fishbein, *Understanding Attitudes and Predicting Social Behavior*: Prentice-Hall, Englewood Cliffs, NJ, 1980.

[25] K.Linck, K.Pousttchi and D.G.Wiedemann," Security issues in mobile payment from the customer viewpoint," *Proc. 14th European Conf. on Information Systems*, Gothenburg, Sweden, 2006.

[26] J. C.Roca, J.Garcia and L.D.Vega,"The importance of perceived trust, security and privacy in online trading systems," *Information Management and Computer Security,* vol.17,no.2,2009.pp. 96–113.

[27] C.Cheung, G.Chan and M.Limayem," A critical review of online purchase behavior: empirical research," *Journal of E-Commerce in Organizations,* vol. 3, no. 4, 2005, pp. 1-19.

[28] K.Pousttchi, "Conditions for acceptance and usage of mobile payment procedures," *Proc. the Int. Conf. on Mobile Business*, Vienna, Austria, 2003, pp. 201–210.

[29] T. C. Cheng, *D.* Lam and *A.* Yeung, "Adoption of internet banking: An empirical study in Hong Kong," *Decision Support Systems* vol. 42, 2006, pp. 1558–1572.

[30] P.Schierz, O.Schilke and B.Wirtz, "Understanding consumer acceptance of mobile payment services: An empirical analysis,'' *Electronic Commerce Research and Applications,* Vol. 9,2010,pp. 209–216.

[31] B.Friedman, P.Kahan and D.C.Howe," Trust online," *Communications of the ACM,* vol.43,no.12,2000,pp. 34-40.

[32] V.Cho, "A study of the roles of trusts and risks in information-oriented online legal services using an integrated model," *Information &Management,* vol. 43, 2006, pp. 502–520.

[33] M.Hansen, *et al.*," Privacy-Enhancing Identity Management," *Information Security Technical Report,* vol.9,2004.

[34] S. Ha and L. Stoel, "Consumer e-shopping acceptance: Antecedents in a technology acceptance model," *Journal of Business Research*, vol. 62, 2009, pp. 565–571.

[35] X.Luo, H.Li, J. Zhang and J.P.Shim,"Examining multi-dimensional trust and multi-faceted risk in initial acceptance of emerging technologies: An empirical study of mobile banking services," *Decision Support Systems*, vol. 48, 2010, pp. 222-234.

[36] P.Pavlou and D.Gafen," Building effective online marketplaces with institution-based trust," *Information Systems Research*, vol. 15, no. 1, 2004, pp. 37–59.

[37] J. W. Creswell, *Research Design Qualitative, Quantitative and Mixed Methods Approaches*, 2nd ed. Chennai, India: Sage Publications, 2003.

[38] W. W. Chin, J. B. Thatcher, and R. T. Wright, "Assessing Common Method Bias:Problems With The ULMC Technique," *MIS Quarterly* vol. 36, pp. 1003-1019, 2012.