Sep. 30
International Journal of advanced studies in Computer Science and Engineering
IJASCSE Volume 4, Issue 9, 2015

A Secure Location-Based Privacy Preserving Framework for M-Learning Adoption to Enhance Distance Education in Kenya:Work in Progress

Peter B. Obiria
Jomo Kenyatta University of Agriculture and Technology,
Nairobi,Kenya.

Micheal W. Kimwele
Jomo Kenyatta University of Agriculture and Technology,
Nairobi,Kenya.

Wilson K. Cheruiyot
Jomo Kenyatta University of Agriculture and Technology,
Nairobi,Kenya.

***Abstract*— Location-based privacy in mobile learning is essential to retain users' trust, key to influencing usage intention. Any risk on privacy can negatively affect users' perceptions of a system's reliability and trustworthiness. While extant studies have proposed frameworks for mobile technologies adoption into learning, few have integrated privacy aspects and their influence on m-learning implementation. The aim of this research is to study m-learning literature in order to propose and develop a privacy-preserving framework which can be used to foster sustainable deployment of m-learning within open and distance education in Kenya. The framework would provide University educators with planned approach to incorporate privacy preserving techniques in m-learning implementation. Also, it could provide informed guidance to mobile learning application developers on the need to cater for learners' privacy aspects.**

Keywords- Location privacy; mobile learning; security; distance education

I. INTRODUCTION

The upsurge of mobile devices and their capabilities thereof in the last few years has made mobile learning (m-learning) to establish itself as a learning more accessible, personalized and flexible for students [19]. Whether formal or informal, m-learning, has significantly evolved over the years from the laptop era to the current generation of ultramodern smartphones [21].

Therefore, with the advent of smart phones equipped with mobile sensing technology into education realm, large scale collection of personal specific data is now possible. Typical sensor information which include GPS, Location, WLAN, cell tower ID, browsing history, microphone and so on; make it easy to infer a user's home address, office location, when and means of movement among others from this personal Big Data collected. Through statistical modelling over the sensor data time-series, it is possible to infer behavior patterns of the user such as their outdoor [17] and indoor [27] mobility patterns. Consequently, such personal data if not protected has serious privacy effects, including a hindrance to seamless adoption of mobile learning technologies.

Preserving location privacy of the learner while sensitive data is stored or processed in m-learning systems is a non-trivial concern. Therefore, a secure location-based privacy mechanism is essential to retain users' trust, key to influencing the intention to use any new technology. This is because any risk on privacy can have drastic effects on users' perceptions of a system's reliability and trustworthiness [20] In the context of m-learning, the provision of privacy-preserving mechanisms is key to safeguard private sensitive data [18] and her presentation in a UNESCO mobile learning symposium, revealed several challenges facing m-learning implementation, among them being data security, privacy and trust. It is therefore the endeavor of this study to establish a location-based privacy preserving framework that can be used to evaluate user location privacy aspects in m-learning domain.

Kenya like other countries in the world is grappling with upsurge in her university distance learning enrollment; fuelled by increased need for education and social-economic factors. However, due to dynamic technological change, the modes of delivery introduced by these institutions have constantly evolved from the crude correspondence, to e-learning and now m-learning. Universities have developed a great interest on how to engage mobile technologies in making learning of students more interactive and supported anywhere, anytime and on the go. Ambitious projects are ongoing with some institutions already rolling out distance learning using portable mobile equipment. This study would follow a schematic diagram as shown in Figure 1 below.

Figure 1: Schematic Diagram for the Study

II. PROBLEM STATEMENT

Developments in mobile learning have seen the adoption of high power, location-aware mobile gadgets like smartphones and iPad in distance education which offer additional freedom through service mobility. However, lack of security and privacy awareness on unauthorized user's location data collected by these devices could hamper sustainable adoption of m-learning systems. This is because data collected can be used by ruthless businesses to overwhelm a mobile device with spam related to that individual's location, leading to overload of m-learning device already known to contain low processing power, resulting to denial of service. In addition, the data collected can lead to stalking and intrusive inferences that could result to user profiling which is generally unacceptable.

III. JUSTIFICATION

Security and privacy aspects in m-learning are quite different from those tackled in e-learning context which is a result of users being worried about the use of sensitive personal data collected without their implicit consent. Mobile devices have the ability to leak its user's location and consequently tracking their movement in space. Vulnerability issues in mobile technologies are becoming common due to lots of ad-hoc mobile networks, high penetration of mobile devices and lack of user security and privacy awareness.

IV. OBJECTIVES

- To determine how secure location-based privacy relate to intention to use m-learning systems.
- To evaluate extant m-learning frameworks in preserving learners' location-based privacy.
- To develop a secure location privacy preserving framework for evaluating learners' behavioral intention to use location-aware m-learning systems.
- To evaluate the effects of the identified constructs on the intention to use m-learning for distance education in Kenya.

V. RESEARCH QUESTIONS

In order to fulfill the above objectives, the study aims at seeking answers to the following questions:

- How does secure location-based privacy relate to intention to use m-learning systems?
- How do extant m-learning frameworks address learners' location-based privacy?
- How can a secure location privacy preserving framework be developed to evaluate learners' behavioral intention to use location-aware m-learning systems?
- What is the effect of the identified constructs on the intention to use m-learning system for distance education in Kenya?

VI. LITERATURE REVIEW

In this section the researcher sought to clarify the concept of location-based privacy in mobile learning to build a stronger case for the study.

A. Privacy

The term "privacy" covers a number of facets, and has seen varying definitions proposed. The first distinction is that often made between bodily privacy (concerned with protection from physically invasive procedures, such as genetic testing), communication privacy (concerned with security of communications, like mail and email), territorial privacy (concerned with intrusions into physical space, like homes and workplaces), and information privacy (concerned with the collection and handling of personal data) [3] In regards to "information privacy," Alan Westin, a privacy pioneer, developed one of the most influential and commonly quoted definitions: "Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to *others* [24]".According to [25]privacy is the condition culminating through authorizing and authenticating users, to ensure data integrity and protecting the personal information against unattended access. These authors, on the context of m-learning further clarifies that while security is a methodology of ensuring integrity of data and protecting policies of the institution; privacy, is maintaining of an environment where the student can control how his private information is stored and shared. In contrast, [26] treats privacy as an internalized norm embedded in the daily life of people engaged in social pursuits. While, [22] argues that privacy is a right to an appropriate flow of information, where appropriate is defined by the context in which the information is generated, disclosed and used. The author adds that privacy rules are context-based informational norms that govern the

transmission of information to protect the integrity of the context.

Mobile technologies provide several possibilities for constantly monitoring learners in regards to protecting user privacy. However, this may sometimes be regarded as trampling on user's privacy sphere. While, collecting and evaluating personal data such as user's preferences and goals could be essential to provide assistance for learners, achieve assessment, or ease collaboration between users; it may become a tradeoff between preserving user's privacy, monitoring and controlling learner's behavior [18]. For example, the monitoring of learners content of communication, geographic location, and/or browsing behavior may be easily assumed to lead to profiling the user in the mid or long term. So, a privacy-preserving mechanism is needed to enable users to be identifiable only when necessary or if they wish.

Location privacy is a special type of information privacy which concerns the right of individuals to determine for themselves when, how, and to what extent location information about them is communicated to others [7]. Therefore, control of location information is a key concern in location privacy. Location privacy is key to this study due to recent developments in mobile learning that has seen adoption of high power, location-aware mobile gadgets like smartphones and iPad in distance education.

B. Location-based Privacy and M-learning Usage Intention

This section presents a case to justify that location-based privacy is worth protecting through a description of various identifiable goals for an ideal location privacy preserving m-learning system. It also includes the challenges germane to location privacy and detailed description of probable effects of vulnerable m-learning location environment.

1) Learners' Location-based Goals

One of the areas of concern in location privacy preservation is user's identity. According to [7], hiding user's identity while keeping the position of the anonymous mobile object visible to clients is one of the possible goals to ensure privacy. The identity of a user can be her name, a unique identifier, or any set of properties uniquely identifying the user. If a user publishes position information without personal information, an attacker can still try to derive the user's identity by analyzing the position information and additional context data such as the visited objects. In general, quasi-identifiers can be used to identify the user as shown in [28].

Another protection goal is to provide position information of a user only with a given precision to clients. For instance, a user might want to provide precise position information to his friends, while coarse positions with city-level granularity are provided to a location-based news feed service. Preserving temporal information is one other expectation that learners would want protected.

2) Challenges Germane to Location-based Privacy

According to in [7], key risks related to failure to protect location privacy within a location-aware computing environment includes:

- *Location-Based Spam:* Location could be used by unscrupulous businesses to bombard an individual with unsolicited marketing for products or services related to that individual's location. Location-based "spam" would lead to overload of an m-learning device which is already known to contain low processing power, eventually resulting to denial of service.
- *Personal Wellbeing and Safety:* Location is indivisibly linked to personal safety. Unrestricted access to information about an individual's location could potentially lead to harmful encounters, for example stalking or physical attacks. Personal safety and wellbeing could affect adoption in that, the moment learners would realize that their whereabouts can easily be tracked and the obtained data used to cause physical injury, then few people will be willing to adopt m-learning.
- *Intrusive Inferences:* Location constrains access to spatiotemporal resources, like meetings, medical facilities, homes, or even crime scenes. Location can therefore be used to infer other personal information about an individual, such as individual's political views, state of health, or personal preferences. Many people would want their information kept private and on occasions when their location data can be accessed and even more information deduced, it becomes a fundamental concern that could hamper seamless adoption of m-learning in education.

3) Effects of Unsecured Location-based Privacy to M-learning Adoption

Failure to protect location privacy within a location-aware computing environment could result to a number of negative effects. For instance, a porous location could be used by ruthless businesses to overwhelm an individual with unsolicited marketing for products or services related to that individual's location. This could lead to overload of an m-learning device which is already known to contain low processing power, eventually resulting to denial of service. Uncontrolled access to information about an individual's location could potentially lead to harmful encounters, like stalking or physical attacks. This could affect adoption in that, the moment learners realize that their whereabouts can easily be tracked and data obtained used to cause physical injury, then few people will be willing to adopt m-learning. Finally, open location access can lead to intrusive inferences. Since location constrain access to spatiotemporal resources, like meetings, medical facilities, homes, or even crime scenes. It can therefore be used to infer other personal information about an individual hence, a fundamental concern that could hamper seamless adoption of m-learning in education.

C. A Review of Extant Theoritical Frameworks

1) The Learning Environment, Learning Processes and Learning Outcomes (LEPO) [12].

In this case the authors conceptualize learning as having three components which are: Learning Environment (which

facilitates learning), Learning Processes -the activities which are part of learning and Learning Outcomes -the knowledge, behaviors, skills or understanding which can be demonstrated. Two general actors interact with these three components, the student and the teacher.

This framework is derived from, and encompasses, various models of learning as well as research about the characteristics of students and teachers. The LEPO framework, while inclusive of all aspects of learning, is largely pedagogically neutral, because it does not specify how students and teachers interact with learning environments, processes and outcomes. At the same time, it is a very broad framework, seeking to include other models and frameworks as subsets of the LEPO 'whole'. Additionally, in the context of privacy preservation, it is also found to lay deficient and cannot be relied upon to preserve learners' location privacy.

2) Examining the Impact of Privacy, Trust and Risk Perceptions beyond Monetary Transactions: An Integrated Model [11].

This study was designed to build an integrated model from existing theories to examine the effect of privacy, trust, risk and related factors on two activities: online transactions and online privileged information searching. The difference in the requirements for privacy and the accuracy of the provided personal information between the two activities were both found to have an effect on the privacy control opportunities that a consumer can exercise. The study majored on offering empirical evidence of privileged information searching, its antecedents and its relationship with online transactions. Whereas our study has borrowed a considerable number of constructs from this model, it does not offer a direct solution to location privacy, a gap we would want to fill.

3) A framework for Sustainable Mobile Learning in Schools [10]

This framework was created to explain the findings and actions of a three-year project investigating M-learning in a secondary school in Australia. It is based on a person-centered model involving leadership and management, teachers, students, technicians and community. The aim of the framework was to explore the varied influences on the sustainability of M-learning programme in schools using PDAs.

The model identified and majored on five components for sustainability of ICT in education which includes: economic sustainability, social sustainability, political sustainability, technological sustainability, and pedagogical sustainability. Therefore this model is seen to run deficient of both security and privacy factors that could influence the intention to use m-learning systems.

4) Toward A Sustainable Deployment of M-learning: A conceptual Model in Higher Education [9]

The authors in this study aimed to develop and evaluate a sustainable M-learning deployment model for higher education with pre- and post-deployment stages. They identified critical success factors essential for successful deployment of m-learning systems. The identified factors for pre-deployment stage included: Cross Management Initiative, Awareness and Motivation, On-going technical support, Usability, and On-going M-learning Innovation. They identified the following factors for post-deployment: Quality of Service, continuous usability testing, Trust and Confidence, Availability and suitability of learning materials, collaborative learning, and achievement evaluation. The model was based on analysis of existing literature and results obtained from two of their previous studies [9], to determine the student readiness for mobile learning. This model just like the others described herein above does not present anything to do with location privacy of users of mobile equipment.

D. Our Location Privacy Preserving Framework

Prior research on privacy has focused on what motivates or hinders personal information disclosure. Among the studies, the construct of privacy concerns is one that feature most in information systems research. Consistently, our study follows the direction of technology adoption literature as described in [11] [16] by specifying a model that directly captures several constructs of these authors. We bring onboard the construct of privacy awareness and investigate its impact on intention to use and its correlation with privacy concerns. This is shown on Figure 2 below.

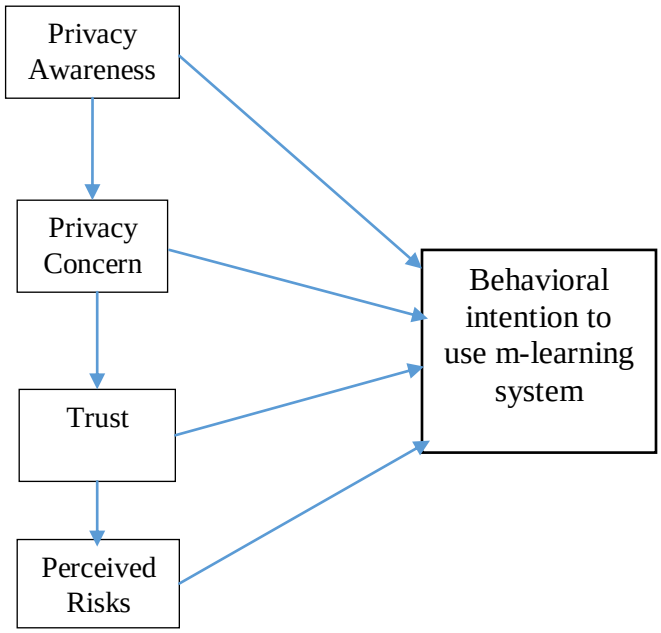

Figure 2: Conceptual Framework

1) Behavioral Intention

The main variable of interest in this study is Behavioral Intention to use location-aware m-learning system. Several studies have already asserted that behavioral intention is the fundamental determinant of actual behavior. Consequently, a number of literature reviews have listed numerous variables that act as factors influencing behavioral intention as shown in the listing by [1]. In the listing, this study focuses on works by [11] [27], which has proposed

Perceived risk, Privacy Concerns and Trust as factors influencing behavioral intention. This study adds the concept of privacy awareness and endeavors to establish its impact on usage intention as well as the correlation with other variables

2) Privacy Awareness

Privacy awareness comes from the concept of social awareness, a passive involvement and raised interest in social issues like naming the problem, speaking out, consciousness raising and researching [37]. On the same note, privacy awareness can be defined as the individuals' knowledge on the privacy risks, privacy concerns, privacy policies associated with the Internet, and the legal implications of privacy invasions and identity theft [11].

Awareness of the effects of new technologies on individual rights to privacy have long been discussed in literature [23]. It is though unclear whether Individuals' perceptions and societal responses are highly attuned to the new and evolving dimension that location privacy presents and how difficult it will be to affect those perceptions. The study by [30], found that technology awareness leads to positive user behavioral intention to use protective technologies against information security threats. Therefore, we believe that, in the same vein, privacy awareness might be associated with learner's behavioral intention.

Moreover, new studies indicate that user electronic privacy awareness is growing [31]. Also, many users of LBS are quite aware that there are privacy risks. However, most users do not understand how location data can potentially be used against them. For example, when an app requests access to the user's current location, will the app also identify them personally and tie that information to their location data? If so, the risks may be exponentially compounded. In this case, the user is not simply an anonymous person with a known location. Rather, it is Peter A. Doe, phone number 123-4567, email peter@doe.com, located at position x. However, the multiplied risk of this information may be lost on many users. Hence, a need to establish means to hide some if not all of these vital user's personal information identifiers.

Studies on factors influencing e-government adoption among Lebanese postgraduate students has found that awareness significantly influence behavioral intention [2]. A similar study by [36], confirmed these findings. Other studies, on the relationship between independent variable and dependent variable has also found that awareness perfectly affects relationships between variables [29].

3) Privacy Concerns

Privacy concerns indicate user concern on personal information disclosure [39]. This has since been conceptualized and operationalized by several studies in more detail: the Concern for Information Privacy (CFIP) instrument was developed by [40], identified four dimensions of information privacy concerns: 1) collection reflected the concern that extensive amounts of personally identifiable data are being collected and stored in databases; 2) unauthorized secondary use reflected the concern that information is collected from individuals for one purpose but is used for another secondary purposes without consent; 3) errors reflected the concern that protections against deliberate and accidental errors in personal data are inadequate; and 4) improper access reflected the concern that data about individuals are readily available to people not properly authorized to view or work with data.

Current studies indicate that privacy concern has significant effects on user adoption of instant messaging [35] web-based healthcare services [34] electronic health records, software firewalls [33] and ubiquitous commerce. Additionally, numerous extant studies have treated the construct of privacy concerns as a precursor to various behavior-related variables. Assertions by [32] confirms that privacy concerns are generally considered as a cost of adopting new technology. Consequently, there are high chances that similar effects can apply in the adoption of location-based systems for m-learning. Negative impact of privacy concerns on behavioral intention has been empirically supported in the e-commerce context [41]. Similarly, we expect a negative relationship between privacy concerns and behavioral intention in the context of LBS for m-learning.

In the context of e-commerce , [15] argued that consumers are concerned about their privacy risks along with the collection or secondary use of personal information that they have not given consent to. Accordingly, rendering personal information to online organizations requires individuals to surrender a certain level of trust. Research by [38] found that privacy concerns were a significant predictor of trust and perceived risk in mobile advertising.

4) Trust

Trust has appeared in several prior research studies. It has been defined as the willingness of a party to be vulnerable to the actions of another party [3]. It is the hope that an exchange partner will not engage in opportunistic behavior [4]. Finally, [13] asserts that trust is the willingness to depend. It often includes three beliefs: ability, integrity and benevolence [42]. Ability means that service providers have the knowledge and skills to fulfill their tasks. Integrity denotes that service providers keep their promise and do not deceive users. While benevolence signifies that service providers care users' interests, not just their own benefits. Trust may directly facilitate usage intention as it ensures that users develop positive outcomes in future. In addition, trust may mitigate perceived risk. When users develop trust in service providers, they believe that service providers have ability and integrity to protect their personal information from risks. Extensive research has shown the effect of trust on behavioral intention and perceived risk [14].

5) Perceived Risks

Perceived risk theory has been widely applied to commerce-related IT innovations in recent years, in which consumers' behavior of IT adoption is viewed as an instance of risk-taking [5]. For example, [6] employs five sub-dimensions of perceived risk in studying Internet banking adoption, including performance, social, time, financial and security risk. However, little prior work has explored how perceived risk of location privacy predicts the intension to use and the adoption thereof of m-learning systems.

According to [43], asserts that, comparing positive effect of trust on usage intention, perceived risk may negatively affect usage intention. This is for the sole reason that when users anticipate negative outcomes in future, they might become reluctant to adopt and use m-learning systems that are already location-aware.

VII. Gaps in Existing Literature

Extant research has proposed frameworks for adoption of mobile technologies into learning. Few have conclusively integrated privacy aspects and their influence on m-learning adoption in institutions of higher learning. Current m-learning advances have focused on course development, deployment and delivery; paying little attention to security and privacy. Therefore, location privacy is worth considering as such concerns can hamper the penetration of mobile technologies into the higher education realm. A considerable gap exists on the effort to determine the effects of location privacy awareness on usage intention as well as its correlation with privacy concerns.

VIII. CONCLUSION AND FUTURE WORK

In this study, we presented a secure location-based privacy preserving framework for mobile learning in distance education, work in progress. This was achieved through a thorough research on existing theories for m-learning adoption and by evaluating learners' behavioral intention to use location-aware m-learning systems. The study affirmed prior literature that indeed perceived risk, privacy concerns and Trust affects the behavioral intention to use new technology. In addition, we established though empirical evidence that privacy awareness has profound impact on behavioral intention to use m-learning systems for distance education.

Future work would involve administering a questionnaire to an identified sample population whose responses would be used to explore the actual impact of the identified construct through a simulation process, using SPSS version 20 and WarpPLS 5.0. Structural and measurement models would be drawn based on the obtained result. In addition, the constructs' correlation would be identified based on how these load amongst each other. In light of Internet globalization and rapid uptake of location-aware mobile gadgets, amongst individual in educational setup; it will also interesting to extend this study to include societal and cultural factors.

References

[1] M. A. Faruq and B. A. Hartini , "The Moderating Effect of Technology Awareness on the Relationship between UTAUT Constructs and Behavioural Intention to Use Technology: A Conceptual Paper," Australian Journal of Business and Management Research Vol.3 No.02 , pp. 14-23, 2013.

[2] . A. Charbaji and . T. Mikdashi, " A path analytic study of the attitude toward e-government in Lebanon.," Corporate Governance, 3(1) , pp. 76-82, 2003.

[3] W. S. Chow and N. K. O. Angie, "A study of trust in e-shopping before and after first-hand experience is gained," Journal of Computer Information Systems, 46, 4,, p. 125–130, 2006.

[4] . M. S. Kim and . J. H. Ahn, "Comparison of trust sources of an online market-maker in the e-marketplace: buyer's and seller's perspectives," Journal of Computer Information Systems, 47, 1, , p. 84–94, 2006.

[5] Liu et al, "A unified risk-benefit analysis framework for investigating mobile payment adoption.," in 2012 International Conference on Mobile Business., 2012.

[6] M.-C. Lee, "Factors influencing the adoption of internet banking: An integration of TAM and TPB with perceived risk and perceived benefit.," Electronic Commerce Research and Applications. 8, 3 , p. 130–141, 2009.

[7] M. Duckham and . L. Kulik, Location privacy and location-aware Computing., Australia: Universiy of Melborne, 2006.

[8] A. Pfitzmann and . M. K¨ ohntopp., "Anonymity, unobservability, and pseudonymity a proposal for terminology. ,," in Designing Privacy Enhancing Technologies, volume 2009 of Lecture Notes in Computer Science,, Springer, 2001., p. 1–9. .

[9] . A. Abu-Al-Aish, . S. Love, . Z. Hunaiti and S. Al-masaeed, " Toward A Sustainable Deployment of M-learning: A conceptual Model in Higher Education," International Journal of Mobile Learning and Organization. , pp. 7(3/4), 253-276, 2013.

[10] W. Ng and H. Nicholas, "A Framework for Suistainable Mobile Learning in Schools," British Journal of Educational Technology vol 44 No. 5, pp. 695-715, 2013.

[11] Liao et al, " Examining the impact of privacy, trust and risk perceptions beyond monetary transactions: An integrated model," Electronic Commerce Research and Applications, 10(6), , pp. 702-715, 2011.

[12] R. Philips, C. McNaught and G. Kennedy, "Towards a genelized conceptual Framework for learning: the learning environment, learning procesess and learning outcomes (LEPO) framework," in Proceeding s of Edmedia:World conference on educational Media and Technology, Association of Advancement of Computing in Education, 2010, pp. 2495-2504.

[13] . P. A. Pavlou, H. Liang and . Y. Xue, "Understanding and mitigating uncertainty in online exchange relationships: a principal-agent perspective.," MIS Quarterly , p. 105–136, 2007.

[14] A. Beldad, M. de Jong and M. Ateehoulder, "How shall i Trust the Faceless and the Intangible? A literature review on the Antecedents of online Trust," Computers in Human Behaviors, pp. 857-869, 2010.

[15] . Y. Pan and . G. Zinkhan, "Exploring the impact of online privacy disclosures on onsumer trust.," Journal of Retailing, 82(4), , pp. 331-338 , 2006.

[16] J. Zhu and . Y. Zhang, "Towards accountable mobility model: A language approach on user behavior modeling in office wifi networks," in Proceedings of The IEEE International Conference on Computer Communications and Networks (ICCCN 2011), Maui, Hawaii, 2011.

[17] S. Buthpitiya, . Y. Zhang, A. Dey and M. Griss, "n-gram geo-trace modeling," in Proceedings of Ninth International Conference on Pervasive Computing, San Francisco, CA,, 2011.

[18] G. Kambourakis, "Security and Privacy in m-Learning and Beyond:challenges and state of the Art," International Journal of u- and e- Service, Science and Technology, pp. 67-84, 2013.

[19] E. D. Wagner, "Realizing the Benefits of Mobile L.earning," Journal of Computing in Higher Education, pp. 4-14, 2008.

[20] A. Adams and A. Blandford, "Security and Online Learning: To Protect or Prohibit," in Usability of Olnine Learning Programs, UK, IDEA Publishing, 2003, pp. 331-359.

[21] G. J. Hwang, C. C. Tsai and S. H. Yang, "Criteria, Strategies and research issues of Context-aware ubiquitous learning," Educational Technology & Society, pp. 81-91, 2008.

[22] M. MacCarthy, "Student Privacy: Harm and Context," International Review of Information Ethics , vol. Vol. 21, pp. 11-24, 2014.

[23] R. O. Mason, "Four Ethical Issues of the Information Age," MIS Quarterly, 10,1, pp. 4-12, 1986.

[24] A. F. Westin, Privacy and Freedom, New York: Antheneum, 1967.

[25] A. Zafar, S. H. Hasan and M. S. Trigui, "Towards Secure m-Learning: An Analysis," MAGNT Research Report (ISSN. 1444-8939) Vol.2 (5)., pp. 148-159 , 2014.

[26] H. Nissenbaum, Privacy in Context: Technology, Policy,and the Integrity of Social Life, Stanford University Press, 2010.

[27] T. Zhou, "EXAMINING LOCATION-BASED SERVICES USAGE FROM THE PERSPECTIVES OF UNIFIED THEORY OF ACCEPTANCE AND USE OF TECHNOLOGY AND PRIVACY RISK," Journal of Electronic Commerce Research, VOL 13, NO 2, 2012 .

[28] C. Bettini, X. Wang and . S. Jajodia, "Protecting privacy against location-based personal identification.," in Secure Data Management. Volume 3674 f Lecture Notes in Computer Science., Springer , Berlin / Heidelberg, 2005, p. 185–199.

[29] . K. Omar, Ala'a and Al-Nasrallah, "Determinants of e-Gov Adopt in Kuwait: The Case of the Traffic Violation E-payment System (TVEPS)," in the Second Kuwait Conference on e-Services and e-Systems,, Kuwait, 2011.

[30] T. Dinev and Q. Hu, "The centrality of awareness in the formation of user behavioral intention toward protective information technologies," Journal of the AIS, 8,7, pp. 386-408, 2007.

[31] GovTech, "Survey Raises Consumer Online Privacy Awareness," Government Technology Magazines, Government Technology, 2009.

[32] T. Dinev and P. Hart , "Internet Privacy Concerns and Social Awareness as Determinants of Intention to Transact,," International Journal of Electronic Commerce Vol. 10, No. 2,, p. 7–29, 2006.

[33] Kumar et al, "Locking the door but leaving the computer vulnerable: Factors inhibiting home users' adoption of software firewalls," Decision Support Systems, Vol. 46, No 1:, pp. 254-264,, 2008.

[34] Bansal et al, ""The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online," Decision Support Systems, Vol. 49, No 2:, pp. 138-150,, 2010.

[35] P. B. Lowry, J. Cao and A. Everrard, "Privacy Concerns versus Desire for Interpersonal Awareness in Driving the sue of Self-Disclosure Technologies: The Case of Instaant Messaging in Two Cultures," Journal of Management Information Systems, pp. 163-200, 2011.

[36] M. Rahman, V. Esichaikul and M. Kamal, "Factors influencing e-government adoption in Pakistan," Transforming Government: People, Process and Policy, 6(3), pp. 258-282, 2012.

[37] S. R. Greene and M. Kamimura , "Ties that Bind: Enhanced Social Awareness Development Through Interactions with Diverse Peers," in Annual Meeting of the Association for the Study of Higher Education, Portland, Oregon, 2003.

[38] Okazaki, Shintoro, L. Hairong and H. Morikazu, "Consumer Privacy Concerns and preferences for degree of regulatory control," Journal of Advertising , pp. 63-77, 2009.

[39] Y. Li, "Empirical Studies on Online Information Privacy Concerns: Literature Review," Communications of the Association for Information Systems, 2011.

[40] H. J. Smith, T. Dinev and H. Xu, "Information Privacy Research: An Interdisciplinary Review," MIS Quarterly, pp. 989-1015, 2011.

[41] R. K. Chellappa and R. G. Sin, "Personalization versus Privacy: An Empirical Examination of the Online Consumer's Dilemma," Information Technology and Management 6, pp. 181–202,, 2005.

[42] D. J. Kim, D. L. Ferrin and H. R. Rao, "A trust-based consumer decision-making model in electronic commerce: The role of trust, perce ived risk,and their antecedents," Decision Support Systems 44, p. 544 – 564, 2008.

[43] S. Glover and . I. Benbasat, "A comprehensive model of perceived risk of e-commerce transactions," International Journal of Electronic Commerce, Vol. 15, No 2, pp. 47-78, 2011.