Towards Secure m-Learning: An Analysis

Aasim Zafar[1], Syed Hamid Hasan[2] and M. Saleem Trigui[3]
Information Security Research Group, Department of Information Systems
Faculty of Computing and Information Technology, King Abdulaziz University
Jeddah, Saudi Arabia

Abstract: M-Learning with its various advantages has been recognized as the need of the hour by the various organizations and universities and they are resorting to online education. However, though it may seem a very simple task the need of security and privacy in the domain is essential and it has been ignored for quite some time. In few of the exceptions made to the above statement, the accommodation of security and privacy has been done at arbitrary level which is not planned. We can term security as the methodology of ensuring integrity of data and to protect the policies of the organization implementing the m-Learning. While privacy is maintaining of an environment where the student can control how his private information is stored and shared. The paper would be discussing the elementary rules and practices of security and privacy. It would also analyze the commonly accepted standard of m-Learning to examine how they deal with security and privacy. Requirement of privacy in the m-Learning system is done keeping 'Privacy principles' in mind.

Keywords: Trust mechanisms, policy based management, network privacy, privacy principles, on-line privacy, information security, m-Learning, Privacy Enhancement Technology (PET).

1. Introduction

Learning and change are the two universal requirements of the modern world of information technology. With change and the growing advancement in the field of technology, the requirement of skills and training is increasing. The pool of skilled staff need to be retained and maintained by each organization and imparting new trainings to the employees is one of the methods adopted by the organizations today. With training them on new soft and hard skills the companies aim to equip the staff to meet the new challenges. One of the most popular and effective methods of imparting these kinds of training is m-Learning, which is an answer to the rising cost of learning and shortage of qualified trainers.

In the eyes of the universities/institutions these trainings are tools that enable the students to enhance their competence levels and be a better asset to the world. The learning can be generic self-development or with specific aims, targeting a specific domain of knowledge. This kind of m-Learning methodology is used for institutions that have specific strategy and targets to be achieved. The major aspects relevant to m-Learning and its privacy are [1]:

- The m-Learning environment has dynamic and more personalized course content to offer that is specific and adaptive to individual style or requirement.
- To know the how's and what's of technology m-Learning is rapidly

(DOI: dx.doi.org/14.9831/1444-8939.2014/2-5/MAGNT.19)

replacing conventional classroom teaching.

- Training has taken the shape of knowledge management with competency of learners being treated as an asset that are enhanced through training. This is leading to specific domain trainings being directed to suit the educational strategy so as to prepare the learners in being supportive in achieving the institutions goals.
- The access to courseware by the students is not limited to a specific kind of device, location or network and we are like to see a mix of all these in a m-Learning environment.
- The standards of learning are becoming more open/ adaptive.

M-Learning with its various advantages has been recognized as the need of the hour by the various organizations and universities and they are resorting to online education. However, though it may seem a very simple task the need of security and privacy in the domain is essential and it has been ignored for quite some time. Consumers and users of technology are becoming more demanding when it comes to privacy and their demands are being supported by rules being put in place. We also know that the m-Learning activities carried out in companies must be kept confidential, as details about the specific trainings provided may divulge critical information related to corporate strategies and goals to competitors.

More and more organizations are using m-Learning in their learning programmes, study shows that [2]

- 62% people use mobile devices for accessing learning content
- 54% people are using m-Learning for supporting collaboration and communication
- 53% people are using m-Learning as a good alternative of delivery to PC based learning content
- 43% people are using m-Learning for supporting application of learning back at the workplace

We would carry out an analysis of the issues related to security and privacy of the online m-Learning systems and the kind of systems that makes it possible for the user to access the training courseware from any compatible device like a PDA, laptop or computer etc. The focus would be on how to protect the user's personal information in the system. We would limit the discussion to exclude important security aspects of copyright of course content. We will discuss the research ethics using m-Learning environment [3]. The different standard of m-Learning system would also be analyzed for weaknesses with respect to Privacy. In the end we would propose certain technologies that can be used to enhance security and privacy in m-Learning systems. Research still needs to be done to identify the best out of the proposed technologies.

2. Principles of Privacy

The events of violation of privacy by hackers has forced the governments to work on policies and rules for protecting privacy. The privacy legislation in some countries requires control in handling of personal information such as disposal, retention, disclosure, use and collection of personal data. The aim of developing Privacy principles was to highlight the impact of the privacy policy and laws implemented by organizations in their online transactions. In order to ascertain the level of compliance of the Privacy Principals by the organization, the application must be analyzed as per the principals. The principals would be referred to while analyzing the PET (Privacy Enhancing Technology). Even though it is

evident that it is difficult to fully implement all the principles yet they do offer a sound checking systems for suitability of the technology [4]. The degree of implementation of each principle may vary in a computer system.

3. m-Learning and its Current Standards of Security and Privacy

In spite of the fact that m-Learning is a relatively new concept but it is being adapted very fast by researchers, companies and academic learning systems. However, standards like the ones existing in e-learning systems are still surfacing. The main issue is that of m-examinations. In e-learning supervised examinations have worked well, but the ability to authenticate the examinee in unsupervised setup is limited [5]. This study has highlighted the impact of Organizational support, Effort expectancy and availability of ICTs. [6]

The learning system online would be influenced by the standards of distance education and learning. Compatibility and Standardization are critical for both the end-users and vendors of m-Learning, so that they would be able to sell and purchase of interchangeable and portable content in the market. The factors also effect the interaction of the m-Learning system with one another.

The noteworthy groups working on standardization are

1. IEEE LTSC (Learning Technology Standard Committee) [6,7],
2. IMS GLC (Global Learning Consortium) [8],
3. AICC (Aviation Industry's Computer Based Training Committee) [9],
4. ARIADNE(Alliance of Remote Instructional Authoring & Distribution Networks-Europe) [10],
5. ADL-SCORM (Advanced Distributed Learning- Sharable Content Object Reference Model) [11].

Even though most of the standards are related to sharable learning objects and components yet some also relate to the m-Learning system's privacy and security requirements. We would now discuss these standards with respect to security and privacy.

3.1 IMS LIP

The IMS GLC (Global Learning Consortium) is also working for development of Distributed learning's open specifications. The problems of Learner's information package specifications, simple sequencing specifications, test & question specifications, Packaging & content specifications, enterprise specifications and meta data specifications are addressed by this group. The interoperability of learner's information among systems supporting internet learning is discussed by the IMS LIP Specifications. It specifies ways of making the system more responsive to user's needs by organizing the learner's information that include Community service record, Life Long learning records, Professional development records, training log and education record.

The IMS LIP enables security and privacy of the learner's information. A server regulates exchange of information with the other learning systems or servers. It supports defining by the information owner about which information can be shared. Even though, data privacy and integrity is critical in IMS LIP, it still does not specify details of architecture or implementation mechanism for Privacy protection. The only thing specified by the final version of LIP specifications V1.0 [12], is guidelines that would support any appropriate architecture that implements protection.

3.2 IEEE P1484

The LTSC proposed IEEE P1484 standards of for learning technology. P1484.2 specifies the semantics and syntax of the leaner's information as well as the security and privacy specification

for use, retrieval, storage and creation of the information. It is also known as PAPI (Public and Private Information) specifications for the learning systems or individuals. The elements specified cover how to records information about Portfolios, Performance, preferences, relationships, contact information and learning process of the learner. The different viewpoint of the users, regulators, institutions and developers are used for categorization of privacy and security concerns. Table 1 specifies the P1848 standards' security features.

However, detailed technology or model is not specified by the P1484.2 with respect to privacy concerns. It suggests possible use of security techniques like confidentiality, physical security for providing privacy, even though it does not have a specific policy in privacy. The users and the administrators may together act as the policy makers of privacy in the system. It also has a standard called "Learner's information logical division" that defines the features of privacy protection. As per this standard the learner's information can be tagged, split and concealed. Thus in turn addressing many concerns of privacy by the users [7].

Table 1: P1484 - Security features

Model	Specification	Model	Specification
Access Control	D	Confidentiality	N
Authentication	O	Data Integrity	N
Authorization	I	Digital Signature	N
Deidentification	O	Validation of Certificates	N
Delegation	I	Encryption	N
Identification	I	Privacy	N
Security Extension	D	Repudiation	I
Security Parameter Negotiation	D	Non-Repudiation	I
Session-View	D		
Security			

Legend: N - Non-specified.
O - Outside the scope:
I - Implementation-dependent:
D - Defined.

3.3 Additional M-Learning Standard

We have various other organizations and standards that can be applied to distant learning already listed earlier. ADL-SCORM (Advanced Distributed Learning- Sharable Content Object Reference Model), ARIADNE (Alliance of Remote Instructional Authoring & Distribution Networks-Europe) and AICC (Aviation Industry's Computer Based Training Committee). Yet most of them pay little attention to privacy and security, e.g. :

- ADL-SCORM focuses on treatment of instructional content.
- ARIADNE emphasizes on reusability and sharing of content through specifying the meta-data.
- AICC is concerned with aspects of implementation, digital audio and peripheral specifications for m-Learning systems.

4. Security and Privacy Requirements for m-Learning

With privacy and security we mean authorizing and authenticating users, ensuring data integrity and protecting the personal information against unattended access. We will be concentrating on the requirement of data integrity and privacy. In the beginning we would describe the m-Learning architectural model based on LTSA's (Learning Technology System Architecture) [13] IEEE P1484.1/D9. The model is analyzed for its application to distributed & mobile m-Learning with reference to the Privacy Principles, to get the requirements for data integrity & Privacy.

4.1 Essential Requirement for Privacy

The Principles of Safeguards warrant placement of safeguards on every m-Learning system component that is related to learner's private information. The dense lines in Figure 1 represent these components, which primarily are transmission channels between:

- Learner Records and the Coach
- Learner Records and the Evaluation,
- Coach module and Evaluation module,
- Coach & Evaluation modules and the Learner entity.

The transmission channels between the Coach, Learning resources, Delivery and Learner entity also need to be protected if the content holds sensitive data.

4.2 Privacy Requirements for Location

There are quite a few systems that provide the learners the choice of choosing the content and time as per the learner's convenience and preference, additional freedom is offered through service mobility i.e. the learner can access the system through any suitable device like Smart Phones and PDAs, anywhere through Wireless communication channels.

Keeping the location of the learner private becomes all the more important with reference to service mobility. Some of the learners may not wish to reveal where they are accessing the m-Learning system from. The information related to the location of the learner may be combined to establish his movement patterns that may be of interest to some third party.

4.3 Privacy Requirement for Networks

The readily accessible tools for monitoring network traffic and the open structure of the internet makes is possible for even a novice to snoop on information. Even though the SSL and VPN may present as foolproof safeguards for privacy of data transmission, yet there are quite a few inert attacks that can reveal sensitive communicators' information contributing in this transmission. [14]. E.g. the Communication and Timing patterns attack, reveal information about the amount of data, location of participants and timing of transmission that can lead to deciphering the relationship between the communicating entities. It is critical to safeguard such information for certain activities in the organizations. For example a company that wants to purchase an online training module from an m-Learning provider would want to keep its relationship with the provider secret as revealing of any connection between these entities would lead to exposing of the critical function/initiative the training is aimed to achieve. Even the provider would want to keep things confidential for assuring customers about privacy against competitors.

With reference to Figure 1, communication channels between Multimedia, Behavior and learning preference need to be made secure against traffic analysis. If the *Evaluation* process is residing on machine of the learner a secure channel of transmission between the coach and the *Learner Entity* may be utilized for assessment and learning preferences, thus making is unnecessary for protecting the channel between the Evaluation and the Learner Entity.

4.4 LTSA

The architectural model from LTSA specifies the information flow, storage areas and processes for m-Learning. The relation amongst these elements are shown in Figure 1. Dashed arrows depict control flow while solid arrows shows data flow. The learning preference that includes the learning methods, strategies and styles etc. are handed over to the coach from the learner. The information is reviewed by the coach and suitable content for learning is queried by the coach from the learning resources. The content from Catalog Information is extracted by the *Coach* from the *Locator*s which is then passed to *Delivery*, that in turn utilizes it for retrieving content to be presented to the learner as *multimedia.* The learner exhibits certain behavior in response to content that goes through evaluation with the resultant assessment

or performance evaluation. This information is stored in the Learner's record.

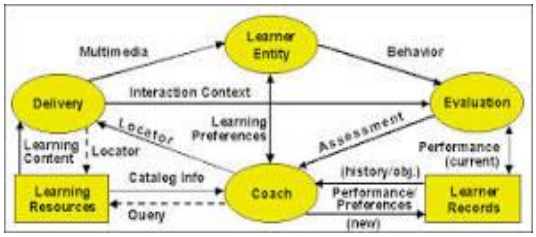

Fig. 1. Relation among LTSA elements

5. Likely m-Learning PET

We would now examine various PET with respect to requirements of Security and Privacy of an m-Learning system starting with analyzing P3P (Platform for Privacy Preference) [15], then the network privacy approach.

5.1 P3P (Platform for Privacy Preference) (P3P)

Any learner will always have the following concerns related to his privacy, when using an m-Learning system:

- What all information is gathered by the system and for what purposes?
- If the information related to the learner's privacy accessible to him?
- What is the duration of information storage?
- Whether the information is shared with other entities, if yes, what is the purpose of sharing?

W3C (World Wide Web Consortium) developed P3P, has possible answers to the above questions. It allows the websites to present the privacy policies in a specified format, readily available for retrieval by the user or his agent. P3P has defined an XML format for policies on Privacy that websites can use to post their policies in and the users can use to specify their preferences as well. The users can specify their preferences about the P3P policies using an exchange language called APPEL. It is on the basis of these preferences that the agents of the users can make decisions weather a web site's policy is acceptable. Based on this matching of the user preference and the website privacy policy the user proceeds or stops with an m-Learning service.

i) Weak Security and Privacy and Protection Model

The P3P specifications is based on the information provided to the user regarding the privacy and security policy of the website, if they do not agree to the specified policies they may simply leave the site, which is a weak model of ensuring security and privacy.

W3C is making positive efforts for protection of privacy and security in domain of P3P. However, P3P is not sufficient for protection of privacy due to its inherent weaknesses, thus additional steps are required to have better control of use and collection of information.

ii) Privacy protection - Partial coverage

P3P covers only a part of the privacy principles described which are as follows:

- Openness: The privacy policy of the Web site are open for review to the public.
- Consent: The consent of the individual is taken for disclosure, use or collection.
- Identification of Purpose: The purpose of collection of the information is declared.

Rest of the principles Challenging Compliance, Individual Access, Safeguards, Accuracy, Limiting Retention / Disclosure/ Use, Limiting Collection and Accountability

are either not covered or minimally touched by P3P.

iii) No Enforcement of Privacy Policies

The P3P does not provide any mechanism that ensures that the specified privacy policies are indeed implemented by the websites, it only ensure informing the users about the Privacy policies of the web sites.

5.2 Network Privacy Approach

In order to strengthen the privacy of the information over the network we come across a number of other methodologies apart from the ones described above. One such approach is that of use of proxies for fulfilling request of m-Learning from the users. [16,17]. The method of redirecting the web requests through the proxy along with other secure channels of communication would protect data against casual attacks. However, it is still susceptible to Pattern & Timing attack along with the access logs of the service providing a pool of information related to the users. Additionally if all the logs are kept in a single place then it is a possible hackers magnet. Apart from that an organization may not be confident of a single proxy provider for handling its data. Thus other methods of protecting the privacy like Freedom Network [18], Crowds [19], DC-Net [20,21], MIX Networks [22], and Onion Routing [23], are required in addition to the previously described ones. The methodologies involved in routing information amongst members uses Chaum Mixes [22]. The relationship between the outgoing and incoming messages is hidden by the technique of tailoring the packet cryptographically in a single mix, whereas using the mixes if chains means better network security. It is essential for using the chain of mixes that the intermediate node routing be statically pre decided by the source nodes, like Onion routing, or the intermediate node probabilistically like in Crowds. Another advantage offered by chain mixes is that they have distributed administration, so the possibility of compromise is reduced unlike a single mix.

Yet, there is a cost of anonymity that is achieved by the techniques of network privacy, Onion Routing has its overhead for every connection established. It also may incur delay in large data transfer since the shortest path might not be always chosen to ensure privacy. Increase in the number of intermediate nodes would increase the delay, which is added upon by Cryptographic functions. This delay (session quality) may not be a cause of concern for communications like emails (asynchronous applications) but for synchronized application like video chat it would be detrimental. Thus a balance must be achieved between session quality and privacy.

The following figure illustrates data communication through different means. Figure 2 shows usage of mixes to protect privacy while Figure 3 shows a connection secured through conventional means (SSL or VPN). It is evident in conventional security scheme the determination of the location of the parties and the kind if interaction is easy, while in the Mixes setting the service and user side use the traffic management and cryptographic technique to modify data making is impossible to determine the ends and nature of data.

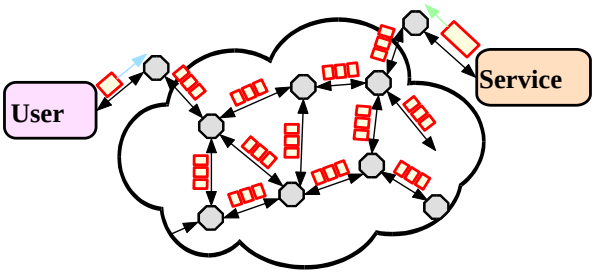

Fig.2. MIX network

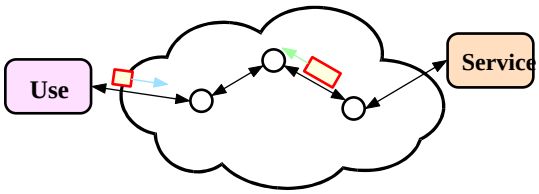

Fig.3. Conventional Secured Network

The level of privacy requirements for different applications varies. The Privacy Principles statutes the network privacy as an important aspect yet a simple secure channel may be enough for information exchange. However, with the increasing dependence on third party vendors would warrant concealing location and nature of the transmission. The capacity of providing a secured network would determine preferability for m-Learning vendors by the companies.

5.3 Mechanisms of Trust

Similar to conventional education system, m-Learning system also have an integral place for Trust. There should be trust between different systems which use the services offered by each other. The interaction between the provider and the user must be Trusted as it us an underlying requirement for all interactions. The provider must trust the user with authorization against forging and the user must trust the provider with his personal information against misuse or any use not specified. Digital Certificates form the basis of most of the system based on Trust Management.

a) Systems for Trust Management

We also have systems that aim at providing general purpose and standard mechanisms for Trust management. E.g. “KeyNote” [24] and “REFEREE” [25].

A unified approach for interpreting and specifying relationships, credentials and security policies is provided by KeyNote [24]. The 5 components/ concepts used in KeyNote are :

- 'Compliance Checker' – determines handling of a request from a principal in accordance with the policy and credentials.
- 'Credentials' – means of delegating authorization by principals to other principals.
- 'Policies' – specifies the actions that a Principal is authorized to perform.
- 'Principals' – means an entity that is authorized for performing any action.
- 'Actions' – is an operation that effects/ comes under the preview of system security.

Rule-controlled Environment for Evaluation of Rules and Everything Else (REFREE) is another system for managing trust. This system is pertinent to allowing access to documents on the internet; Yanh-Hua Chu used the Policy Maker [26] to develop this system. PICS labels [27] are used by this system to specify properties like “prototypical credential” of a resource on the internet. The concept of "programmable credentials" is introduced by the system which can be used for examining the statement made by various credentials and for fetching information over the network in order to make decisions.

b) Mechanisms based on Digital Certificates

This mechanism is built upon the assumption that a certificate represents a trusted source/party and Digital Certificates are a key component of this approach. A certificate issued by a certification authority signifies the rightful ownership of a public key by the claimant, thus the certificate contains the digital signature of the issuer,

the information about the certificate (User's Name and identification details) and the public key. Thus the certificate assures that the User is the rightful owner of the public key in the certificate. PGP and PKIX/X.509 are the basis of the most commonly used approaches.

The framework for authenticating services is defined in X.509/PKIX [28]. It is a PKI that is a hierarchically structured, and has an RCA (Root Certificate Authority). All the users in the network hierarchically derive the Trust from the Root through CA (Certificate Authorities).

PGP (Pretty Good Privacy)[29] (PGP) provides a methodology to do away the PKI infrastructure overhead, but still yet encrypt information and digitally sign Objects. The decision to trust whomsoever they want, lies with the users in PGP. Thus the CA is replaced by the "Web of Trust" mechanism in PGP, where the validity of a certificate is attested by multiple key holders.

Digital certificates, such as PGP and X.509/PKIX form the basis of Trust Mechanism through providing methods of defining, verifying and managing of trust parties. This has proved to be an effective mechanism for establishing credentials during online transactions. The entire trust and confidence of the user is dependent on the Public Key's authenticity. However, we still have risks and uncertainties challenging the Mechanisms based on certificates [26]. Like, trusting the PKI vendor itself and the rules employed by the vendor in issuing certificates. Thus application specific adjustments need to be made for providing Privacy and security, on Vendor as well as user side, in these kind of mechanisms.

c)Multiagent Systems

One of the most important aspects of deploying e-learning applications is security. Here multiagent systems, secure systems development standards and e-learning systems have been considered for support of secure learning situations. The various security requirements for e-learning applications have been assessed and a security model has been recommended. Privacy, access control and integrity have been targeted to adopt security use cases [30].

5.4 Approach based on Policy

The approach of managing distributed and large system based on policy has been effective. The policies govern the behavior of the system in policy based approach. They define the obligation and authorization over subject and object entities. The policy on obligation statute the negative and positive obligations that a subject has with respect to an object. The authorization policy governs the actions that a subject is authorized or unauthorized to take with respect to an object.

Like stated above, the m-Learning system may also use the policies for managing the privacy and security of the system's objects. In order to confirm with the Principles of Privacy discussed previously, the policies may be made to govern the Individual access and collection of information. While policies on obligation may specify: Openness, Safeguards, Limiting Retention/Disclosure/Use, to supply proof for limiting collection, Consent and Identifying Purpose.

The m-Learning system based on Policies might have basic policies specified for general operations while entity (course material, student, teacher, administrator, etc.) preferences may decide additional policies. Hence for each entity there would be a set of different policy along with the policy governing the interaction amongst them. Regulatory and privacy laws might also be enforced as well [6]. This might be part of the general policies after being adopted for electronic use [31]. Since there is a

possibility of conflicts between different policies, a mechanism for detecting and resolving policy conflict should also be in place. This could also be in the form of a facility where the provider and the learner in the m-Learning system may identify and negotiate on policy conflicts resolution.

Even though, policy based management enables specification and management of privacy aspect, yet it poses as challenge in enforcing real controls around or within the objects itself. E.g. Limiting collection is an Obligation policy, yet is it very difficult or nearly impossible to limit the extent to which personal information is collected. Let us consider an organization that specifies that names of the students would purely be collected for managing records during the tenure of the course. However, it is practically impossible for a system to exist that would not collect other information like student behavior during the course or Yet it is difficult to imagine a system that would prevent collection of other information regarding the students' behavior during course or mining of data from other sources about the student for any purpose the organization may choose. Thus for ensuring compliance to Limiting Use and collection the approach of audit or trust is more relevant than automated means.

6. Need for Research and Conclusion

The principals of Privacy and the present standards of m-Learning were investigated for the security and privacy provisions they have. The basis for analysis of prospective PET were provided by Privacy Principals, for their capability to establish security and privacy in m-Learning. The treatment given to security and privacy by the current standards of m-Learning is just superficial. A high level model for m-Learning is provided by IEEE P1484.1/D9 an LTSA architectural model. In combination with the Principals of privacy the model helps to identify the m-Learning system components that need to be treated for security and Privacy. Such components were identified in Section 4.2. The requirements of location and network privacy were also discussed. It was also discovered that current technologies like VPN or SSL fail to protect detection of location or nature of relationship through analyzing traffic.

Various PET were then examined for their candidature for m-Learning, though we must keep in mind that they may not be the best suitable for the job, and are just candidates. The research to identify the best fit needs to be continued. Despite being quite weak on security and privacy, P3P can still be treated as a starting point for protecting the privacy online. Quite a few technologies like Mixed Networks and Onion Routing were looked upon for network privacy, as they provide protection against traffic analysis. It was also discussed that not all the application in the m-Learning environment require strict privacy protection provided by the aforesaid technologies, yet the importance of stringent privacy levels is growing for more and more organizations due to their reliance on third party providers of m-Learning. The approaches of Policy and Security management were also examined for identifying their level of compliance with Privacy Principals. Trusted interactions between the vendor and users of m-Learning systems were sought to be provided through Trust mechanisms. Course access authorization and safeguards for learner's privacy may be established through a trust management system based on policies. Security and Privacy management can be achieved through policy based approach as well.

The following areas of research need further work for improving the Security and Privacy aspects of the systems of m-Learning.

- Trust Mechanisms: How the Principals of Privacy can be satisfied by application of these mechanisms.

- Security and Privacy Management through Policy-based approach: How the approach can be used for complying m-Learning system with negotiation mechanisms, policy specification and Privacy Principles
- Location Privacy: Which technologies can be used for ensuring privacy of location for e-learners that are mobile.
- Network Privacy: Finding more technologies like Onion Routing for protecting system against attacks like traffic analysis.

Acknowledgement

This project was supported by the NSTIP strategic technologies program in the Kingdom of Saudi Arabia – Project No. (12-INF2259-03). The authors also, acknowledge with thanks Science and Technology Unit, King Abdulaziz University for technical support.

References

[1] Hodgins HW. Into the Future: A Vision Paper. A white paper for **ASTD** and **NGA,** Submitted to the Commission on Technology and Adult Learning, February 2000.

[2] Garg A. Mobile Learning at work - Towards Maturity 2013. http://www.towards maturity.org/mobile 2013.

[3] Hodges J, Stead G. Research Ethics in the Mobile Learning Environment (MoLE) m-Learning Project. Connections Volume XII, Number 1, Winter 2012.

[4] Privacy Technology Review, http://www. health-canada.ca/ohih-bsi/available/tech/ tech_ e.html.

[5] Hasan SH, Alghazzawi DM and Zafar A. E-Learning Systems and their Security. BRIS Journal of Adv. Science & Technology, 2014, Vol.2 (3):pp. 83-92.

[6] Macharia J. Mobile Applications to Enhance Versatility of Mobile Learning in Higher Education. Proceedings and reports of the 6th UbuntuNet Allainace annual conference, 2013, pp 135-144.

[7] IEEE LTSC - Learning Technology Standards Committee, http://ltsc.ieee.org/wg1/index.html

[8] IEEE LTSC PAPI - Public and Private Information (PAPI) for Learners, http://ltsc.ieee.org/wg2/index.html.

[9] IMS Global Learning Consortium, http://imsproject.org.

[10] AICC-Aviation Industry CBT [Computer-Based Training] Committee, http://aicc.org.

[11] ARIADNE - Alliance of Remote Instructional Authoring and Distribution Networks for Europe, http://www.ariadne-eu.org/.

[12] ADL-Advanced Distributed Learning, http://adlnet.org.

[13] IMS Global Learning Consortium, Final Specification of IMS Learner Information Package Information Model, Version 1.0, 2001, http://imsproject.org

[14] IEEE LTSC LTSA – Learning Technology Systems Architecture, http://ltsc.iee.org/wg1/ index.html

[15] Raymond J. Traffic Analysis: Protocols, Attacks, Design Issues, and Open Problems. SpringerVerlag, 2000.

[16] http://www.w3c.org/P3P

[17] Anonymizer web service at: http://www.anonymizer.com/

[18] L. P. W. Assistant, available at http://www.bell-labs.com/projects/lpwa

[19] Boucher P, Shostack A and Goldberg I. Freedom Systems 2.0 Architecture, White paper, 2000.

[20] Reiter MK and Rubin AD. Crowds: Anonymity for Web Transactions. ACM Transactions on Information and System

Security (TISSEC), 1998, Vol.1, Issue 1, pp. 66-92.

[21] Chaum D. Untraceable Electronic Mail, Return Address, and Digital Pseudonyms. Communications of the ACM, February 1981.

[22] Waidner M. Unconditional Sender and Recipient Untraceability in Spite of Active Attacks. Eurocrypt '89, LNCS 434, Springer-Verlag, Berlin 1990.

[23] Chaum D. The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability. J. Cryptology 1(1), 1988, pp. 65-75.

[24] Goldschlag D, Reed M and Syverson P. Onion. Routing for Anonymous and Private Internet Connections. 1999.

[25] Blaze M, Feigenbaum J, Ioannidis J, and Keromytis AD. The Key Note Trust Management System Version 2, Request For Comments (RFC) 2704. September 1999.

[26] Chu Y. Trust Management for the World Wide Web. 1997, Massachusetts institute of Technology, REFEREE: Trust Management for Web Applications, http://www.w3.org/PICS/TrustMgt/presentation/9704-08-referee-www6/

[27] Paul R and Miller J. PICS: Internet access controls without censorship. Communications of the ACM, Vol. 39 No. 10 (1996), pp. 87-93.

[28] Public-Key Infrastructure (X.509) (pkix), last modified: 11-Jan-02, http://www.ietf.org/html. charters/pkixcharter.html

[29] An Open Specification for Pretty Good Privacy (openpgp), last modified: 31-Jul-01, http://www.ietf.org/html.charters/openpgp-charter.html

[30] Webber CG, Fatima MD, Lima WP, Casa ME, and Ribeiro AM. Towards Secure e-Learning Applications: a Multiagent Platform. Journal of Software Vol.2, No. 1, February 2007.

[31] Ellison C, Schneier B. Ten risks of PKI: what you're not being told about Public Key Infrastructure. Computer Security Journal, V.XVI, N.1, 2000.