Malaysian Journal of Educational Technology
Volume 12, Number 3, September 2012

Designing Ensemble Based Security Framework for Secure M-Learning System in Malaysian Higher Learning Institution

Sheila Mahalingam
Technical University of Malaysia, Melaka, MALAYSIA
sheilamahalingam@yahoo.com

Abstract

Mobile Learning has a potential to improve efficiency in the education sector and expand educational opportunities to underserved communities in remote areas. However there are a multitude of challenges faced when introducing and implementing m-learning. It is possible that within 10 to 20 years there will be one global mobile campus. Very much unfocused issues are security management even though statistically proven that threats are increasing each day on mobile application and ensemble devices. This has been seriously discussed in many research that security need to bring in to the lime light of each complex and larger systems using variety of mobile devices that interconnected each other via internet or wireless environment. In order to provide a secure guideline for m-learning platform, an ensemble based security framework for mobile learning is designed and improved. One of the major benefits in the framework is it integrates the security with dependability to provide trustworthiness in learner and providers perspective. Besides that in also encompasses the suggested secure engineering model to be used in developing secure m-learning system which mapped with countermeasures and solutions to be used involving common threats and vulnerabilities in ensemble based m-learning.

Mahalingam, S. (2012). Designing Ensemble Based Security Framework for Secure M-Learning System in Malaysian Higher Learning Institution. *Malaysian Journal of Educational Technology, 12*(3), pp. 33-41.

Introduction

At present , higher learning institution in global and Malaysia has well adopt the e-learning concept and now the new revolution in learning technologies has given a big bang towards rapid growth in mobile learning (m- learning) environment . In near future wireless and mobile application has become a very famous technology among the 21st century generation. M-learning capabilities will continue to expand with the introduction of smaller, more sophisticated and powerful gadgets capable of delivering data in a variety of format anywhere, at any time. As mentioned by (Schooler, Jelinek, & Dahle, 2010) developing countries continue to explore the mobile learning models there is need to explore the suitability of mobile technologies with a secure platform for the learner support in the mobile learning systems.

In recent Asia Pacific Future Gov Online , Educational IT article by (Gou, 2011) stated University Sains Malaysia has created a mobile learning research team and as a future plan of the research team is to propose to the Ministry of Higher Education ; to extend the M-learning methodology to all universities as the cost is much less compared to the conventional methods. ("SEAMO RIHED ANNUAL REPORT," 2007)Report of the 2nd Meeting of Director General/ Secretary General/ Commissioner of Higher Education in Southeast Asia hosted by Malaysia has put focus on several areas, which one of it is E-Learning and Mobile Education Programme. The meeting have notified that importance of lifelong learning programmes in the region especially open learning activities such as e-learning and m-learning. They have requested for a paper to be presented in collaborative efforts by Malaysia, Thailand and Indonesia on M-Learning that address the possibility in developing general platform in delivering methods.

Furthermore m-learning and security are among the expected services in ubiquitous computing. Global user expectation and initiative taken in wireless and mobile technologies is towards Ubiquitous computing. (Bhd, 2008)Presented one of Malaysian Government initiatives is The MyICMS886 strategy which has focused to three areas: First is the Services include high speed broadband, 3G & Beyond, Mobile TV, Digital Multimedia Broadcasting and etc. Second is Infrastructure contributes to Multiservice Convergence Networks, 3G Cellular Network, Information and Security Network and etc. Third is Growth which points out areas in ICT and Education Hub, Communication Devices, embedded component and device.

Another major issue in m-learning system is implementation of secure and trusted system. This is an essential requirement in m-learning applications and systems where sharing information is needed. The system should prevent data losses or corruption due to network disconnection and mobile failures. At present security tools are adequate for securing systems on small scale but most security breaches are caused by faulty and ad-hoc software. To rely on an m-learning system, learners need to know to what extent it can be trusted.

Providers of M-learning need a guided platform to introduce and implement a secure mobile learning system in their organization. To overcome the drawbacks associated with m-learning system and ensemble computing, it is essential that m-learning system must have an integrated security framework, which offers different security techniques to provide an overall secure system. As a solution to be a successful provider and meet universities business management aim, m-learning should be highly secured and implemented in a trusted environment for the learners.

In line with this issue there is an urgent need for framework that can be used to analyze and evaluate trustworthiness of m-learning system where both security and dependability can be measured. According to the project report by Steering Committee for European Security & Dependability Task Force under the Sixth Framework Programme 2002-2006 in the Issue 1.0 (Technologies et al, 2010) mentioned that as size and complexity of this digital world grow, so too does our dependency on it for all aspects of personal and public, social and economic activity. There is a greater need to concentrate attention and effort on the security and dependability aspect as well as the design and implementation of components and system together with their interrelationships.

Literature Review

Since mobile learning is a new paradigm of a new networking structure with mobile and wireless technology,according to (Alaysia, 2010) the confusion that happened by using the unnecessary functions on the current e-learning system can be solve by implementing learning processes using mobile devices. Mobile applications and devices are likewise booming and becoming the fastest growing consumer technology. However mobile applications security is severely lacking and the security issues are present on all major platforms. There is a steady growth in the number of application infected with malware with the rise of 80 to 400 applications from January to June 2011 reported by (“Lookout Mobile Security,” 2011) and also has stated in the report that worldwide unit sales of mobile devices expected to increase from 300 million in 2010 to 650 million on 2012 . One of the top five threats grown substantially in year 2011 is mobile threat reported in (“Malware Report,” 2012) More than 50 third-party applications on Google’s Android Marketplace were infected with Trojan that was designed to gain administrative privileges over personal phone without user’s permission.

Mobile threats are evolving quickly and more sophisticated and it’s important to change their existing security or software development models. The existing technical security measures such as firewalls, antivirus, and encryption are uncommon on latest mobile devices and mobile operating systems. Therefore an advance secure software engineering design is needed to develop secure mobile applications and to gain learners trust in using the mobile application in the m-learning platform.

In this paper key security problems are identified along with the severity involved as barrier and possible solutions while implementing ensemble computing based m-learning technology are explained. M – learning method by ensemble computing helps to make m-learning solutions possible for mobile phones and other similar mobile devices to be integrated in a secured and reliable environment. Learners and m-learning provider are very conscious on the security features of the technology when it comes to ensemble. (Schooler et al, 2010) comprehensively discussed examples of ensemble found in health care information system. He stated an ensemble is based on body worn devices such as a watch or a cell phone, in combination with environmental monitors in the home, can provide care givers with data they need. As (Bill, 2004) aptly phased it, ”ensemble computing is dynamically coordinated collections of computers, which include both mobile and infrastructure components integrating the techniques for programming and orchestrating their applications.”Integration within the wired and wireless network also plays a main role in m-learning platform. There is a need to examine the challenges in mobile technologies and ensemble computing in areas such as manageability, usability, power constraint, accessibility, security standards and privacy issues, new programming models and ad hoc applications and wireless limitation.

To put in briefly, m-learning learning system face danger experience associates to cyber and physical damage that affect to vulnerable points in the learning platform. There are method in protecting this system by technological solution according to C.I.A triad; availability, confidentiality and integrity. Hence, the m-learning provider needs to think over in part of cost estimated for each asset involved and forecast for potential waste in each vulnerability point in order to increase the level of risk in each point to define a secure mobile learning environment.

Related Work

In order to design, prepare and implement a mobile learning system platform , elements and characteristics of mobile learning are organized in an appropriate framework in advance to get an efficient result in implementing m-learning successfully. Therefore a study towards the related work has been divided into two categories: environmental influences and secure system model integrated with security and dependability.

Environmental Influences

(Ozdamli & Cavus, 2011) stated basic elements of a complete mobile learning are learner, teachers, environment, content and assessment. The researcher has mentioned "environment must be design properly to obtain positive learning experiences." The environment should be design by considering the available ensemble devices such as mobile phones, laptops and other handheld mobile tools.

Researchers have argued about creating a group network for collaborative framework to improve learning in both awareness content and environment perspective(Chen et al, 2008). The research effort has indicated that handheld devices (ensemble devices) have a positive impact on learning because of it easy operating and use characteristic. However (Vassiljev, 2010) stated current security community with desired protective measures does not fit fell in the learning environment. (Jonssonet al, 2000) Classified environmental influence on intrusion detection which is divided into three areas (Threat Reduction, Boundary Protection and Recovery) Together he has proposed protection mechanism for these three areas (prevention protection-threat reduction, boundary protection, and internal protection-recovery). These findings effort comes from the hypothesis of the research, IT system that are complex must adopt the biological paradigm where continuous protection process is needed in every level and must be adaptive.

Hence environmental influences need to be narrowed down to m-learning attack and threats taxonomy. (Wiesauer & Sametinger, 2007) has proposed taxonomy based on attack patterns. Researchers has discussed about planning a secure system, one need to identify which attack the system has to resist and which security requirement the system has to full fill. Furthermore as result from the previous research a taxonomy based on vulnerabilities and threats identified in m-learning , mobile technologies and ensemble devices , enables the secure model in m-learning to select the appropriate countermeasures and solution towards the threats and vulnerabilities identified.

Security and Dependability

There are a few recent research effort has been done to integrate dependability and security. Since that time, investigators from several studies have used and indentified the importance of this integration in several areas. (Hu et al, 2011) contributed their research in the area of service oriented architecture (SOA) functionality layer for the basic fault building blocks. They have used feedback control system which controls the behaviour and expended dependability and security tree, where faults classes has been categorized to several types of faults and mapped to three main attributes of security (availability, integrity and confidentiality) which are interrelated to dependability and non-repudiation as an independent attribute.

(Meadows, 1995) Presented the same results, she identified different ways to handle faults which is the diversion from security paradigm to dependability paradigm by discussing the impacts of extending security paradigm which covers the full options of dependability. As a result she have developed and outlined of fault model for security by placing both fault tolerance and fault forecast in computer security. This model is defined as an approach to design dependable system. Continuous research has been done by (Meadows & McLean, 1999) after four years of her first paper was published; security has become more complex and need changes in the taxonomy. Significant gaps are found that dependability covers an

important aspect of security where it is true in the area of fault tolerance. Taxonomy of security needs to be extended to new ways in the case of fault prevention and removal. A summarization of few research paper in this area presented by (Pudar, 2006) on concepts and taxonomy of dependable & secure computing. Here researchers have identified malicious and non malicious faults incorporating with classification of service failures. Researchers have incorporated dependability and security specification to address the service failure and faults. There are interrelationship between fault, error and failure.

Nicol et al (2004) developed a model based evaluation from dependability to security. There is important need to validate the efficiency of system security. Therefore security parameter, attacker behavior needs to be defined and characterized. Three type of models are reviewed which a combinatorial methods, model checking and state based stochastic methods. Finding shows that most of the dependability analysis could be transferred to security analysis and security needs to be qualified by modeling attacker behavior. Stochastic model are used as security evaluation for dependability model. Similarly (Sallhammar, 2007) has few contribution in integrating security and dependability. He has discussed about applying security related context in "fault-error-failure" demonstrating stochastic approach in computing expected time to failure in a system. Other than that expected system attacker behavior is computed and also risk in real time is been developed. Final contribution is combining these two features to new qualitative measures. Whereas (Spanoudakis, 2008) have proposed a framework that provides increased support for security and dependability attributes . They have presented this framework to monitor mobile P2P applications to detect on property violations.

Conversely (Jonsson et al, 2000) has furthered his research in modelling metrics and evaluation techniques to archive the goal of what is security. The modelling technique presents dependability and security in a common concept. In his perception integrated system model are combining both security aspect vs. object system with dependability attributes vs. object system. As a result a fundamental system model for dependability and security is proposed. The proposed model has still future work to be done and is lack in common coordination between security and dependability that could not solve security problem properly. The integrated model suggested is only based in terms of correctness, protective and behavioural characteristics. Therefore a unified approach is still needed in terms of concepts, tools, and terms used.

Basic Concepts

According to (Sallhammar, 2007) to consider the trustworthy, m-learning system must be both dependable and secure which historically these two main features have been always identified separately. Security encompasses the basic concept of CIA which is confidentiality, integrity and availability. On the other hand dependability generic attributes overlap extensively on security concept explained by (Jonsson et al, 2000) as illustrated in Figure 1, which closely interrelated to one another to get maximum benefits of research results.

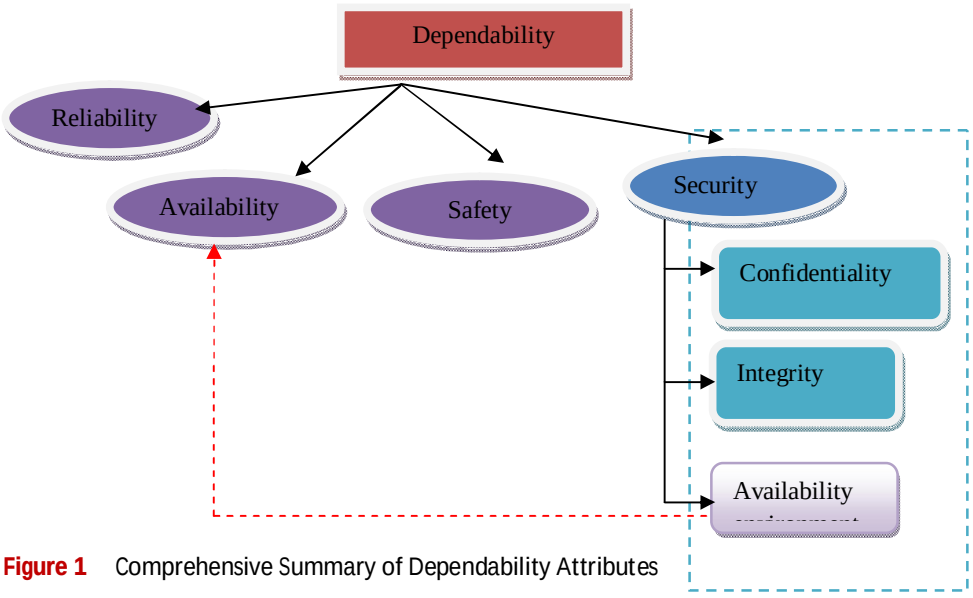

Figure 1 Comprehensive Summary of Dependability Attributes

Security attribute in dependability shows about the services that the system delivers to the environment, this is availability and system's ability to resist external attacks which is integrity. The m-learning system needs the integration of security and dependability because the system is large and complex with rich human interaction which the specifications are likely to be incomplete, ambiguous or inconsistent. Therefore the basic concept of security does not address the problem of ensuring security satisfactory in m-learning system. Dependability attributes are not enough and often conflicting with each other (Nicol et al, 2004).Both dependability and security full fills the basic concept of a computer system which is correct service, service failure, service outage, fault, error and vulnerabilities (Pudar, 2006) and motivates researchers to bring together these two features. In this study the most appropriate integration of attributes are between security and dependability which are theoretically described that behavioural security is an integrated part of dependability and cannot readily be distinguished from it (Jonsson et al., 2000) .

Nevertheless (Ramjan, 2005) has performed a harmonized comparison among eight countries connecting the m-learning problems with solutions by C.I.A and vulnerable points. Almost all the problem faced encounters to the dimension of C.I.A and technological solutions such as authentication, power failure, spyware, virus, malware and server network communication

M-learning need standardization in term of interoperability, portability and reusability with ensemble based mobile devices. As discussed by (Bill, 2004) ensemble devices are getting great effect on individual work, where in ubiquitous computing "an expending array of intelligent handheld devices an increasingly mobile lifestyle are enabling new form of ensemble computing:" Many industries and researchers focus device interoperability in ensemble computing on four major layers in OSI layer (link layer , network layer, data layer and application layer). This standardization is needed for ensemble devices to be used at home, at work and on road. Moreover (Mikic & Anido, n.d.) Stated accessibility plays a key role in learning technology standardization. "Access able design grants a wider range of learners, more options, and greater flexibility in learning environment"

Based on study conducted by (Mostakhdemin-hosseini, 2005) defined framework of mobile learning system is based on three domain: mobile usability, e-learning system and wireless technology. Furthermore a comprehensive research has been conducted on basic elements and characteristic of mobile learning. (Ozdamli & Cavus, 2011) claimed that the core characteristic of mobile learning are ubiquitous, portable, blended, private, interactive, collaborative and instant information

Proposed Framework

After analysing the overall research problem three sub problems has be derived in Table 1.

Table 1 Summary of Sub Research Problem

No	Research problem
RP1	Increase in security vulnerabilities in ensemble and mobile technologies
RP2	In appropriate model for building secure mobile learning content and application
RP3	Unsecured and inadequate dependability towards ensemble based m-learning environment addressing to security issues.

Research Questions

The research question that is addressed in this paper deals with how security framework can be constructed to resolve the mobile learning problem without introducing high cost or restraining the mobile technologies and ensemble computing mobility, performance and lightweight operation. Even though there are promising research result related to the first question, not much effort has been put in second till fourth question. The research will focus on these areas and hopefully provide and answer these questions. The questions have been put into a summary to relate the research question with research problem in Table 2.

Table 2 Summary of Relationship between Research Question and Research Problem

(RP)	(RQ)	Research Question
RP1	RQ1	What are the security issues in m-learning system and ensemble computing?
RP2	RQ2	What are the secure software engineering approaches available for mobile learning systems?
RP1 RP2 RP3	RQ3	Are there models that can be used to evaluate the m-learning system's trustworthiness, in terms of security and dependability behaviour?
	RQ4	How to improve the success of m-learning addressing to security issues

Methodology

Table 3 Summary of Research Methodology

Phase	Task Description	Outcome
Literature Review	To review , analyze and classify The vulnerabilities and threat in ensemble and mobile technologies The countermeasures and detection techniques The attributes of dependability interrelationship with vulnerabilities and countermeasures	Classification of vulnerabilities /threats Classification of countermeasures /detection Improved taxonomy of vulnerabilities and countermeasures integrated with dependability attributes
Analyse	To identify the secure model integrated with security and dependability	Identified improved secure engineering model mapped with taxonomy of vulnerabilities and countermeasures integrated with dependability for ensemble based m-learning system
Design **Implementation** **Test & Validate**	To built , implement and evaluate the improved framework	A secure framework for ensemble based m-learning

Features of Framework

M-learning is a sophisticated learning system which is developed to provide services that place great trust to learners and providers. As suggested here, an integrated system model for dependability and security is highly needed to describe the system in terms of accessibility, behavioural and protective characteristic, in which this complete combination would produce a trusted system. Secure Ensemble Based Mobile Learning System Model (SEBAMOLS) is defined as a proposed secure model in this paper. SEBAMOLS can be defined as end product satisfaction and fitness for use that include availability, reliability and accessibility.

SEBAMOLS will work closely in between the two main attributes; security and dependability in order to evaluate the trust of the learner. The behavioural attributes (availability and reliability) will be mapped with protective attributes (confidentiality, integrity) in the SEBAMOLS model. Taxonomy for threat /vulnerabilities in m-learning and ensemble based mobile devices will be integrated in the model. As

guidelines to the developer, learners and providers standards, policy and best practices will be introduced according to each attributes mapped and layer in the SEBAMOLS.

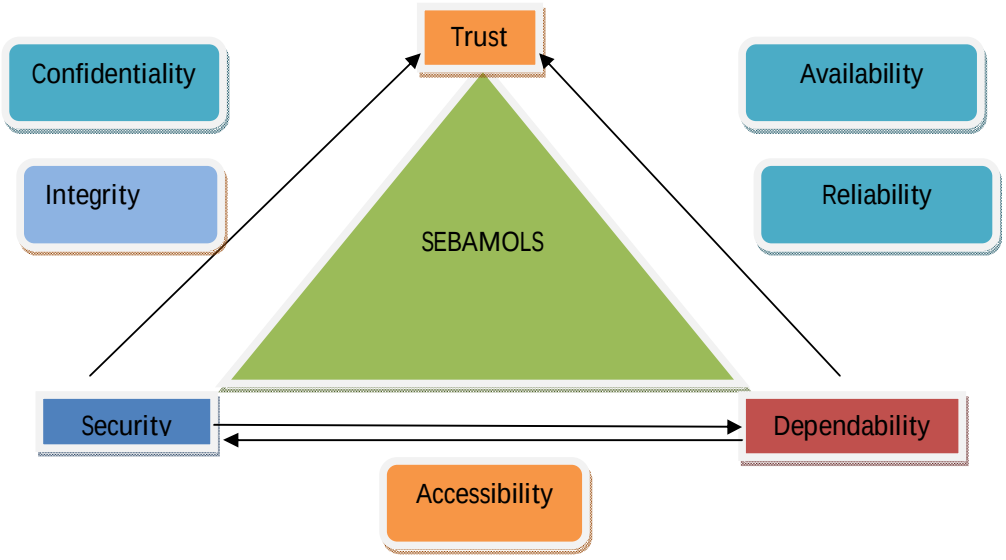

Figure 2 Proposed SEBAMOLS model to be design for M-Learning Security Framework

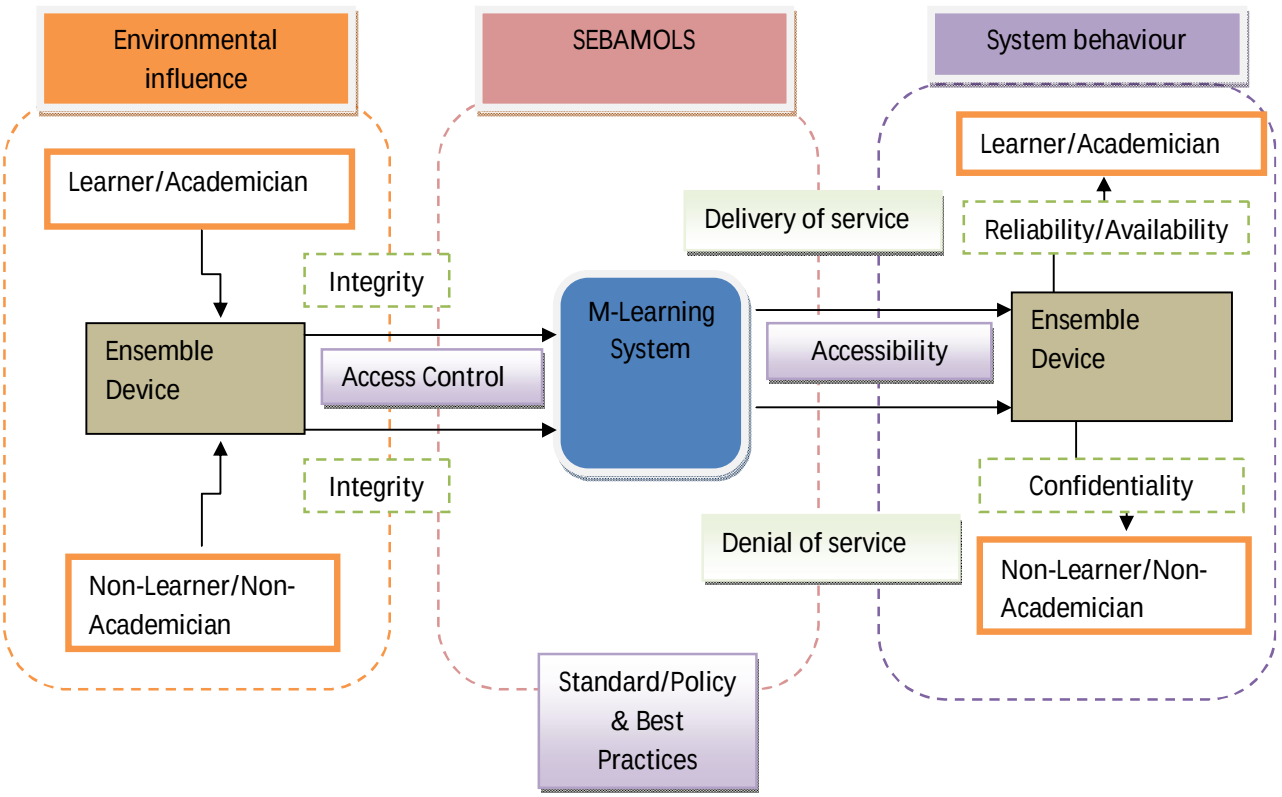

Figure 3 Illustration of Ensemble Based Security Framework for Secure M-Learning System

Since mobile is referring to portability of learning devices, therefore the devices are seen as a transport vehicle of contents accessible at anywhere, anytime, without limitation or constraints. At this point SEBAMOLS works closely during the design phase to standardize the usability and compatibility elements in hardware and software of ensemble devices so that the interoperability of the hardware and software can be continuously work without interruptions. The SEBAMOLS model will be centred on data synchronization between ensemble devices for example Bluetooth synchronization between net book, I pad, iPod, hand phone, I phone and etc. SEBAMOLS manage the ensemble devices and network between the Local LAN which is the M-Learning Cloud and the personal LAN within a low power range of communication which encompasses on green saving, high bandwidth and continuous connectivity.

Security comes in line in this cloud to manage and only allow the learners, academician and devices that are included in the m-learning system to interoperate and access the content. This will be measured on the access control attributes which authorized to the m-learning groups. The key objectives of the SEBAMOLS model here is the capabilities to built a communication among the ensemble devices to have automatic discovery when it is in the m-learning cloud which is announcement of presence in the "neighbourhood" features, ability to request for devices capabilities and easy of plug and play of new devices in the m-learning cloud with secure self organizing network group.

Despite this, the application in M-learning will be organized such away to be used by whatever ensemble device in hand that are registered in the cloud , for example even though email programs viewed differently on each device but the basic functionality remains the same and comes from a single email server. Content of m-learning should be the same in all devices even though the display or interfaces are in different mode. Accessibility should be gain when one device fails to view the content and could be interconnected straight away with another device to able to retrieve the content

Conclusion /Research Contribution

In order to achieve trust and excellent performance from learners who are using m-learning system, the elements of m-learning should be integrated into a model of secure framework. Otherwise positive outcome will not be expected from m-learning applications. These reasons have motivated for a study on the security aspect of m-learning which brings in the trust towards the system in use. The major contribution of this chapter is to propose a secure framework on ensemble based m-learning where security threats and countermeasures are mapped with the dependability and security attributes in a unified model to generate trustworthiness in m-learning. Many important concepts have been illustrated in this framework in order to map the threats and countermeasures, classification of security countermeasures for mobile and ensemble computing are grouped with an improved taxonomy.

References

Alaysia, M. A. I. N. M. (2010). M-L EARNING : A NEW P ARADIGM OF L EARNING. *International Journal*, *2*(4), pp. 76-86.

Bhd, M. (2008). National Wireless Communications Technology Roadmap. *Communications*, 0-37.

Bill, N. (2004). Device Ensembles. *Computer*.

Chen, N.-shing, Wei, C.-wang & Yang, S. J. H. (2008). Designing a Self-contained Group Area Network for Ubiquitous Learning. *Educational Technology & Society*, *11*, pp. 16-26.

Gou, X. (2011). Malaysia uni to use sms for m-learning Articles FutureGov - Transforming Government Education Healthcare. Education IT, Asia Pacific Future Gov.

Hu, J., Khalil, I., Han, S. & Mahmood, A. (2011). Journal of Network and Computer Applications Seamless integration of dependability and security concepts in SOA : A feedback control system based framework and taxonomy $. *Journal of Network and Computer Applications*, *34*, 1150-1159. doi:10.1016/j.jnca.2010.11.013

Jonsson, E., Strömberg, L., & Lindskog, S. (2000). On the functional relation between security and dependability impairments. *Proceedings of the 1999 workshop on New security paradigms NSPW 99*, 104-111. ACM Press. doi:10.1145/335169.335204

Malware Report. (2012), (January).

Meadows, C. (1995). Applying the Dependability Paradigm to Computer Security. *Proceedings of 1995 New Security Paradigms Workshop* (pp. 75-81). IEEE Computer Society Press. doi:10.1109/NSPW.1995.492346

Meadows, C. & McLean, J. (1999). Security and dependability: then and now. *Proceedings Computer Security, Dependability, and Assurance: From Needs to Solutions (Cat. No.98EX358)*, 166-170. IEEE Comput. Soc. doi:10.1109/CSDA.1998.798363

Mikic, F., & Anido, L. (n.d.). Towards a Standard for Mobile E-Learning. *International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies (ICNICONSMCL'06)*, pp. 217-217. IEEE. doi:10.1109/ICNICONSMCL.2006.213

Mostakhdemin-hosseini, A. (2005). Mobile learning framework. *Development*, *3*, 203-207.

Nicol, D. M., Sanders, W. H. & Trivedi, K. S. (2004). *Model-based evaluation: from dependability to security*. *Ieee Transactions On Dependable And Secure Computing* (Vol. 1, pp. 48-65). IEEE Computer Society. doi:10.1109/TDSC.2004.11

Ozdamli, F. & Cavus, N. (2011). Social and. doi:10.1016/j.sbspro.2011.11.173

Pudar, S. (2006). Basic concepts and Taxonomy of Dependable and Secure Computing. *Security*.

Ramjan, S. (2005). The conceptual framework of mLearning security for university in Thailand. *International Journal*.

Sallhammar, K. (2007). *Karin Sallhammar Stochastic Models for Combined Security and Dependability Evaluation*. *Science And Technology*.

Schooler, E., Jelinek, L. & Dahle, D. (2010). ENSEMBLE COMPUTING : OPPORTUNITIES AND CHALLENGES components , Device Ensembles Ensembles .", *14*(1), pp. 118-141.

Spanoudakis, G. (2008). Monitoring Security and Dependability in Mobile P2P Systems. *Architecture*.

Technologies, I. S., Dooly, Z., Clarke, J., Fitzgerald, W., Donnelly, W., Riguidel, M., Howker, K., et al (2010). D3 . 3 – ICT Security & Dependability Research beyond 2010 : Final strategy. *Security*, (004547).

Vassiljev, A. (2010). MASTER 'S THESIS Enhancing the Hierarchical Framework Model of Mobile Security. *Review Literature And Arts Of The Americas*.

Wiesauer, A. & Sametinger, J. (2007). A SECURITY DESIGN PATTERN TAXONOMY Findings of a Systematic Literature Review.