



A NEW LEARNER'S SECURITY BEHAVIOR MODEL FOR M-LEARNING IN MALAYSIAN HIGHER EDUCATION INSTITUTION

SHEILA MAHALINGAM

DOCTOR OF PHILOSOPHY

2017



Faculty of Information and Communication Technology

**A NEW LEARNER'S SECURITY BEHAVIOR MODEL FOR M-
LEARNING IN MALAYSIAN HIGHER EDUCATION INSTITUTION**

Sheila Mahalingam

Doctor of Philosophy

2017

**A NEW LEARNER'S SECURITY BEHAVIOR MODEL FOR M-LEARNING IN
MALAYSIAN HIGHER EDUCATION INSTITUTION**

SHEILA MAHALINGAM

**A thesis submitted
in fulfillment of the requirements for the degree of Doctor of Philosophy**

Faculty of Information and Communication Technology

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

2017

DECLARATION

I declare that this thesis entitled “A New Learner’s Security Behaviour Model for M-Learning in Malaysian Higher Education Institution” is the result of my own research except as cited in the references. The thesis has not been accepted for any degree and is not concurrently submitted in candidature of any other degree.

Signature :

Name :

Date :

APPROVAL

I hereby declare that I have read this thesis and in my opinion this thesis is sufficient in term of scope and quality for the award of Doctor of Philosophy.

Signature :

Supervisor Name :

Date :

DEDICATION

Dear God

I devoted my life and death to You, God. May my life is within your guidance.

Dear Parent

Thank you for your sacrifice and love. No such compensate except from God.

Dear Beloved Husband and Children

Thank you for your love, support, patience and encouragement that give me strength to finish this study. May God bless us, guide us and protect us to be good person.

Dear Teachers and Supervisors

Thank you for all the knowledge. May your knowledge are beneficial and useful for all humanity.

Dear Siblings

Thank you for your motivation and love.

Dear Friends

Thank you for all the knowledge, guide, encouragement and love. May our friendships blessed by God.

ABSTRACT

The motivation to conduct this research came from the awareness that the mobile device exposes m-Learning to security threats and vulnerabilities. The most unfocused issues were the mobile security behavior on learners itself; despite statistically determined that the risks are developing each day on mobile application and devices. Literature has pointed out that learners' security behavior required to be addressed to control the mobile security threats. This research proposes a learner's security behavioral model for mobile learning in Malaysia Higher Education Institutions (HEIs). With the security behavior reflection, this model aimed to improve the implementation and management of mobile security in m-Learning taking consideration of the learners' perspective. This research consisted of four phases, Planning phase, Data Collection Phase, Analysis Phase and Model Development Phase. Four mix-method studies were conducted to generate the dimensions for the model development. Review from the experts and risk based analysis approach confirmed the research findings and validated the practicality of addressing the learners' behaviors in mobile security. This research contributed to better understanding of the learners' complexity in mobile security. The research suggested that learners' security behavior view is significant in preparing mobile security model. This model found to be compatible and qualified, providing the m-Learning learners' perception within possible security threats that significantly controls to defend against malicious and non-malicious attacks. This approach can guide on what can be done to improve learners' participation and responsibilities on securing m-Learning. This research also extended the existing knowledge of mobile security and m-Learning fields by focusing analytically on the intersection of both fields. New knowledge about mobile security in the m-Learning from the learners' security behavior perspective was derived in this research.

ABSTRAK

Motivasi untuk menjalankan penyelidikan ini telah datang daripada kesedaran bahawa peranti mudah alih mendedahkan m-pembelajaran kepada ancaman keselamatan dan kelemahan. Isu yang paling tidak difokuskan adalah tingkah laku keselamatan peranti mudah alih pada pelajar itu sendiri, walaupun statistik menunjukkan bahawa risiko yang tinggi pada aplikasi mudah alih dan peranti. Kajian literasi telah menunjukkan bahawa tingkah laku pelajar yang perlu ditangani untuk mengawal ancaman keselamatan mudah alih. Penyelidikan ini mencadangkan model tingkah laku keselamatan peranti mudah alih pelajar untuk pembelajaran mudah alih di Institusi Pengajian Tinggi Malaysia(IPT). Dengan berlandaskan refleksi tingkah laku keselamatan, model ini bertujuan untuk menambah baik pelaksanaan dan pengurusan keselamatan mudah alih dalam m-pembelajaran yang mengambil kira perspektif pelajar. Penyelidikan ini terdiri daripada empat fasa iaitu fasa perancangan, fasa pengumpulan data, fasa analisis dan fasa pembangunan model. Empat kajian yang berasaskan kaedah campuran kuantitatif dan kualitatif telah dijalankan untuk menjana dimensi untuk pembangunan model. Penyelidikan yang disyorkan menunjukkan bahawa pandangan tingkah laku keselamatan pelajar adalah penting dalam menyediakan model keselamatan mudah alih. Model ini didapati serasi dan layak memberikan persepsi m-pembelajaran pelajar dalam ancaman keselamatan yang mungkin terkawal untuk mempertahankan serangan berniat jahat atau sebaliknya. Pendekatan ini boleh menjurus kepada apa yang boleh dilakukan untuk meningkatkan penyertaan dan tanggungjawab pelajar ke arah m-pembelajaran. Kajian ini juga memperluaskan pengetahuan sedia ada dalam bidang keselamatan dan m-pembelajaran mudah alih dengan memberi tumpuan secara analisis di dalam kedua-dua bidang. Pengetahuan baharu tentang keselamatan mudah alih dalam m-pembelajaran daripada perspektif tingkah laku keselamatan pelajar telah diperolehi melalui kajian ini.

ACKNOWLEDGEMENTS

This has been a long journey and it is full with memories. The journey has indeed been unforgettable. Nevertheless, a lot of lessons have been learned; and a lot of effort has been invested. First and foremost, I would like to thank God for giving me excellence health, physical and mental strength and comfortable study environments for me to complete this thesis as scheduled. I would like to take this opportunity to express my sincere acknowledgement to my supervisor Professor Madya Dr. Mohd Faizal bin Abdollah from the Faculty of Information and Communication Technology, for his continues support, motivation, guidance, patience and understanding concerning my family throughout the study has been greatly appreciated. I would like to thank my co-supervisor of this project Professor Datuk Dr.Hj. Shahrin bin Sahib, Vice Chancellor of Universiti Teknikal Malaysia Melaka (UTeM) for his guidance and supervision. My greatest thanks is to my parents and family you all are the source of inspirations with the word of wisdoms and straight talking, who has always been with me. Supported my ups and down on this journey. Thanks to my family members for their continuous understanding, motivation, and encouragement throughout my PhD journey. I would like to extend my thanks to the staff of Fakulti Teknologi Maklumat dan Komunikasi (FTMK) and Pusat Pengajian Siswazah (PPS UTeM) for their time, guidance and support during my studies. Greatest appreciation goes to Universiti Teknikal Malaysia Melaka and Jabatan Perkhidmatan Awam Malaysia for sponsoring this study. Lastly, but in no sense the least, I am thankful to all colleagues and friends for their valuable time, understanding, suggestions comments and continuous motivation which made my PhD years a memorable and valuable experience.

TABLE OF CONTENTS

	PAGE
DECLARATION	
APPROVAL	
DEDICATION	
ABSTRACT	i
ABSTRAK	ii
ACKNOWLEDGEMENTS	iii
TABLE OF CONTENTS	iv
LIST OF TABLES	vii
LIST OF FIGURES	x
LIST OF APPENDICES	xii
LIST OF ABBREVIATIONS	xiii
LIST OF PUBLICATIONS	xv
CHAPTER	
1. INTRODUCTION	1
1.1 Introduction	1
1.2 Background of Research	1
1.3 Research Problem	2
1.3.1 Mobile Technologies Security	3
1.3.2 m-Learning Security	4
1.3.3 Learners Security Behaviour	5
1.4 Research Question	7
1.5 Research Objectives	9
1.6 Operational Framework	10
1.7 Contribution of Knowledge	11
1.8 Research Scope	13
1.9 Operational Definition	14
1.9.1 Mobile Learning (m-Learning)	15
1.9.2 Learner	15
1.9.3 Learner's Security Behavior	16
1.10 Thesis Organization	17
2. LITERATURE REVIEW	19
2.1 Introduction	19
2.2 Chapter Objective	19
2.3 Literature Review Process	19
2.4 Overview Mobile Technologies	20
2.4.1 Mobile Security Threats and Vulnerabilities	23
2.4.2 Mobile Technologies Threats and Vulnerabilities in Malaysia	26
2.4.3 Mobile Threats (Malicious/Intended Threats)	27
2.4.4 Mobile Threats (Non-Malicious/Unintended Threats)	30
2.4.5 Mobile Security Management	36
2.4.6 Mobile Security Risk Management	39

2.4.7	Summary of Mobile Technologies Security	40
2.5	Mobile Learning	41
2.5.1	Malaysia Higher Education Institution (HEI) and Mobile Learning	46
2.5.2	Framework and Model Involved in M-Learning	49
2.5.3	Summary of Mobile Learning and Malaysia Context	54
2.6	Security in m-Learning	55
2.6.1	Security in Mobile Learning (Malaysia Context)	57
2.6.2	Mobile Learning Issues and Challenges	59
2.6.3	Mobile Learners' Security Risk	61
2.6.4	Summary of Security in M-Learning	62
2.7	Mobile Learner Security Behaviour	64
2.7.1	Integration of Security and Dependability	66
2.7.2	Summary of Integration of Security and Dependability	71
2.8	Gaps in Literature	77
2.9	Theoretical Background and Hypothesis	79
2.9.1	Research Variables and Hypothesis	84
2.10	Research Framework	90
2.11	Chapter Summary	91
3.	RESEARCH METHODOLOGY	93
3.1	Introduction	93
3.2	Research Philosophies	93
3.3	Mixed Method and Triangulation	94
3.4	Research Design	95
3.5	Quantitative Method	99
3.5.1	Population and Sampling	99
3.5.2	Phase1: Study 1(Descriptive)	99
3.5.2.1	Sampling Procedure (Study 1)	101
3.5.3	Phase 2: Study 3 (Correlation and Regression)	102
3.5.3.1	Sampling Procedure (Study 3)	103
3.5.4	Instrumentation Development and Measurement (Study 1 and Study 3)	106
3.5.5	Operationalization of the Construct	108
3.5.6	Common Method Variance	109
3.5.7	Pre Testing of Research Instrument	111
3.5.7.1	Phase 1: Study 1	111
3.5.7.2	Phase 2: Study 3	111
3.5.8	Reliability and Validity (Study 1 and Study 3)	112
3.5.9	Data Collection	113
3.5.10	Data Analysis	114
3.6	Qualitative Method	117
3.6.1	Phase 1 Study 2(Focus Group Interview)	117
3.6.2	Sampling procedure (Focus Group Interview)	118
3.6.3	Method of Focus Group Interview	119
3.6.4	Analysis Method for Focus Group Interview	122
3.6.5	Verification Procedures	123
3.6.6	Phase 2: Study 4 (Focus Group Discussion)	125
3.6.7	Sampling Procedure (Focus Group Discussion)	126

3.6.8	Method of Focus group Discussion Conducted	126
3.6.9	Analysis Method for the Focus Group Discussion	127
3.6.9.1	Likelihood Definition	129
3.6.9.2	Impact	130
3.7	Validation Method	135
3.7.1	Risk Based Approach	136
3.7.1.1	Method	136
3.7.2	Expert Review	139
3.7.2.1	Method	140
3.7.2.2	Model Evaluation Question	141
3.7.2.3	The Expert Background	141
3.8	Chapter Summary	143
4.	DEVELOPMENT OF M-LEARNING SECURITY MODEL	145
4.1	Introduction	145
4.2	Study 1 : Learner's Perception on Mobile Security in M-Learning	147
4.2.1	Purpose	147
4.2.2	Findings and Results	147
4.2.2.1	Demographics	148
4.2.2.2	Mobile Device Usage	149
4.2.2.3	Security Feelings	151
4.2.2.4	Security Awareness	152
4.2.2.5	Summary and Key Findings of Study 1	166
4.3	Study 2 : Stakeholder in (Ministry, ICT Directors in HEI and Expert) Perception of Mobile Device Security in M-Learning	167
4.3.1	Purpose	167
4.3.1.1	M-Learning Implementation	168
4.3.1.2	Challenges and Issues in M-Learning environment	169
4.3.1.3	Acceptance of M-Learning among students	171
4.3.1.4	Security Threats and Incidents	173
4.3.1.5	Current plans on policy and guidelines on addressing the Security Challenges	177
4.3.1.6	Summary and Key Findings of Study 2	179
4.4	Phase 2: Study 3 (Regression Analysis)	182
4.4.1	Respondent Background	183
4.4.2	Correlation Analysis	183
4.4.3	Hypothesis Testing	184
4.4.4	Hypothesis Conclusion	187
4.4.5	Summary of Key Findings of Study 3	189
4.5	Phase 2 : Study 4 (Threat and Risk Analysis)	191
4.5.1	Step1: Understand Environment Requirement & Objectives, Risk Tolerance and Boundaries	191
4.5.2	Step 2: Mobile Device & Mobile VLE application Vulnerabilities, Threats and Existing Controls	193
4.5.3	Step 3: Assess Risk Based on Impact and Likelihood	202
4.5.4	Step 4: Determination Risk Response Document, Final Risk Determination and Approval /Acceptance	211
4.5.5	Step 5: Ongoing Monitoring of Risk and Responses	219
4.6	Construct Mobile Learners Security Model	228

4.7	Summary and key Findings	231
5.	CHAPTER 5 MODEL EVALUATION AND VALIDATION	233
5.1	Chapter Objectives	233
5.2	Chapter outline	233
5.3	Study 5a : Control Focus Group of Final Risk Based Assessment	234
5.3.1	Result and Findings	244
5.3.2	Summary and Research Implication	248
5.4	Study 5b: Panel Expert review	250
5.4.1	Findings of Expert Review Session	257
5.4.1.1	Practicality of Using MOBILES in M-Learning	257
5.4.1.2	Degree to Which Findings Reflect Reality	259
5.4.1.3	The applicability of Research Findings	259
5.4.1.4	Use of Research Findings in the Wider Context Of Mobile ISM	261
5.5	Chapter Summary	262
6.	CHAPTER 6 DISCUSSION AND CONCLUSION	263
6.1	Introduction	263
6.2	Discussion of the Research Findings	264
6.2.1	Research Question 1	266
6.2.2	Research Question 2	269
6.2.3	Research Question 3	271
6.3	Summary of Findings & Implication	272
6.3.1	Field of Mobile technologies security	272
6.3.2	Field of M-Learning Security & Malaysia Context	272
6.3.3	Field of Social Technical System	274
6.4	Conclusion	274
6.4.1	Summary of Research Process	274
6.4.2	Summary of Research Findings	275
6.4.3	Contribution to Theoretical Knowledge	277
6.4.3.1	Mobile Security Community	277
6.4.3.2	M-Learning Community	278
6.4.3.3	Other Mobile Service Community	279
6.4.4	Research Limitations	279
6.4.5	Future Work	280
6.5	Research Summary	280
	REFERENCES	282
	APPENDICES	317

LIST OF TABLES

TABLE	TITLE	PAGE
1.1	Summary of Sub Research Problem	6
1.2	Research Question	6
1.3	Summary of Research Question & Research Problem	7
1.4	Summary of Research Objective	8
1.5	Summary of Research Contribution	10
2.1	Summary of Mobile Threats & Attack from Various Researchers	21
2.2	Summarized Cyber Security Incidents Categorized by Threats Attack	24
2.3	Mobile Device & Mobile Application Human Error Classification	28
2.4	Characteristic of m-Learning	36
2.5	Existing m-Learning Model	41
2.6	Review of Theoretical Foundation	65
2.7	Hypothesis Definition	70
3.1	Total number second year undergraduate	81
3.2	Summary of proportionate sample size	84
3.3	Total of scale item to measure each content	86
3.4	Constructs & Sources of the instruments	87
3.5	Guilford's Rule of	93
3.6	List of Focus Group Interviewees	96

3.7	Likelihood	99
3.8	Impact Definition	104
3.9	Simplified Risk Matrix	105
4.1	Demographic Information for Respondents	118
4.2	Frequently Used Application in Mobile Device	116
4.3	Information Stored in Mobile Device	120
4.4	Security Awareness Category	122
4.5	Type of Wi-Fi Connection on Mobile Device	126
4.6	Security (Password and Authentication)	127
4.7	Cross Tabulation between Mobile Phone IMEI and Age	129
4.8	Awareness of Mobile Security Threats among IT Professional in HEI	140
4.9	Challenges for IT Department in HEIs	141
4.10	Demographic Features of study respondent	146
4.11	Correlation Matrix	147
4.12	Regression Analysis Result	148
4.13	The result of Hypothesis Testing	151
4.14	Mobile Device Overview	153
4.15	Mobile VLE Application in m-Learning	154
4.16	Mobile Device and Mobile VLE Application Threats	155
4.17	Mobile VLE application and Mobile Device Vulnerabilities Category	157
4.18	Threats per application in m-Learning VLE	160
4.19	Threats per application in mobile device	161
4.20	Value of impact designed for mobile learners VLE App	164

4.21	Value of impact designed for mobile device	165
4.22	Mobile Learning VLE application Threat Risk Matrix	173
4.23	Mobile Device Threat Risk Matrix	174
4.24	Mobile VLE application Threat Ranking	176
4.25	Mobile Device Threat Ranking	178
4.26	Non- Malicious Threat Category, Security Pillar, & Countermeasure	182
5.1	Summary of Probability Occurrence	194
5.2	Threats (Human Error) with the impact value	196
5.3	Template of Effectiveness Value for Student	197
5.4	Existing Risk Control & Proposed Risk Control	198
5.5	Critical Threat by m-Learning VLE App	205
5.6	Critical Threat by Mobile Device	206
5.7	Overall Summary of Security Behavior	208
5.8	Risk Controls Mapped with ISM Elements	210

LIST OF FIGURES

FIGURE	TITLE	PAGE
1.1	Four Phases of Operational Framework	9
2.1	Type of Smartphone Operating System	17
2.2	Mobile Penetration Rates	18
2.3	Relationship with E-Learning	35
2.4	The FRAME Model	40
2.5	Introducing Security into Dependability	52
2.6	Interrelated Security Attributes	53
2.7	Taxonomy of Dependability & Security	54
2.8	An Integrated Model of Security and Dependability	54
2.9	New Threat Combination between Security and Dependability	57
2.10	Summary of Dependability Attributes	58
2.11	Summary of Security Attributes	59
2.12	Summary of Gaps in Literature	63
2.13	The Proposed Research Hypothesis	71
2.14	Identified Independent and Dependent Variable	72
3.1	Data Collection and Analysis Phase	77
3.2	General Risk Analysis Model	102
4.1	Framework of Phase 1 and Phase 2 Analysis	116

4.2	Mobile operating system	119
4.3	Downloading Mobile App	123
4.4	Data Backup in Mobile Device	124
4.5	Important Password and Sensitive Data Stored	125
4.6	Auto login setting for social networking application	127
4.7	Retrieving data from lost mobile device	128
4.8	Wi-Fi & Bluetooth status	130
4.9	Update security features & operating system on mobile device	131
4.10	Antivirus Usage of Mobile Device	132
4.11	Graphical Representative of Beta Value	149
4.12	Mobile Learners Security Model (MOBILES)	191
5.1	Framework for Model Evaluation and Validation	195

LIST OF APPENDICES

APPENDIX	TITLE	PAGE
APPENDIX A	Desk Analysis Top Mobile Threats Report (2011-2015 April)	259
APPENDIX B	Summarized Malicious Threat (Intentional Threats)	261
APPENDIX C	Questionnaire (Study 1)	263
APPENDIX D	Questionnaire (Study 3)	266
APPENDIX E	Survey/Interview Validation Rubric	269
APPENDIX F	Form Validation Specialist	271
APPENDIX G	Interview Question (Study 2)	275
APPENDIX I	Online Risk Assessment (Study 5a)	277
APPENDIX J	Mobile Security Awareness Workshop (Focus Group Discussion Study 5a)	278
APPENDIX K	Consent Letter to Panel Experts Validation	280
APPENDIX L	Sample Threat Analysis Result (Mobile VLE App and Mobile Device)	284

LIST OF ABBREVIATIONS/SYMBOLS

BYOD	Bring Your Own Device
CAPs	Critical Agenda Projects
CIA	Confidentiality , Integrity, Availability
CPA	Critical Agenda Projects
E-Learning	Electronic Learning
FMEA	Failure Mode and Effect Analysis
GPS	Global Positioning System
GSM	Global System for Mobile Communication
HD2	High Definition 2
HEI	Higher Education Institution
HSPA	High Speed Packet Access
ICT	Information Communication and Technology
IEEE	Institute of Electrical and Electronics Engineers
IFIP WG	International Federation For Information Processing Working Group
IMT-2000	Is the term used by the International Telecommunications Union (ITU) for a set of globally harmonized standards for third generation (3G) mobile telecoms services and equipment
iOS	an operating system used for mobile devices manufactured by Apple Inc.
IT	Information Technology
ITU	International Telecommunication Union
ISM	Information Security Management
KRA	Key Result Area

LTE	Long-Term Evolution
MAFTIA	Malicious and Accidental Fault Tolerance for Internet Applications
MIS	Management Information System
M-Learner	Mobile Learners
M-Learning	Mobile Learning
MMS	Multimedia Messaging Service
MOBILES	Mobile Learners Security Model
MOE	Ministry Of Education
MOHE	Ministry of Higher Education
MyCert	Malaysia Computer Emergency Response Team
NMT	Nordic Mobile Telephony
PC	Personal Computer
PDA	Personal Device Assistance
RPN	Risk Priority Number
SMS	Short Messaging Service
TAM	Technology Acceptance Model
UMTS	Universal Mobile Telecommunications System
UNESCO	United Nations Educational, Scientific and Cultural Organization
VM	Virtual Machine
WAP	Wireless Application Protocol
WiMAX	Worldwide Interoperability for Microwave Access

LIST OF PUBLICATIONS

CONFERENCE PUBLICATION

1. Presented Research Paper of Title: “Mobile Learning: Towards Secure Learning Environment” Sheila M, Faizal M. A., Shahrin S , in the 12th International Conference on Information (ICI 12)12th to 13th Dec 2012. Abstract and Full Paper is published in the Conference Proceedings.
2. Presented research paper title: Learner Centric in M-Learning: Integration of Security, Dependability and Trust (Short Paper) and Learners’ Ensemble Based Security Conceptual Model For M-Learning System in Malaysian Higher Learning Institution (Reflection Paper), Sheila M *1, Faizal M. A.*2, Shahrin S at 10th International Conference on Mobile Learning 2014 , Madrid , Spain 28 February -2 March 2014 . Both papers are published in Proceeding of the 10th International Conference on Mobile Learning IADIS ML2014 Book (ISBN: 978-989-8704-02-3).
3. Presented research paper title: The Implementation of Mixed Method in Developing a Mobile Learners Security Framework at International Conference on Computational Science and Technology, Sheila M, Faizal M. A., Shahrin S, 2014 (ICCST’14) organized by University Malaysia Sabah with IEEE organization, 27-28 August 2014, Kota Kinabalu, Sabah. DOI:10.1109/ICCTST.2014.7045177. <http://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?punumber=7031546>
4. Presented paper title: “BYOD: Managing Mobile Learning Security in Malaysia Higher Learning Institutions”, Sheila M, Faizal M. A., Shahrin S, for presentation in 1st international Conference on Educational Studies (ICES-2015), at Pulai Spring Resort, Johor Bahru, Malaysia to be held on June 3-4, 2015.
5. Presented Paper Title: “A Conceptual Framework for Learner’s Security Behavior in M-Learning Environment”. International Conference on Teaching and Learning (ICTL 2016) on 5-6 October, 2016 in Kuala Lumpur.

JOURNAL PUBLICATION

1. Published Article on The Malaysian Journal of Education Technology (MJET) impact factor 0.7490 9 (2012) Global Institute for Scientific Information (GISI). Volume 12, Number 3, September 2012 pp. 33-41. Title: Designing Ensemble Based Security Framework for Secure M-Learning System in Malaysia Higher Learning Institution.
2. Published Article in European Journal of Scientific Research (ISSN 1450-216X/1450-202X). Vol. 114 No 2, November, 2013, pp.408-422.
Title: Systematic Review on Mobile Learning Research Initiatives and Implementation.
<http://www.europeanjournalofscientificresearch.com>. Journal is indexed in Scopus Database with impact factor 0.713.
3. Published article in International Journal of Distance Education Technologies (IJDET), Vol.12, No 2, April-June 2014, pp 66-81. Title: Designing Ensemble Based Security Framework for M-Learning System, [Sheila Mahalingam](#), [Mohd Faizal bin Abdollah](#), Shahrin bin Sahib, ISSN: 1539-3100. doi:[10.4018/ijdet.2014040104](https://doi.org/10.4018/ijdet.2014040104). IGI Publishing Hershey, PA, USA .Journal index in ISI and Scopus. SJR value 0.18
4. Published article in International Journal of Mobile Learning and Organization (IJMLO) Inderscience Publishers, Geneva, Switzerland, accessible through the ACM digital library and *indexed* in Scopus. Title: Dimension of Mobile Security Model: Mobile User Security Threats and Awareness, Sheila M, Faizal M. A., Shahrin S. Int. J. Of Mobile Learning and Organization, 2015vol.9, No.1, Pp.66–85. ISSN: 1746-725x, EISSN: 1746-7268, DOI: 10.1504/IJMLO.2015.069718
5. Sheila M., Faizal M. A. and Shahrin S. [“Managing Mobile Learning Security in Malaysia Higher Learning Institutions.”](#) In Man in India, Serials Publications Quarterly, ISSN: 0025-1569, No.96 (2016), No.1 (2016), pp. 19-37. http://serialsjournals.com/articles.php?volumesno_id=917&journals_id=40&volumes_id=836

/

CHAPTER 1

INTRODUCTION

1.1 Introduction

The specific components discussed in this chapter include background of the research, the research problem, the research questions, the research objectives and the conceptual framework that guide this research.

1.2 Background of Research

Today, wireless and the mobile application has become a very famous technology among the 21st century generation. According to Gartner's report Gartner (2011) there is a massive increase in mobile device technology penetration. As stated by Magdirila (2013) in Nielson Report, Malaysia is ranked as the 3rd in Asia region for mobile device adoption. Hence, On Device Research (2014) reported Malaysia has the youngest users which the age ranked between 20 to 49. The transformation of mobile technologies continues to develop with the entrance of smaller, more complicated and powerful devices which are capable of transferring data in a variety of formats anywhere, at any time. Certainly, the openings for changes in this area are diverse and continually supporting the focus of all the stakeholders associated from higher learning institutions.

Without a doubt, Malaysia is characterized as having established market for mobile technology, demonstrating high market penetration of mobile phones that enables Mobile