FEASIBILITY STUDY OF THE ACCEPTANCE OF E-ASSESSMENT BY LECTURERS FROM SECURITY PERSPECTIVE

KAVITHA A/P THAMADHARAN

A project report submitted in partial fulfilment of the requirements for the award of the degree of Master of Science (Information Assurance)

Advanced Informatics School
Universiti Teknologi Malaysia

JUNE 2015
To my beloved father and mother
ACKNOWLEDGEMENT

First of all, I would like to express my gratitude to my supervisor, Dr Nurazean Maarop, for the guidance throughout this research and to introduce me to the topic as well as for the support all the way to complete this project paper. Without her continuous support, I would have not able to present the thesis as here.

Furthermore, I would like to thank my parents for being supportive and for all the prayers for me to complete the project paper successfully. At the end, I would like to express appreciation to my fiancé and friends who had provided assistance, motivate and supported me in writing this project paper.
ABSTRACT

The role of technology in education system has enriched the teaching and learning process, be it from preschool to higher universities education. The development of online education systems such as e-learning and e-assessment provide many advantages to the users especially the flexibility in teaching and learning. The online education system has the capability to improve the quality of delivery education. However, security risks have been the major weakness in the acceptance of technology in education field which limits the user acceptance of the online education system. Even though there are other studies providing solutions for identified security threats in online education usage, there is no particular model which addresses the factors that influences the acceptance of e-assessment system by lecturers from security perspective. The aim of this study is to explore security aspects of e-assessment in regard to the acceptance of technology. A conceptual framework of secure acceptance of e-assessment is proposed and analysed. Both human and security factors are considered in the formulation of this conceptual framework. The data for this study was collected through online survey and paper-based survey. This study proves that security factors mainly influence the acceptance of e-assessment by lecturers. This study will be useful in providing more insightful understanding regarding relationships of factors towards the acceptance of e-assessment system considering the security perspective.
ABSTRAK

# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>CHAPTER</th>
<th>TITLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>DECLARATION</td>
<td></td>
<td>ii</td>
</tr>
<tr>
<td>DEDICATION</td>
<td></td>
<td>iii</td>
</tr>
<tr>
<td>ACKNOWLEDGEMENT</td>
<td></td>
<td>iv</td>
</tr>
<tr>
<td>ABSTRACT</td>
<td></td>
<td>v</td>
</tr>
<tr>
<td>ABSTRAK</td>
<td></td>
<td>vi</td>
</tr>
<tr>
<td>TABLE OF CONTENTS</td>
<td></td>
<td>vii</td>
</tr>
<tr>
<td>LIST OF TABLES</td>
<td></td>
<td>xiii</td>
</tr>
<tr>
<td>LIST OF FIGURES</td>
<td></td>
<td>xvii</td>
</tr>
<tr>
<td>LIST OF ABBREVIATIONS</td>
<td></td>
<td>xviii</td>
</tr>
<tr>
<td>LIST OF APPENDICES</td>
<td></td>
<td>xix</td>
</tr>
<tr>
<td>1</td>
<td>INTRODUCTION</td>
<td>1</td>
</tr>
<tr>
<td>1.0 Overview</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>1.1 Background of the Problem</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>1.2 Problem Statement</td>
<td></td>
<td>4</td>
</tr>
<tr>
<td>1.3 Project Aim</td>
<td></td>
<td>5</td>
</tr>
<tr>
<td>1.4 Research Objectives</td>
<td></td>
<td>5</td>
</tr>
<tr>
<td>1.5 Research Questions</td>
<td></td>
<td>5</td>
</tr>
<tr>
<td>1.6 Scope of Study</td>
<td></td>
<td>6</td>
</tr>
</tbody>
</table>
1.7 Significance of Study

1.7.1 Theoretical Significance 7
1.7.2 Practical Significance 7
1.7.3 Methodological Significance 8

1.8 Summary 8

2 LITERATURE REVIEW 9

2.0 Introduction 9

2.1 Role of Technology in Education System 9

2.2 E-Learning 11

2.2.1 Definitions of E-Learning 11
2.2.2 Benefits of E-Learning 12
2.2.3 Summary of E-Learning 13

2.3 E-Assessment 14

2.3.1 Definitions of E-Assessment 14
2.3.2 Advantages of E-Assessment 15
2.3.3 Disadvantages of E-Assessment 16
2.3.4 Summary of E-Assessment 16

2.4 Definition of Security 17

2.5 Factors that Influence Acceptance of Online Learning System from Security Perspective 17

2.5.1 Summarized table on Factors that Influence Acceptance of Online Learning System from Security Perspective 17

2.5.2 Summary of Factors that Influence Acceptance of Online Learning System from Security Perspective 26

2.6 Security Issues in E-Assessment System 27

2.7 Theory Model Related to Acceptance of E-Learning and E-Assessment 30

2.7.1 Theory of Reasoned Action (TRA) 30
2.7.2 Technology Acceptance Model (TAM)  
31
2.7.3 Theory of Planned Behaviour (TPB)  
32
2.7.4 Unified Theory of Acceptance and Use of Technology (UTAUT)  
33
2.7.5 Teachers’ E-Assessment Acceptance Model (TEAM)  
35
2.7.6 Information System Success Model (IS)  
36
2.7.7 SERVQUAL Model  
37
2.7.8 Theory Model by Findik and Ozkan (2010)  
38

2.8 Theory Model related to Acceptance of Technology from Security Perspective  
39
2.8.1 Theory Model by Alkis and Ozkan (2010)  
40
2.8.2 Theory Model by Abbad (2012)  
41
2.8.3 Theory Model by Zaman et al (2013)  
42
2.8.4 Theory Model by Wang (2010)  
43

2.9 Base Model and Key Findings that Contributes to the Acceptance of Online Learning  
44
2.9.1 Summarized Base Model and Key Findings that Contributes to the Acceptance of Online Learning  
52

2.10 Related Studies as Per User Type  
53
2.10.1 Summary of Related Studies as Per User Type  
60

2.11 Conclusion  
63

3 CONCEPTUAL FRAMEWORK AND HYPOTHESES  
64
3.0 Introduction  
64
3.1 Findings of Theoretical and Models Review  
65
3.1.1 Model Selection and Justification for Human Behaviour and Information System Factors  
65
3.1.2 Summary of Model Selection and Justification for Human Behaviour and Information System Factors 72
3.1.3 Model Selection and Justification for Perceived Security Factors 74
3.1.4 Summary of Model Selection and Justification for Perceived Security Factors 79
3.2 Secure Acceptance of E-Assessment Framework 81
3.3 Variables and Hypotheses Formulation 82
  3.3.1 Expected Behavioural Intention (EBI) 83
  3.3.2 Human Behaviour and Information System Factors 83
    3.3.2.1 Expected Usefulness 84
    3.3.2.2 Quality 84
  3.3.3 Perceived Security Factors 85
    3.3.3.1 Trust 85
    3.3.3.2 Information Security Knowledge 86
    3.3.3.3 Ethical Behaviour 86
3.4 Construct Items 87
3.5 Summary 92

4 RESEARCH METHODOLOGY 93
  4.0 Introduction 93
  4.1 Research Design 94
  4.2 Operational Framework 96
  4.3 Questionnaire Development 99
    4.3.1 Survey Scale 100
  4.4 Data Collection Method 100
  4.5 Sampling and Population 101
  4.6 Data Analysis Techniques 101
    4.6.1 Data Screening Process 102
4.6.2 Descriptive Analysis 102
4.6.3 Reliability Analysis 102
4.6.4 Correlation Analysis 103
4.6.5 Multiple Regression Analysis 103

4.7 Summary 103

5 DATA ANALYSIS 104

5.0 Introduction 104
5.1 Pilot Study 104
5.2 Data Screening 106
5.3 Respondent’s Characteristics 107
  5.3.1 Gender 107
  5.3.2 Length of Teaching Experience 108
  5.3.3 Academic Qualification 109
  5.3.4 Designation 109
5.4 Descriptive Analysis 110
5.5 Correlation Analysis 143
  5.5.1 Correlation between Expected Usefulness and Expected Behavioural Intention 145
  5.5.2 Correlation between Quality and Expected Behavioural Intention 145
  5.5.3 Correlation between Trust and Expected Behavioural Intention 145
  5.5.4 Correlation between Information Security Knowledge and Expected Behavioural Intention 146
  5.5.5 Correlation between Ethical Behaviour and Expected Behavioural Intention 146
5.6 Regression Analysis 146
5.7 Findings Discussion 148

5.7.1 Expected Usefulness 149

5.7.2 Quality 150

5.7.3 Trust 151

5.7.4 Information Security Knowledge 152

5.7.5 Ethical Behaviour 153

5.8 Hypotheses Testing 154

5.9 Summary 156

6 DISCUSSION AND CONCLUSION 157

6.0 Introduction 157

6.1 Findings and Discussion 157

6.1.1 Research Question 1/Objective 1 158

6.1.2 Research Question 2/Objective 2 158

6.1.3 Research Question 3/Objective 3 159

6.1.3.1 Hypothesis 1 160

6.1.3.2 Hypothesis 2 160

6.1.3.3 Hypothesis 3 161

6.1.3.4 Hypothesis 4 161

6.1.3.5 Hypothesis 5 162

6.2 Contribution 162

6.3 Limitations and Future Work 163

6.4 Summary 164

REFERENCES 165

PUBLICATIONS 174

APPENDICES A-B 175
## LIST OF TABLES

<table>
<thead>
<tr>
<th>TABLE NO.</th>
<th>TITLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>Factors that Influences Acceptance of Online Learning System from Security Perspective</td>
<td>18</td>
</tr>
<tr>
<td>2.2</td>
<td>Base Model and Key Findings that Contributes to the Acceptance of Online Learning</td>
<td>44</td>
</tr>
<tr>
<td>2.3</td>
<td>Related Studies as Per User Type (E-Learning)</td>
<td>53</td>
</tr>
<tr>
<td>2.4</td>
<td>Related Studies as Per User Type (E-Assessment)</td>
<td>58</td>
</tr>
<tr>
<td>3.1</td>
<td>Criteria of E-Assessment Acceptance for Human Behaviour and Information System Factors</td>
<td>65</td>
</tr>
<tr>
<td>3.2</td>
<td>Criteria of E-Assessment Acceptance for Perceived Security Factors</td>
<td>74</td>
</tr>
<tr>
<td>3.3</td>
<td>Construct Items</td>
<td>87</td>
</tr>
<tr>
<td>4.1</td>
<td>Operational Framework of the Study</td>
<td>97</td>
</tr>
<tr>
<td>5.1</td>
<td>Overall Reliability Statistics</td>
<td>105</td>
</tr>
<tr>
<td>5.2</td>
<td>Reliability Statistics Results for Each Construct</td>
<td>106</td>
</tr>
<tr>
<td>5.3</td>
<td>Frequency Analysis on Gender</td>
<td>108</td>
</tr>
<tr>
<td>5.4</td>
<td>Frequency Analysis on Length of Teaching Experience in UTM KL</td>
<td>108</td>
</tr>
<tr>
<td>5.5</td>
<td>Frequency Analysis on Highest Academic Qualification</td>
<td>109</td>
</tr>
<tr>
<td>5.6</td>
<td>Frequency Analysis on Designation</td>
<td>110</td>
</tr>
<tr>
<td>5.7</td>
<td>Descriptive Statistics for Expected Behavioural Intention</td>
<td>111</td>
</tr>
<tr>
<td>Section</td>
<td>Title</td>
<td>Page</td>
</tr>
<tr>
<td>---------</td>
<td>----------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>5.8</td>
<td>Frequency Analysis for Question 1 (EBI)</td>
<td>111</td>
</tr>
<tr>
<td>5.9</td>
<td>Frequency Analysis for Question 2 (EBI)</td>
<td>112</td>
</tr>
<tr>
<td>5.10</td>
<td>Frequency Analysis for Question 3 (EBI)</td>
<td>112</td>
</tr>
<tr>
<td>5.11</td>
<td>Descriptive Statistics for Expected Usefulness</td>
<td>113</td>
</tr>
<tr>
<td>5.12</td>
<td>Frequency Analysis for Question 1 (EU)</td>
<td>113</td>
</tr>
<tr>
<td>5.13</td>
<td>Frequency Analysis for Question 2 (EU)</td>
<td>114</td>
</tr>
<tr>
<td>5.14</td>
<td>Frequency Analysis for Question 3 (EU)</td>
<td>115</td>
</tr>
<tr>
<td>5.15</td>
<td>Descriptive Statistics for Quality</td>
<td>116</td>
</tr>
<tr>
<td>5.16</td>
<td>Frequency Analysis for Question 1 (IQ)</td>
<td>117</td>
</tr>
<tr>
<td>5.17</td>
<td>Frequency Analysis for Question 2 (IQ)</td>
<td>117</td>
</tr>
<tr>
<td>5.18</td>
<td>Frequency Analysis for Question 3 (IQ)</td>
<td>118</td>
</tr>
<tr>
<td>5.19</td>
<td>Frequency Analysis for Question 4 (IQ)</td>
<td>118</td>
</tr>
<tr>
<td>5.20</td>
<td>Frequency Analysis for Question 5 (IQ)</td>
<td>119</td>
</tr>
<tr>
<td>5.21</td>
<td>Frequency Analysis for Question 6 (IQ)</td>
<td>119</td>
</tr>
<tr>
<td>5.22</td>
<td>Frequency Analysis for Question 1 (SQ)</td>
<td>120</td>
</tr>
<tr>
<td>5.23</td>
<td>Frequency Analysis for Question 2 (SQ)</td>
<td>120</td>
</tr>
<tr>
<td>5.24</td>
<td>Frequency Analysis for Question 3 (SQ)</td>
<td>121</td>
</tr>
<tr>
<td>5.25</td>
<td>Frequency Analysis for Question 4 (SQ)</td>
<td>121</td>
</tr>
<tr>
<td>5.26</td>
<td>Frequency Analysis for Question 5 (SQ)</td>
<td>122</td>
</tr>
<tr>
<td>5.27</td>
<td>Frequency Analysis for Question 1 (SE)</td>
<td>122</td>
</tr>
<tr>
<td>5.28</td>
<td>Frequency Analysis for Question 2 (SE)</td>
<td>123</td>
</tr>
<tr>
<td>5.29</td>
<td>Frequency Analysis for Question 3 (SE)</td>
<td>123</td>
</tr>
<tr>
<td>5.30</td>
<td>Frequency Analysis for Question 4 (SE)</td>
<td>124</td>
</tr>
<tr>
<td>5.31</td>
<td>Frequency Analysis for Question 5 (SE)</td>
<td>124</td>
</tr>
<tr>
<td>5.32</td>
<td>Descriptive Statistics for Trust</td>
<td>125</td>
</tr>
<tr>
<td>5.33</td>
<td>Frequency Analysis for Question 1 (TR)</td>
<td>125</td>
</tr>
<tr>
<td>5.34</td>
<td>Frequency Analysis for Question 2 (TR)</td>
<td>126</td>
</tr>
<tr>
<td>5.35</td>
<td>Frequency Analysis for Question 3 (TR)</td>
<td>126</td>
</tr>
<tr>
<td>5.36</td>
<td>Frequency Analysis for Question 4 (TR)</td>
<td>127</td>
</tr>
<tr>
<td>5.37</td>
<td>Frequency Analysis for Question 5 (TR)</td>
<td>127</td>
</tr>
<tr>
<td>5.38</td>
<td>Descriptive Statistics for Information Security Knowledge</td>
<td>128</td>
</tr>
<tr>
<td>5.71</td>
<td>Summary Result of Expected Usefulness and Expected Behavioural Intention</td>
<td>149</td>
</tr>
<tr>
<td>5.72</td>
<td>Summary Result of Quality and Expected Behavioural Intention</td>
<td>150</td>
</tr>
<tr>
<td>5.73</td>
<td>Summary Result of Trust and Expected Behavioural Intention</td>
<td>151</td>
</tr>
<tr>
<td>5.74</td>
<td>Summary Result of Information Security Knowledge and Expected Behavioural Intention</td>
<td>152</td>
</tr>
<tr>
<td>5.75</td>
<td>Summary Result of Ethical Behaviour and Expected Behavioural Intention</td>
<td>153</td>
</tr>
<tr>
<td>5.76</td>
<td>Hypothesis Summary</td>
<td>154</td>
</tr>
</tbody>
</table>
## LIST OF FIGURES

<table>
<thead>
<tr>
<th>FIGURE NO.</th>
<th>TITLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>Theory of Reasoned Action (TRA) Model</td>
<td>31</td>
</tr>
<tr>
<td>2.2</td>
<td>Technology Acceptance Model (TAM)</td>
<td>32</td>
</tr>
<tr>
<td>2.3</td>
<td>Theory of Planned Behaviour (TPB) Model</td>
<td>33</td>
</tr>
<tr>
<td>2.4</td>
<td>Unified Theory of Acceptance and Use of Technology (UTAUT) Model</td>
<td>35</td>
</tr>
<tr>
<td>2.5</td>
<td>Teachers’ E-Assessment Acceptance Model (TEAM)</td>
<td>36</td>
</tr>
<tr>
<td>2.6</td>
<td>Information System Success Model (IS)</td>
<td>37</td>
</tr>
<tr>
<td>2.7</td>
<td>SERVQUAL Model</td>
<td>38</td>
</tr>
<tr>
<td>2.8</td>
<td>Theory Model by Findik and Ozkan (2010)</td>
<td>39</td>
</tr>
<tr>
<td>2.9</td>
<td>Theory Model by Alkis and Ozkan (2010)</td>
<td>40</td>
</tr>
<tr>
<td>2.10</td>
<td>Theory Model by Abbad (2012)</td>
<td>41</td>
</tr>
<tr>
<td>2.11</td>
<td>Theory Model by Zaman et al (2013)</td>
<td>42</td>
</tr>
<tr>
<td>2.12</td>
<td>Theory Model by Wang (2010)</td>
<td>43</td>
</tr>
<tr>
<td>2.13</td>
<td>Summary of Related Studies as Per User Type</td>
<td>61</td>
</tr>
<tr>
<td>2.14</td>
<td>Summary of Related Studies as Per Security Studies</td>
<td>62</td>
</tr>
<tr>
<td>3.1</td>
<td>Secure Acceptance of E-Assessment Framework</td>
<td>81</td>
</tr>
<tr>
<td>4.1</td>
<td>Research Design of the Study</td>
<td>94</td>
</tr>
<tr>
<td>5.1</td>
<td>Hypothesis Results</td>
<td>155</td>
</tr>
</tbody>
</table>
**LIST OF ABBREVIATIONS**

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICT</td>
<td>Information Communication Technology</td>
</tr>
<tr>
<td>KL</td>
<td>Kuala Lumpur</td>
</tr>
<tr>
<td>SPSS</td>
<td>Statistical Package for the Social Science</td>
</tr>
<tr>
<td>TAM</td>
<td>Technology Acceptance Model</td>
</tr>
<tr>
<td>TPB</td>
<td>Theory of Planned Behaviour</td>
</tr>
<tr>
<td>TRA</td>
<td>Theory of Reasoned Action</td>
</tr>
<tr>
<td>UTAUT</td>
<td>Unified Theory of Acceptance and Use of Technology</td>
</tr>
<tr>
<td>UTM</td>
<td>Universiti Teknologi Malaysia</td>
</tr>
</tbody>
</table>
## List of Appendices

<table>
<thead>
<tr>
<th>Appendix</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Example complete text of email</td>
<td>175</td>
</tr>
<tr>
<td>B</td>
<td>Survey Questionnaires</td>
<td>176</td>
</tr>
</tbody>
</table>
CHAPTER 1

INTRODUCTION

1.0 Overview

The development of information technology field has impressively transformed the education field into a new face. Hilmi et al. (2011) mentioned that the ways of learning has evolved and e-learning phasing in into the current education system replacing the traditional classroom education. E-learning allows users either teachers or students to access notes, assignments, discuss in forums and interact with others from anywhere and anytime and it is available on a large scale to everyone.

In additional, Mu’azu and Lawal (2012) explained that e-learning may benefit students that do not concentrate in traditional classroom environment. They added that the e-learning system provides opportunity for faster learning method for gifted students and allow the students to develop independent learning abilities through personalised way to learn.

According to research paper done by Alwi and Fan (2009), explains that e-learning covers a wide set of applications and processes such as web based learning, computer based learning, virtual classrooms and digital collaboration.
The main advantage of e-learning system is that it allows the students to access notes, assignments, discussions, and even to interact with their lecturers and it offers much convenience and efficiency for those students who are interested in pursuing their studies. The flexibilities offered by e-learning system is the main reason on why students choose online learning compare to traditional classroom as stressed by Alwi and Fan (2009) in their study. In addition to that, e-learning allow students to save money and time spent on travelling and in getting the necessary materials for their study.

Yao and Ji (2011) describes only little security protection are provided for e-learning system as it focuses more on the quality of education compare to the system security. Attacks can happen anytime and a strong security protection is required everywhere over the Internet to protect the information and user in the e-learning environment. Security elements in e-learning system is important as when it comes to certify the students with certifications on the course, it is important to ensure the right students are certified for the course (Irfan et al., 2009).

This project will focus on how security elements will influence the acceptance of e-assessment by lecturers. There are many factors that need to be taken into consideration when designing an e-assessment system especially on security perspective in how the lecturers will be able to accept the system as it will need to create trust and friendly environment for the lecturers to use the system in long term. Research articles will be searched to support the title in major online databases such as Science Direct, IEEE Xplore, and Google Scholar using keywords such as e-assessment, e-learning, security in e-assessment, security awareness of e-assessment and security culture of e-assessment.
1.1 Background of the Problem

There are many security issues associated to e-assessment system. In order to create the trustworthiness, it is important to design a secure e-assessment system. Since, the development of information technology has affected the education field positively and negatively mainly on the implementation of e-assessment system, it is important to make sure the user able to accept the system in their daily use. However, there are many security issues related to the e-assessment system need to be solved in order to create more comfortable online learning environment for the users.

Agulla et al. (2008) highlighted one of the main issue in the e-assessment system, which is lack of proper mechanisms to avoid cheating during online assessment. Examinations and tests are generally used as online assessment tools to assess the students capability on the course. However, the online assessment does not provide the same level of confidence as face-to-face exams in such that the lecturers are not trusting the students whether is that his/her students on the other side in online assessment?

Not only had that, Hilmi et al. (2011), also agreed that student may pay someone else to participate on their behalf to sit for the test. Thus, this creates untrustworthiness among the lecturers to use the e-assessment system. In addition to that, in the research article by him, he also added that hackers could have gain access to student information and steal personal information related to students which may cause non-confidentiality issue.

In a research article by Miguel et al. (2014), the availability of the system to the students will create an issue as is it the e-assessment available to be performed by the student at the scheduled time and during the time period given by the lecturers. The system should be available to the users which are students and lecturers to access when it is required to. In addition to that, he is also concern on the integrity issues in such that the contents of e-assessment should not be changed, destroyed, or lost intentionally or accidentally.
Pei (2011) in her research article, emphasized that the failure of security technology in e-assessment system will likely to fail the system performance as the personal privacy can be easily shared without permission of the owner. Furthermore, she added that security issues are not only based on technical problem, but also from human being problem such as the e-assessment administrator will take advantage to abuse their position to do an assault of user’s privacy.

Imtiaz and Maarop (2014) has done a complete study on the lecturers’ acceptance of e-assessment in Universiti Teknologi Malaysia (UTM), Kuala Lumpur but there are no security elements included in the study to show the acceptance of e-assessment system by lecturers’ in terms of security. Hence, this study will help to enhance the feasibility study of the acceptance of e-assessment system by lecturers’ in terms of security perspective.

The implementation of e-assessment system will not be feasible if without security components in the system. Even though there are many theories related to e-assessment acceptance, however there is no particular security conceptual framework to assess e-assessment acceptance by lecturers from security perspective.

1.2 Problem Statement

Based on the review done on the list of journals, it shows that there are fewer research done on the acceptance of e-assessment system by lecturers. Most of the previous studies conducted on acceptance of e-assessment system are on the student’s perspective. Not only that, it is found that very less e-assessment acceptance research from security view has been done on both lecturers’ and student’s perspective. In order to fill the research gap, e-assessment acceptance by lecturers’ from security perspective will be analysed in this study.
1.3 **Project Aim**

The aim of the study is to explore the contributing security aspects towards better acceptance of e-assessment in Universiti Teknologi Malaysia, Kuala Lumpur by lecturers from security perspective.

1.4 **Research Objectives**

(i) To identify the factors that affects lecturers’ acceptance of e-assessment in Universiti Teknologi Malaysia, Kuala Lumpur from security perspective.

(ii) To enhance the framework of secure acceptance of e-assessment.

(iii) To examine how important is security features in determining the acceptance of e-assessment system.

1.5 **Research Questions**

(i) What are the factors that affects lecturers’ acceptance of e-assessment in Universiti Teknologi Malaysia, Kuala Lumpur from security perspective?

(ii) What is the framework of secure acceptance of e-assessment?

(iii) How important the security features in determining the acceptance of e-assessment system?
1.6 Scope of Study

The scope for this study will be focusing on Universiti Teknologi Malaysia, Kuala Lumpur. Universiti Teknologi Malaysia is the pioneer university in Malaysia which specializes on engineering and technology courses. This study will focuses on the lecturers who are currently working in Universiti Teknologi Malaysia, Kuala Lumpur. The Unit of Analysis for the project will be the lecturers not the top management of Universiti Teknologi Malaysia (UTM), Kuala Lumpur as it only involves on acceptance of e-assessment system by lecturers. The methodology which will be used in collecting data on the study of feasibility study of lecturers’ acceptance of e-assessment from security perspective is quantitative method using online survey and paper-based survey. The online survey will be developed using Google forms and will be distributed to the lecturers working at Universiti Teknologi Malaysia (UTM) Kuala Lumpur. Statistical Package for the Social Sciences or also known as SPSS will be used to analyse the data collected through the survey.

1.7 Significance of Study

The contribution of this study will benefit the implementers of the e-assessment system mainly in designing the system for lecturers from security perspective. Previous study by Imtiaz and Maarop (2014) proves that it is feasible to implement the e-assessment system in Universiti Teknologi Malaysia, Kuala Lumpur as the results of their study shows positive significant of factors influencing the acceptance of e-assessment system by lecturers. This study will focus on the factors that contribute to the acceptance of e-assessment system by lecturers from security perspective. Thus, this study will contribute on the security factors that influences the acceptance of e-assessment system by lecturers and will be helpful for the implementer of the e-assessment system to consider mainly on security issues when designing the system for their users. The significance of this study are divided further into three sub-sections.
which are theoretical, practical and methodological significance. These three significances will be explained in the following sub-sections.

1.7.1 Theoretical Significance

The significance of this study from theoretical perspective is that the previous research studies of acceptance of e-assessment by lecturers from security perspective are lack of conceptual framework. There is no proper conceptual framework to define the acceptance of e-assessment system by lecturers from security perspective. The outcome of this research will be a specific conceptual framework to discuss on the security elements that will contribute to the acceptance of e-assessment by the lecturers. The framework will serve as a future reference to the implementers especially when designing the system and to prioritize security elements in the e-assessment system.

1.7.2 Practical Significance

The significance of this study from practical perspective is to find factors on how lecturers will be able to accept the e-assessment system from security perspective. The main user of the e-assessment system are lecturers in which most likely will be rejecting the e-assessment system due to security issues. This study will help to identify on what are the main security issues need to be considered and to improve the acceptance of e-assessment among lecturers.
1.7.3 Methodological Significance

The significance of this study from methodological perspective is to use quantitative method as opposed to qualitative method as because the research of this study will be conclusive as opposed to exploratory. This study will be focusing on how security perspective will be influencing the acceptance of e-assessment by lecturers and the whole study will be narrowed and focused into the acceptance of e-assessment from security perspective by lecturers. This research will be based on the previous study by Imtiaz and Maarop (2014) and it leads to future studies focusing on acceptance of e-assessment by lecturers from security perspective.

1.8 Summary

This chapter provides a brief explanation on what will be the study about. It starts off with a brief introduction to the research topic and background problem was discussed. The problem statements are clearly defined and it leads to the formulation of research questions and project objectives. The scope on which the study will be conducted was established by describing on the unit of analysis and significance of this study.

In the next chapter, previous works will be analysed to create a strong platform to form an understanding on the study.
REFERENCES


Tobi S.U.M. (2014) *Qualitative Research & NVIVO 10 Exploration*. (1st ed.) Malaysia: Aras Publisher


