



REGRESSION ANALYSIS ON E-ASSESSMENT ACCEPTANCE BY LECTURERS FROM SECURITY PERSPECTIVE

Kavitha Thamadharan, Nurazeen Maarop, Ganthan Narayana Samy, Rasimah Che Mohd Yusoff, Rosmah Ali, Yazriwati Yahya and Roslina Ibrahim

Advanced Informatics School, Universiti Teknologi Malaysia, Kuala Lumpur

E-Mail: nurazeen.kl@utm.my

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 by lecturers. A conceptual model of secure acceptance of e-assessment is proposed considering both human and perceived security aspects. The data for this study was collected through online survey and paper-based survey. The conceptual model is analyzed using multiple regressions to identify the predictive power between dependent variable and independent variable. The final result of this study demonstrates how security factors influence lecturers' attitudes towards the acceptance of e-assessment from security perspective with a strong significant contribution to the e-assessment acceptance by lecturers. This study will be useful in providing more insightful understanding regarding the factors that influence the lecturers' acceptance of e-assessment system from security perspective.

Keywords: technology acceptance, education technology, regression analysis.

INTRODUCTION

Technology had made a lot of changes in human lives and helped us to improve our life style in many ways. The role of technology in education system has enriched the teaching and learning process, be it from preschool to higher university education. The ways of learning has changed from traditional classroom setting to online learning [1]. The entry of ICT into educational field provides a valuable chance for performing some modifications and innovations which promotes in efficiency and more effects on education system. The role of technology in education promotes effective teaching and learning and it contributes to two main field which are learning and assessment in education [2]. There are many security issues associated to e-assessment system. Yao and Ji [3] describe that online learning system developed mostly focuses on the quality of the education compare to the system security. Security elements in online 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 [4-5]. There are many factors need to be taken into consideration when designing e-assessment system especially from security perspective on how users will be able to accept the system as security factors are important in promoting user acceptance. This study firstly finds out the factors that affects lecturers' acceptance of e-assessment in Universiti Teknologi Malaysia (UTM) and to propose and evaluate the conceptual model of secure acceptance of e-assessment.

LITERATURE REVIEW

E-assessment

E-assessment as computer assisted testing (CAT), computer-based testing (CBT), e-exam, computerized testing and computer-administered testing which has grown rapidly ranging from all sectors which includes academic to professional circles [5]. According to Gusev *et al.* [6], e-assessment is a process of evaluating the student skills and knowledge by using Information Communication Technology (ICT) tools. This explains that e-assessment is the use of ICT tools to facilitate testing and evaluation of learning of the learners and then to grade the learners accordingly. E-assessment is also used for the recording purpose of the grading evaluation. Prakash and Saini [7] defines e-assessment as the end-to-end electronic assessment processes where ICT is used for the presentation of assessment activities and the recording of responses.

The use of e-assessment benefits the higher education in many ways. It helps to increase in number of assessments that encourage students to learn and participate more and helps teachers to develop different ways of assessment methods to assess the students [8].

Security in E-assessment

Computer security is the process of preventing and detecting the unauthorized actions by users of a computer system [9]. In previous studies, it was proven



that one of the reasons why users reject the online learning system is due to computer security reasons such as they are worried that they may lose their privacy or the online learning system may not be available when they need it [10].

The security aspects should be incorporated in the system without affecting the performance of the system. To determine whether e-assessment system is secure, it should meet all the computer security properties: confidentiality, integrity, availability and non-repudiation [11]. Organizations should also play an important role in educating and improving user's knowledge in information security. Based on previous studies, it is found that very less users are aware of information security risks in online learning system [12-13]. ICT role in preserving the security of e-assessment system has been seen as one of the important element as per previous studies. The owner of the system, which are the ICT administrators should be responsible in identifying the potential threats and risks to the online learning system and to educate the users on how to overcome the security threats in the online learning system [13]. Proper information security policy mechanism for protection of privacy within online learning system must be incorporated in the organization to protect the system and to be proper guidelines to educate the users on how to use the system [14].

Security issues are not only from technical aspects, but also from human being. For example, the system manager may abuse their position convenience to conduct an invasion of users' personal data [14]. This is highly correlated to the ethical behavior of the system users. Also, user's behavior towards security interaction can be related to the ethical behavior practices in an organization. Mostly, users have negative feelings to security notifications, especially when it requires them to react on it. According to Shava and Greunen [12], it is identified that users tend to ignore security information without reading it. Attitude and behavior has important relationship to confidentiality where the users of the online learning system should be aware of their responsibilities in maintaining confidentiality of information and resources [15].

CONCEPTUAL FRAMEWORK AND HYPOTHESES FORMULATION

The conceptual framework of this study are developed based on previous studies and divided into two domains which are Human Behavior and Information System Factors and Perceived Security Factors.

Human factors are one of the important factors that need to be considered which influences the acceptance of e-assessment system. The human factors for this study are derived from Imtiaz and Maarop [16] research model as shown in Figure-1. Based on Imtiaz and Maarop [16] findings, it is found that the acceptance of e-assessment system is feasible among lecturers in UTM. Their final research model yielded that Subjective Norm (SN), Expected Usefulness (EU), and Job Relevance (JR) are the

direct significant factors towards the e-assessment acceptance.

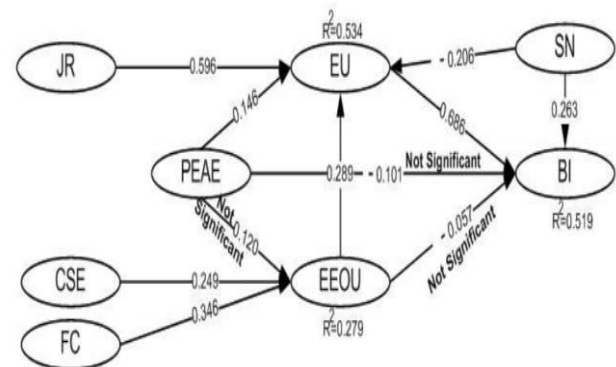


Figure-1. Research model by Imtiaz and Maarop [16].

Therefore, Expected Usefulness (EU) have been adapted into the proposed conceptual model for this study. Subjective Norm (SN) and Job Relevance (JR) have been excluded from the formulation of conceptual model in this study. Based on the literature review analysis many other previous studies [16-20] point out that Subjective Norm (SN) variable is significant to the acceptance of e-assessment. However, as according to Findik and Ozkan [21], in their study, all their proposed external variables are accepted except for Subjective Norm (SN) which was found insignificant to be in relationship with the acceptance of e-assessment. Due to different population concern, Subjective Norm (SN) will not be regarded as highly significant in this study. Job Relevance (JR) has been excluded from the proposed conceptual framework because all users of the system are the lecturers who share the same degree of job relevance. Further, this study is more concern on suitable construct that can relate to the security factors.

This study has considered to adapt another construct which was not included in previous models of e-assessment. This includes quality construct from DeLone and McLean IS Success Model [22]. DeLone and McLean [22] explains that excellent quality of system encourages user satisfaction, and when user is satisfied with the system, they will intend to use it. In addition to that, it is found that there are many other previous studies by other researchers that certainly proved that quality is one of significant element that contributes to the technology acceptance [23-27]. Table 1 explains in summary the analysis on how human and information system factors are selected.

Table-1. Summary of E-assessment acceptance analysis from human and information system perspective.

References	Significance	Construct
[16]	/	Expected Behavioural



		Intention
[16-20]	X	Subjective Norm
[16]	/	Expected Usefulness
[22-27]	/	Quality
[16]	X	Job Relevance

[16]	Accepting Responsibility, Avoiding Conflicts, No Abuse of Employer's Resources, Act with Honesty, Protecting Confidentiality. Socially Responsible	Expected Usefulness
------	--	---------------------

Perceived security factors that are considered to be adapted into the proposed conceptual model of this study are derived from the analysis of literature review done earlier. Based on the analysis done, it is identified that reasons why people reject the online learning system is because computer security reasons in which they are worried that they will lose their privacy in the system or the system may not be available when they need it [10]. This leads to users' untrustworthiness towards the system and they will not intend to use the system. This proves that trust is an important element in ensuring the acceptance of e-assessment system. According to Montague *et al.* [28], trust in technology includes many measuring items. In regard of this study, some measurements of trust are to be considered and these include confidentiality of data, integrity of the system and availability of the system.

Information Security is an important factor in influencing the acceptance of e-assessment system as users will feel satisfied to use a system when they know well on how to make use of it. According to Wang [29], Information Security Knowledge is defined as contextual information, awareness, and personal experience ready to be used for decisions and actions in information security area. The items to be measured under this element will be information security knowledge, security awareness, security policy and security culture [12].

Ethical Behaviour is defined as the degree to pursue or not to pursue an action. According to Sakri *et al.* [30], ethical behavior in technology may include measuring items such as accepting responsibility, avoiding conflicts, not abusing employer's resources for personal gain, act with honesty, protect the confidentiality assigned to you, and socially responsible in the use and distribution of information. These items will be considered and to be measured in this study under the Ethical Behaviour (EB) variable. Table 2 explains in summary the analysis on how perceived security factors are selected.

Table-2. Summary analysis from perceived security perspective.

References	Construct	Item
[10], [31-32]	Data Confidentiality, System Integrity, System Availability	Trust
[12], [14-15], [33]	Information Security, Knowledge, Security Awareness, Security Policy, Security Culture	Information Security Knowledge

Considering the integrated model of established technology acceptance studies and findings of published studies related to security in Information Technology management, the proposed conceptual model is formulated. This study aims to extend the previous model of e-assessment acceptance among lecturers that was suggested by Imtiaz and Maarop [16]. This study will also consider other important factors related to secure use of e-assessment. The conceptual framework of this study is divided into two dimensions which are human behavior and information system factors and perceived security factors. Two variables from Imtiaz and Maarop [16] are adapted into this framework namely Expected Behavioral Intention (EBI) and Expected Usefulness (EU). Quality variable is adapted from IS Success Model by DeLone and McLean. Security factors, which include trust, information security knowledge, and ethical behavior variables, are derived from literature reviews that have been discussed earlier. All the factors identified will contribute to expected behavioral intention (EBI) construct. The final proposed conceptual model is as illustrated in Figure 2.

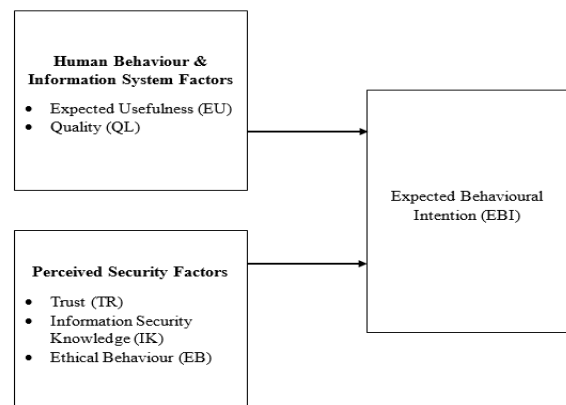


Figure-2. Conceptual model of secure acceptance of e-assessment.

Five hypothesis have been identified and will be analysed in this study. The research hypothesis and definitions of the proposed factors towards secure acceptance of e-assessment are as follows:

- Expected Behavioral Intention (EBI): EBI is defined as the intention of the user to use e-assessment system in the future, the prediction of using e-assessment in the future, and the plan to use e-assessment in the future [16]. EBI is the most important factor in the conceptual model, Secure Acceptance of E-Assessment as it will be the indicator for feasibility of



acceptance of e-assessment from security perspective.

- Expected Usefulness (EU): EU is defined as the extent to which a person believes that by using a particular system would enhance his or her job performance [16].

Hypothesis 1 (H1): Expected Usefulness (EU) will have significant influence towards Expected Behavioral Intention (EBI).

- Quality (QL): QL is defined as excellent quality of system encourages user satisfaction, and when user is satisfied with the system, they will intend to use the system [22].

Hypothesis 2 (H2): Quality (QL) will have significant influence towards Expected Behavioral Intention (EBI).

- Trust (TR): Trust is defined as the feeling of certainty that a person or thing will not fail and is often based on inconclusive evidence [32]. The items to be measured under trust element will be information security components which are data confidentiality, system integrity and system availability of the e-assessment system.

Hypothesis 3 (H3): Trust (TR) will have significant influence towards Expected Behavioral Intention (EBI).

- Information Security Knowledge (IK): Information Security Knowledge (IK) is defined as contextual information, awareness, and personal experience ready to be used for decisions and actions in information security area [29]. Information Security Knowledge (IK) will be measured in terms of information security knowledge, security awareness, security policy and security culture.

Hypothesis 4 (H4): Information Security Knowledge (IK) will have a positive significant to the acceptance of e-assessment by the lecturers.

- Ethical Behaviour (EB): Ethical Behaviour (EB) is defined as the degree to pursue or not to pursue and actions [30].

Hypothesis 5 (H5): Ethical Behaviour (EB) will have a positive significant to the acceptance of e-assessment by the lecturers.

METHODOLOGY

The unit of analysis for this study was lecturer at Universiti Teknologi Malaysia (UTM). Likert scale was used in all the questions related to the construct items except for demographic questions. According to Nunnally [36], Likert scales are more reliable than single-item scales. A 5-point Likert scale was used in this study as it is balanced on both positive and negative sides of the feedback. The scale has two negative items, which are strongly disagree and disagree and two positive items which are agree and strongly agree together with neither agree nor disagree. Other previous researches like Lim *et al.* [37], Ong *et al.* [38] and De-Smet *et al.* [39] have also

preferred 5-point Likert Scale. Implementing a quantitative approach, the data for this study was collected using both online survey and paper-based survey. Online survey, which is Google Forms, was used to develop the online survey questionnaire. The link was shared to lecturers working in Universiti Teknologi Malaysia through email.

RESULT

Total of 62 valid responses were obtained with 38 responses were received via the google forms and the rest through paper based survey. About 50 paper based survey were distributed, in which only 24 responded. Out of 62 respondents, total of 54.8% of respondents with the position as senior lecturer in UTM contributed as the majority respondents to the survey. Whereas, rest of the participants are with the position of lecturer with 27.4%, associate professor with 14.5% and only 3.2% professors responded to the survey. 35.5% of lecturers with less than 5 years of teaching experience, followed with 22.6% of lecturers with length of teaching experience ranging from 6 to 10 years.

Cronbach's alpha (α) was used to measure the reliability of the instrument items [19]. The reliability coefficient finding shows that reliability of all measurement scales were above the recommended minimum level 0.7 [40]. The result is shown in Table-3.

Table-3. Cronbach alpha and overall mean.

Scale (item)		Cronbach's alpha (α)	Overall mean
EBI (3)		.931	4.407
EU (3)		.735	3.876
QL	IQ (6)	.796	3.767
	SQ (5)	.882	3.634
	SE (5)	.865	3.474
	Overall IQ (16)	.911	3.634
TR (5)		.956	3.451
ISK	ISK (4)	.810	3.550
	SA (5)	.852	3.674
	SP (5)	.906	3.406
	SC (5)	.893	3.794
	Overall ISK (19)	.941	3.609
EB (6)		.893	4.505
Overall (52)		.933	3.752

This study focuses to look into identifying the predictive power between dependent variable that is Expected Behavioral Intention (EBI) and independent variables including Expected Usefulness (EU), Quality



(QL), Trust (TR), Information Security Knowledge (IK) and Ethical Behavior (EB). Thus, multiple regression analysis was conducted to test the hypothesis proposed earlier. Table 4 shows the result of the multiple regression analysis.

Table-4. Results of multiple regression analysis.

Expected Usefulness (EU) $\beta = .602$ $p\text{-value} = .000 < 0.05$	Expected Behavioral Intention (EBI) $R^2 = 0.733$
Quality (QL) $\beta = .301$ $p\text{-value} = .001 < 0.05$	
Trust (TR) $\beta = .550$ $p\text{-value} = .001 < 0.05$	
Information Security Knowledge (IK) $\beta = .334$ $p\text{-value} = .001 < 0.05$	
Ethical Behavior (EB) $\beta = .561$ $p\text{-value} = .000 < 0.05$	

According to Table-4, the R^2 value of 0.733 represents 73% of the factors which includes ethical behavior, expected usefulness, trust, information security knowledge, and quality, explains the change in user's intention to accept the e-assessment system among lecturers in Universiti Teknologi Malaysia, Kuala Lumpur. Pallant [41] explains that if the significance value is less than 0.5, the variable is making a significant contribution to the equation. Table 4 shows a significant relationship between expected usefulness, quality, trust, information security knowledge, and ethical behavior towards secure acceptance of e-assessment system by lecturers in Universiti Teknologi Malaysia, Kuala Lumpur with significant value < 0.05 .

It is found that, expected usefulness is the most significant independent variable that influence lecturers' in accepting e-assessment system securely, followed by ethical behavior, with $\beta = .561$, trust, with $\beta = .550$, information security knowledge, with $\beta = .334$ and quality, with $\beta = .301$. Multiple regression analysis was used to evaluate the secure acceptance of e-assessment by lecturers in UTM, Kuala Lumpur. The factors may include expected usefulness, quality, trust, information security knowledge and ethical behavior. The significant value for expected usefulness, quality, trust, information security knowledge and ethical behavior were < 0.05 which is significant towards expected behavioral intention. Furthermore, positive sign from the β -coefficient value indicating positive influence of the independent variables towards expected behavioral intention in secure acceptance of e-assessment system by lecturers in UTM Kuala Lumpur. Table-5 summarizes the hypothesis findings for this study.

Table-5. Hypothesis summary.

Hypothesis	Findings	Strength
H1	Supported	Strong
H2	Supported	Strong
H3	Supported	Strong
H4	Supported	Strong
H5	Supported	Strong

Figure-3 shows the final conceptual model for the acceptance of e-assessment by lecturers from security perspective.

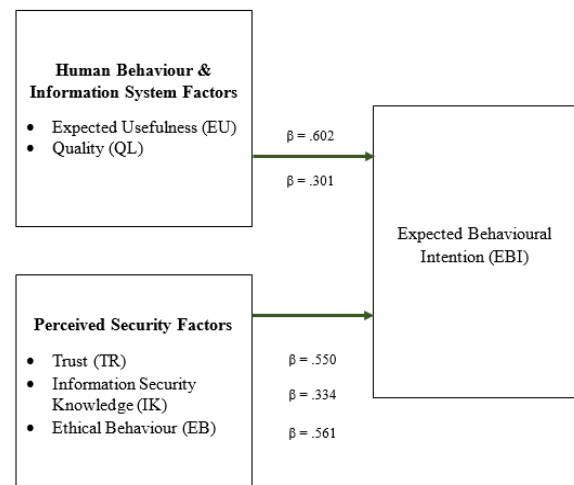


Figure-3. Final conceptual model of secure acceptance of E-assessment.

CONCLUSIONS

The e-assessment acceptance from lecturers' perspective was studied at a public university in Malaysia. Firstly, based on the previous studies, human behavior and information system factors are identified that may impact the acceptance of technology. Previous studies also suggested that security aspects should be considered in determining more secure use of technology including in the context of online education and conceptual framework are developed based on the analysis. Secondly, the hypothesized conceptual model was found to be significant after SPSS analysis. The e-assessment system is feasible to be implemented in UTM due to high level of intention to use the e-assessment system. Support of H1, H2, H3, H4 and H5 provides a justification for this. The result shows that the lecturers positively intend to use the e-assessment system in the future and they believe that the e-assessment system will be useful and relevant to their job. The quality of the system also highly influence the intention of the lecturers to use the system, as excellent quality of system will encourages user satisfaction and to use the system [22]. The lecturers positively trust that the



system will provide a secure service to them and this leads to the intention to use the e-assessment system. In addition to that, information security knowledge also have a positive influence towards the intention to use the system. Hence, the lecturers believe they will have proper information security knowledge equipped through training and awareness by their organization to use the e-assessment system. They also believe that ethical behavior of the users will influence to accept the e-assessment system. These results will be very helpful to the IT administrators of the university who plan to implement the e-assessment system in the future.

ACKNOWLEDGEMENTS

This work was supported in part by Ministry of Education, Advanced Informatics School, Universiti Teknologi Malaysia and Vote No. 11J40

REFERENCES

- [1] M.F. Hilmi, S. Pawanchik, and Y. Mustapha. 2011. Exploring Security Perception of Learning Management System (LMS) Portal. International Congress on Engineering Education. 7 - 8 December. IEEE, pp. 132-136.
- [2] S. Bidarian, S. Bidarian, A.M. Davoudi. 2011. A Model for Application of ICT in the Process of Teaching and Learning. Procedia - Social and Behavioural Sciences. Vol. 29, pp. 1032- 1041.
- [3] H. Yao and Y. Ji. 2011. Security Protection for Online Learning of Music. Computer Communications and Networks (ICCCN). 31 July-4 August. IEEE pp. 1- 4.
- [4] C.M. Althaff-Irfan, S. Nomura, K. Ouzzane, and Y. Fukumura. 2009. Face-based Access Control and Invigilation Tool for E-Learning Systems. International Conference on Biometric and Kansei Engineering. 25 - 28 June. IEEE pp. 40-44.
- [5] C. Ke, Y. Yajun, and W. Yingwei. 2010. E-Assessment in FLT settings: the Past, Issues and Trends. International Conference on Networking and Digital Society. 30 – 31 May. IEEE. pp. 257 -260.
- [6] M. Gusev, S. Ristov, G. Armenski, P. Gushev, and G. Velkoski. 2014. E-Assessment with Interactive Images. IEEE Global Engineering Education Conference (EDUCON). 3-5 April. IEEE. pp. 484-491.
- [7] L.S. Prakash and D.K. Saini. 2012. E-Assessment for E-Learning. International Conference on Engineering Education: Innovative Practices and Future Trends. 19 -21 July. IEEE. pp 1 - 6.
- [8] M. Honarmand. 2009. Computer Aided Assessment and its Situation in Higher Education: A case study from the Islamic Azad University in Iran. International Conference on Information Management and Engineering. 3 - 5 April. IEEE. pp.736 - 739.
- [9] D. Gollman. 2011. Computer Security, 3rd Edition. Wiley, Chichester.
- [10] Z.F. Zamzuri, M. Manaf, and Y. Yunus, and A. Ahmad. 2013. Student perception on security requirement of e-learning services. 6th International Conference on University Learning and Teaching. 10 October. pp. 923 - 930
- [11] J. Miguel, S. Caballe, F. Xhafa, and J. Prieto. 2014. Security in Online Learning Assessment towards an Effective Trustworthiness Approach to Support e-Learning Teams. International Conference on Advanced Information Networking and Applications (AINA). 13 – 16 May. IEEE. pp. 123-130.
- [12] F.B. Shava, and D. Van-Greunen. 2013. Factors Affecting User Experience with Security Features: A case study of an academic institution in Namibia. Information Security for South Africa. 14 – 16 August. IEEE. pp. 1- 8.
- [13] A.A. Mu'azu and I.A. Lawal. 2012. E-Learning System Vulnerabilities: Threats and Promises for Students' Information System. E-learning, E-Management and E-Services (IS3e) Symposium. 21 – 24 October. IEEE. pp 1- 6.
- [14] J. Pei. 2011. How to Solve the Security and Privacy Problems within E-Learning. International Symposium on IT in Medicine and Education (ITME). 9 – 11 December. IEEE. pp. 66-69.
- [15] J. Kaur and N. Mustafa. 2013. Examining the Effects of Knowledge, Attitude and Behaviour on Information Security Awareness: A Case on SME. 3rd International Conference on Research and Innovation in Information Systems. 27 - 28 November. IEEE. pp. 286-290.
- [16] A. Imtiaz and N. Maarop. 2014. Feasibility Study of Lecturers' Acceptance of E-Assessment. 25th Australasian Conference on Information System. 8-10 December.
- [17] M. Abbad. 2012. Proposed Model of E-Learning Acceptance. International Conference on Education and e-Learning Innovations. 1 - 3 July. IEEE. pp. 1- 9.
- [18] B. Pynoo, P. Devolder, J. Tondeur, J.V. Braak, W. Duyck and P. Duyck. 2011. Predicting secondary school teachers' acceptance and use of digital learning



environment: A cross-sectional study. *Computers in Human Behaviour*. Vol. 27, pp. 568-575.

- [19] R. Cheung and D. Vogel. 2013. Predicting user acceptance of collaborative technologies: An extension of the technology acceptance model for e-learning. *Computers & Education*. Vol. 63, pp. 160-175.
- [20] V. Venkatesh, M.G. Morris, G.B. Davis and F.D. Davis. 2003. User acceptance of information technology: Toward a unified view. *MIS quarterly*, Vol. 27, pp. 425 -478.
- [21] D. Findik and S. Ozkan. 2010. Identifying success factors for WBLMS use by instructors of engineering departments. *Frontiers in Education Conference*. 27 - 30 October. IEEE. pp. 1- 3.
- [22] W.H. DeLone and E.R. McLean. 1992. Information system success: the quest for the dependent variable. *Information Systems Research*. Vol. 3, pp. 60-95.
- [23] X. Song. 2011. Teaching and Learning experience with Learning Management Systems: an adapted IS Success Model in LMS Context. *International Symposium on IT in Medicine and Education*. 9 – 11 December. IEEE. pp. 148 - 152
- [24] V. Khayun and P. Ractham. 2011. Measuring e-Excise Tax Success Factors: Applying the DeLone and McLean Information Systems Success Model. *International Conference on System Sciences*. 4-7 January. IEEE. pp. 1 - 10
- [25] J. Li and J. Sun. 2009. An empirical study of e-commerce website success model. *International Conference on Management and Service Science*. 20 - 22 September. IEEE. pp 1-4.
- [26] H.A. Baraka and I.H. Gamily. 2013. Assessing call centers' success: A validation of the DeLone and McLean model for Information System. *Egyptian Informatics Journal*. Vol. 14, pp 99-108.
- [27] Y.S. Wang and Y.W. Liao. 2007. Assessing e-Government systems success: A validation of the DeLone and McLean model of Information System success. *Government Information Quarterly*. Vol 25. pp. 717 - 733
- [28] E.N.H. Montague, B.M. Kleiner and W.W Winchester. 2009. Empirically Understanding Trust in Medical Technology. *International Journal of Industrial Ergonomics*. Vol. 39, pp. 628-634.
- [29] P.A. Wang. 2010. Information Security Knowledge and Behaviour: An adapted model of technology acceptance. *2nd International Conference on Education Technology and Computer*. 22 – 24 June. IEEE. pp. 364 - 367.
- [30] S. Sakri, J. Salim, and T.M.T. Sembok. 2012. Information Communications and Technology (ICT) Abuse in the Malaysia Public Sector: The Influence of Ethical, Organizational Bond and General Deterrence Factors. *Akademika*. Vol. 82, pp. 125-137.
- [31] Luminita D.C. 2011. Information Security in E-Learning Platforms. *Procedia Social and Behavioral Sciences*, 15, 2689-2693. Elsevier Ltd.
- [32] B.J. Blazic and T. Klobucar. 2005. Privacy Provision in E-Learning Standardized Systems: Status and Improvements. *Computer Standards and Interfaces*. Vol. 27, pp. 561-578.
- [33] N. Hassan, Z. Ismail and N. Maarop. 2013. A Conceptual Model for Knowledge Sharing towards Information Security Culture in Healthcare Organization. *International Conference on Research and Innovation in Information Systems*. 27-28 November. IEEE. pp. 516-520.
- [34] S. Conger, K.D. Loch and B.L. Helft. 1995. Ethics and Information Technology Use: A factor analysis of attitudes to computer use. *Information Systems Journal*. Vol. 5, pp. 161-184.
- [35] U.E. Gattiker and H. Kelly. 1999. Morality and Computers: Attitudes and Differences in Moral Judgments. *Information Systems Research*. Vol. 3. pp. 233-54.
- [36] J. Nunnally, 1978. *Psychometric methods*. McGraw-Hill, New York, NY.
- [37] H. Lim, S.G. Lee, and K. Nam. 2007. Validating E-learning factors affecting training effectiveness. *International Journal of Information Management*. 27(1), 22-35.
- [38] C.S. Ong, J.Y. Lai, and Y.S. Wang. 2004. Factors affecting engineers' acceptance of asynchronous e-learning systems in high-tech companies. *Information and management*, Vol. 42, pp. 795-804.
- [39] C. De-Smet, J. Bourgonjon, B. De-Wever, T. Schellens, and M. Valcke. 2012. Researching instructional use and the technology acceptance of learning management systems by secondary school teachers. *Computers and Education*. Vol. 58, pp. 688-696.
- [40] H. Wu and C.W. Wei. 2010. Factors affecting learners' knowledge sharing intentions in web-based learning. *International Symposium on Computer*,



Communication, Control and Automation. 5 - 7 May.
IEEE 83-86.

[41] J. Pallant. 2013. SPSS survival manual. McGraw-Hill
International.