International Journal of Business, Human and Social Sciences
ISSN: 2517-9411
Vol:9, No:3, 2015

The Acceptance of E-Assessment Considering Security Perspective: Work in Progress

Kavitha Thamadharan, Nurazean Maarop

Abstract**—**The implementation of e-assessment as tool to support the process of teaching and learning in university has become a popular technological means in universities. E-Assessment provides many advantages to the users especially the flexibility in teaching and learning. The e-assessment system has the capability to improve its quality of delivering education. However, there still exists a drawback in terms of security which limits the user acceptance of the online learning system. Even though there are studies providing solutions for identified security threats in e-learning 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 the technology. As a result a conceptual model of secure acceptance of e-assessment is proposed. Both human and security factors are considered in formulation of this conceptual model. In order to increase understanding of critical issues related to the subject of this study, interpretive approach involving convergent mixed method research method is proposed to be used to execute the research. This study will be useful in providing more insightful understanding regarding the factors that influence the user acceptance of e-assessment system from security perspective.

Keywords**—**Secure Technology Acceptance, E-Assessment Security, E-Assessment, Education Technology.

I. Introduction

THE development of information technology field has impressively transformed the education field into a new face. The ways of learning has evolved and e-assessment and e-learning have been part of the current education system and to some extent 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 [1].

However, there is only little security protection are provided for e-learning system as it focuses more on the quality of education compare to system security. [2] 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 system. Security elements in e-learning are 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. [3]

There are many factors that need to be taken into consideration when designing e-assessment system especially from security perspective on how the user especially lecturers will be able to accept the system as security factors are important in promoting user acceptance. The point of this study is, to primarily identify the factors that affects lecturers' acceptance of e-assessment in Universiti Teknologi Malaysia (UTM) and to propose the conceptual model of secure acceptance of e-assessment.

II. Literature Review

A. Importance of Security Aspects

Security has been an important element that contributes to the acceptance of a technology. While any previous studies have been performed to identify what are the factors that influences the acceptance of e-assessment system but there is a lack of aspect has been considered from security perspective. The role of security in online learning system is providing secure end-to-end session between the user and the institution's online learning network. It was proven by previous study 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 available when they need it. [4].

The development of educational system needs to consider security protocols which include authentication, encryption, access control, managing users and their permissions to ensure secure use and access [5]. The security aspects should be incorporated in the system without affecting the performance of the system [5]. The degree of security threats in e-assessment should be higher than e-learning as e-assessment involves student assessment. Nevertheless, computer security components which are confidentiality, integrity, availability and non-repudiation [6] have been used to determine the degree of the security threats of e-learning but not in the e-assessment.

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 should be responsible to identify the potential threats and risks to the system [7] Security management should be well practiced by the ICT people in an organization to secure the system [8]. Organization should also play an important role in educating and improving user's knowledge in information security [9]. 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. To overcome such issues, a proper

Kavitha Thamadaran is a postgraduate research student at the Universiti Teknologi Malaysia (phone: 603-22031341; e-mail: vitha07@gmail.com).

Dr. Nurazean Maarop is a senior lecturer at the Universiti Teknologi Malaysia (phone: 603-22031341; e-mail: nurazean.kl@utm.my).

information security policy mechanism for protection of privacy within online learning must be built to protect the system [10].

User's behavior towards security interaction also plays an important role in accepting the online learning. Mostly, users have negative feelings to security notifications, especially when it requires them to react on it. It is identified that users tend to ignore security information without reading it [11]. Attitude and behavior has important relationship to confidentiality in which users of a system should be aware of their responsibilities in maintaining confidentiality of information and resources [9].

B. Related Technology Acceptance Studies

There are many other previous studies have greatly contributed to the understanding of acceptance of online learning system. However, there are very less research done on the development of the general acceptance of online learning system by lecturers from security perspective. From the analysis of literature review conducted, it has revealed that most of the studies on online learning acceptance have been done on students. Table I provides a summary of previous related studies as per user type.

TABLE I
RELATED STUDIES AS PER USER TYPE

Field of Study	User Type	Authors	Occurrence
Online Learning	Lecturers	[12], [13]	2
	Lecturers/ Administrators	[11]	1
	Lecturers/Students	[7], [14], [15]	3
	High School Teachers	[16]	1
	Students	[1], [4], [17]-[24]	13

Most of the previous studies used Technology Acceptance Model (TAM) and extended it with other elements included in the model. Two studies have been conducted to test the feasibility of acceptance of e-assessment by lecturers. Both of the studies used TAM as their base model.

Imtiaz & Maarop [12] used TAM as their base model and extended their model by adding in another five external variables which are Job Relevance (JR), Computer Self-Efficacy (CSE), Facilitating Condition (FC), Previous E-Assessment Experience (PEAE) and Subjective Norm. The results of their study prove that Expected Usefulness (EU) and Subjective Norm (SN) contributed to the acceptance of e-assessment.

Findik & Ozkan [13] has conducted a study regarding the acceptance of web based learning management system among lecturers proposing four independent variables which are Compatibility (CMP), Technological Simplicity (TS), System Self-Efficacy (SSE) and Subjective Norm (SN). All their proposed external variables are accepted except for Subjective Norm which was found insignificant to be in relationship with the acceptance of the e-assessment [13].

In summary, most of the previous studies in the area of e-assessment acceptance, TAM has been used as base model and the researchers have added other external variables developed through the analysis of literature review.

III. Research Model and Proposition Formulation

A. Human Behavior & Information System Factors

Human factors are the important factors when considering the factors that influence the acceptance of e-assessment system. The human factors are derived from [12] research model. The constructs in the model proposed by Imtiaz & Maarop has been tested previously and it is found that the acceptance of e-assessment 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. Hence, Expected Usefulness (EU) has been adapted into the proposed conceptual model for the purpose of this study.

In the formulation of the conceptual model proposed in this study, Subjective Norm (SN) and Job Relevance (JR) have been excluded. There are many other previous studies [12] [15], [16], [20], [25] finding shows that Subjective Norm (SN) variable is significant to the acceptance of the e-assessment. However, as according to [13], in the study, all their proposed external variables are accepted except for Subjective Norm which was found insignificant to be in relationship with the acceptance of the e-assessment [13]. Due to different population concern, subjective norm 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 associate to the security factors.

Another factor that was not considered in previous model of e-assessment is quality construct from DeLone and McLean IS Success Model [26]. The study [26] has divided quality element into three items namely information quality, system quality and service quality. There are many other previous studies by other researchers that positively have proved that quality is one of important factor that contributes to the acceptance of e-learning and e-assessment system [26]–[31]. Excellent quality of system encourages user satisfaction, and when user is satisfied with the system, they will intend to use it [26]. In particular, according to [32], a quality checklist should be prepared before the e-learning assessment is used by the system participants. Hence, this study will consider the inclusion of system quality in the proposed conceptual model.

TABLE II
CRITERIA OF E-ASSESSMENT ACCEPTANCE FROM HIS PERSPECTIVE

References	Significance	Theme
[13]	X	Subjective Norm
[12], [15], [33]	/	Expected Usefulness
[26]- [31]	/	Quality
[12]	X	Job Relevance

Table II shows the summary of the inclusion of factors from human and information system (HIS) perspective for the proposed conceptual model.

B. Security Factors

Security factors that can be considered in the proposed conceptual model derived from the analysis of literature review done earlier. Zamzuri et al. [4] stress that reasons why people reject the online system is due to 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. This may lead to that the users' untrustworthiness towards the use of system and they will not intend to use the online learning system.

This proves that trust is an important element in ensuring the acceptance of e-assessment system. According to [34], trust in technology includes many measuring items. In regard to 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 Knowledge (IK) is defined as contextual information, awareness, and personal experience ready to be used for decisions and actions in information security area [18]. Information Security Knowledge is important in influencing the acceptance of the system as users will feel satisfied to use a system when they know well on how to make use of it [18]. Some items to be measured in this study under Information Security Knowledge (IK) variable are information security knowledge, security awareness, security policy and security culture [11].

Ethical Behaviour (EB) is defined as the degree to pursue or not to pursue and action [36]. According to [35], 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 III summarizes the inclusion of security factors in the proposed conceptual model.

TABLE III
CRITERIA OF E-ASSESSMENT ACCEPTANCE FROM SECURITY PERSPECTIVE

References	Item	Theme
[4]-[6], [36]	Data Confidentiality System Integrity System Availability	Trust
[9]-[11], [37]	Information Security Knowledge Security Awareness Security Policy Security Culture	Information Security Knowledge
[35], [38], [39]	Accepting responsibility Avoiding Conflicts No Abuse of Employer's Resources Act with Honesty Protecting Confidentiality Socially Responsible	Ethical Behaviour

C. Formulation of Hypotheses

The proposed model derived from a consideration of integrated model of established technology acceptance and findings of published studies related to security in IT management. In particular, this study aims to extend the previous model of e-assessment acceptance among lecturers which was postulated by [12]. Hence, this study is considering other important factors related to secure use of e-assessment.

Two variables from [12] are adapted into this framework which are expected behavioral intention (EBI), and expected usefulness (EU). Quality variable is adapted from IS Success Model [26] considering a checklist of items regarding quality of e-assessment from [32]. Security factors which include trust, information security knowledge, and ethical behaviour variables are derived from the literature review which has been discussed earlier. All the factors identified will contribute to expected behavioral intention construct. The final proposed conceptual model is illustrated in Fig. 1.

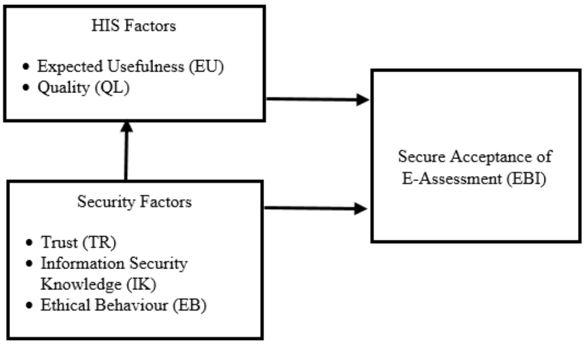
HIS Factors
• Expected Usefulness (EU)
• Quality (QL)
Security Factors
• Trust (TR)
• Information Security Knowledge (IK)
• Ethical Behaviour (EB)
Secure Acceptance of E-Assessment (EBI)

Fig. 1 Conceptual Model of Secure Acceptance of E-Assessment

Hence, eight propositions have been identified in this study. The research propositions 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. [12] 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. [12]

Proposition 1: Expected Usefulness (EU) will have a positive significant to the acceptance of e-assessment by the lecturers.

- 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. [26]

Proposition 2: Quality (QL) will have a positive significant to the acceptance of e-assessment by the lecturers.

- 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 [34]. 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.

Proposition 3: Trust (TR) will have significance influence on Expected Usefulness (EU).

Proposition 4: Trust (TR) will have a positive significant to the acceptance of e-assessment by the lecturers.

- 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 [18]. Information Security Knowledge (IK) will be measured in terms of information security knowledge, security awareness, security policy, and security culture.

Proposition 5: Information Security Knowledge (IK) will have significance influence on Expected Usefulness (EU).

Proposition 6: 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 action [35].

Proposition 7: Ethical Behaviour (EB) will have significance influence on Expected Usefulness (EU).

Proposition 8: Ethical Behaviour (EB) will have a positive significant to the acceptance of e-assessment by the lecturers.

IV. Proposed Methodology

A. Methodological Approach

The majority of the research in technology acceptance has solely used quantitative approach. Those studies are confirmatory, engrossing theory verification. Indeed, the original study regarding the acceptance of e-assessment by [12] had only revealed the findings from quantitative results and the qualitative components and consideration remained absent. There is a lack of findings in this area of knowledge considering qualitative perspective. As many qualitative researches are exploratory, aiming at theory generation, the combination of these two research perspectives may enable the researcher to simultaneously answer confirmatory and exploratory questions, and therefore verify and generate theory in the same study [40]. Therefore, the proposed research methodology of this study is to be based on convergent parallel design [41], in which the qualitative and quantitative data were concurrently collected and analysed separately on the same phenomenon and then the results were used to validate, confirm and corroborate the qualitative result with the quantitative result. This convergent model applying more than one method to find solution related to the similar aspects can enhance the credibility of the research findings [41], [42].

B. Sampling and Data Collection

The population of interest for quantitative approach in this study will be lecturers who are working in Universiti Teknologi Malaysia (UTM), Kuala Lumpur. The reason why lecturers are chosen to be the respondents of the study is because they are the main user of the e-assessment system. In regard to qualitative perspective, this study will consider applying the purposive sampling as the methodological approach of this study is exploratory in nature. On the other hand, online survey will be employed for the quantitative data collection. Online survey website will be used to develop and distribute the online survey questionnaire. The link will be shared through email to lecturers of different department at the university.

A key-informant interview approach involving those who are in charged with the student learning and assessment system will be used to obtain the insights of the secure acceptance of the e-assessment. The target key informants of this study are not only those who experience using any student assessment system but also those who manage the system and take responsibility for the security of the university system This approach is regarded advantageous to gather information effectively, to gain access to unobtainable information and to gain specific understanding and interpretation of the cultural information [43].

C. Data Analysis Method

The proposed data analysis will involve two data sets and the study will employ the general guidelines for analyzing the concurrent mixed methods data proposed by [40]. Both data will be analyzed separately and then to be merged so that the interpretation and discussion can be made based on the overall results. The qualitative analysis will be based on deductive themes and at the same time allowing the emerging of other new themes. On the other hand, the objective of the survey questions is to measure the strength and direction of relationships between aspects conceptualized in this study.

V. Conclusion

Previous studies suggested that behavioral intention indicating technology acceptance has been impacted by many human and information system factors. Previous studies also suggested that security aspects should be considered in determining more secure use of technology including in the context of online education. Considering appropriate security aspects in either the formulation of conceptual model for interpretive research or validation of research model for explanatory study is essential in technology acceptance in educational context. The conceptual model proposed in this paper will be evaluated in the next phase of research. This in-progress-study will use both quantitative and qualitative methodology. It is expected that the findings will benefit the university in embracing more secure use of e-assessment technology in near future.

Acknowledgment

We would like to thank the Ministry of Education, Universiti Teknologi Malaysia & Vote No. (01K11) for supporting this research.

References

[1] Hilmi M.F., Pawanchik S., and Mustapha Y. (2011). Exploring Security Perception of Learning Management System (LMS) Portal. *International Congress on Engineering Education.* 7 – 8 December. IEEE 132 – 136.

[2] Yao H., Ji Y. (2011). Security Protection for Online Learning of Music. *Computer Communications and Networks (ICCCN).* 31 July – 4 August. IEEE 1 – 4.

[3] Althaff Irfan C.M., Nomura S., Ouzzane K., Fukumura Y.(2009) Face-based Access Control and Invigilation Tool for E-Learning Systems. *International Conference on Biometric and Kansei Engineering.* 25 – 28 June. IEEE 40 – 44.

[4] Zamzuri Z.F., Manaf M., Yunus Y., Ahmad A. (2013). *6th International Conference on University Learning and Teaching.* 10 October. 923 – 930.

[5] Luminita D.C. (2011). Information Security in E-Learning Platforms. *Procedia Social and Behavioral Sciences*, 15, 2689 – 2693. Elsevier Ltd.

[6] Miguel J., Caballe S., Xhafa F., Prieto J. (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 123 – 130.

[7] Mu'azu A.A., Lawal I.A. (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 1 – 6.

[8] Alwi N.H.M., Ip-Shing Fan (2009). Information Security Management in E-Learning. *International Conference for Internet Technology and Secured Transactions (ICITST).* 9 – 12 November. IEEE 1 – 6.

[9] Kaur J., Mustafa N. (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 286 – 290.

[10] Jiao 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 66 – 69.

[11] Shava F.B., Van Greunen D. (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 1 – 8.

[12] Imtiaz A., Maarop N. (2014) Feasibility Study of Lecturers' Acceptance of E-Assessment. *25th Australasian Conference on Information System.* 8 – 10 December.

[13] Findik D., Ozkan S. (2010) Work in Progress – Learning Management Systems acceptances of instructors from various departments: Empirical investigation. *Frontiers in Education Conference.* 27 – 30 October. IEEE 1- 3.

[14] Persico D., Manca S., Pozzi F. (2014) Adapting the Technology Acceptance Model to evaluate the innovative potential of e-learning systems. *Computers in Human Behaviour.* 30. 614 – 622.

[15] Abbad M. (2012) Proposed Model of E-Learning Acceptance. *International Conference on Education and e-Learning Innovations.* 1 – 3 July. IEEE 1 – 9.

[16] Pynoo B., Devolder P., Tondeur J., Braak J.V., Duyck W., Duyck P. (2011) Predicting secondary school teachers' acceptance and use of digital learning environment: A cross-sectional study. *Computers in Human Behaviour.* 27. 568 – 575.

[17] Lui S.M., Hui W. (2011) The effects of knowledge on security technology adoption: Results from a quasi-experiment. *Information Science and Service Science (NISS).* 24 – 26 October. IEEE 328 – 333.

[18] Wang P.A. (2010) Information Security Knwoledge and Behaviour: An adapted model of technology acceptance. *2nd International Conference on Education Technology and Computer.* 22 – 24 June. IEEE 364 – 367.

[19] Lin S.C., Persada S.F., Nadlifatin R. (2014) A study of student behavior in accepting the blackboard learning system: a technology acceptance model (TAM) approach. *18th International Conference on Computer Supported Cooperative Work in Design.* 21 – 23 May. IEEE 457 – 462.

[20] Cheung R., Vogel D. (2013) Predicting user acceptance of collaborative technologies: An extension of the technology acceptance model for e-learning. *Computers & Education.* 63. 160 – 175.

[21] Wu H., Wei C.W. (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.

[22] Sumak B., Polancic G., Hericko M. (2010) An empirical study of virtual learning environment adoption using UTAUT. *2nd International Conference on Mobile, Hybrid, and On-Line Learning.* 10 – 16 February. IEEE 17 – 22.

[23] Udo G.J., Bagchi K.K., Kirs P.J. (2011) Using SERVQUAL to assess the quality of e-learning experience. *Computers in Human Behaviour.* 27. 1272 – 1283.

[24] Lee B.C., Yoon J.O., Lee I. (2009) Learners' acceptance of e-learning in South Korea: Theories and Results. *Computers & Education.* 53. 1320 – 1329.

[25] Venkatesh V., Morris M.G., Davis G.B., Davis F.D., (2003) User acceptance of information technology: Toward a unified view. MIS quarterly, 425 -478.

[26] DeLone W.H., McLean E.R. (1992) Information system success: the quest for the dependent variable. *Information Systems Research.* 3. 60.

[27] Song X. (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 148 – 152.

[28] Khayun V., Ractham P. (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 1 – 10.

[29] Li J., Sun J. (2009) An empirical study of e-commerce website success model. *International Conference on Management and Service Science.* 20 – 22 September. IEEE 1 – 4.

[30] Baraka H.A., Baraka H.A., Gamily I.H. (2013) Assessing call centers' success: A validation of the DeLone and McLean model for Information System. *Egyptian Informatics Journal.* 14. 99 – 108.

[31] Wang Y.S., Liao Y.W. (2007) Assessing e-Government systems success: A validation of the DeLone and McLean model of Information System success. *Government Information Quarterly.* 25. 717 – 733.

[32] Sung Y-T, Chang K-E, Yu Wen-Cheng (2011) Evaluating the reliability and impact of a quality assurance for E-learning courseware. *Computers and Education.* 57, 1615-1627.

[33] Alkis N., Ozkan S. (2010) Work in Progress – A modified technology acceptance model for e-assessment: Intentions of Engineering Students to use web-based assessment tools. *Frontiers in Education Conference.* 27 – 30 October. IEEE 1 – 3.

[34] Montague E.N.H., Kleiner B.M., Winchester W.W. (2009) Empirically understanding trust in medical technology. *International Journal of Industrial Ergonomics.* 39. 628 – 634.

[35] Sakri S., Salim J., Sembok T.M.T. (2012) Information Communications and Technology (ICT) Abuse in the Malaysia Public Sector: The Influence of Ethical, Organisational Bond and General Deterrence Factors. *Akademika.* 82(1) 125 – 137.

[36] Blazic B.J., Klobucar T. (2005) Privacy Provision in E-Learning Standardized Systems: Status and Improvements. *Computer Standards & Interfaces.* 27. 561 – 578.

[37] Hassan N.H., Ismail Z., Maarop N. (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 516 – 520.

[38] Conger S., Loch K.D., Helft B.L. (1995) Ethics and Information Technology Use: A factor analysis of attitudes to computer use. *Information Systems Journal.* 5. 161 – 84.

[39] Gattiker U.E., Kelly H. (1999) Morality and Computers: Attitudes and Differences in Moral Judgments. *Information Systems Research.* 10(3). 233-54.

[40] Teddlie, C. and Tashakkori, A. Major Issues and Controversies in The Use of Mixed Methods in The Social And Behavioral Sciences. In: Tashakkori, A., and Teddlie, C. (Eds), *Handbook of mixed method in social and behavioural research*. Thousand Oaks, CA: Sage, pp 3-50, 2003.

[41] Creswell, J.W and Plano Clark, V.L. *Designing and conducting mixed methods research*. Thousand Oaks, CA: Sage, 2011.

[42] Teddlie, C. and Tashakkori, A. *Foundations of Mixed Methods Research: Integrating Quantitative and Qualitative Approaches in the Social and Behavioral Sciences*. Thousand Oaks, CA: Sage, 2009.

[43] Gilchrist, V. J. and R. L. Williams (1999). Key Informant Interviews. Doing Qualitative Research. B. F. Crabtree and W. L. Miller. Thousand Oaks, CA, Sage**:** 195-218.