ISSN:
Print - 2277 - 0593
Online - 2315 - 7461
© FUNAAB 2016

Journal of Natural Science, Engineering and Technology

AN ENHANCED TECHNOLOGY ACCEPTANCE MODEL TO MEASURE CUSTOMERS' WILLINGNESS TO PAY MORE FOR SECURE SOFTWARE DEVELOPMENT

*[1]O.T. AROGUNDADE, [2]O. MUSTAPHA, [3]A.M. IKOTUN, [4]A.O. ADEJIMI

Department of Computer Science, Federal University of Agriculture, Abeokuta, Nigeria
***Corresponding author:** arogundadeot@funaab.edu.ng, **Tel:** +2347030700561

ABSTRACT

Securing information system (IS) has become a critical concern within many sectors of business organisations with significant resources being devoted to the control of security threats. Recently, it has been discovered that incorporating security at the time of development is the best option for having a robust system. This study explores factors that motivate IS owner's willingness to pay extra cost for a secure software development and validates the relationships among the various variables. Enhanced Technology Acceptance Model (TAM) was used to investigate the factors that influences IS owner's willingness to pay extra cost for secured software development. Out of all the constructs considered, Self-Efficacy (SE) is found to be significant (β= 0.617, P<0.05) which suggests that self-efficacy is useful for investigating willingness to pay for a secure software development. In addition, the strength of the linear association between Self-Efficacy and Behavioural Intention (BI) (R^2=0.354) implies that Self Efficacy has direct moderate impact on Behavioural Intention to pay extra cost for a secure software development.

Keywords: Information system, Security, Technology Acceptance Model (TAM), Self-Efficacy Software development,

INTRODUCTION

The entire processes of procurement, integration, modification, maintenance and security of an information system are the sole responsibility of the owner. Many systems are being automated using the computer system making software an indispensable part of our daily lives and as the society depends more on it, its malfunctioning becomes more disastrous. Today, software control large financial systems, communication systems, databases and even deadly missile program (Syed, 2007). Meanwhile, there are several threats posed against the security of the system and among these threats are malicious codes written to corrupt software which results in its malfunctioning. The high speed connections of millions of computing devices through the Internet have increased the possibility of spreading viruses and worms that can exploit the vulnerabilities of operating systems on this vast network in a matter of minutes. As reported in (Syed, 2007), today's software is more vulnerable to attacks due to increase in complexity, connectivity and extensibility. In view of this, information system security has become a critical concern within many sectors of business and organisation and significant resources have been devoted to control security threats. Security control mechanisms such as a combination of anti-virus / anti –

spyware software, firewalls intrusion detection and prevention systems with content filtering software have been used to combat various threats against information security. Information System's attackers mostly targets software due to vulnerabilities introduced at the various stages of its development. These points of vulnerability can be exploited to violate one or more of the software security properties. Logically, building a secured information system is vital to a long term success and a business that implements and maintains a strong security posture has the opportunity to have a competitive edge above her counterparts. "*Software Security is an emergent property of a complete system, not a feature*" (McGraw, 2004). However, enforcing and maintaining security is a daunting task for any organization and it is tasking for software developers because developing secured software takes more time and effort.

There is a great risk of losing vital data and the entire information system if proper security measures are not embedded in the system in the course of developing the information system. The amount of loss that organisations have incurred over the years due to security flaws in software has invited researcher to find out better ways of securing software (Syed, 2007). This study explore factors that motivate IS owner's willingness to pay extra cost for a secured software development and validates the relationships among the various variables in the proposed enhanced Technology Acceptance Model (TAM) framework.

The paper is organised as follows: Section 1 gives the introduction to the research work. Section 2 discusses the conceptual background of the study with details on the concept of TAM. This is followed by the description of the research model and its hypotheses in Section 3. The research methodology is presented in Section 4 and Section 5 gives the discussion of the analysis and results as well as the findings and suggestions on future research direction.

CONCEPTUAL BACKGROUND

Secured software development:

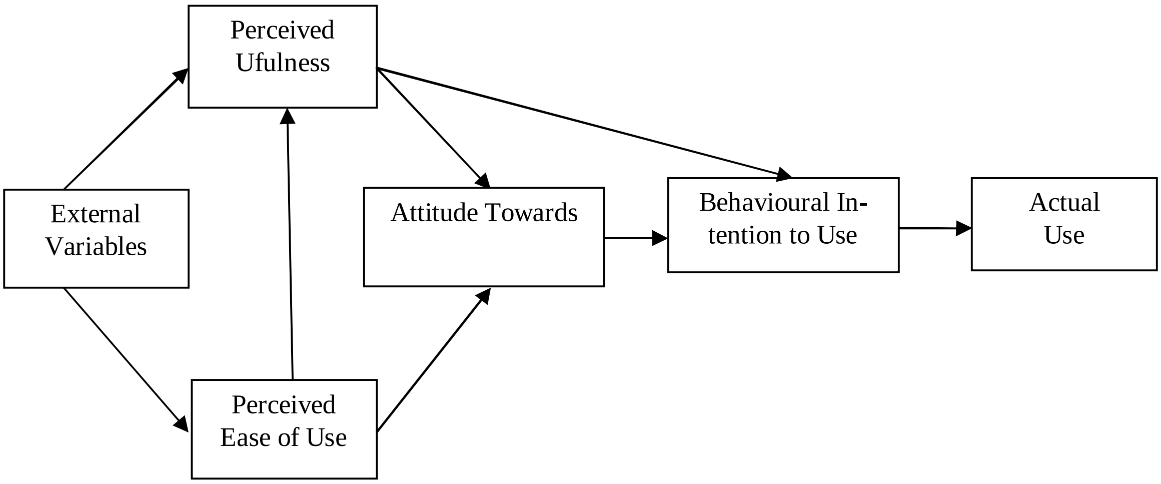
Security is part of software development process. It is an on-going process which involves people and practices that ensures application confidentiality, integrity and availability. Secure Software is the result of security aware software development process where security is built in and thus software is developed with security in mind (Stewart, 2012)

Secure software development involves the use of several processes including the implementation of a security development lifecycle and secure coding during software development. Secure development is a practice to ensure that the code and processes that go into developing an application are as secure as possible. Due to the vast amount of threats against software applications, there is a growing need for considering securing these applications right from the point of development. Integrating security practices into the software development lifecycle and verifying the security of internally developed applications before they are deployed can help mitigate risk from internal and external sources (Glynn, 2016).

The Security Development Life cycle is divided into six phases: training, requirements and design, construction, testing, release and response. Security development can be incorporated into software development stages. Incorporating these into system development requires application owner to pay more for the application because of the cost in terms of money and time on the part of the software developer. This study explore factors that motivate IS owner's willingness to pay extra cost for a secure software development and validates the relationships among the various variables in the proposed enhanced Technology Acceptance Model (TAM).

Technology Acceptance Model (TAM)

Fred Davis (Davies *et al*, 1989) formulated the Technology Acceptance Model (TAM) which is based on the stimulus-response model (Burton-Jones et al, 2007), TAM builds on the Theory of Reason Action (TRA). According to him, two variables influence people's behavioural intentions in accepting new technologies. These two variables: perceived ease of use and perceived usefulness, are shaped by the technology's features and capabilities: These behavioural intentions in turn drives the actual behaviour of the users. External variables were later integrated into the TAM model resulting in an improved TAM model which is illustrated in Figure 1.



Source: David *et al.,* 1989

Figure 1: Improved Technology Acceptance model

There are two major differences between Technology Acceptance Model and Theory of Reasoned Action. One, two new constructs are introduced in the Technology Acceptance Model which are perceived usefulness (the belief that using an application will increase one's performance) and perceived ease of use (the belief that one's use of an application will be free of effort). These two beliefs could predict an individual's attitude concerning the use of an application. Two, a subjective norm is not included in Technology Acceptance Model as a determinant of intention. Technology Acceptance Model, since its introduction by (Davies *et al,* 1989) and (Cronbach, 1951), has been widely used for predicting the acceptance, adoption, and use of information technologies. (Adams, 1992) associates the TAM model with a high degree of validity and reliability while (Cronbach, 1951), (Livari *et al,* 1995) associates it with simplicity, and higher predictive ability than the TRA and TPB. However, (Burton-Jones, 2006) has criticized it for its fewer constructs relative to the TBP stating that it is not capable of capturing some behavioural aspects and thus yielding less rich information, and (Subramanian, 1994),(Cronbach, 1951), (Sanayei, 2013), (Fishbein *et al,* 1975) reported the inconsistencies in the nature of the relationship between its variables. Other criticisms are also reported in (Al-Qeisi, 2009), (Taylor and Todd, 1995b) stating that the model fails to explain how adoption or usage can be improved using the variables and that apart from the perceived ease of use and perceived usefulness and that it also fails to incorporate other factors which have an influence on technology acceptance.

The TAM 2 model was proposed by (Taylor and Todd, 1995b).Several variables including "subjective norms, image, job relevance, quality output, and result demonstrability" were incorporated into the TAM. All these variables are viewed as influencing the perceived usefulness of the technology. TAM2 proposed that experience and voluntariness interact with subjective norms shapes perceived usefulness and adoption intentions. In (Taylor and Todd, 1995b) , six other factors : computer self-efficacy, perceptions of external control, computer anxiety, and computer playfulness which were viewed as impacting perceived ease of use, as well as "perceived enjoyment and objective usability" which impacts adjustments were incorporated into the TAM. These made the TAM 2 model to be considered as a more robust model with a higher predictive ability (Burton-Jones, 2006). However, in (Lee, 2003),(Hyeun-Suk Rhee, 2009), (Bhattacherjee 20001a), (Bagozzi, 2007) , (Brown, 2000) . The TAM 2 has been associated with several weaknesses, including: its reliance highly-subjective self-reported data, the failure to incorporate the attitude variable into the use intentions since attitudes, its deterministic nature, as well as inconsistencies in the relationships among its variables.

Self-Efficacy's role in Technology Acceptance

Ozer and Bandura, 1990 defines Self Efficacy as people's belief in their abilities to mobilize the motivation, cognitive resources and course of actions needed to exercise control over given event. According to (Bandura, 1982), it is an important construct of Social cognitive theory which is concerned with how perceptions of self-efficacy affect people's motivation and action.(Starjkovic, 1998) says it is a form of self-evaluation which is a proximal determinant of individual behaviour. People with a high level of self – efficacy have a stronger form of self-conviction about their ability to mobilise motivation, cognitive resources and course of action needed to successfully execute a task (Starjkovic, 1998). (Bandura, 1982) argued that Self Efficacy is the most pervasive mechanism of human agency which motivates and regulates individual behaviour.

With this understanding of the Technology Acceptance and the role of Self Efficacy in Technology Acceptance, the purpose of this research work is to study the willingness of Information System owners in paying extra-cost for a secured software development. The intention is to apply the idea in Technology Acceptance Model (TAM) in addition with self-efficacy to know the rate at which the IS owners are willing to pay-extra cost for a secure software development as well as the factors that motivate them to pay extra-cost and the outcome of the action to the organization. The influence of Self Efficacy in Information Security on the User's Information Security Performance behaviour is reported in (Hyeun-Suk *et. al.,* 2009). Individuals with high Self Efficacy in Information Security (SEIS) use more security software and features and they have high rate of adopting major security application and additional security tools. Such people apply security updates/patches more often. It was also reported that SEIS influences the security care behaviours related to computer /internet usage such as frequent backing up of important files, usage of strong and multiple passwords for different online account(Griffin, 2010) .

On the investigation with respect to the willingness to pay, several studies have been carried out using different models such as technology acceptance theories and models which comprises of: Theory of Reasoned Action (TRA)(Davis, 1989), Theory of Planned Behaviour (TPB) ((Livari, 1996, the Technology Acceptance Model (TAM) (Davis, 1989). These studies provide useful insights in understanding individual's intention of willingness to pay using the Technology Acceptance Model (TAM) in addition with self-efficacy. A number of factors such as Product usefulness, Perceived usefulness, Perceived ease of use, Self-efficacy, external influence, interpersonal influence and facilitating conditions have been identified to determine the willingness to pay.

From these studies, it has been reported that TAM emphasizes that two particular beliefs, perceived usefulness (PU) and perceived ease of use (PEOU) are main determinants of the attitudes (AT) toward using a new technology. According to (Davis, 1989), (Cronbach, 1951), PU is concerned with the degree to which a person believes that using a particular system would enhance his or her job performance, while PEOU is defined as the degree to which a person believes that using a particular system would be free of effort. Perceived playfulness is created when consumer perceives the product exceeds their expectation which gives rise to satisfaction.

The use of Technology Acceptance Model (TAM) in examining the factors such as perceived usefulness and perceived ease of use on consumer willingness to use mobile payment services was proposed in (Venkatesh, 2000).

A revised technology acceptance model was used to measure customers' acceptance of internet banking in Iran (Petersen, 2001). The study used the Technology acceptance model, Theory of planned behaviour and Theory of perceived risk to build a comprehensive model which incorporated five categories of perceived risk to investigate the positive and negative aspects of internet banking that include security, financial, social, time, and performance loss.

In (Arunkumar, 2007), the Technology Acceptance Model was used to study attitude and intention towards Internet banking. Technology acceptance model of Davis was used to study the consumer readiness to use Internet Banking. TAM determined IT adoption, implementation and diffusion in terms of perceived ease of use and perceived usefulness.

THE RESEARCH MODEL AND HYPOTHESIS

With the knowledge of the TAM in studying the behavioural pattern of technology user with regard to their acceptance of various technologies, we intend to enhance the TAM to investigate the factors that influences IS owners' willingness to pay extra cost for secured software development. Fig. 2 illustrates our research model. As shown in the figure, the TAM deals with the antecedents of attitude and self-efficacy which in turn determines the intention and actions. The research suggests that human action is influenced by a favourable or unfavourable evaluation of the behaviour (that is, attitude towards the behaviour) and self-efficacy (that is, the belief or confidence in one's ability necessary to perform a behaviour). In combination, attitude and self-efficacy lead to the formation of a behavioural intention.

Attitude toward the behaviour is defined as the individual's positive or negative feelings about performing an action. It is determined through two sub-constructs as shown in the diagram.

Product usefulness refers to the usefulness of paying extra-cost for a secure software system on improving the product (software).

Perceived playfulness is created when the customer perceives the product exceeds their expectation which in turn is the necessary variable that gives rise to behaviour such as satisfaction.

Self-efficacy refers to the belief or confidence in one's ability necessary to perform the behaviour.

Capability is the power or practical ability to perform the behaviour

Comfort-ability is the ease of practising the behaviour.

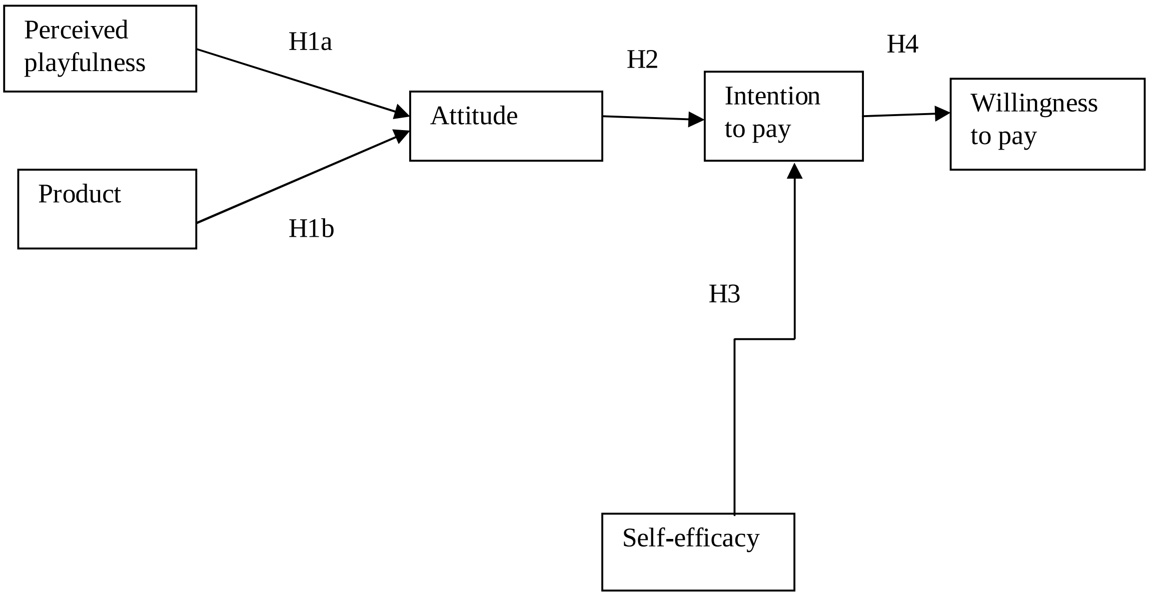


Fig. 2: Research Model (Modified Technology Acceptance Model: adapted from Davis *et al.,* 1989)

Based on the research model, the following research hypotheses are proposed:

Hypothesis 1a: Perceived playfulness is positively related to attitude towards intention to pay extra-cost for a secure software system.

Hypothesis 1b: Product usefulness is positively related to attitude towards intention to pay extra-cost for a secure software system.

Hypothesis 2: Attitude is positively related to intention to pay extra-cost for a secure software system.

Hypothesis 3: Self-efficacy is positively related to intention to pay extra-cost for a secure software system.

Hypothesis 4: Intention is positively related to attitude towards willingness to pay extra-cost for a secure software system.

RESEARCH METHOD

The data for this survey were collected through a survey instrument (questionnaire) from different organizations both in Lagos and Abeokuta. Survey questionnaire was personally distributed and 35 were collected from the respondents. The sample size is not very large because industries are the focus of the study and not individuals. Some soft copy of questionnaires was given to the contact person who distributed them within the organization. 72% of the respondents were male and 28 % were female. The majority of respondents (64.0%) were between 26 and 40 years old. 16% were between 18 and 25 and 20% were 40 and above. With respect to the education levels of respondents, 16% were below graduate level, 64% of the respondents were graduates and 20% falls in the range of master

degree and above. In considering the years of experience of using software, 12% of the respondents had the experience of less than a year, 44% had 1 to5years of experience, 28% had 6-10years level of experience and respondents with more than 10years had 16% of the respondents. Finally, position of the respondents in the organizations falls between the level of manager down to data processing officer.

Instruments

The research model involves five constructs: Perceived Usefulness (PU), Perceived Playfulness (PP), Attitude (AT), Self-Efficacy (SE) and Behavioural Intention (BI). To
IS owners' willingness to pay extra-cost for a secure software development, existing measures on IS owners' WTP literature were reviewed e.g. (Legris, 2003), (Bhattacherjee, 2001a), (Taylor and Todd, 1995a), (Agarwal, 2000). Items were adapted from the existing measures to reflect tasks that relates to Product Usefulness. Participants were asked to rate their opinion on their willingness to pay more if it will reduce cost of applications maintenance, ensure job security, enabled security requirement, guaranteed application robustness with regard to security, ensure enhancement of organisation competitive edge and prestige.

For Perceived playfulness, two items requiring the opinion of participants on the probable relationship that exists between the willingness to pay more and software quality and consumer satisfaction were included. In order to develop a measure for Self Efficacy, respondents were required to give their opinion on their organization's willingness to pay extra-cost for a secure software development whenever possible, the capability of their organization in paying extra-cost for a secure software system, the readiness of the organization to pay extra-cost for a secure software development reasonably well on her own and the comfortability of the organization to pay more cost for a secure software system. Some of these were adapted from the works of (Bhattacherjee, 2001a),(Taylor and Todd, 1995a), (*Ozer, 1990)*.

In seeking for response from the participants, based on the idea obtained fromExpert source(Taylor and Todd, 1995a), two items were put forth to the respondent seeking to know their opinion if paying extra-cost for a secure software development is a good idea and if their organization likes the idea of paying extra cost for a secure software system. For measures regarding the Behavioural Intention's , the opinion of respondents were sought to know if their organization would pay extra-cost for a secure software system whenever possible and the intention of their organization to pay extra-cost for secure software system (Agarwal, 2000) ,(Taylor and Todd, 1995a).
A seven-point bipolar scale ranging from strongly agree to strongly disagree i.e. (1= extremely agree, 2= quite agree, 3= slightly agree, 4= neither agree nor disagree, 5= slightly agree, 6= quite disagree, 7= extremely disagree) was used to assess the respondents' perception with respect to investigating the respondents' attitudes, self-efficacy and intention.

Steps were taken to ensure that the research actually measures what is supposed to measure (validity). A pre-test of the research was conducted on 10 information system users which did not form part of the sample. The findings were quite relevant and some actions were taken to enhance the research. Questions were rephrased, additional response choices were added to certain questions, certain heading were removed because it is unnecessary.

DATA ANALYSIS AND RESULTS

The reliability of research measures was done with Cronbach's alpha. The reliability threshold for Cronbach's alpha must reach a value of 0.7 and above before it can be consideredto be reliable and acceptable. The survey had strong internal consistency with all multiple-item constructs achieving Cronbach's alpha of 0.70 or higher (Cook, 1979). It could be observed in table 1 that the Cronbach value for PU is 0.898, for PP is 0.792, for AT is 0.704, for SE is 0.762 and BI is 0.774 respectively which makes the threshold acceptable.

Table 1: Items validity

Construct	No of items	Cronbach's alpha
Perceived usefulness (PU)	6	0.898
Perceived playfulness (PP)	2	0.792
Attitude (AT)	2	0.704
Self –Efficacy (SE)	4	0.762
Behavioural intention (BI)	2	0.774

The validity of the research instruments were examined using factor analysis. All the items were tested for validity by using factor analysis with principal component analysis and varimax rotation. Convergent validity was assessed by checking the loadings to see if the items for same construct correlate highly among themselves. Determinant validity also was assessed by examining the factor loading to see if items loaded more highly on their intended construct than on other constructs (Comrey, 1973). Thus, the research instrument was found to be valid and reliable (Mathieson, 1991).

Principal Component Analysis

In this research, Principal Component Analysis (PCA) is used to investigate the convergent and discriminant validity of our questionnaire. It is one of the most commonly used analysis methods used to investigate the discriminant and convergent validity of an instrument. The benefits of this dimensionality reduction include providing a simpler representation of the data, reduction in memory, and faster classification. We accomplish by projecting data from a higher dimension to a lower dimensional manifold such that the error incurred by reconstructing the data in the higher dimension is minimized.

Mathematically, PCA details;

From k original variables: $x_1, x_2,\ldots,x_k$:

$$\left.\begin{aligned} &\text{Produce } k \text{ new variables: } y_1,y_2,\ldots,y_k:\\ &y_1 = a_{11}x_1 + a_{12}x_2 + \ldots + a_{1k}x_k\\ &y_2 = a_{21}x_1 + a_{22}x_2 + \ldots + a_{2k}x_k\\ &\ldots\\ &y_k = a_{k1}x_1 + a_{k2}x_2 + \ldots + a_{kk}x_k \end{aligned}\right\} \quad \begin{gathered} y_k\text{'s are}\\ \textbf{Principal Components}\end{gathered}$$

such that:

y_k's are uncorrelated (orthogonal)

y_1 explains as much as possible of original variance in data set

y_2 explains as much as possible of remaining variance, etc.

This work employed statistical software SPSS version 20 for its analysis and PCA was performed using Component extraction method based on Eigenvalues greater than 1 and Varimax rotation method. The analysis is done using factor reduction. The eigenvalue greater than one is significant (implies that each item account for the variance of at least a single construct). The orthogonal rotation method (Varimax) maximizes the sum of variances of the factor matrix and factor analysis was used to check the convergent and discriminant validity of questions.

Table 2: Result of Principal Component Analysis Component Matrix

	Components				
Constructs	1	2	3	4	5
PU1	**.742**	.398	-.089	.412	.119
PU2	**.768**	.104	.247	-.254	.345
PU3	**.664**	.566	-.060	-.255	-.139
PU4	**.742**	.398	-.089	.412	.119
PU5	**.768**	.104	.247	-.254	.345
PU6	**.664**	.566	-.060	-.255	-.139
PP1	-.038	.084	**.869**	.361	-.189
PP2	.136	.077	**.861**	-.199	-.264
SE1	-.511	**.526**	.233	.154	-.142
SE2	-.587	**.621**	.004	-.087	.033
SE3	-.426	**.699**	.105	-.052	.270
SE4	-.236	.380	-.005	**.718**	.224
AT1	-.116	**.548**	-.190	-.105	-.632
AT2	.047	**.854**	-.224	-.011	-.124
BI1	-.628	.337	.199	-.190	**.475**
BI2	-.619	**.410**	-.046	-.325	.238

Factor loading shows the correlation between each item and the related constructs. Loading of 0.45-0.54 are considered fair, 0.55-0.62 are considered good and 0.63-0.70 are considered very good and above 0.70 are considered excellent (Chuttur, 2009).

From Table 2 it shows that BI1, SE1 has a fair loading then PU3, PU6, SE3 has a very good loadings and PU1, PU2, PU4, PU5, PP1, PP2, AT2, SE4 has an excellent loadings except BI2 which did not load strongly onto any factor was retained as its deletion would result in a loss of content validity.

Model Validity and Hypotheses Testing Regression Analysis

In statistical modelling, regression analysis is a statistical process for estimating the relationships among variables. It includes many techniques for modelling and analyzing several variables, when the focus is on the relationship between a dependent variable and one or more independent variables (or 'predictors').

The equation is of the form:

$$a = \frac{(\Sigma y)(\Sigma x^2) - (\Sigma x)(\Sigma x y)}{n(\Sigma x^2) - (\Sigma x)^2}$$

$$b = \frac{n(\Sigma xy) - (\Sigma x)(\Sigma y)}{n(\Sigma x^2) - (\Sigma x)^2}$$

Linear regression is a way to model the relationship between two variables. The equation has the form Y=a+bX, where Y is the dependent variable (that's the variable that goes on the Y axis), X is the independent variable (i.e. it is plotted on the X axis), b is the slope of the line and a is the y-intercept. The variable we are predicting is called the criterion variable and is referred to as Y. In this study the criterion variable is willingness to pay. The variable we are basing our predictions on is called the predictor variable and is referred to as X. In this study we have five predictor variables which are perceived usefulness, perceived playfulness, self efficacy and attitude.

Simple linear regression was used to test the model. The hypotheses were tested by the Statistical Package for Social Sciences (SPSS) software. Table 3 shows that one out of all the hypotheses was supported. This research postulate that product usefulness is not significant and has no direct/ indirect impact on attitude (β= 0.284, Standardized path coefficient, P<0.05) while perceived playfulness is not significant and has no direct/indirect impact on attitude (β= -0.057 P<0.05). This suggests that product usefulness is not useful for investigating willingness to pay for a secure software development. Also, attitude is not significant and has no direct/indirect impact on behavioural intention (β= 0.172, P<0.05) but self-efficacy is significant (β= 0.617, P<0.05) and has a direct impact on behavioural intention which suggests self-efficacy is useful for investigating willingness to pay for a secure software development. In addition, the strength of the linear association between SE and BI (R^2 =0.354) implies that Self Efficacy has direct moderate impact on Behavioural Intention to pay extra cost for a secure software development

Table 3. Result of Simple Linear Regression

Regression Equation	Adjusted R2	B	Significant	Hypothesis
PP → AT	-0.040	-0.057	0.786	H1a (not supported)
PU → AT	0.040	0.284	0.170	H1a (not supported)
AT → BI	-0.013	0.172	0.410	H2 (not supported)
SE → BI	0.354	0.617	0.001	H3 (supported)

Appendix

Questionnaire item

Construct	Items	Source
Product usefulness (1-6)	Willingness to pay extra-cost for a secure software development would reduce the cost of application maintenance? Willingness to pay extra-cost for a secure software development would increase the organization job security? Willingness to pay extra cost for secure system would enable security requirement to be better capture. Willingness to pay extra-cost for a secure software development would make the application more robust (better withstand attack or misuse). Willingness to pay extra cost for a secure software development would give the organization a cutting edge Willingness to pay extra cost for secure system would enhance the prestige of the organization.	Livari (1996) Green and Hevner (1999)
Product playfulness (7-8)	Willingness to pay extra-cost for a secure software development would increase the organization software quality. Willingness to pay extra-cost for a secure software development would increase consumer satisfaction	

Self-efficacy (16-19)	My organization is willing to pay extra-cost for a secure software development whenever possible My organization would be capable of paying extra-cost for a secure software system? My organization will pay extra -cost for a secure software development reasonably well on her own. My organization feel comfortable paying extra-cost for a secure software system	Bhattacherjee(2000),Taylor and Todd(1995),Pedersen (2001),
Attitude (22-24)	Paying extra-cost for a secure software development is a good idea. The organization likes the idea of paying extra cost for a secure software system.	Taylor and Todd(1995),Expert source
Behavioural intention (30-31)	My organization would pay extra-cost for a secure software system whenever possible. My organization intends to pay extra-cost for secure software system.	Agarwal and Prasad (2000), Taylor and Todd(1995)

DISCUSSION

This paper proposes an enhanced technology acceptance model to measure customer's willingness in paying extra cost for a secure software development. This research uses the Technology Acceptance Model (TAM) in addition with self-efficacy to build a comprehensive model. A questionnaire was designed and used to survey a randomly selected sample of customers using information system. This research postulate that self-efficacy is significant ($\beta = 0.617$, $P<0.05$) has a direct impact on behavioural intention which suggests self-efficacy is useful for investigating willingness to pay for a secure software development. In addition, the strength of the linear association between SE and BI ($R^2 = 0.354$) which implies Self Efficacy has direct moderate impact on Behavioural Intention to pay extra cost for a secure software development.

CONCLUSION

This study investigates IS owners' willingness to pay more for a secure software development. TAM model in addition to self-efficacy was employed to develop the research questionnaire. The result of the study shows that self-efficacy has a significant and positive impact on behavioural intention to pay more for a secure software development. According to the research model a positive BI implies customers' willingness to pay extra cost for secured software.

This project recommends self-efficacy as a construct/factor to measure information system owners' willingness in paying more for a secure software development. This outcome will aid software developers in making decisions with respect to whether or not to develop secure software for organizations. Therefore it should be taken into consideration in further research.

REFERENCES

Adams, D. A., Nelson, R. R., Todd, P. A. 1992. "Perceived usefulness, ease of use, and usage of information technology: A replication", *MIS Quarterly*, 16(2), 227–247.

Agarwal, R., Prasad, J. 2000. A field study of the adoption of software process innovations by information system profession", *Engineering Management, IEEE Transactions*, 47(3), 295-308

Agarwal, R., Sambamurthy, V., Stair, R. 2000. Research report: The evolving relationship between general and specific computer self-efficacy - An empirical assessment", *Information Systems Research*, 11(4), 418 -430.

Al-Qeisi, K. 2009."Analyzing the use ofUTAUT model in explaining an online behaviour: internet banking adoption". *Unpublished doctoral dissertation.UK, Brunel University. Ph.d, theses*.

Arunkumar, S. 2007. A study on attitude and intention towards Internet banking with reference to Malaysian consumers in klang valley region. *The International Journal of Applied Management and Technology*, 6, 1.

Bagozzi, R.P. 2007. The Legacy of the Technology Acceptance Model and a Proposal for a Paradigm Shift. *Journal of the Association for Information Systems*. 8(4), 43-254.

Bahaman Abu Samah., HayrolAzril Mohamed Shaffril., Musa Abu Hassan., Jeffrey Lawrence D'Silva. 2011. "Can Technology Acceptance Model be Applied on the Rural Setting: The Case of Village Development and Security Committee in Malaysia". *Journal of Social Sciences* 7 (2): 113-119.

Bandura, A. 1986. The explanatory and predictive scope of self-efficacy theory. *Journal of Clinical and Social Psychology*, 4, 359-373.

Bandura, A. 1982. Self -Efficacy mechanism in Human Agency", *American Psychologist*, 37 (2), 122-147.

Bandura, A. 1995. "Self-efficacy, impact of self-beliefs on adolescent life paths. *R. M. Lerner, A.C. Peterson, & J. Brooks-Gunn (Eds.), Encyclopaedia of adolescence* , New York, Garland, Vol. 2, 1991, pp. 995-1000.

Bhattacherjee, A. 2001. "Understanding information systems continuance: An expectation confirmation model". *MIS Quarterly*, 25(3), 351-370.

Brown, S., Massey, A., Montoya-Weiss, M., Burkman, J. 2000**.** Do I really have to? User Acceptance of Mandated Technology. *European Journal of Information System*. 11, 283 – 295.

Burton-Jones, A., Hubona, G.S. 2006. The Mediation of External Variables in the Technology Acceptance Model". *Information and Management* . 43(6), 706 -717.

Chuttur, M.Y. 2009. Overview of the Technology Acceptance Model: Origins, Developments and Future Directions".*Working Papers on Information Systems*, Indiana University, USA, Sprouts, 297 – 334.

Comrey, A.L. 1973. "A First Course in Factor Analysis". *Academic Press, NY.*

Cook, T.D., Campbell, D.T. 1979. "Quasi-Experimentation: Design and Analysis for Field Settings", Rand McNally, Chicago, Illinois.

Cronbach, L.J. 1951. "Coefficient Alpha and Internal Structure Tests. *Psychometrika*, 22(3),

Davis, F.D., Bagozzi, R.P., Warshaw, P.R. 1989. "User acceptance of computer technology: a comparison of two theoretical models", *Management Science*, 35(8), 982-1003.

Davis, F. 1989. "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology". *MIS Quarterly*, 13 (3), 319-340.

Fishbein, M.A., Ajzen, I. 1975. "*Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research"*, Addison-Wesley, Reading, MA.

Gallivan, M.J., Shen, Y. 2005. "Examining User-Technology Interaction: Toward a Sociotechnical Theory for Understanding User Adjustment to Mobile Technologies" *Eleventh Americas Conference on Information Systems,* Omaha.

Glynn Fergal 2016. "Secure Software Development Practices"; Veracode publication on The State of Software Security, Vol. 7,

Griffin, A., Viehland, D. 2010. "Perceived Risk and Risk Relievers Associated with Online Shopping", *ACIS Proceedings*, Paper 31.

Hyeun-Suk Rhee, Cheongtag Kim, Young u. Ryu. 2009. Self-efficacy in Information Security: Its influence on end users' information security practice behaviour", *Computer and Security, Elsevier Ltd*, 28(8), 816-826.

Lee, Y., Kozar, K.A., Larsen, K.R.T. 2003. "The Technology Acceptance Model, Past, Present and Future", *Communication of the AIS*, 12(50), 752 – 780.

Legris, P, Ingham, J, Collerette, P. 2003. "Why do people use information technology? A critical review of the technology acceptance model", *Information & Management*,40 (3), pp. 191–204.

Livari, J. 1996**.** Why are CASE tools not used? *Communication of the ACM* , 9(10), 94 – 103

Livari, J., Igbara, M. 1995**.** The effect of Self-efficacy on Computer Usage. *Omega Int'l Journal of Management Science*, 23(6), 587 – 605.

Mathieson, K. 1991. Predicting user intentions: Comparing the technology acceptance model with the theory of planned behaviour. *Information Systems Research*, 2(3), 173-191.

McGraw, G. 2004. Managing Software Security Risks", IEEE Security & Privacy. 2 (2) Mar-Apr, 80-83.

Nunnally, J. C. 1978. Psychometric Theory. *McGraw-Hill*, *New York*.

Ozer*, E., Bandura,* A. 1990.*"* Mechanisms governing empowerment effects: A self-efficacy analysis", *Journal of Personality and Social Psychology* 58, 472-486.

Petersen R.C., Doody R, Kurz A, Mohs R.C, Morris J.C, Rabins P.V, 2001**.** "Current concepts in mild cognitive impairment. *Arch Neurol* 58, 1985-1992.

Sanayei, Ali; Shahin, Arash; Salimian, Hamideh. 2013**.** "Analyzing Factors Influencing Virtual Bank Acceptance as New Generation of e-Banking with a Case Study on e-Citizens". *New Marketing Research Journal*; Autumn, Vol. 3 Issue 3.

Subramanian, G. H. 1994**.** " A replication of perceived usefulness and perceived ease of use measurement", *Decision Sciences*, 25 (5/6), 863–873.

Szajna, B. 1994**.** Software evaluation and choice: predictive evaluation of the Technology Acceptance Instrument", *MIS Quarterly*, 18 (3), 319–324.

Starjkovic, A.D., Luthans, F. (1998). Self-Efficacy and work related performance: A meta analysis. Psychological Bulletin", 124(2), 240-261.

Starjkovic, A.D., Luthans, F. (1998). Social Cognitive Theory and Self-Efficacy : Going beyond traditional motivational and behavioural approaches. *Organisation Dynamics*, 26(4), 62–74.

Stewart, James."CISSP Certified Information System Security Professional Study Guide Sixth Edition" Canada: John Wiley & Sons, Inc. Pp. 275-319. ISBN 978-1-118-31417- 3.

Syed Rizwan Ahmed (2007). "Secure Software Development – Identification of Security Activities and Their Integration in Software Development Lifecyle", Master Thesis, Blekinge Tekniska, Hogskola- Sweden, March 2007.

Taylor, S., Todd, P.A. 1995a. "Understanding information technology usage: a test of competing models", *Information Systems Research*, 6(2), 144-176.

Taylor, S., Todd, P.A. 1995b. "Assessing IT Usage, The role of Prior Experience", *MIS Quarterly*, 19(4), 561-570.

Venkatesh, V., Davis, F. D., 2000**.** A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field", *Management Science*, 46(2), 86-204.

Viehland, Dennis, Zhao, Fei 2010. The Future of Personal Area Networks in a Ubiquitous Computing World. In: IJAPUC, 2 (2), 30-44.

(Manuscript received: 10th November, 2015; accepted: 18th April, 2017).