Contents lists available at Science-Gate

International Journal of Advanced and Applied Sciences

Journal homepage: http://www.science-gate.com/IJAAS.html

The role of Internet security awareness as a moderating variable on cyber security perception: Learning management system as a case study

Adel Abdulmohsen Alfalah *

Management and MIS Department, College of Business Administration, University of Hail, Hail, Saudi Arabia

ARTICLE INFO

Article history:
Received 5 October 2022
Received in revised form
18 January 2023
Accepted 22 January 2023

Keywords:
Technology adoption
Learning management system
Internet security awareness
SmartPLS

ABSTRACT

The purpose of this study is to investigate the influence of different dimensions of cyber security perception on university students' attitudes towards using a learning management system (LMS) and to what extent these relationships can be moderated by Internet security awareness. To accomplish this, an extensive review of technology adoption literature has been conducted, and a theoretical model was presented. The study applied a quantitative-based approach that used a survey questionnaire to collect 261 responses from college-level students in the Kingdom of Saudi Arabia. To test the research model, the researcher used SmartPLS version 3 which applies partial least squares-based structural equation modeling (PLS-SEM). Analysis showed that perceived privacy, trust in the Internet, trust in the university, and perceived cyber risk are key influencers factors on attitude and that all these correlations are moderated by Internet security awareness except for the association between trust in the university and attitude. The outcome of the study contributes to academia by enriching the existing literature on technology adoption in educational settings. The results also benefit practitioners and policymakers in terms of enhancing the awareness of LMS users which in turn leads to a better attitude towards system use.

1. Introduction

Due to advancements in online learning technologies, many countries around the world have incorporated such technologies into their educational systems (Han and Shin, 2016). Trending learning technology is the Learning Management System (LMS) which is a web-based software application that facilitates many teaching and learning administrative tasks such as reporting, discussion, exams delivery, sharing course materials, and tracking activities (Khan, 2020). Many universities and other higher education institutions have made substantial investments in incorporating LMSs into their strategic plans and teaching modes in order to benefit from the wide range of smart services and capabilities LMSs would bring about. These systems are available to learners regardless of their diverse lifestyles and circumstances, and they are not restricted by time and place (Chawdhry et al., 2011). They can also provide instructors with the necessary tools to manage their courses in terms of content delivery, assignment submission, group discussions, attendance tracking, and exams assessment (Heirdsfield et al., 2011).

Throughout the years, the domain of information systems adoption has been extensively researched and investigated in order to find out critical success factors impacting users' attitudes towards such systems (Vichitvanichphong et al., 2013; Purarjomandlangrudi et al., 2015; Alfalah, 2021). Under the umbrella of information systems comes LMSs, and for them to be successful, universities and higher education institutions must motivate students and learners to adopt and incorporate LMSs into their learning journey and process (Al-Fraihat et al., 2020). The current literature pertaining to the successful adoption of LMSs by college-level students identified various factors leading to such acceptance and adoption. For example, but not limited to, user-friendly interfaces, organizational support and self-efficacy (Zanjani, 2017); virtual attractiveness and perceived admin presence (Ghapanchi et al., 2020); social influence and instructor role (Binyamin et al., 2017); perceived usefulness (Akman and Turhan, 2017); perceived ease of use (Saroia and Gao, 2019).

* Corresponding Author.
Email Address: a.alfalah@uoh.edu.sa
https://doi.org/10.21833/ijaas.2023.04.017
Corresponding author's ORCID profile:
https://orcid.org/0000-0001-7770-4004

However, since LMSs are dependent on Internet services, concerns regarding using the Internet should be adequately addressed. Many view the Internet as a non-secure place due to the lack of rules and official regulations as well as the low level of user awareness, including college-level students (Potgieter, 2019). Therefore, this study will concentrate on some influential factors that are related to Internet use concerns that impact students' attitudes towards adopting and using LMSs. The aim of this study is to investigate the impact of perceived privacy, trust in the Internet, trust in the institution, and perceived cyber risk on higher education students' attitudes towards using LMSs, and to what extent these relationships can be moderated by Internet security awareness. The next section provides a review of existing literature on technology adoption in general and in educational settings in particular; followed by the development of a conceptual framework and hypotheses.

2. Related works

Technology adoption literature in educational settings shows that the enormous amount of effort and investment higher education institutions are putting into the utilization and deployment of LMSs has not been completely reflected in the students' adoption rate of those systems (Ghapanchi et al., 2020). Many students are still negatively influenced by various factors affecting their attitudes toward LMSs. Reasons vary from individual and institutional factors (psychological and managerial) to social and cultural factors. For example, literature identified perceived website assistance as a major player in the willingness to adopt and use LMS (Zanjani, 2017; Zheng et al., 2018). While good technical support drives up the probability to adopt LMS, poor technical assistance was found to be a major hindrance to the successful adoption of LMS (Asiri et al., 2012). Computer Self-efficacy is another factor highlighted by researchers to have an impact on positive attitudes toward LMS (Ghapanchi et al., 2020; Grandon and Pearson, 2004).

Similarly, within the literature on technology adoption in developing countries, researchers have identified multi-faceted factors influencing learners' effective use of LMS. Yakubu and Dasuki (2019) found that behavioral intentions are remarkably influenced by effort expectancy and performance expectancy whereas facilitating conditions considerably impacted students' actual use of LMS. Findik-Coşkunçay et al. (2018) applied technology acceptance model (TAM) in their research and found that perceived ease of use and perceived usefulness along with other related constructs, including perceived satisfaction, enjoyment, and interactivity are of high importance. The previous review implies that the literature includes an abundance of research investigating a wide range of technology acceptance models and theories, including TAM, the unified theory of acceptance and use of technology (UTAUT), the theory of reasoned action (TRA) and the extended UTAUT. Further, researchers have also widely investigated trust dimensions, privacy issues, and perceived risk within different areas of technology adoption, such as e-government (Taiwo et al., 2012; Choudrie et al., 2018; Alfalah, 2021), e-commerce (Pavlou, 2003; Zanjani, 2017), and web-based platforms (Swaak et al., 2009). However, only a little research has been done studying the influence of trust, privacy, and cyber risk in the literature on educational technology adoption. Another gap in the literature was identified; that is how Internet security awareness would moderate the relationship between trust, privacy, and cyber risk on one side and attitudes towards using LMS on the other side. Accordingly, this research will focus on studying those factors by applying quantitative research methods. The next section will discuss the development of the study model and hypotheses.

3. Development of conceptual framework and hypotheses

3.1. Privacy

The online environment has created notable concerns with regard to users' information privacy. The concept of privacy refers to users' right to be free from unsanctioned intrusion; that is to have control over what information is acquired and used by other parties (Westin, 1968). The advancements in the technologies of the online environment whether in the form of electronic commerce or online education, reflect the increased capabilities of such technologies to collect, use, and store users' personal information beyond the original transaction (Liu et al., 2005). Therefore, a main threat to users' willingness to interact in the online environment is their perceived concerns that their personal information will be disclosed (Malhotra et al., 2004). Given the fact that e-LMS has been a major part of today's educational systems, the current study proposes that:

H1: Greater levels of perceived privacy (PP) will be positively related to attitudes toward using e-LMSs.

3.2. Trust

Further, trust factors have always been one of the major issues hindering users from the constant online presence (Alfalah, 2021) There are two sources of having trust dilemma: Perceived lack of security of online transactions, and doubts about how users' information will be handled by institutions when submitted online (Bélanger and Carter, 2008). Trust refers to "the expectation that the promise of another can be relied upon and that, in unforeseen circumstances, the other will act in the spirit of goodwill and in a benign fashion toward the trustor" (Grazioli and Jarvenpaa, 2000). Having identified the significance of trust in online settings, the current study model includes two trust factors, namely trust on the Internet and trust in the

institution. Those factors were proposed by McKnight et al. (2002), which in turn used the Theory of Reasoned Action TRA as a guiding framework. This will help in understanding how users' (in this case students) perceptions of trust on both the Internet and the institution providing the service (in this case universities) will impact their attitudes towards using e-LMS. Therefore, it is proposed that:

H2: Greater levels of trust in the Internet (TII) will be positively related to attitudes towards using e-LMSs.
H3: Greater levels of trust in the institution (university in this case) TIU will be positively related to attitudes towards using e-LMSs.

3.3. Risk

In addition to the aforementioned factors, technology adoption literature highlights perceived risk as a fundamental factor that influences users' attitudes toward participating in online transactions. The concept of risk reflects the possibilities of attainments or losses (Warkentin et al., 2002). In online settings, perceived risk is closely related to the notion that the institution providing the online service might treat users dishonestly and fraudulently, taking advantage of the nonphysical nature of the Internet. Perceived cyber risk also reflects the degree to which users of online systems have doubts with regard to unfortunate incidents that might take place beyond their control (Pavlou, 2003). Accordingly, many users find themselves reluctant to partake in online systems due to the probability of cybercrimes, such as privacy breaches, identity theft, and intellectual property violations (Choudrie et al., 2017). Therefore, perceived risk is also anticipated to have a great influence on students' attitudes toward using e-LMSs. This study proposes that:

H4: Greater levels of perceived cyber risk (PCR) will be negatively related to attitudes toward using LMSs.

3.4. Internet security awareness

Further, a student in traditional educational settings, that is the physical environment, used to worry only about their physical security. However, this has considerably changed due to technological advancements and the modern impersonal nature of many educational systems around the world, which has brought about many challenges and worries regarding the newly imposed cyber security concerns (Rezgui and Marks, 2008). Further, being aware of such concerns is rather critical for higher education students in particular due to their lengthy online presence. This extensive online presence has made university students targets of phishing attacks and information privacy violations. This is particularly true for students who participate extensively in e-LMS activities, such as online classes and discussion forums. As a result, the matter of Internet security awareness has become of extreme importance to be discussed at university level education. Internet security awareness reflects the degree to which Internet users have the necessary knowledge to guard themselves against suspicious activities while present in cyberspace (Gurung et al., 2008). This knowledge includes awareness of the importance of using security controls, such as patches and updates, antispyware and personal firewalls, etc. Therefore, security awareness is not a synonym for training, it is only to keep security at the forefront of Internet users in order to keep threats to a minimum (Bada et al., 2019). Unfortunately, lack of awareness was found to be a major factor behind Internet users' lack of information security knowledge (Aldawood and Skinner, 2018). It was also found in technology adoption literature that increased perceived risk within the online environment is a direct result of the lack of awareness of privacy protection significance (Gurung et al., 2008). Therefore, in order to investigate the role that Internet security awareness might play in shaping students' attitudes toward using e-LMS, it is proposed that:

H5: The relationship between PP and attitude (ATT) is moderated by Internet security awareness (ISA), and the tendency for PP to be positively related to ATT will be significantly more pronounced when ISA is high rather than low.
H6: The relationship between TII and ATT is moderated by ISA, and the tendency for TII to be positively related to ATT will be significantly more pronounced when ISA is high rather than low.
H7: The relationship between TIU and ATT is moderated by ISA, and the tendency for TIU to be positively related to ATT will be significantly more pronounced when ISA is high rather than low.
H8: The relationship between PCR and ATT is moderated by ISA, and the tendency for PCR to be negatively related to ATT will be significantly dampened when ISA is high rather than low.

Based on the hypotheses presented above, Fig. 1 depicts the conceptual framework for this research.

3.5. Research design

This study adopted a quantitative approach in which an online-based survey questionnaire was distributed among undergraduate students from different public universities in the Kingdom of Saudi Arabia in May 2021 during the COVID-19 pandemic. The questionnaire consisted of two main parts. The first part collected the respondents' demographic information whereas the second part was based on a 5-point Likert scale in which 5 represents (strongly agree) and 1 represents (strongly disagree). To examine learners' attitudes toward using LMS, the questionnaire included 20 measurement items. As a result, 298 responses were received, of which 261 responses were considered valid to be included in the analysis.

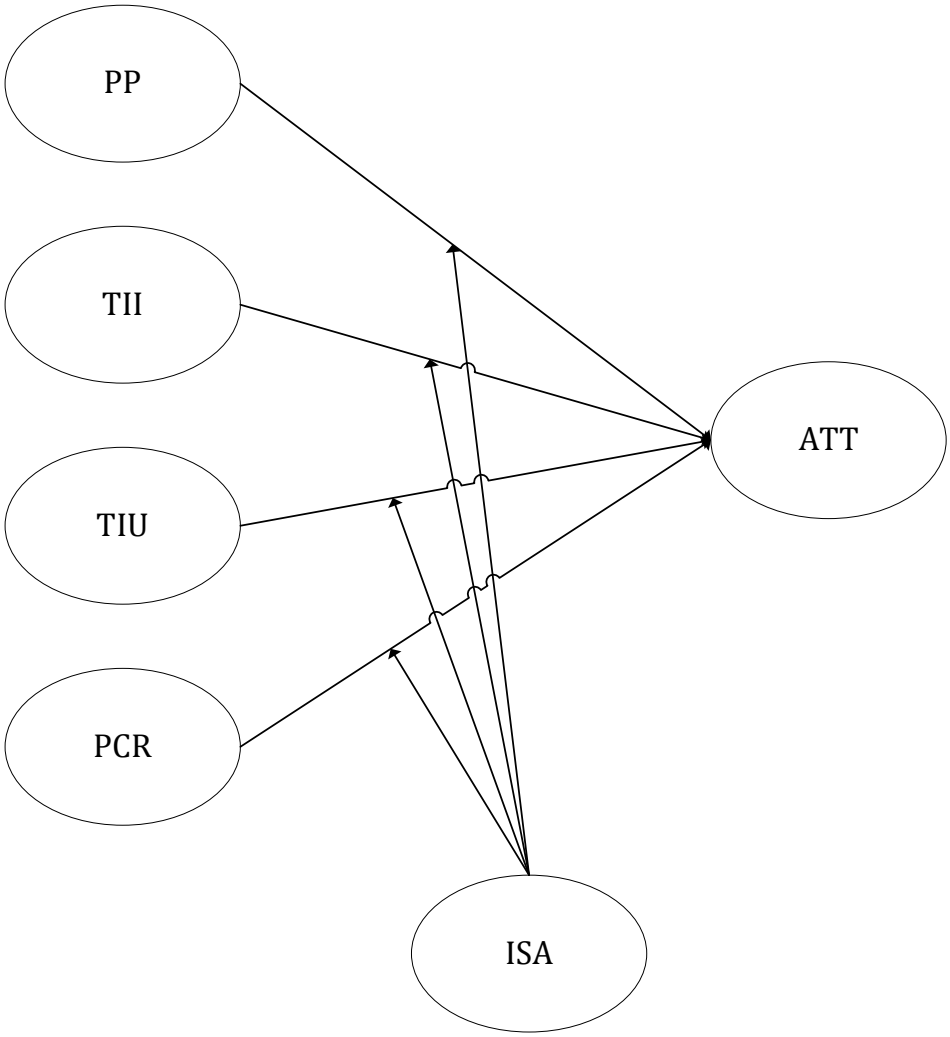

Fig. 1: Research model

4. Data analysis

4.1. Measurement model

To measure the reliability of the model, three widely used tests are used, namely Cronbach's Alpha, Composite Reliability, and Average Variance Extracted (AVE) (Litwin and Fink, 1995). Cronbach's Alpha and Composite Reliability gauge the internal consistency of tests by determining the degree to which the indicators of the scale measure the same factor in which a value of 0.7 is considered adequate for both measures (Tavakol and Dennick, 2011; Henseler et al., 2009). Accordingly, as shown in Table 1, all constructs have met the criterion except for Perceived Privacy with a Cronbach alpha value of 0.665, which is very close to the threshold value of 0.707; therefore, it doesn't affect the validity of the construct. In addition, factor loadings were also calculated to further establish the constructs' validity. They are indications of the extent to which each item correlates to its construct. A value of 0.7 is considered sufficient, which is met by all this study's items (Table 1) (Henseler et al., 2009).

Further, to establish the convergent validity of constructs, the AVE test is applied to check whether the items of a construct explain more variance than the items of the other constructs (Zaiţ and Bertea, 2011). Table 1 shows that all constructs have met the satisfactory level of 0.5 for AVE. As for discriminant validity, Table 2 shows that criterion is met in all the instances because the square root of AVE of each construct was greater than its cross-correlation with the other constructs.

4.2. Structural model and hypotheses testing

To test the model presented in this study, the researcher used SmartPLS version 3 which applies partial least squares-based structural equation modelling (PLS-SEM). Fig. 2 depicts the path coefficients between the explanatory variables and the dependent variable. Based on these standardized regression coefficients, the proposed hypotheses were supported (H1, H2, H3, H4) indicating a significant impact of the independent variables on the dependent variable attitude. Further, Figs. 3, 4, and 5 show the moderation effect of ISA on PP, TII, and PCR toward ATT respectively. Based on these results, H5, H6, and H8 were supported. On the other hand, H7, which proposed the existence of a moderation effect of ISA on TIU towards ATT, was not supported.

Table 1: Reliability and validity measurements

Construct	Item	Factor Loading1	Cronbach alpha2	Composite reliability3	AVE4
PP	PP1	0.887	0.665	0.758	0.536
	PP2	0.779			
	PP3	0.921			
TIU	TIU1	0.944			
	TIU2	0.840	0.912	0.936	0.785
	TIU3	0.845			
	TIU4	0.909			
TII	TII1	0.896	0.849	0.906	0.764
	TII2	0.926			
	TII3	0.793			
PCR	PCR1	0.886	0.784	0.851	0.729
	PCR2	0.683			
	PCR3	0.913			
	PCR4	0.881			
ATT	ATT1	0.894	0.891	0.932	0.821
	ATT2	0.909			
	ATT3	0.916			

1=Satisfactory if>=0.7; 2=Satisfactory if>=0.7; 3=Satisfactory if>=0.7; 4=Satisfactory if>=0.5

Table 2: Discriminant validity

Construct	ATT	PP	TII	TIU	PCR
ATT	0.906				
PP	0.521	0.732			
TII	0.405	0.128	0.874		
TIU	0.227	0.232	0.732	0.886	
PCR	0.306	0.439	0.562	0.363	0.787

In addition to path coefficient analysis and critical p-values, Table 3 presents the Coefficient of Determination (R2), which provides an idea of the extent to which independent variables within a model can explain the dependent variable. In terms of this study, R^2 (*ATT*)=0.702, indicating that approximately 70% of the variability within higher education students' attitudes toward using Learning Management Systems can be explained by the model, which is considered sufficient explanatory power (Hair et al., 2011).

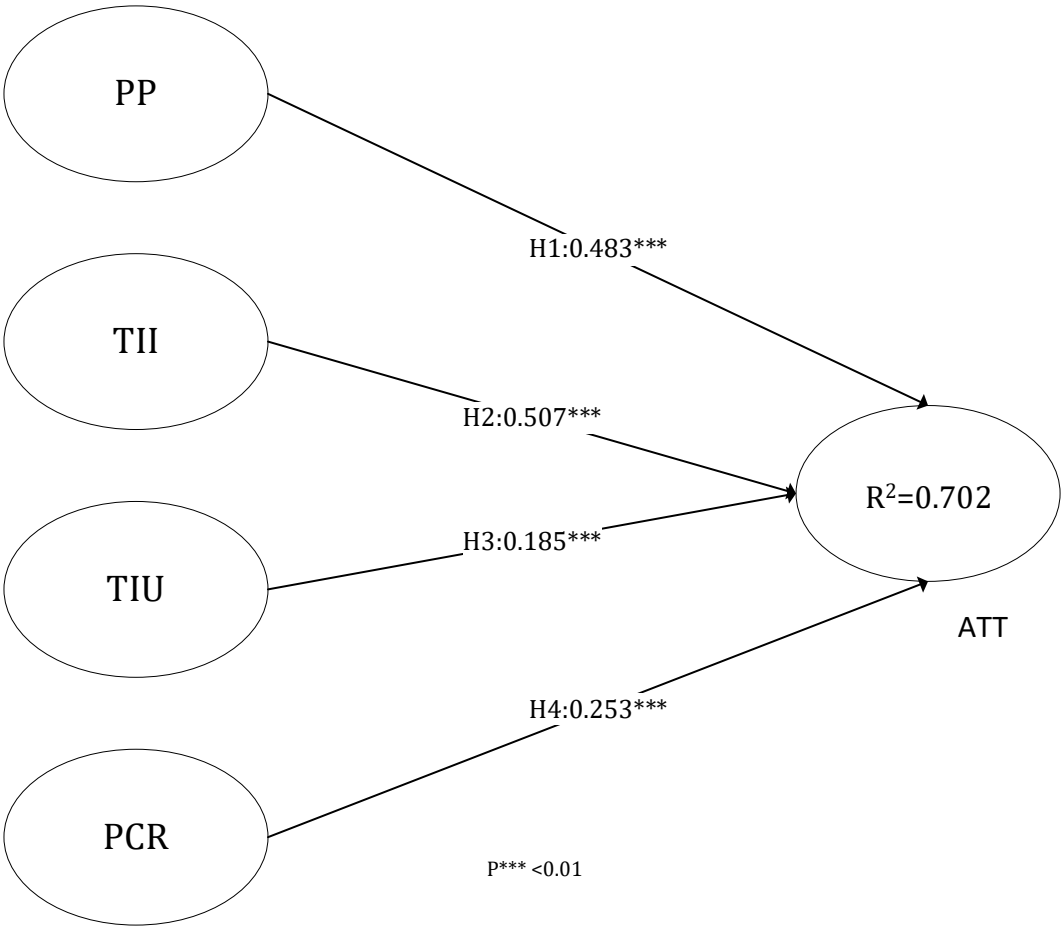

Fig. 2: Structural measurement model

Table 3: Hypothesis testing

#	Hypothesis	Path coefficient	*t*-value	p-value	Result
H1	PP-->ATT	0.483	11.033	0.000***	Supported
H2	TII-->ATT	0.507	5.920	0.000***	Supported
H3	TIU-->ATT	0.185	2.459	0.014**	Supported
H4	PCR-->ATT	-0.253	4.623	0.002***	Supported
H5	PP*ISA->ATT	0.216	2.511	0.012**	Supported
H6	TII*ISA->ATT	0.383	4.702	0.000***	Supported
H7	TIU*ISA->ATT	0.024	0.833	0.229	Not supported
H8	PCR*ISA->ATT	0.155	2.169	0.013**	Supported

R^2 (ATT)=0.702; P*<0.1 P** <0.05 P*** <0.01

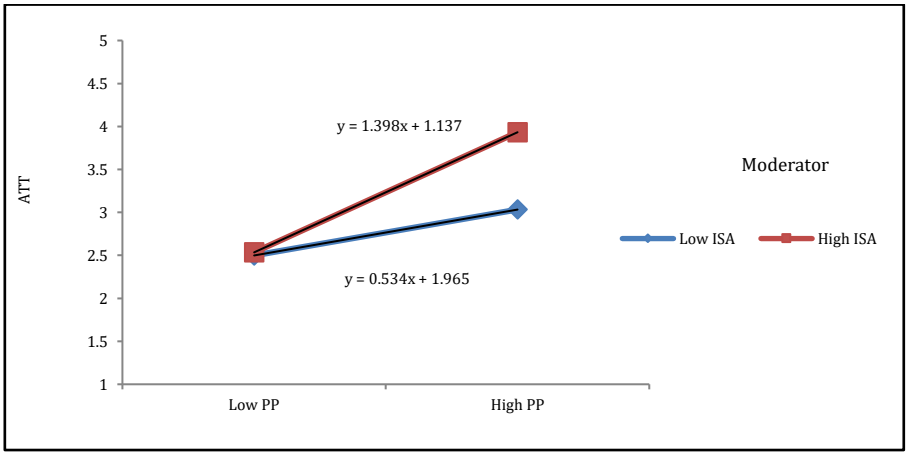

Fig. 3: The moderation effect of ISA on PP*ATT

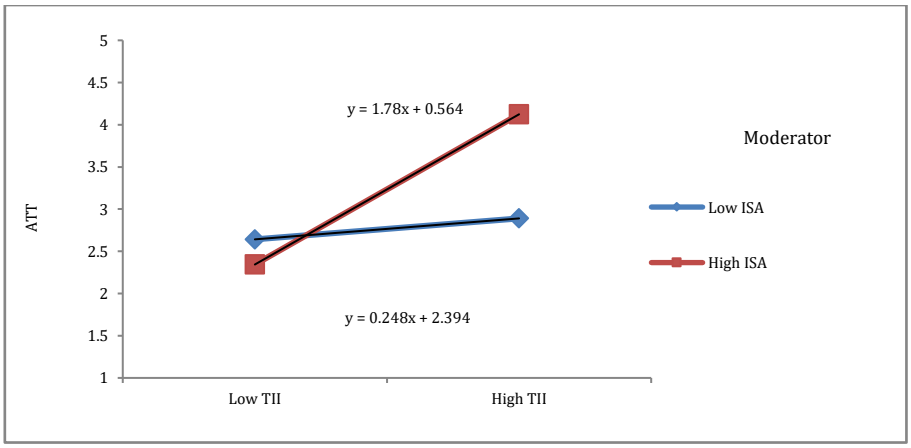

Fig. 4: The moderation effect of ISA on TII*ATT

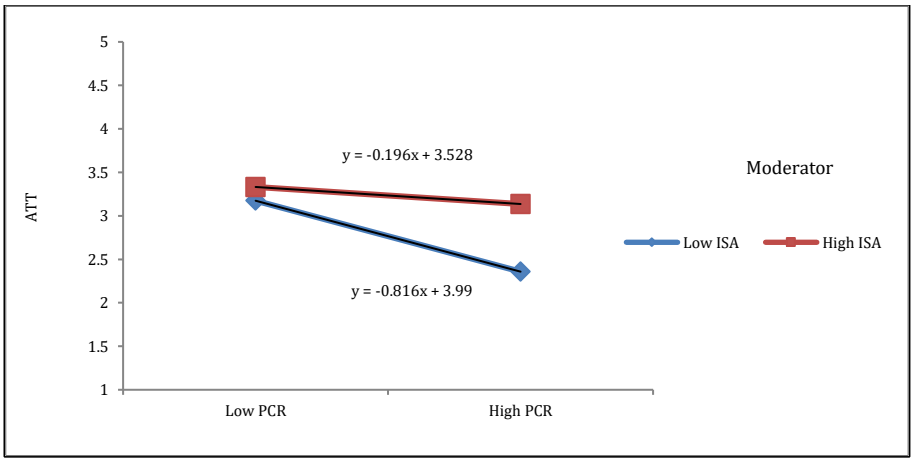

Fig. 5: The moderation effect of ISA on PCR*ATT

5. Discussion

This study was conducted to accomplish two main objectives. The first objective is to investigate the impact of the factors of perceived privacy, trust, and perceived cyber risk on the attitude of college-level students toward using LMS. The second objective is to understand the role of Internet security awareness in moderating the relationship between previously mentioned factors and attitude.

According to analysis, perceived privacy showed a significant positive effect on attitude towards use which comes in accordance with existing literature on technology adoption in educational settings (Zanjani, 2017; Singh and Miah, 2020). This indicates that learning systemsthat give students reasonable control over privacy settings, such as anonymous posting is likely to encourage them to be actively engaged in the learning process.

Further, trust in the Internet was found to have a considerable impact on learners' attitudes to use LMS. This is not surprising since the literature on technology adoption in general and in educational settings, in particular, has comprehensively discussed how Internet-based trust influences users' attitudes (Choudrie et al., 2018; Almaiah et al., 2020). As mentioned previously, the Internet is considered an unsafe place to the degree that many users are reluctant to participate in online activities. Successful adoption of any technology is directly related to building trust in the channel that provides the service. Thus, for learners to view an LMS as a trustworthy technology, they must first believe that the mediator carrying out the process is trustworthy and safe (Shapiro, 1987). Similarly, trust in the institution (university) also showed significance regarding learners' attitudes to using. This outcome has been previously confirmed not just in higher education settings (Saroia and Gao, 2019) but also in similar settings, such as e-government and e-commerce (Gurung et al., 2008; Bélanger and Carter, 2008). When a user engages in online activity or transaction, this usually means he or she considers the party providing the service as a reliable entity in terms of integrity and capability. Therefore, part of the successful adoption of LMS is derived from students' beliefs that their universities and educational institutions are capable of providing robust, secure, credible, and up-to-date online-based services and transactions.

In addition, perceived cyber risk showed a significant negative impact on students' attitudes to use LMS. Higher education institutions are constantly subject to cyber-attacks that may cause disruption of their services and jeopardize students' valuable data (Chapman, 2019). Such cyber risks can be mitigated by incorporating them into their governance and management strategies and plans rather than addressing them solely from a technical viewpoint. When the institution has a well-established and robust strategy and plans regarding possible cyber risks, the trust of stakeholders increases which in turn mitigates their perceived cyber risk when engaging in online-based systems.

This study also found that Internet security awareness plays a considerable moderating role. For example, Figs. 3 and 4 indicate that the tendency for PP and TII to be positively related to ATT is significantly more pronounced when ISA is high rather than low. When students have the necessary knowledge to protect themselves against cyber-attacks and privacy violations, their attitudes toward using LMS will be positively influenced. Comparably, when their level of awareness of Internet risks is high and their ability to apply protection tools and mechanisms is reasonable, their perceived cyber risk will have a less negative influence on their attitude towards LMS (Fig. 5). On the other hand, ISA did not show any moderating effect on the relationship between trust in the university TIU and attitude ATT. In this regard, it seems that believing the university is capable of carrying out and running online learning systems and that it will always serve students' best interests is only influenced by whether this is true or not regardless of any other external variables.

The first implication of this research is the validation of the applied conceptual model. The literature on learning technology adoption lacks studies focusing on the different dimensions of cyber security perception and how they might influence attitudes. This study also provides a deep understanding of the significance of Internet security awareness ISA as a moderating variable within the model. Therefore, policymakers and higher education officials can use this result and focus on enhancing the awareness of LMS users which in turn should lead to a better attitude towards engaging in such online-based learning systems. Further, both systems developers and university management should build trust in LMSs by practically convincing students of their capability of building robust and secure systems in one hand and keeping the best interest of students throughout the different processes and activities.

6. Conclusion and future research

This study was conducted with two main objectives. The first was to investigate the perceived security and trust factors that influence the attitudes of higher education students in terms of LMS use. The second was to understand the role of Internet security awareness in moderating the relationship between the aforementioned security and trust factors and attitudes. 8 hypotheses were proposed based on the theoretical model which was empirically tested using partial least squares-based structural equation modelling (PLS-SEM). The study adopted a quantitative-based approach that used a survey questionnaire as the research instrument for data collection resulting in 261 responses from higher education students being collected. Results confirmed 7 out of the 8 proposed hypotheses. PP, TII, TIU, and PCR all showed significance in shaping the attitude of college-level students toward using LMS. Results also confirmed the considerable role of ISA in moderating the attitude of learners. Only H7 was not supported by the analysis in which ISA showed no moderating effect on the relationship between TIU and ATT.

The researcher is aware of the limitation of this study. First, the study was conducted only in Saudi Arabia; thus, the outcome cannot be generalized to other contexts. Second, although the sample size was somewhat reasonable, a larger sample size would

have offered an even deeper understanding of the topic. Lastly, the study did not include other important contextual variables (e.g. level of Internet use experience, years of LMS use, etc.) in the analysis which might provide clearer insights and explanations about users' cyber security perception. For future research, this study can be expanded into other geographical contexts with a larger sample size to get a broader understanding of the topic. Future research could also contribute by adding important contextual variables to the analysis which were not included in this study.

Compliance with ethical standards

Conflict of interest

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

References

Akman I and Turhan C (2017). User acceptance of social learning systems in higher education: An application of the extended technology acceptance model. Innovations in Education and Teaching International, 54(3): 229-237. https://doi.org/10.1080/14703297.2015.1093426

Aldawood H and Skinner G (2018). Educating and raising awareness on cyber security social engineering: A literature review. In the 2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering, IEEE, Wollongong, Australia: 62-68. https://doi.org/10.1109/TALE.2018.8615162

Alfalah A (2021). Visualization of e-gov adoption models in a developing region: A review of the predictors in empirical research. International Journal of Electronic Government Research, 17(4): 103-121. https://doi.org/10.4018/IJEGR.2021100106

Al-Fraihat D, Joy M, and Sinclair J (2020). Evaluating e-learning systems success: An empirical study. Computers in Human Behavior, 102: 67-86. https://doi.org/10.1016/j.chb.2019.08.004

Almaiah MA, Al-Khasawneh A, and Althunibat A (2020). Exploring the critical challenges and factors influencing the e-learning system usage during COVID-19 pandemic. Education and Information Technologies, 25(6): 5261-5280. https://doi.org/10.1007/s10639-020-10219-y **PMid:32837229 PMCid:PMC7243735**

Asiri MJS, Bakar KA, and Ayub AFBM (2012). Factors influencing the use of learning management system in Saudi Arabian higher education: A theoretical framework. Higher Education Studies, 2(2): 125-137. https://doi.org/10.5539/hes.v2n2p125

Bada M, Sasse AM, and Nurse JR (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? ArXiv Preprint ArXiv: 1901.02672. https://doi.org/10.48550/arXiv.1901.02672

Bélanger F and Carter L (2008). Trust and risk in e-government adoption. The Journal of Strategic Information Systems, 17(2): 165-176. https://doi.org/10.1016/j.jsis.2007.12.002

Binyamin S, Rutter M, and Smith S (2017). Factors influencing the students' use of learning management systems: A case study of King Abdulaziz University. In the International Conference on e-Learning, Academic Conferences International Limited.7, Orlando, USA: 298-297. https://doi.org/10.21125/inted.2017.2205

Chapman J (2019). How safe is your data? Cyber-security in higher education. Higher Education Policy Institute, Oxford, UK.

Chawdhry A, Paullet K, and Benjamin D (2011). Assessing Blackboard: Improving online instructional delivery. Information Systems Education Journal, 9(4): 20-26.

Choudrie J, Alfalah A, and Spencer N (2017). Older adults adoption, use and diffusion of e-government services in Saudi Arabia, Hail City: A quantitative study. Proceedings of the 50th Hawaii International Conference on System Sciences, IEEE, Hawaii, USA: 2953-2962. https://doi.org/10.24251/HICSS.2017.357

Choudrie J, Alfalah A, Spencer N, and Sundaram D (2018). Are older citizens using the E-Moi portal in Saudi Arabia, Hail City: A quantitative study. In the 51st Hawaii International Conference on System Sciences, IEEE, Hawaii, USA. https://doi.org/10.24251/HICSS.2018.295

Findik-Coşkunçay D, Alkiş N, and Özkan-Yildirim S (2018). A structural model for students' adoption of learning management systems: An empirical investigation in the higher education context. Journal of Educational Technology and Society, 21(2): 13-27. https://doi.org/10.1037/t70573-000

Ghapanchi AH, Purarjomandlangrudi A, McAndrew A, and Miao Y (2020). Investigating the impact of space design, visual attractiveness and perceived instructor presence on student adoption of learning management systems. Education and Information Technologies, 25(6): 5053-5066. https://doi.org/10.1007/s10639-020-10204-5

Grandon EE and Pearson JM (2004). Electronic commerce adoption: An empirical study of small and medium US businesses. Information and Management, 42(1): 197-216. https://doi.org/10.1016/j.im.2003.12.010

Grazioli S and Jarvenpaa SL (2000). Perils of Internet fraud: An empirical investigation of deception and trust with experienced Internet consumers. IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans, 30(4): 395-410. https://doi.org/10.1109/3468.852434

Gurung A, Luo X, and Raja MK (2008). An empirical investigation on customer's privacy perceptions, trust and security awareness in E-commerce environment. Journal of Information Privacy and Security, 4(1): 42-60. https://doi.org/10.1080/2333696X.2008.10855833

Hair JF, Ringle CM, and Sarstedt M (2011). PLS-SEM: Indeed a silver bullet. Journal of Marketing Theory and Practice, 19(2): 139-152. https://doi.org/10.2753/MTP1069-6679190202

Han I and Shin WS (2016). The use of a mobile learning management system and academic achievement of online students. Computers and Education, 102: 79-89. https://doi.org/10.1016/j.compedu.2016.07.003

Heirdsfield A, Walker S, Tambyah M, and Beutel D (2011). Blackboard as an online learning environment: What do teacher education students and staff think? Australian Journal of Teacher Education (Online), 36(7): 1-16. https://doi.org/10.14221/ajte.2011v36n7.4

Henseler J, Ringle CM, Sinkovics RR, Sinkovics RR, and Ghauri PN (2009). New challenges to international marketing: Advances in international marketing. Emerald Group Publishing Limited, Bingley, UK.

Khan IA (2020). Electronic learning management system: Relevance, challenges and preparedness. Journal of Emerging Technologies and Innovative Research, 7(5): 471-480.

Litwin MS and Fink A (1995). How to measure survey reliability and validity. SAGE, Thousand Oaks, USA. https://doi.org/10.4135/9781483348957

Liu C, Marchewka JT, Lu J, and Yu CS (2005). Beyond concern-A privacy-trust-behavioral intention model of electronic commerce. Information and Management, 42(2): 289-304. https://doi.org/10.1016/j.im.2004.01.003

Malhotra NK, Kim SS, and Agarwal J (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. Information Systems Research, 15(4): 336-355. https://doi.org/10.1287/isre.1040.0032

McKnight DH, Choudhury V, and Kacmar C (2002). Developing and validating trust measures for e-commerce: An integrative typology. Information Systems Research, 13(3): 334-359. https://doi.org/10.1287/isre.13.3.334.81

Pavlou PA (2003). Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model. International Journal of Electronic Commerce, 7(3): 101-134. https://doi.org/10.1080/10864415.2003.11044275

Potgieter P (2015). The Awareness behaviour of students on cyber security awareness by using social media platforms: A case study at the central University of Technology. In: Njenga K (Ed.), Proceedings of 4th International Conference on the Internet, Cyber Security and Information Systems 2019, vol. 12: 272–262. Kalpa Publications in Computing, Johannesburg, South Africa.

Purarjomandlangrudi A, Chen D, and Nguyen A (2015). A systematic review approach to technologies used for learning and education. International Journal of Learning and Change, 8(2): 162-177. https://doi.org/10.1504/IJLC.2015.074068

Rezgui Y and Marks A (2008). Information security awareness in higher education: An exploratory study. Computers and Security, 27(7-8): 241-253. https://doi.org/10.1016/j.cose.2008.07.008

Saroia AI and Gao S (2019). Investigating university students' intention to use mobile learning management systems in Sweden. Innovations in Education and Teaching International, 56(5): 569-580. https://doi.org/10.1080/14703297.2018.1557068

Shapiro SP (1987). The social control of impersonal trust. American Journal of Sociology, 93(3): 623-658. https://doi.org/10.1086/228791

Singh H and Miah SJ (2020). Smart education literature: A theoretical analysis. Education and Information Technologies, 25(4): 3299-3328. https://doi.org/10.1007/s10639-020-10116-4

Swaak M, De Jong M, and De Vries P (2009). Effects of information usefulness, visual attractiveness, and usability on web visitors' trust and behavioral intentions. In the 2009 IEEE International Professional Communication Conference, IEEE, Waikiki, Hawaii: 1-5. https://doi.org/10.1109/IPCC.2009.5208719

Taiwo AA, Mahmood AK, and Downe AG (2012). User acceptance of eGovernment: Integrating risk and trust dimensions with UTAUT model. In the 2012 International Conference on Computer and Information Science. IEEE, Kuala Lumpur, Malaysia: 109-113. https://doi.org/10.1109/ICCISci.2012.6297222

Tavakol M and Dennick R (2011). Making sense of Cronbach's alpha. International Journal of Medical Education, 2**:** 53-55. https://doi.org/10.5116/ijme.4dfb.8dfd **PMid:28029643 PMCid:PMC4205511**

Vichitvanichphong S, Kerr D, Talaei-Khoei A, and Ghapanchi AH (2013). Analysis of research in adoption of assistive technologies for aged care. In the 24th Australasian Conference on Information Systems, Association for Information Systems AIS Electronic Library, Melbourne, Australia.

Warkentin M, Gefen D, Pavlou PA, and Rose GM (2002). Encouraging citizen adoption of e-government by building trust. Electronic Markets, 12(3): 157-162. https://doi.org/10.1080/101967802320245929

Westin AF (1968). Privacy and freedom. Washington and Lee Law Review, 25(1): 1-6.

Yakubu MN and Dasuki SI (2019). Factors affecting the adoption of e-learning technologies among higher education students in Nigeria: A structural equation modelling approach. Information Development, 35(3): 492-502. https://doi.org/10.1177/0266666918765907

Zaiţ A and Bertea PSPE (2011). Methods for testing discriminant validity. Management and Marketing Journal, 9(2): 217-224.

Zanjani N (2017). The important elements of LMS design that affect user engagement with e-learning tools within LMSs in the higher education sector. Australasian Journal of Educational Technology, 33(1): 19-31. https://doi.org/10.14742/ajet.2938

Zheng Y, Wang J, Doll W, Deng X, and Williams M (2018). The impact of organizational support, technical support, and self-efficacy on faculty perceived benefits of using learning management system. Behaviour and Information Technology, 37(4): 311-319. https://doi.org/10.1080/0144929X.2018.1436590