Global Business and Management Research: An International Journal
Vol. 14, No. 3s (2022)

Conceptual Framework on the Factors Influencing Users' Intention to Adopt AI-Based Cybersecurity Systems at Workplaces in the UAE

Mohammed Rashed Mohamed Al Humaid Alneyadi
School of Management, Universiti Sains Malaysia
Email: mohammed.alneyadi@student.usm.my

Normalini Md Kassim*
School of Management, Universiti Sains Malaysia
Email: normalini@usm.my

Teh Sin Yin
School of Management, Universiti Sains Malaysia
Email: tehsyin@usm.my

**Corresponding Author*

Abstract
Purpose: Artificial intelligence (AI) technologies are having revolutionizing effects in many industries, including the cybersecurity domains. However, research has consistently shown that the intention to adopt and use AI-based cybersecurity systems at both the organizational and individual levels is relatively low, yet such systems are associated with many potential benefits. In response to this research problem, the present study aims at investigating the factors that influence users' intention to adopt AI cyber-security systems at workplaces in the UAE.
Design/methodology/approach: This cross-sectional study will be conducted using the quantitative research methodology, where the correlational research design will be adopted. In this regard, the intended data will be collected through a web-based survey questionnaire from a sample of 178 respondents selected using the purposive sampling method. Upon collection, the data will be cleaned and prepared using the Statistical Package for Social Sciences (SPSS) software. It will then be analyzed using the Partial Least Squares structural equation and Modelling (PLS-SEM) program.
Findings:
Findings made in this research are expected to help organizations intending to adopt AI-based cybersecurity systems in determining the factors to consider before investing in and implementing AI-based cybersecurity systems. Such knowledge can help in enhancing a successful implementation of such a technology, characterized by minimal resistance from the employees. The insights gained may also be helpful to developers or firms creating AI-based cybersecurity technologies in understanding the considerations they should make when designing such technologies to enhance their adoption rate.
Research implications: This study is expected to make significant academic contributions. It is expected to enrich the currently elusive scholarly body of knowledge on the implementation and use of AI-based cybersecurity systems. So far, very little scholarly attention has been directed in this area. The study will also contribute to theory development by integrating and extending PMT and UTAUT2 models with a new variable. Doing so is expected to enhance

the predictive power of these two models in explaining the determinants of users' intention to use semi-autonomous systems such as AI-based systems.
Practical implications: This study is expected to help AI-based cybersecurity systems developers in developing systems that users can relate with, hence higher adoption and use rates. The findings of this study may also help decision-makers of organizations intending to embrace AI-based cybersecurity systems in establishing the factors to consider before investing in and implementing AI-based cybersecurity systems.
Originality/value: The theoretical contribution of this study is that it has sought to test the application of a hybrid of the two technology acceptance theories (PMT and UTAUT2) in a new context (UAE), and using a relatively novel technology, which is semi or fully autonomous. These theories had not been tested in such contexts and with that kind of technology. The study further contributes to theory development by introducing new variables and relationships to a hybrid of the two theories adopted. In practice, this study contributes to the growing evidence on the factors influencing the adoption and use of AI-based cybersecurity systems at workplaces.

Keywords: AI-based cybersecurity systems, PMT, UTAUT2, behavioral intention

Introduction

Cybercrimes are currently among the main challenges that the world is grappling with (Omelyan et al., 2021). This is because of the ever-increasing adoption of the internet and other emerging technologies such as the Internet of Things (IoT), cloud computing, and artificial intelligence, among others. Indeed, as Omelyan et al. (2021) note, though such technologies have proven to be a doorway to a more efficient and cost-effective future for businesses and individuals, they have provided avenues for the criminal fraternity to execute devastating, excessively expensive, and potentially more sophisticated cybercrimes. Indeed, a report compiled by Varonis (2021) on the most recent trends in cybercrimes indicated that cyberattacks are not only increasing, becoming complex, and unpredictable, but their adverse impacts are also growing at an alarming rate. This trend was mainly attributed to the rampant adoption of emerging technologies and the increase in the volume of data to be analyzed to detect and stop possible attacks (Varonis, 2021).

With cyber-security threats becoming more sophisticated and damaging, speedy identification and mitigation are increasingly becoming essential because one second can be the difference between losing confidential information and saving an organization (Omelyan et al., 2021). As a result, AI-based cybersecurity systems have emerged as a possible solution to the advancing complexity of cybercrimes, even though this technology is still in the development stages. According to Sharma (2021), one of the primary advantages that AI brings to the cybersecurity field is the ability to perform tasks faster and more accurately, thus enhancing the detection and neutralization of threats in real-time (Taddeo, 2019). In addition, AI can significantly help in the discovery of the most hidden vulnerabilities and techniques by analyzing enormous volumes of data and using the results obtained to classify suspicious activities. As explained by Sharma (2021) and AbuOdeh et al. (2021), an AI system can detect patterns of malpractices such as excessive utilization of resources (processors, memory, and others), strange connections, questionable transfer of data, unusual traffics, and suspicious login activities. These threats are then classified quickly in terms of their severity, and the information is sent to the administrators to take appropriate actions. Thirdly, AI-based cybersecurity systems can continually update themselves with more input data, meaning they can evolve with the changing cybercrime techniques (AbuOdeh et al., 2021).

Nonetheless, despite the growing evidence showing that AI-based cybersecurity systems have numerous potential benefits in preventing and mitigating the ever-escalating

problem of cybercrimes, research shows that the adoption of this semi or fully autonomous technology is still low (Azar & Haddad, 2019). This could be attributed to the fact that some potential users perceive this technology as relatively new and still in the infancy stages. Nonetheless, the novelty of this technology cannot be termed as the only factor influencing its acceptance at organizational and individual levels. This is because the technology has been tested and proven to be effective. Besides that, there seems to be selective adoption of this technology, with a report by Technavio (2021) showing that a majority of the Fortune 500 companies (in the USA) use AI-based cybersecurity systems. This is an interesting observation considering that the adoption rate of these systems is relatively low in the UAE, a country that is known to quickly embrace emerging technologies and trends such as the blockchain technology, intelligent automation, robotic process automation (RPA), and digital identity, among others (Desk, 2020; The Arab Weekly, 2018; Wilson, 2020). The selective adoption of some technologies and in some sectors begs the question of what could be driving users' choices for accepting/embracing new technologies such as AI in cybersecurity systems (Desk, 2020; The Arab Weekly, 2018; Wilson, 2020).

As noted by Jacobs et al. (2019), effective implementation of information systems or information technologies has revealed that users' acceptance plays an indispensable role in such a process and that it (user acceptance) can be predicted and explained by a wide range of factors such as the ease of use, usefulness, self-efficacy, and subjective norm to list just a few. Indeed, numerous theoretical models have been developed in the domains of information systems, psychology, and sociology, seeking to predict and explain user acceptance of an information system or information technology. However, though most of these theories have widely been adopted, doubts still exist over their capability to predict and explain the organizational and individual acceptance of some of the modern technologies such as the artificial intelligence. As noted by Lu, Cai, and Gursoy (2019), some of the components listed in the previously developed theories of user acceptance and effective implementation of information systems are no longer applicable or relevant in the upcoming technologies. This is because most of the emerging technologies such as AI have human-like intelligence, yet the existing theories had originally been developed for the adoption of non-intelligent technologies. As a result, variables such as ease-of-use and perceived usefulness may be irrelevant in predicting users' intention to accept AI technologies since such technologies do not require users to learn how to use them. Instead, they are designed to work like real human beings (Gursoy et al., 2019; Lu et al., 2019).

Such observations warrant conducting further research involving modern intelligent technologies and developing comprehensive models that delineate the psychological path-way to users' willingness/ intention to accept/ use such technologies. So far, there is scanty technology acceptance research capturing technologies that feature the multi-faceted role of smart/ intelligent technologies, and the few studies conducted in this area are based on the existing technology acceptance theories. This makes it difficult to predict and explain the factors that could be explaining the slow user adoption rate of AI cybersecurity systems in the UAE, especially in the public sector, yet the sector has been rapidly embracing other emerging technologies, as stated earlier. As a result, it is necessary to conduct research that would empirically determine the reasons why that is the case. In response to this research problem and literature gap, the present study aims at investigating the factors that influence users' intention to adopt AI cyber-security systems at workplaces in the UAE.

Literature Review

Various theoretical models have been developed in the domains of information systems, psychology, and sociology, seeking to predict and explain user acceptance of an information system or information technology. Some of the most widely used theories of technology

acceptance at the individual level include the technology acceptance model (TAM), unified theory of acceptance and use of technology (UTAUT) model, protection motivation theory (PMT), Theory of Reasoned Action (TRA), and DeLone and McLean Information Systems Success Model (ISSM). Most of these theories share some closely related features, and they were developed for old non-intelligent technologies, thus raising questions over their applicability in some of the emerging technologies with human-like intelligence such as AI. Nonetheless, following a critical review of these theories and models, UTAUT2 and PMT appeared to lay a suitable foundation for the present study, as explained in the subsequent sections.

Protection Motivation Theory

Protection Motivation Theory (PMT) is one of the most widely used theories in explaining users' technology acceptance behavior. The theory was originally developed in 1975 by Ronald Rogers to explain how people are motivated to protect themselves from perceived health-related threats, or rather what Rogers referred to as "fear appeals" (Rogers, 1975). Since then, the model has been revised severally, and the most updated version of the theory comprises of two constructs, namely, threat appraisal (adopted from expectancy-value theory (Lazarus & Folkman, 1984)) and coping appraisal (adopted from coping theory (Vroom, 1964) and the social cognitive theory (Bandura, 1977). Threat appraisal refers to a person's assessment of the probability of threats occurring and the magnitude of the noxiousness (harm). It comprises of perceived severity and vulnerability, where severity reflects the loss in value triggered by the failure to adopt the recommended behavior, while perceived vulnerability captures the likelihood of an individual experiencing harm (Farooq, Ndiege, & Isoaho, 2019). The coping appraisal, which consists of self-efficacy, response-efficacy, and response costs, refers to the extent to which an individual can avoid the potential harm by adopting the recommended behavior (response-efficacy), the degree to which an individual can implement the recommended behavior (self-efficacy), and the cost linked to adopting the recommended behavior (in this case, response costs of adopting AI cybersecurity systems). The figure below illustrates the revised PMT model.

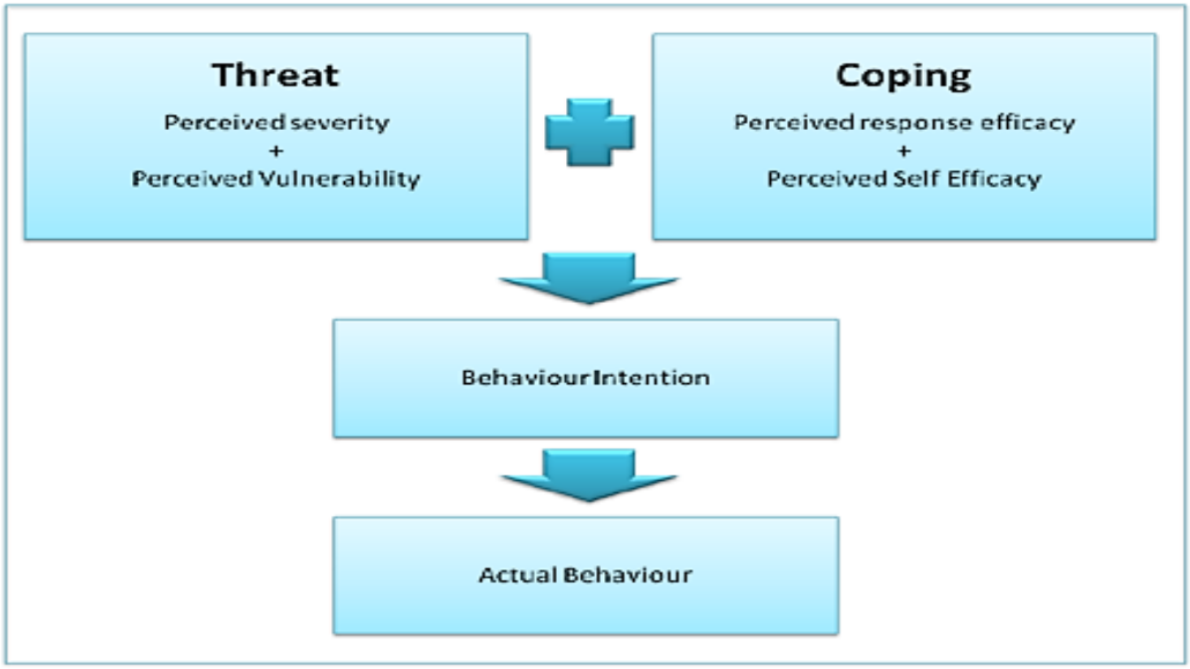

Figure 1: Protection Motivation Theory
Source: Rogers (1975; 1983)

Unified Theory of Acceptance and Use of Technology (UTAUT2)

The Unified Theory of Acceptance and Use of Technology (UTAUT2) was developed by Venkatesh, Morris, Davis, and Davis, as a modification of the initial UTAUT, which had been developed by the same authors in 2003. The revised model (UTAUT2) has two dependent variables (behavioral intention and use behavior) and seven independent variables (social influence, facilitating conditions, performance expectancy, effort expectancy, hedonic motivation, price value, and habit). The influence of these independent variables is moderated by three variables, namely, gender, age, and experience, as illustrated in the figure below.

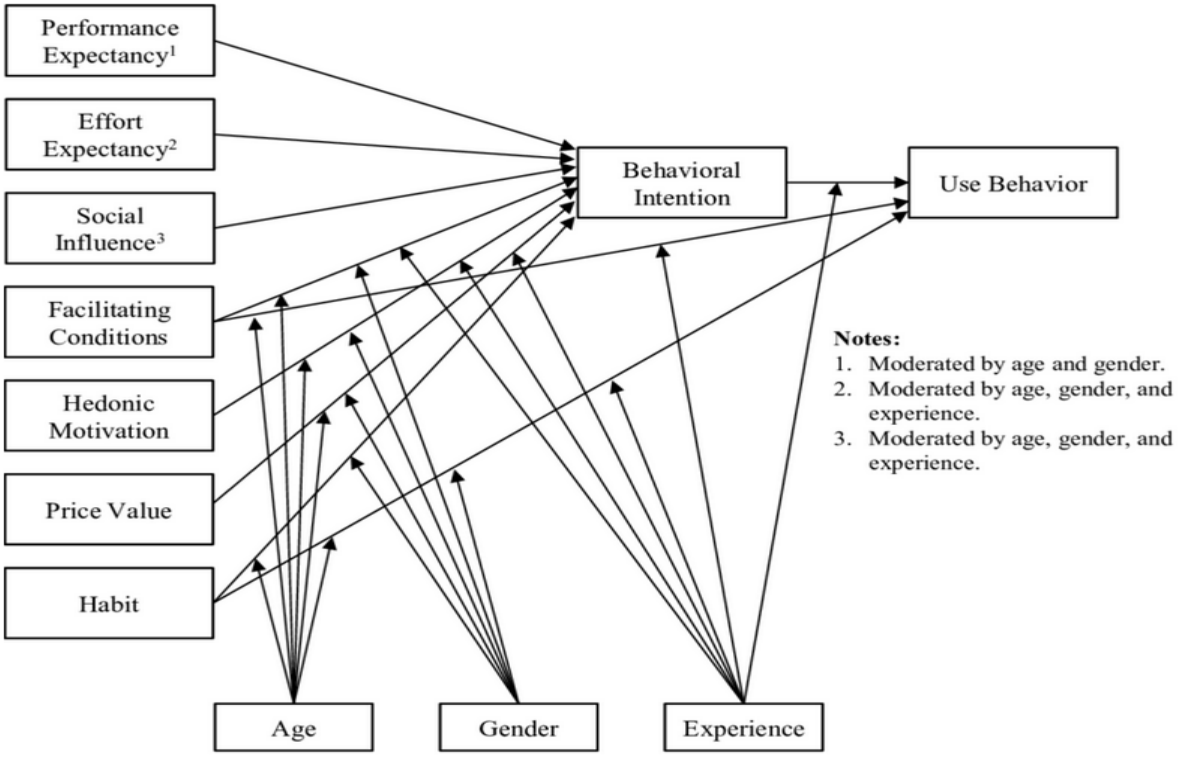

Figure 2: UTAUT2 research model
Source: Venkatesh et al. (2012)

The model holds that the seven independent variables play a critical role in determining users' acceptance of an information technology (IT) solution and usage behaviors. Nonetheless, the first three factors (effort expectancy, performance expectancy, social influence) are regarded as direct influencers of user intent and behavior, while the rest are identified as strong predictors of individual behaviors. According to Venkatesh, Thong, and Xu (2012), hedonic motivation is a critical predictor, hence the reason why it was added into the model for more stressful utility. Venkatesh and colleagues also established that the quality of a product and its cost play a vital role in adoption decisions, thus warranting the incorporation of the price value construct. Venkatesh and colleagues found that behavioral intention has been emphasized in recent studies, and therefore, there was a need to include the habit construct into the model (Venkatesh et al., 2012).

Conceptual Framework

After comprehensively reviewing the five prominent technology adoption theories/models (TAM & TAM2, UTAUT & UTAUT2, and PMT) and critical consideration of the research problem being investigated, it emerged that the Protection Motivation Theory (PMT) and the extended version of the Unified Theory of Acceptance and Use of Technology (UTAUT2) were the most suitable models for laying the best foundation for the present study.

This is because though the two models come with their own set of weaknesses, each one of them has its own strengths that complement the weaknesses of the other. This aspect makes the two models, together with the security control investment literature, a suitable basis for developing a research model for the present study.

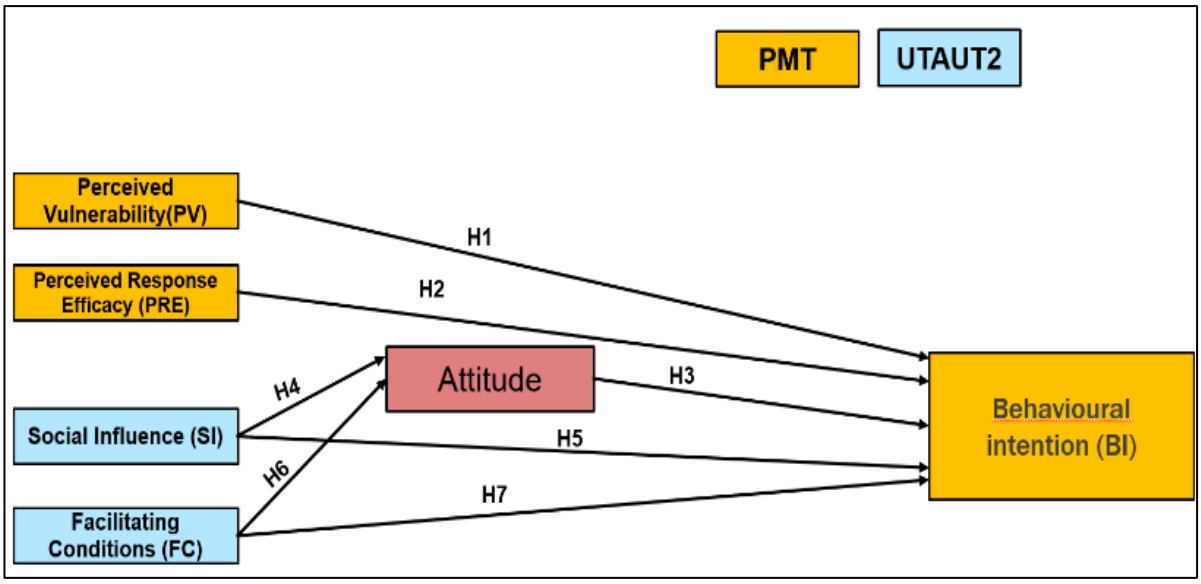

Figure 3: Research framework

This study seeks to test the research model illustrated above. The model has six variables whereby the independent variables include perceived vulnerability (PV), perceived response efficacy (PRE), social influence (SI), and facilitating conditions (FC). The model also sets behavioral intention (BI) as the dependent variable, with the attitude towards AI security systems (AT) serving as a mediator variable. The hypothesized correlation between these variables is discussed in the sub-sections below.

Hypothesis Development

Perceived vulnerability

Perceived vulnerability is one of the two threat appraisals of PMT, and it refers to the degree to which an individual believes that they are likely to experience a threat (Huang & Kao, 2015; Rogers, 1983). According to PMT, there is a direct relationship between users' perceived vulnerability and their intention to adopt the recommended coping response/ actions. This insinuates that if an individual believes that they are likely to be attacked, they are likely to comply with the provided security guidelines or adopt the necessary measures such as having a security system. So far, various studies have confirmed this relationship, especially in studies seeking to determine the factors influencing the adoption of security technologies such as ant-virus software (Al-Ghaith, 2016; Debb & McClellan, 2021), desktop security behavior (Hanus & Wu, 2016; van Bavel, Rodríguez-Priego, Vila, & Briggs, 2019), and other information systems security innovations (Hameed & Arachchilage, 2019; Suhaimi et al., 2021). As a result, it seems likely that perceived vulnerability to cyber-attacks is a predictor of user's intention to adopt AI base cybersecurity systems, hence, hypothesized that:

***H1*:** Perceived vulnerability (PV) positively influence intention to adopt AI cybersecurity systems.

Perceived response efficacy

Response efficacy is another crucial variable that has been reported to influence users' intention to adopt technology, inclusive of information security systems. It refers to the

perceived effectiveness of the recommended coping mechanism at averting a threat (Hanus & Wu, 2016; Rogers, 1975). In the context of security information systems, response efficacy refers to the confidence that users have that adopting a security measure/ system will prevent a threatening security event from happening and becoming a threat. So far, there exists a large body of literature that confirms that response efficacy is a key determinant of users' intention to adopt a technology (Hanus & Wu, 2016; Johnston & Warkentin, 2010; Park & Lee, 2014). In Hanus and Wu (2016) study, for example, it emerged that response efficacy was one of the primary factors that influenced users' intention to comply with desktop security behavior, with Johnston and Warkentin (2010) reporting this variable as a key determinant of users' security policy compliance intentions. Similarly, Tsai et al. (2016) observed that response efficacy had a significant and positive impact on users' intention to adopt online security behaviors. Overall, the definition provided for this variable and the confirmed relationship between response efficacy and users' intention to accept a technology confirm the suitability of this variable in the present research, hence the following research hypothesis.

***H2*:** Perceived response efficacy (PRE) positively influence intention to adopt AI cybersecurity systems

Social influence

Social influence refers to a user's perception that others would recognize him/her if he/she accepts to use a new technology or rather would recommend them to use new technology (Venkatesh et al., 2012). The term is also used to the belief that a significant number of people feel that a person should accept and use a specific information system. Its influence on behavioral intention to use a novel technology has received significant attention from researchers, with most of them finding it crucial in shaping users' behaviors. For example, Rogers (2010) observed that the decision-making process of accepting a technology is highly influenced by social conceptions beyond a user's rational thinking. Taylor, Voelker, and Pentina (2011) also investigated the factors that influence the acceptance and use of mobile apps among Midwest university students and established that friends' opinions played an influential role in shaping prospective users' attitudes about mobile apps and the overall intention to use them. Similarly, Catherine et al. (2018) reported that social influence had a positive and significant impact on the adoption and use of biometric fingerprint ATMs in Uganda. These findings indicate that opinions of the important people in one's life can directly or indirectly influence prospective users' attitudes and decisions regarding the acceptance and use of new technology, hence the following hypothesis.

H5: Social influence (SI) positively influence intention to adopt AI cybersecurity systems

Facilitating conditions

This construct is defined as the extent to which an individual believes that both technical and organizational infrastructure is available to support the use of new technology (Huang & Kao, 2015; Venkatesh et al., 2012). Several studies have investigated the relationship between this variable and technology acceptance, and most of them have established that facilitating conditions have a substantial direct influence on the intention to adopt innovative technology, and indirectly by influencing users' attitudes (Catherine et al., 2018; Lee et al., 2018; Mtebe & Raisamo, 2014; Yu, 2012). For instance, Mtebe and Raisamo (2014) investigated students' behavioral intention to adopt and use mobile learning in higher education in East Africa and found that facilitating conditions were influential. Yu (2012) also explored factors that influence individuals' behavioral intention to adopt mobile banking and established that facilitating conditions were influential, though their effect was being moderated by age. Catherine et al. (2018) also discovered that facilitating conditions influenced the adoption of fingerprint authentication-based ATMs in Uganda. With these findings, it is hypothesized that:

***H7*:** Facilitating conditions (FC) positively influence intention to adopt AI cybersecurity systems.

Attitude towards AI security systems

Past research has confirmed that there exists a relationship between users' attitudes and intention to adopt new technologies. Indeed, many theories, among them the technology adoption model (TAM), the theory of reasoned action (TRA), and the theory of planned behavior (TPB), have confirmed that an individual's intention to adopt and use new technology is influenced by his or her attitude towards that technology. Many studies, especially in the healthcare domain, have also confirmed the existence of the attitude-technology acceptance relationship (Jung, 2008; Losova, 2014; Oh, Seo, & Kim, 2019). In Jung's study, for example, results obtained indicated that Swedish citizens' intention to use e-health was mainly determined by their attitude towards the technology and that their attitude was shaped by the overall compatibility of the e-health technology with their needs, its perceived usefulness, as well as the potential risks associated with it. In the present study, it is anticipated that users are more likely to adopt AI cybersecurity systems if they possess the right attitude towards them, thus leading to the following hypothesis:

H3: User's attitude towards AI security systems (AT) positively influences intention to adopt AI cybersecurity systems.

As stated earlier, other factors such as perceived usefulness (synonymous to performance expectancy) and perceived ease of use (synonymous to effort expectancy), facilitating conditions, and social influence shape prospective users' intention to use new technologies. For example, according to Sandeep and Ravishankar (2014), facilitating conditions such as help desks and training programs play a key role in enabling persons to develop a positive attitude towards technology. Naranjo-Zolotov et al. (2019) shared similar sentiments by reporting a significant relationship between facilitating conditions and users' attitudes towards e-participation platforms. These findings imply that attitude towards technology mediates the effect of facilitating conditions and social influence on technology acceptance (Dwivedi, Rana, Jeyaraj, Clement, & Williams, 2019; Naranjo-Zolotov, Oliveira, & Casteleyn, 2019; Wang, Jeng, & Huang, 2017). As a result, the following hypotheses will be tested.

***H4*:** Attitude mediates the relationship between social influence and intention to adopt AI cybersecurity systems.

H6: Attitude will mediate the relationship between facilitating conditions and intention to adopt AI cybersecurity systems.

Methods

This cross-sectional study is quantitative, and it is based on the correlational research design, where a systematic investigation of the phenomenon will be explained using numbers, statistics, and structured data. The targeted study population include IT officers serving as IT technicians (IT technical support officers), information security officers, cybersecurity specialists, system security officers, Chief Information Security Officers (CISO), and/or Chief Technology Officers (CTO). The reason why the study population will include a spectrum of users ranging from technicians to C-suite level personnel in charge of information security is that the latter play a crucial role in decision making in an organization while the former are the actual users of the introduced cybersecurity/ information security system. As a result, the two levels of personnel ought to be involved in the study in order to get a holistic view of the factors influencing users' intention to use AI cyber-security systems at workplaces in the UAE.

A sample of 178 respondents will be selected using the purposive sampling technique and guided by the G*Power analysis software on the ideal sample size for the proposed study.

The intended data will be collected through a web-based survey questionnaire whose link will be sent via email. Upon collection, the data will be cleaned and prepared using the Statistical Package for Social Sciences (SPSS) software. It will then be analyzed using the Partial Least Squares structural equation and Modelling (PLS-SEM) program to assess the hypothesized relationships between variables and the predictive power or rather the quality of the proposed model of users' intention to use/ adopt AI cyber-security systems at workplaces in the UAE. Both the outer and the inner model assessments will be performed during the data analysis phase.

Findings

Results of this study are anticipated to help decision-makers in organizations intending to embrace AI-based cybersecurity systems in making more informed decisions concerning the functionality and design of such systems. In particular, the findings made are expected to help them choose AI-based cybersecurity systems whose design and functionality match most of the factors found to positively impact users' intention to use AI-based cybersecurity systems. Doing so can minimize employees' resistance to change or the new technology, thereby facilitating smooth adoption of these ingenious systems. In addition, the findings of this study may help developers of AI-based cybersecurity systems in understanding the parameters they should consider when designing AI-based cybersecurity systems since doing so can enhance their adoption and use rate among the users and organizations.

Discussion and Conclusion

The present study mainly depended on the literatures available on the adoption of security technologies to determine the factors that could be possibly influencing users' intention to adopt or use AI-based cyber security systems at workplaces. The developed model is founded on an integration of both PMT and UTAUT2. However, the two theories have been extended by introducing attitudes towards AI cyber security systems to enhance their predictive power. This knowledge is expected to enhance the current understanding on the determinants of AI based technologies acceptance.

Theoretical Implications

Upon completion, this study is expected to contribute to the available body of knowledge by enriching the scanty literature available on adopting and using autonomous or semi-autonomous technologies such as technologies powered by artificial intelligence. The study will also contribute to theory development by introducing new a new variable to a hybrid of PMT and UTAUT2 models.

Practical and Social Implications

The anticipated practical contributions of this study include shedding light on the factors influencing users' intention to use AI-powered cybersecurity systems. Such knowledge would be helpful in enhancing the adoption and use of such security systems, thus significantly improving the preparedness and effectiveness of organizations in detecting and countering cybercrimes. In general, such knowledge is expected to help organizations anticipating embracing AI-based cybersecurity technologies in determining the factors they should consider to enhance flawless adoption of the technologies with minimal resistance. It is also expected to help AI cybersecurity developers identify features that they may incorporate in such systems to promote users' adoption without compromising the functionality of the systems.

Limitations and Suggestions for Future Research

One of the main limitations of this study is its constrained scope, where the intended data will be collected from a sample of respondents working in organizations based in Dubai and Abu Dhabi. This limitation renders the generalization of the results obtained to the entire country (UAE) and other geographical regions questionable. It is worth noting that conducting a study with a large sample collected across the country was not possible for the present study because of the limited resources and time. As a result, researching the same topic while involving a large and more representative sample is reserved for future studies. Such a study can lead to more generalizable results.

Acknowledgement

I wish to sincerely thank and appreciate my supervisors, Dr. Normalini Md Kassim and Associate Professor Dr. Teh Sin Yin, for your encouragement, advice, and guidance in every stage of my research. You alleviated the initial fears and concerns at the beginning of this research and expressed confidence in my ability to turn this topic into a reality. You motivated me when I felt like giving up and showed me that it is not over until it is done. I am sincerely grateful for that. Your feedback and suggestions helped me address challenges that I felt were above my capability. Through this study, you have become my mentors and friends. I am honored and privileged to work with you.

References

AbuOdeh, M., Adkins, C., Setayeshfar, O., Doshi, P., & Lee, K. H. (2021, May). A Novel AI-based Methodology for Identifying Cyber Attacks in Honey Pots. In *Proceedings of the AAAI Conference on Artificial Intelligence* (Vol. 35, No. 17, pp. 15224-15231).

Al-Ghaith, W. (2016). Extending protection motivation theory to understand security determinants of anti-virus software usage on mobile devices. *Int J Comput*, *10*, 125-38.

Azar, E., & Haddad, M. A. N. (2019). Artificial Intelligence in the Gulf: Prospects and Challenges.

Bandura, A. (1977). Self-efficacy: toward a unifying theory of behavioral change. *Psychological review, 84*(2), 191.

Catherine, N., Geofrey, K. M., Moya, M. B., & Aballo, G. (2018). Effort expectancy, performance expectancy, social influence and facilitating conditions as predictors of behavioural intentions to use ATMs with fingerprint authentication in Ugandan banks. *Global Journal of Computer Science and Technology*.

Debb, S. M., & McClellan, M. K. (2021). Perceived Vulnerability as a Determinant of Increased Risk for Cybersecurity Risk Behavior. *Cyberpsychology, Behavior, and Social Networking*, *24*(9), 605-611.

Desk, E. S. (2020). UAE Embraces Blockchain Technology and Digital Identity to Fight Covid-19! Retrieved from https://blockchainmagazine.net/uae-embraces-blockchain-technology-and-digital-identity-to-fight-covid-19/

Dwivedi, Y. K., Rana, N. P., Jeyaraj, A., Clement, M., & Williams, M. D. (2019). Re-examining the unified theory of acceptance and use of technology (UTAUT): Towards a revised theoretical model. *Information Systems Frontiers, 21*(3), 719-734.

Farooq, A., Ndiege, J. R. A., & Isoaho, J. (2019). *Factors Affecting Security Behavior of Kenyan Students: An Integration of Protection Motivation Theory and Theory of Planned Behavior.* Paper presented at the 2019 IEEE AFRICON.

Gursoy, D., Chi, O. H., Lu, L., & Nunkoo, R. (2019). Consumers acceptance of artificially intelligent (AI) device use in service delivery. *International Journal of Information Management, 49*, 157-169.

Hameed, M. A., & Arachchilage, N. A. G. (2019). On the impact of perceived vulnerability in the adoption of information systems security innovations. *arXiv preprint arXiv:1904.08229*.

Hanus, B., & Wu, Y. A. (2016). Impact of users' security awareness on desktop security behavior: A protection motivation theory perspective. *Information Systems Management, 33*(1), 2-16.

Huang, & Kao, Y.-S. (2015). UTAUT2 based predictions of factors influencing the technology acceptance of phablets by DNP. *Mathematical Problems in Engineering, 2015*.

Jacobs, J. V., Hettinger, L. J., Huang, Y. H., Jeffries, S., Lesch, M. F., Simmons, L. A., ... & Willetts, J. L. (2019). Employee acceptance of wearable technology in the workplace. *Applied ergonomics*, *78*, 148-156.

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: an empirical study. *MIS quarterly*, 549-566.

Jung, M.-L. (2008). *From health to e-Health: Understanding citizens' acceptance of online health care.* Luleå tekniska universitet,

Lazarus, R. S., & Folkman, S. (1984). *Stress, appraisal, and coping*: Springer publishing company.

Lee, Roh, E. H., & Han, K. S. (2018). A study on factors of information security investment in the fourth industrial revolution. *International Journal of Advanced Science and Technology, 111*, 157-174.

Losova, V. (2014). Technology acceptance model: A case of electronic health record in Estonia. *Unpublished master's thesis). Copenhagen Business School, Copenhagen*.

Lu, L., Cai, R., & Gursoy, D. (2019). Developing and validating a service robot integration willingness scale. *International Journal of Hospitality Management, 80*, 36-51.

Mtebe, J., & Raisamo, R. (2014). Investigating students' behavioural intention to adopt and use mobile learning in higher education in East Africa. *International Journal of Education and Development using ICT, 10*(3).

Naranjo-Zolotov, M., Oliveira, T., & Casteleyn, S. (2019). Citizens' intention to use and recommend e-participation: Drawing upon UTAUT and citizen empowerment. *Information Technology & People*.

Oh, J. H., Seo, J. H., & Kim, J. D. (2019). The Effect of Both Employees' Attitude toward Technology Acceptance and Ease of Technology use on Smart Factory Technology Introduction Level and Manufacturing Performance. *Journal of Information Technology Applications and Management, 26*(2), 13-26.

Omelyan, O. S., Melnyk, D. S., Yudenko, Y. V., Fornoliak, V. M., & Koshel, O. Y. (2021). Cybercrime as a Global threat to the World Economy. *Studies of Applied Economics*, *39*(9).

Park, C., & Lee, S.-W. (2014). A study of the user privacy protection behavior in online environment: Based on protection motivation theory. *Journal of Internet Computing and Services, 15*(2), 59-71.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change1. *The journal of psychology, 91*(1), 93-114.

Rogers, R. W. (1983). Cognitive and psychological processes in fear appeals and attitude change: A revised theory of protection motivation. *Social psychophysiology: A sourcebook*, 153-176.

Rogers. (2010). *Diffusion of innovations*: Simon and Schuster.

Sandeep, M., & Ravishankar, M. (2014). The continuity of underperforming ICT projects in the public sector. *Information & management, 51*(6), 700-711.

Sharma, S. (2021). Role of Artificial Intelligence in Cyber Security and Security Framework. *Artificial Intelligence and Data Mining Approaches in Security Frameworks*, 33-63.

Suhaimi, S. N., Othman, N. F., Syahirah, R., Anawar, S., Ayop, Z., & Foozy, C. F. M. (2021). Determinants of Privacy Protection Behavior in Social Networking Sites.

Taddeo, M. (2019). Three ethical challenges of applications of artificial intelligence in cybersecurity. *Minds and Machines, 29*(2), 187-191.

Taylor, Voelker, T. A., & Pentina, I. (2011). Mobile application adoption by young adults: A social network perspective.

Technavio. (2021, June 21). *Artificial intelligence-based cybersecurity market grows by $ 19 billion during 2021-2025 | Technavio*. PR Newswire: press release distribution, targeting, monitoring and marketing. Retrieved October 16, 2021, from https://www.prnewswire.com/news-releases/artificial-intelligence-based-cybersecurity-market-grows-by--19-billion-during-2021-2025--technavio-301315494.html

The Arab Weekly. (2018). UAE embraces emerging technologies in education. Retrieved from https://www.blockchainmagazine.net/uae-embraces-blockchain-technology-and-digital-identity-to-fight-covid-19/

Tsai, H.-y. S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J., & Cotten, S. R. (2016). Understanding online safety behaviors: A protection motivation theory perspective. *Computers & Security, 59*, 138-150.

van Bavel, R., Rodríguez-Priego, N., Vila, J., & Briggs, P. (2019). Using protection motivation theory in the design of nudges to improve online security behavior. *International Journal of Human-Computer Studies*, *123*, 29-39.

Varonis. (2021, March 16). *134 cybersecurity statistics and trends for 2021*. Inside Out Security. Retrieved October 16, 2021, from https://www.varonis.com/blog/cybersecurity-statistics/

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.

Venkatesh, V., Thong, J. Y., & Xu, X. (2012). Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology. *MIS quarterly*, 157-178.

Vroom, V. H. (1964). Work and motivation.

Wang, Jeng, Y.-L., & Huang, Y.-M. (2017). What influences teachers to continue using cloud services? *The Electronic Library*.

Wilson, G. (2020). Blue prism: UAE leaders embrace intelligent automation | Technology | Business chief EMEA. *Business Chief Magazine,*. Retrieved from https://businesschief.eu/technology-6/blue-prism-uae-leaders-embrace-intelligent-automation

Yu, C.-S. (2012). Factors affecting individuals to adopt mobile banking: Empirical evidence from the UTAUT model. *Journal of electronic commerce research, 13*(2), 104.