Interdisciplinary Journal of Information, Knowledge, and Management

An Official Publication of the Informing Science Institute InformingScience.org

IJIKM.org

Volume 20, 2025

INTELLIGENT PROTECTION: A STUDY OF THE KEY DRIVERS OF INTENTION TO ADOPT ARTIFICIAL INTELLIGENCE (AI) CYBERSECURITY SYSTEMS IN THE UAE

Mohammed Rashed Mohamed Al Humaid Alneyadi	School of Management, Universiti Sains Malaysia, Malaysia	Mohammed.alneyadi@student.usm.my
Md Kassim Normalini *	School of Management, Universiti Sains Malaysia, Malaysia *and* Graduate School of Management, Management & Science University, Malaysia	normalini@usm.my

* Corresponding author

ABSTRACT

Aim/Purpose	This research investigates factors influencing consumers' decisions to use artificial intelligence cybersecurity technology in the United Arab Emirates.
Background	The cyber-security risks are getting more complex as technology develops, putting the United Arab Emirates (UAE) businesses and government agencies at risk of severe losses from cybercrime.
Methodology	A correlational study design and a quantitative research approach were employed, and 340 professionals working for different government and semi-government organizations in the United Arab Emirates were given questionnaires. The PLS-SEM approach was used to analyze the replies.
Contribution	The present research framework remedies the inherent limitations in the PMT model by adding factors used to explain the influence of environmental factors

Accepting Editor Dimitar Grozdanov Christozov | Received: October 15, 2024 | Revised: December 10, December 27, 2024 | Accepted: January 4, 2025.

Cite as: Alneyadi, M. R. M. A. H., & Normalini, M. K. (2025). Intelligent Protection: A Study of the Key Drivers of Intention to Adopt Artificial Intelligence (AI) Cybersecurity Systems in the UAE. *Interdisciplinary Journal of Information, Knowledge, and Management, 20,* Article 3. https://doi.org/10.28945/5430

	and individual difference factors on behavior. This research framework is an extended application of the PMT model in the context of AI-based cybersecurity systems. Meanwhile, this study confirms the importance of perceived vulnerability in AI technology scenarios.
Findings	The findings demonstrated that users' adoption intentions were significantly and favorably impacted by social influence, facilitating conditions, perceived vulnerability, and perceived response efficacy. Meanwhile, job insecurity enhanced employees' resistance to change, making resistance to change a major resistance to the intention to adopt AI-based cybersecurity systems.
Recommendations for Practitioners	The report offers crucial insights that organizations can utilize to evaluate their readiness for adopting AI-based cybersecurity technologies and create plans to lessen employee resistance to advancements in the cybersecurity industry.
Recommendations for Researchers	Researchers on this specific application can make use of the extension of the framework.
Impact on Society	The research can be utilized to evaluate their readiness to adopt AI-based cybersecurity technologies.
Future Research	Future research should broaden the scope to acquire a more thorough understanding of the behavioral intentions to use AI-cybersecurity systems in the United Arab Emirates. Other elements that could be considered include facilitating settings, Artificial Intelligence knowledge, social impact, effort efficacy, and other frameworks.
Keywords	artificial intelligence (AI), cybersecurity systems, PMT, intelligent systems, cyber threats, information security

INTRODUCTION

CYBERSECURITY BACKGROUND

Artificial intelligence (AI) has attracted much interest in the last few years because it is revolutionizing several industries, including industry, transportation, government, and research. With the use of this technology, complicated tasks that formerly required human intelligence can now be completed by robots (Gursoy et al., 2019). Better decision-making, forecasting, and work automation are some of its advantages. While humans have been able to automate jobs using earlier computer technologies, AI technologies like machine learning (ML) and deep learning (DL) have elevated automation to a new level. For instance, they brought in the intelligence component and made it possible to analyze vast amounts of data from various sources, which enables organizations to increase productivity, comprehend the market, and forecast their growth prospects. These revolutionary effects have given rise to proposals that AI technology can significantly enhance cybersecurity measures by automating threat detection and response processes.

Cybersecurity refers to a set of technologies, processes, and practices to protect and defend networks, devices, software, and data from attack, disruption, or unauthorized access (Sarker et al., 2021). With the increasing complexity of digital business models, cybersecurity has become a priority on the agenda of the leadership of public and private organizations (de Azambuja et al., 2023). Organizations around the world have invested heavily in cybersecurity yet still face the challenge of cyberattacks. With the widespread availability of the Internet and the emergence of innovative technologies such as AI, cloud computing, and the Internet of Things (IoT), which have made cyber-attacks increasingly stealthy and sophisticated (Alneyadi et al., 2022), businesses and government organizations are exposed to an increased risk of serious losses due to cybercrime. With the rapid

growth of cybercrime, traditional cybersecurity measures are no longer sufficient to deal with complex and advanced cyberattacks (Shamiulla, 2019), and AI-based cybersecurity solutions have become an important technological tool to combat cybercrime and defend against cyberattacks (Rizvi, 2023). Artificial intelligence technologies such as machine learning and deep learning in AI cybersecurity solutions can detect and analyze large amounts of data in real time, identify potential cybersecurity anomalies, and automate response actions to help organizations or individuals stay ahead of cyber threats (Bhatele et al., 2019; Rizvi, 2023).

Problem Statement About Cybersecurity

Due to its location in the center of Middle Eastern commerce and trade and the importance of its geopolitical position, an increasing number of hacktivists and cyberattackers are identifying the UAE as a target (Lemos, 2024b). In the first nine months of 2023, the UAE government detected and blocked more than 71 million cyberattacks, and the vast majority of companies in the UAE have faced cyberattacks in the past two years (Lemos, 2024a). Eighteen months of dark web data collected by Moscow-based threat research firm Positive Technologies concluded that the number of Distributed Denial of Service (DDoS) attacks in the Gulf region countries increased by 70% in the first half of 2024 compared to the same period last year. Public sector organizations in the UEA alone face nearly 50,000 cyberattacks per day (PositiveTechnologies, 2024).

In addition, the UAE reported 34 cyber threat incidents formed by ransomware attacks between January and November 2024, up from 27 in all of 2023, according to Acronis Threat Research. Meanwhile, malware detection paths increased by 65.3 percent. This figure is also significantly higher than that of its neighboring countries such as Saudi Arabia (11 incidents), Lebanon (7), Oman (4), and Jordan (1) (MEIR Team, 2024). This makes the UAE the most affected country in the region, facing more and more sophisticated cyber threats than its neighbors. The average cost of a data breach in the Middle East is $8.7 million, almost twice the global average. The UAE's energy-critical infrastructure sector is also at higher risk. Experts predict that cyberattacks targeting industrial control systems and operational technologies could seriously disrupt production and lead to significant financial losses. Financial institutions in the UAE are under increasing pressure to strengthen cybersecurity measures to protect sensitive data and avoid significant financial and reputational losses (MEIR Team, 2024).

However, the increase in these cyberattacks coincides with the UAE government's modernization program, which aims to integrate technologies such as cyber-physical systems (CPS) and the Internet of Things (IoT) to make the country a smart nation. In light of this, strong cyber security will be more important than ever as the country will inevitably become a target for cybercrime due to the growth of digital infrastructure. This will provide opportunities for hackers to exploit. Despite this awareness, many organizations are still hesitant to enhance or strengthen their cybersecurity procedures.

According to Al-Khater et al. (2020) and Guven (2018), the approach used by the UAE to deal with cyber dangers is mainly human-centered. This means that if all the advantages of AI-based cybersecurity solutions are to be realized, there is an urgent need to first address the acceptance and use of people, especially in public sector organizations. Despite this country's reputation for being quick to embrace new technologies, studies have shown that the adoption of AI cybersecurity solutions has not been as fast as in other countries (Editor's Desk, 2020; Malek, 2018; Wilson, 2020). This unexpected finding emphasizes the need to study the factors that influence the uptake and adoption of AI-based cybersecurity solutions, such as the cybersecurity industry in the UAE.

To shed insight on the factors influencing intentions to adopt new technology or innovations, scholars have developed several technology acceptance models. These include the theory of reasoned action (TRA) (Ajzen & Fishbein, 1975), the theory of planned behavior (TPB) (Ajzen, 1991), the task-technology fit model (TTF) (Goodhue & Thompson, 1995), the unified theory of acceptance and use

of technology (UTAUT) (Venkatesh et al., 2003), the technology acceptance model (TAM) (Davis, 1989), and the protection motivation theory (PMT) (Rogers, 1975).

Although these models have been widely used to explain user adoption behavior of technology, Lu et al. (2019) noted that some components of previous models are not suitable or applicable to complex technologies, especially artificial intelligence (AI) technologies designed to mimic human behavior. This is because AI-based technological solutions do not necessarily require the user to learn how to use them but are designed to be autonomous with human-like characteristics to interact with the user to accomplish the appropriate task (Gursoy et al., 2019). Therefore, certain components inherent in previous models, such as perceived usefulness and ease of use, may be irrelevant or ineffective in predicting users' intentions to adopt AI technologies. This finding raises the contribution that a study examining the variables influencing the desire to embrace new technologies is necessary to create an integrated model outlining the main drivers of users' intent to utilize them. The studies that are currently accessible on this topic have primarily concentrated on the current models of technological acceptance, which makes it difficult to identify the variables impacting the adoption of AI-based cybersecurity systems, particularly in UAE public institutions. The current empirical study was motivated by this gap in the literature and aims to fill this void by providing a comprehensive analysis of the factors that influence the adoption of AI-based cybersecurity systems in the UAE, thereby offering novel insights into the region's unique challenges and opportunities.

LITERATURE REVIEW AND HYPOTHESIS DEVELOPMENT

Previous research has shown that understanding cybersecurity behavior relies heavily on identifying which behavioral factors are the most predictive through human, technological, and social factors in different information systems models and theories for inclusion in interventions or prevention programs. From the context of being used to explain cybersecurity behavior, Protection Motivation Theory (PMT) has been widely used for explaining people's responses to fearful appeals (Addae et al., 2019; Ameen et al., 2021; Shahbaznezhad et al., 2021; Simonet & Teufel, 2019). Protection Motivation Theory (PMT) was first proposed by Rogers in 1975 as a framework to explain how individuals are motivated to protect themselves against threats. Initially developed in the context of health behavior, PMT has since been applied in various fields, including psychology, public health, and cybersecurity. The theory highlights the cognitive processes that lead individuals to adopt protective behaviors based on perceived threats. PMT posits that an individual's motivation to protect themselves is influenced by two main appraisals: threat appraisal and coping appraisal.

> *Threat Appraisal:* This component assesses the severity and vulnerability of the threat. If individuals perceive a threat as severe and believe they are vulnerable to it, they are more likely to engage in protective behaviors (Maddux & Rogers, 1983). Research has shown that higher perceived threat levels correlate with increased motivation to take preventive actions (Floyd et al., 2000).
>
> *Coping Appraisal:* This aspect evaluates the effectiveness of the recommended protective behavior and the self-efficacy of the individual to execute the behavior. If individuals believe that the protective behavior is effective and they have the capability to perform it, they are more likely to adopt it (Champion & Skinner, 2008). Studies have demonstrated that self-efficacy plays a crucial role in translating intention into action (Rippetoe & Rogers, 1987).

While PMT has provided valuable insights, it is not without limitations. Previous research has shown that PMT does not give enough consideration to the environmental factors that influence behavior. In addition, the PMT model assumes that everyone reacts similarly to threats, thus failing to take into account the influence of individual differences on behavior (Almansoori et al., 2023). Therefore, to compensate for the inherent limitations of PMT, this study incorporates social influence and facilitation conditions from the UTAUT2 model to explain and predict the effects of environmental factors on user behavior. The influence of social influence on intention tends to be context-dependent, and

in coercive environments (e.g., employees of government organizations), the positive influence of social influence on intention stems from compliance. However, social influence shapes voluntary users' (e.g., customers') perceptions and decisions about technology by internalizing perceptions of influence (Venkatesh et al., 2003). As a result, users will refer to the subjective culture and beliefs of the group and internalize them into their self-perceptions to make decisions accordingly (Thompson et al., 1991). Facilitating conditions refer to resources and assistance that can facilitate the use of technology (Brown & Venkatesh, 2005). The successful implementation of AI-based cybersecurity solutions requires the establishment of a strong underlying network environment to minimize barriers to user access.

With the addition of environmental factors, two new constructs will be added to this study: job insecurity and resistance to change, which are used to compensate for the lack of individual differences in behavior in the PMT model. Prior research has shown that job insecurity is associated with resistance to change, especially when digital technology is involved. Although AI will reshape people's lives, most employees see it as a threat rather than an opportunity (Bhargava et al., 2021). If employees perceive digital technology (AI) as a threat to their jobs or positions, they will tend to resist the technology either consciously or unconsciously (Bhargava et al., 2021; Nam et al., 2021; Tabrizi et al., 2019). Thus, perceived job insecurity becomes one of the barriers to the adoption of innovative digital technologies (Nam et al., 2021). In this context, this study identifies job insecurity and resistance to change as individual factors that may influence the intention to adopt AI-based cybersecurity systems in the UAE.

Ultimately, six factors made up the study's framework, as shown in Figure 1, and these variables were used to generate six hypotheses. The six variables are perceived vulnerability (PV) and perceived response efficacy (PRE) from the PMT model, as well as social influence (SI) and facilitating conditions (FC), which came from the UTAUT2 theory. Job insecurity (JI) and resistance to change (RTC) were added to the model to increase its efficacy and predictive ability in explaining the variables influencing adoption intentions. This section goes into great detail on these variables and the theories that go along with them.

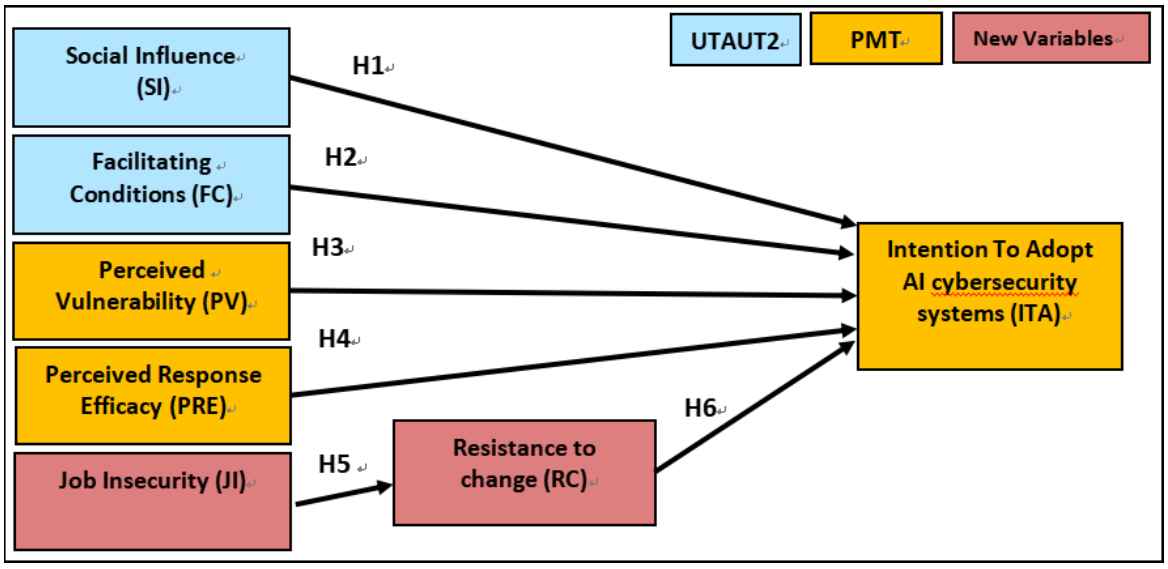

Figure 1. Research framework

Social Influence (SI)

According to Venkatesh et al. (2012), self-identification (SI) is the belief held by a user that others will recognize them if they adopt or recommend a new technology. Stated differently, it is the conviction that the actions of others justify technology adoption or use. The influence of the construct on

the desire to embrace and use new technology is considerable in the majority of studies that have looked into this relationship. For instance, Taylor et al. (2011) looked at what factors affected Midwest University students' adoption and use of mobile applications and discovered that peers' opinions mattered. According to Catherine et al. (2018), SI has a positive and noteworthy influence on Uganda's adoption and use of fingerprint biometric ATMs in security. These studies demonstrate how a person's attitude toward new technologies and plans to adopt them can be greatly influenced by the opinions of important people in their lives. To achieve this, the following study hypothesis was created:

H1: Social influence (SI) positively influences intention to adopt AI cybersecurity systems.

Facilitating Conditions (FC)

FC is the infrastructure and technical capacity required to enable the adoption of the new technology (Huang & Kao, 2015; Venkatesh et al., 2012). The most crucial element of using AI for cybersecurity research is securing sufficient resources (such as compute infrastructure, human capital, etc.) to effectively address novel topics and significantly advance knowledge (Samtani et al., 2020). According to several studies (Catherine et al., 2018; Lee et al., 2018; Mtebe & Raisamo, 2014; Yu, 2012), FC is one of the most crucial predictions of adoption intention. The adoption of fingerprint authentication-based ATMs in Uganda was found to be significantly influenced positively by FC, according to Catherine et al.'s (2018) study. The adoption of AI cybersecurity systems in the UAE can thus be argued to be strongly and favorably influenced by FC, which leads to the following hypothesis:

H2: Facilitating conditions (FC) positively influence the intention to adopt AI cybersecurity systems.

Perceived Vulnerability (PV)

PV is the target user's estimation of their vulnerability to an attack (Huang & Kao, 2015; Rogers, 1983). According to the PMT hypothesis, PV directly affects the intention to adopt the suggested coping strategy. Put another way, if the target users think they are vulnerable to assaults, they will likely accept and implement the suggested security solution. Though the two variables are positively associated, most studies looking into this relationship have found indirect association. Nguyen (2013), for example, found that while PV did not directly affect the decision to provide vitamin supplements, it did modulate the link between the intention to provide vitamin supplements and the perceived benefits. Liang and Xue (2010) found an indirect association between FC and adoption intention, with perceived threat acting as a mediator. This finding lends validity to the previous findings. These results suggest that although there is an indirect relationship between FC and adoption intention, the construct has a beneficial impact on adoption intention. Considering this, it was proposed that:

H3: Perceived vulnerability (PV) positively influences intention to adopt AI cybersecurity systems.

Perceived Response Efficacy (PRE)

PRE is the target user's belief that the suggested security solution will successfully prevent or avoid a danger (Hanus & Wu, 2016; Rogers, 1975). In the context of IS systems, RE refers to target users' belief that implementing a given security measure or system would assist them in mitigating security threats. Several researchers have shown that RE is an important predictor of consumers' adoption intentions (Hanus & Wu, 2016; Johnston & Warkentin, 2010; Park & Lee, 2014). Against this backdrop, it was hypothesized that:

H4: Perceived response efficacy (PRE) positively influences intention to adopt AI cybersecurity systems.

Job Insecurity (JI)

JI refers to the uncertainty or anxieties associated with the potential loss of a livelihood/job, authority, or power in the workplace when a new change is about to be implemented. This concept has been shown to have a detrimental influence on consumers' attitudes towards new technology. For example, Eren et al. (2020) discovered that technology adoption might cause a sense of JI since employees expect the business to reduce the number of employees. If perceived JI among employees is not addressed, it causes a shift in mindset, with employees developing a negative attitude towards the change and even resisting it. To back up this result, Feng et al. (2023) identified JI as one of the primary drivers of employee resistance to organizational change, which may include the introduction of new technology. Similarly, Alneyadi and Normalini (2023) established that job insecurity is a statistically significant predictor of adoption intentions, especially when AI-based technologies are involved. These findings imply that JI might cause employees to reject the implementation of AI cybersecurity solutions in their workplaces. As a result, the following theory was developed:

H5: Job insecurity is positively related to users' resistance to AI cybersecurity systems adoption.

Resistance to Change (RTC)

RTC is a statement of discontent/dissatisfaction with a change because of its perceived harmful consequences. Several researchers have shown that this construct is an accurate predictor of intentions to adopt new technology. For example, Tsai et al. (2020) believe that the introduction of new technology generates anxiety among target users due to fears about making irreversible errors when utilizing it. This uncertainty, as well as the related anxiety, frequently causes individuals to oppose technology. Nonetheless, age and experience are important factors, as indicated by Guo et al. (2013). Because of their high levels of technological fear, they discovered that older people are more likely than their younger counterparts to oppose mobile health services. According to this research, RTC has a detrimental impact on people's perceptions of and intentions to adopt new technologies. To that goal, the following theory was developed:

H6: Resistance to change (RC) negatively influences users' intention to adopt AI cybersecurity systems.

Materials and Methods

The quantitative technique and a correlational research design were utilized in the study. This decision was founded on positivist research philosophy, which promotes inductive reasoning and an objective approach to study problems. The quantitative approach was also suitable for the present study because it sought to establish causal relationships between variables using recommended statistical methods and computer applications. Furthermore, quantitative data is vital in explaining, controlling, and predicting phenomena, whereby the hypotheses formulated are confirmed or disconfirmed. As Creswell and Creswell (2017) observed, the approach involves identifying the different variables describing the study phenomena and testing them using the data collected. To this end, the six hypotheses identified above helped collect relevant data and interpret them using inferential and descriptive statistics.

The study participants were recruited using the purposive sampling technique, which involves choosing study participants based on predetermined criteria for their qualities. It is worth noting that the research needed professionals in the IT field and/or in charge of the cybersecurity tasks in the targeted UAE government and semi-government organizations. These workers were targeted because of the finding that they are the primary targets for cyber-attacks (Al-Khater et al., 2020) and one of the early adopters of new technologies despite their reluctance to embrace AI-based cybersecurity systems (Editor's Desk, 2020; Malek, 2018; Wilson, 2020). The sampling process started by identifying organizations that met the required criteria, including the following:

- Being a UAE government or semi-government organization.
- Have an established online presence, allowing them to offer some of their services digitally through their websites or mobile applications.
- Are yet to implement or are planning to adopt AI-based cybersecurity systems.

These organizations were identified through preliminary research, whereby the researcher visited the UAE government website (https://u.ae/en/information-and-services#/) to get relevant details regarding different online services offered by government organizations. The link (https://u.ae/en/help/contact-us/the-government) was also used to get information regarding the locations and services provided by various government organizations. These two links allowed the researcher to identify and examine organizations' relevance to the present study. The rationale for using this approach was the realization that organizations offering their services online must have IT departments and systems to safeguard their cyberspace. Such organizations are also susceptible to cyber-attacks due to the type of services they provide and the number of people they serve. Since establishing whether these organizations have AI-based cybersecurity systems was impossible, the researcher visited them to determine whether they have implemented those systems or are planning to do so. Those who have implemented them were excluded, while those who have not or are planning to implement them were evaluated further to establish whether they have met the above criteria. Once the specified criteria were met, the researcher requested contact details, especially email addresses of employees working in IT and other relevant departments. These details were vital in the recruitment process, especially in communicating with the participants.

While the recruitment focused on organizations in Abu Dhabi and Dubai, the scope was expanded to the neighboring Emirates to improve the chances of obtaining a sufficient sample size. The two emirates were prioritized because of their socio-political, economic, and administrative functions. It is worth noting that the status of Abu Dhabi as the UAE capital implies that a significant number of government and semi-government organizations are hosted there. On the other hand, Dubai is the most populous and diverse city in the UAE, meaning that various government organizations are situated there to serve the people. The potential subjects had to meet several requirements to be recruited. First, they had to be employees of the UAE government and semi-government organizations. Second, they had to somehow be involved in their respective organizations' security of information systems. Those working in organizations that had not adopted AI cybersecurity systems but were considering adopting them were also considered in the recruitment process. Individuals who did not meet these requirements were not recruited. Overall, 370 respondents were recruited.

To collect data from the identified participants, the researcher relied on web-based survey questionnaires, whose links were distributed through participants' email addresses. These questionnaires were developed based on the guidelines proposed by scholars such as Krosnick (2018) and Regmi et al. (2016). It involved two primary stages: (1) designing the questions based on the research questions and hypotheses and (2) pre-testing the questionnaires. When designing the questionnaires, the researcher ensured that each contained an opening paragraph describing the research purpose and ethical considerations and thanking the respondents for agreeing to participate in the study. The paragraph also contained definitions of key terms used in the questionnaires to ensure the respondents understood what was expected. All the questionnaires contained two sections, the first of which featured questions about the respondents' demographic profile (age, gender, educational background, specialization, and years of experience in using AI and in the cybersecurity profession). The other section contained questions that sought to establish the factors influencing the adoption of AI-based cybersecurity systems. These questions were based on the research hypotheses developed and the theoretical models discussed in the literature review section.

Each variable tested in the questionnaire was measured using three to seven items derived from the available literature. For instance, the measurement items for SI and FC were adapted from Naranjo-Zolotov et al. (2019), while those for behavioral intention, PV, and PRE were adapted from Sun et al. (2013). The measurement items for job insecurity and resistance to change were adapted from

Dabbous et al. (2021) and White et al. (2020), respectively. A 5-point to 7-point Likert scale was applied throughout to gauge the statements that needed scaling, with the respondents being asked to indicate the extent to which they agreed or disagreed with the statement. The scale ranged from 1, representing 'strongly disagree,' to 5/7, representing 'strongly agree.' Combining 5-point and 7-point Likert scales was deemed necessary to reduce the common method bias/variance (CMV), as suggested by scholars such as Lin et al. (2015). The questionnaires were closed-ended to make the responses uniform and facilitate the use of mathematical or quantitative analysis.

The pre-testing stage of the instrument development process involved subjecting the draft questionnaire to a test, whereby a sample of ten experts from the target population was used to test the questionnaires three times. This step was taken to improve the questionnaire and the findings' validity. It was meant to test whether the responses would match the researcher's expectations and whether the research questions were addressed comprehensively and effectively. Online meetings between the researcher and the experts were arranged based on their availability, convenience, and schedule. They were asked to fill out the survey questions while thinking aloud so that their views concerning the questions could be established. The researcher also observed and recorded the respondents' behaviors as they answered the questions, including nonverbal reactions to the questions and areas they were hesitating to answer or asked for clarification before answering. They were also asked to give their feedback after filling out the questionnaires. This feedback helped the researcher to make the necessary changes to improve the questionnaires' validity and reliability.

The data collection process started by seeking consent, whereby an invitation email message was sent to them requesting their participation. The study collected data through web-based survey questionnaires distributed to IT professionals and cybersecurity personnel in UAE government and semi-government organizations. The questionnaires included sections on demographic information and factors influencing the adoption of AI-based cybersecurity systems. Each variable was measured using multiple items adapted from existing literature, employing a combination of 5-point and 7-point Likert scales.

- *Social Influence (SI):* Measured using items adapted from Naranjo-Zolotov et al. (2019), capturing the belief that others will recognize a user if they adopt or recommend a new technology.
- *Facilitating Conditions (FC):* Measured using items from Naranjo-Zolotov et al. (2019), referring to the infrastructure and technical capacity required to adopt new technology.
- *Perceived Vulnerability (PV):* Measured using items from Sun et al. (2013), capturing the user's estimation of their vulnerability to an attack.
- *Perceived Response Efficacy (PRE):* Measured using items from Sun et al. (2013), reflecting the belief that the suggested security solution will effectively prevent or avoid danger.
- *Job Insecurity (JI):* Measured using items from Dabbous et al. (2021), capturing the anxiety associated with potential job loss due to new technology adoption.
- *Resistance to Change (RTC):* Measured using items from White et al. (2020), reflecting dissatisfaction with change due to perceived harmful consequences.

The PLS-SEM approach using the SmartPLS program was used to examine the data gathered in two key phases. To begin, the measurement model was assessed using three criteria: internal consistency validity, indicator reliability, convergent validity, and discriminant validity. These metrics were taken from previous research, including Hair et al. (2016), who determined that the three are the most critical factors for evaluating measurement models. The second phase entailed analyzing the structural model, in which the SmartPLS program was used to build structural relationships between variables and test hypotheses. Lateral collinearity, path coefficients, coefficient of determination (R2 value), F2-effect size, and predictive significance (Stone-Geisser's Q2) were among the parameters utilized.

ANALYSIS AND RESULTS

DEMOGRAPHIC PROFILE

The demographic parameters assessed throughout the data-gathering procedure comprised gender, age, occupation, educational level, and employment level, as indicated in Table 1. The researcher believed that these elements may impact users' actions, perceptions, attitudes, and, eventually, their intentions to use technology. According to Morris et al. (2005), gender, occupation, and employment level all have a substantial impact on people's adoption and usage of technology. They discovered that older workers had a greater effect on adoption intentions and eventual use of new technologies than younger employees. Baker et al. (2007) discovered that a greater education level improves the chance of accepting or adopting a technology. These findings made it imperative to capture the above demographic characteristics to establish whether they could have a major impact on intention to adopt AI-based cybersecurity systems in the UAE.

Table 1. Respondents' demographic profile

		Frequency	Percent	Valid Percent	Cumulative Percent
Gender	Female	160	47.1	47.1	47.1
	Male	180	52.9	52.9	100
	Total	340	100	100	
Age (years old)	21 – 30	226	66.5	66.5	66.5
	31 –40	81	23.8	23.8	90.3
	41 –50	22	6.5	6.5	96.8
	51 – 60	11	3.2	3.2	100
	Total	340	100	100	
Occupation	Government employee	125	36.8	36.8	36.8
	Semi-government employee	172	50.6	50.6	87.4
	Outsourced employees working in the government	43	12.6	12.6	100
	Total	340	100	100	
Educational level	Bachelor's degree	303	89.1	89.1	89.1
	Master's degree	24	7.1	7.1	96.2
	Doctor's degree	13	3.8	3.8	100
	Total	340	100	100	
Job level	Junior level	33	9.7	9.7	9.7
	Middle level	231	67.9	67.9	77.6
	Senior Level	76	22.4	22.4	90.3
	Total	340	100	100	

COMMON METHOD VARIANCE (CMV)

The presence of CMV was determined using the marker and baseline models, as indicated in Table 2. The main rationale for developing the CMV was the discovery that it might deflate or inflate data, resulting in incorrect conclusions (Craighead et al., 2011). After incorporating the marker variable into the route model, the R^2 of adoption intention and resistance to change was determined to be -0.33% and 0.00%, respectively. This increase was less than the 10% criterion established by Lindell and Whitney (2001), indicating that the route model utilized lacked the CMV.

Table 2. Common method variance test results (CMV)

Variable	Base model - R-square	Marker model - R-square	%
Intention to adopt AI cybersecurity systems	0.613	0.615	-0.33%
Resistance to change	0.107	0.107	0.00%

Assessment of the Measurement Model

The measurement model was assessed to determine the instruments' dependability and validity based on recommendations from Hair et al. (2019) and Ramayah et al. (2018). The metrics applied included convergent validity and discriminant validity. Figure 2 represents the measurement model used for this study.

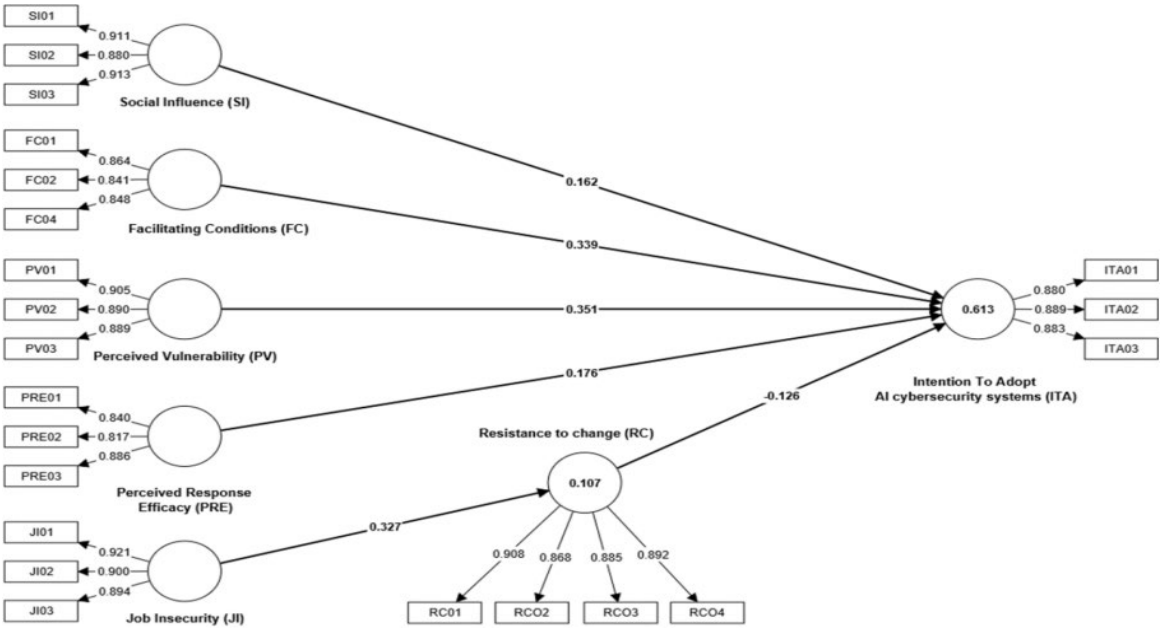

Figure 2. Measurement model

Convergent Validity

Convergent validity is concerned with the convergence of different variables' indicators. It was determined, based on Hair et al.'s (2021) recommendation, whereby the average variance extracted (AVE) was calculated, and the total squared loadings were divided by the number of indicators attributed to a variable. As such, AVE describes a variable's commonality. AVE's threshold was set at 0.50, with Hair et al. (2021) noting that values exceeding this number indicate that the variable can explain more than 50% of the construct indicators' variance. As Table 3 indicates, the AVE values exceeded 0.719 (after rounding off), implying that it surpassed the 0.50 threshold recommended by Hair and colleagues.

Table 3. Convergent validity

Variable	Item	Loading	Cronbach's alpha	Composite reliability (CR)	Average variance (AVE)
Facilitating Conditions (FC)	FC01	0.864	0.811	0.888	0.725
	FC02	0.841			
	FC04	0.848			

Variable	Item	Loading	Cronbach's alpha	Composite reliability (CR)	Average variance (AVE)
Intention to Adopt AI cybersecurity systems (ITA)	ITA01	0.880	0.860	0.915	0.782
	ITA02	0.889			
	ITA03	0.883			
Job Insecurity (JI)	JI01	0.921	0.890	0.931	0.819
	JI02	0.900			
	JI03	0.894			
Perceived Response Efficacy (PRE)	PRE01	0.840	0.805	0.885	0.719
	PRE02	0.817			
	PRE03	0.886			
Perceived Vulnerability (PV)	PV01	0.905	0.876	0.923	0.801
	PV02	0.890			
	PV03	0.889			
Resistance to change (RC)	RC01	0.908	0.911	0.937	0.789
	RCO2	0.868			
	RCO3	0.885			
	RCO4	0.892			
Social Influence (SI)	SI01	0.911	0.885	0.929	0.812
	SI02	0.880			
	SI03	0.913			

Note: FC03 was deleted due to low loadings

Discriminant Validity

The goal of discriminant validity is to determine the degree of uniqueness among the notions used in the study model (Hair et al., 2021). To test discriminant validity, the Fornell-Larcker criterion (Fornell & Larcker, 1981) and the Heterotrait-Monotrait Ratio (HTMT) of correlations are utilized. The Fornell-Larcker criterion compares each construct's AVE to its squared inter-construct correlation with all other variables in the research model (Table 4).

Table 4. Discriminant validity (Fornell-Larcker criterion)

	FC	ITA	JI	PRE	PV	RC	SI
FC	0.851						
ITA	0.663	0.884					
JI	0.044	-0.069	0.905				
PRE	0.447	0.496	-0.007	0.848			
PV	0.560	0.653	0.000	0.456	0.895		
RC	-0.029	-0.122	0.327	0.019	0.028	0.888	
SI	0.280	0.346	0.068	0.069	0.222	0.001	0.901

Note: FC = Facilitating Conditions, ITA = Intention to Adopt AI cybersecurity systems, JI = Job Insecurity, PRE = Perceived Response Efficacy, PV = Perceived Vulnerability, RC = Resistance to change, SI = Social Influence

Convergent validity is concerned with the convergence of indicators from diverse variables. It was determined using Hair et al.'s (2021) approach, which involved calculating the average variance extracted (AVE) and dividing the total squared loadings by the number of indicators associated with a variable. As such, AVE describes the commonality of variables. The AVE threshold was chosen at 0.50, with Hair et al. (2021) stating that values over this level imply that the variable may explain more than 50% of the variation in the construct indicators. As seen in Table 3, the AVE values above 0.719 (after rounding off) indicate that they exceeded the 0.50 level established by Hair and

colleagues. In models with conceptually identical variables, 0.90 is defined as the discriminant validity threshold, with numbers beyond the threshold indicating a lack of discriminant validity. Nonetheless, a lower threshold of 0.85 is seen to be reasonable (Hair et al., 2021; Henseler et al., 2015). As shown in Table 5, all HTMT values were less than the threshold for theoretically distinct structures, with the highest being 0.86. To that aim, the researcher contended that the respondents recognized the distinctiveness of the constructs utilized.

Table 5. Discriminant validity (HTMT criterion)

	FC	ITA	JI	PRE	PV	RC	SI
FC							
ITA	0.787						
JI	0.115	0.078					
PRE	0.547	0.594	0.081				
PV	0.662	0.751	0.034	0.539			
RC	0.063	0.135	0.351	0.032	0.036		
SI	0.323	0.396	0.077	0.081	0.253	0.018	

Note: FC = Facilitating Conditions, ITA = Intention to Adopt AI cybersecurity systems, JI = Job Insecurity, PRE = Perceived Response Efficacy, PV = Perceived Vulnerability, RC = Resistance to change, SI = Social Influence

Assessment of the Structural Model

The structural model was assessed to determine relations between variables. It entailed the following parameters as recommended by Hair et al. (2019, 2021): lateral collinearity, significance and relevance of path coefficients, R^2 coefficient of determination, f2 effect size, and predictive power Q^2.

Lateral Collinearity

The goal of calculating the lateral collinearity of the structural model was to discover and reduce method biases. To do this, all variables were regressed on a single variable to calculate the variance inflation factor (VIF), which aids in the detection of collinearity. VIF values greater than 5 suggest probable collinearity difficulties in predictor variables, according to Hair et al. (2021). However, as shown in Table 6, the VIFs for all variables were less than 2, indicating the lack of collinearity or bias.

Table 6. Collinearity testing results

Predictors	Variance inflation factor (VIF)	
	Intention to adopt AI cybersecurity systems (ITA)	Resistance to change (RC)
Facilitating Conditions (FC)	1.639	
Perceived Response Efficacy (PRE)	1.366	
Perceived Vulnerability (PV)	1.599	
Resistance to change (RC)	1.004	
Social Influence (SI)	1.102	
Job Insecurity (JI)		1.000

Significance and Relevance of Path Coefficients

Path coefficients help uncover the causal relationships between variables; they indicate the association between endogenous variable changes and a specific predictor variable when all other predictors

are maintained (Hair et al., 2021). Hair and colleagues argued that a path coefficient is deemed significant at 5% if value 0 is not within the 95% confidence level. Conversely, path coefficients are deemed relevant if they lie between -1 and +1; values closer to -1 show a significant negative relationship, with those approaching +1 showing a significant positive relationship (Hair et al., 2021). This study used a 5000-sample re-sample bootstrapping procedure to report the structural model's path coefficients, standard errors, t-values, and p-values (Table 7).

Table 7. Direct hypothesis results (from bootstrapping path coefficients)

Hypothesis	Relationships	Std. beta	Std. dev	T- value	P- value	BCI LL	BCI UL	Decision
H1	SI -> ITA	0.162	0.048	3.391	0.001	0.066	0.254	Accepted
H2	FC -> ITA	0.339	0.067	5.061	0.000	0.212	0.471	Accepted
H3	PV -> ITA	0.351	0.056	6.292	0.000	0.244	0.460	Accepted
H4	PRE -> ITA	0.176	0.052	3.400	0.001	0.076	0.279	Accepted
H5	JI -> RC	0.327	0.049	6.621	0.000	0.234	0.428	Accepted
H6	RC -> ITA	-0.126	0.034	3.654	0.000	-0.192	-0.057	Accepted

Note: FC = Facilitating Conditions, ITA = Intention to Adopt AI cybersecurity systems, JI = Job Insecurity, PRE = Perceived Response Efficacy, PV = Perceived Vulnerability, RC = Resistance to change, SI = Social Influence

As shown in Table 7, all hypotheses in this study were supported. Specifically, of all the direct relationships with the Intention to adopt an AI cybersecurity system (ITA), Perceived Vulnerability (PV) is the strongest predictor of ITA ($t = 6.292$, $\beta = 0.351$, $p < 0.000$), and the more susceptible to cyberattacks that users perceive, the higher will be their intention to adopt an AI cybersecurity system. Second, Facilitation Conditions (FC) ($t = 5.061$, $\beta = 0.339$, $p < 0.000$) have a significant positive effect on UAE users' ITA. In the UAE context, the better the infrastructure and the more adequate the human resources that users perceive when implementing AI cybersecurity systems, the stronger the user's intention to adopt. In addition, Perceived Response Effectiveness (PRE) ($t = 3.400$, $\beta = 0.176$, $p < 0.001$) and Social Influence (SI) ($t = 3.391$, $\beta = 0.162$, $p < 0.001$) also exerted a significant positive influence on UAE users' adoption intentions. However, among these direct relationships, Resistance to Change (RC) had a significant negative effect on UAE users' adoption intentions ($t = 3.654$, $\beta = -0.126$, $p < 0.000$), suggesting that users' uncertainty about the future of AI cybersecurity systems makes them more likely to want to settle for the status quo and not to want to make a change, which is a major resistance to the successful promotion of AI cybersecurity systems. Meanwhile, Job Insecurity (JI) positively internalizes and enhances users' Resistance to Change (RC) psychology (see Figure 3).

R^2-Coefficient of Determination

R^2 was determined to assess the model's predictive power. Shmueli and Koppius (2011) hold that R^2 values range from 0 to 1, whereby those closer to 1 indicate higher predictive power. As shown in Table 8, R^2 values for ITA and RC were (0.613) and (0.107), respectively. The value for ITA (0.613) can be considered significant, while that of RC (0.107) is weak (Hair et al., 2021).

Effect f^2 Size

F^2 was calculated to determine the impact of removing a selected predictor variable on the endogenous variables. According to Hair et al. (2017) and Cohen (2013), f^2 effect size, or rather the effect of omission of a construct on the endogenous construct, is categorized into three groups: small 0.02), medium (0.15), and large 0.35). Selya et al. (2012) asserted that the higher the f^2, the stronger the relationship between the two variables. As shown in Table 9, f^2 for all the constructs ranged between small and medium, suggesting that their relationships were medium.

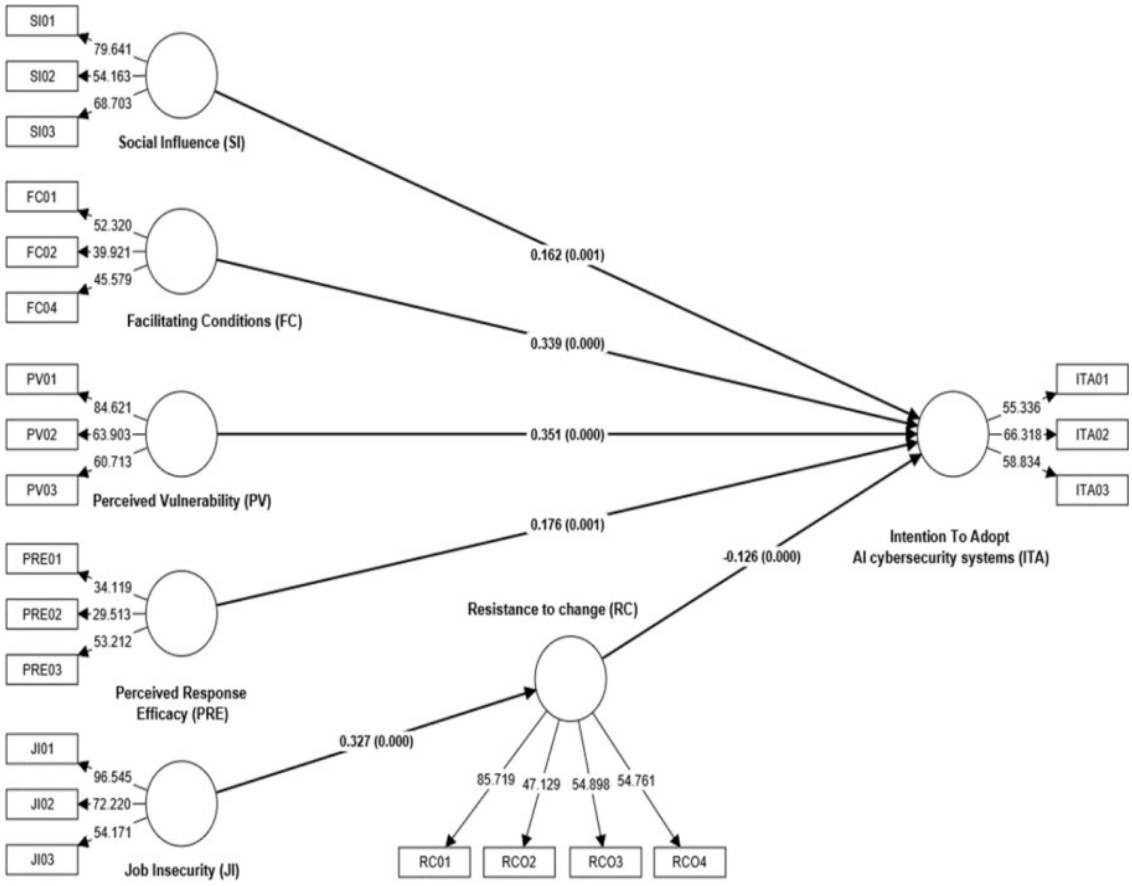

Figure 3. PLS structural model

Table 8. R^2-Coefficient of determination

	R-square	Explanatory Power (R^2)	
		Chin (1998)	Cohen (1988)
Intention to Adopt AI cybersecurity systems (ITA)	0.613	0.613 (Substantial)	0.613 (Substantial)
Resistance to change (RC)	0.107	0.107 (Weak)	0.107 (Moderate)

Table 9. f^2 effect size

Hypothesis	Relationships	F^2	Magnitude
H1	SI -> ITA	0.061	Small
H2	FC -> ITA	0.181	Medium
H3	PV -> ITA	0.199	Medium
H4	PRE -> ITA	0.058	Small
H5	JI -> RC	0.120	Small
H6	RC -> ITA	0.040	Small

DISCUSSION

The purpose of this study is to explore in depth the significant factors that influence employees' intention to adopt AI-based cybersecurity systems in the UAE government sector. The findings indicate that perceived vulnerability (PV) is the most significant positive correlation affecting the intention to adopt AI-based cybersecurity systems in the UAE. This finding is also supported by Huang and Kao (2015) and Liang and Xue (2010), who state that individuals are more likely to take protective measures if they perceive they are vulnerable to threats. This study extends these findings to the context of AI cybersecurity systems in the UAE, emphasizing the importance of perceived vulnerability in driving adoption. In addition, facilitating conditions (FC) had a substantial positive impact on the willingness to adopt AI cybersecurity systems. This finding is in line with studies by Yu (2012), Mtebe and Raisamo (2014), and Lee et al. (2018), who emphasized the importance of adequate infrastructure and technical capabilities in achieving technology adoption. In AI-based cybersecurity systems, the adequacy of facilitation directly affects users' adoption intentions. Users are more likely to take action when they perceive that sufficient resources (e.g., funding, technical support, and training) are available to use the AI system.

Second, Perceived Response Effectiveness (PRE) also had a significant positive effect on the intention to adopt AI cybersecurity systems (H4: $\beta = 0.176$, $p < 0.001$). This result is consistent with the findings of Hanus and Wu (2016) and Johnston and Warkentin (2010), who noted that beliefs about the effectiveness of security measures are critical to their adoption. In the field of cybersecurity, if users believe that an AI-based system is effective in preventing cyberattacks and security threats, they are more inclined to believe that they are better protected after adopting the system.

In addition, social influence (SI) has a substantial positive impact on the willingness to adopt AI cybersecurity systems. This finding is consistent with the findings of Venkatesh et al. (2012) and Taylor et al. (2011), who found that peer opinions significantly influence technology adoption. In organizational settings, colleagues, leaders, and industry standards are important social influences. If users are surrounded by coworkers and industry pioneers who are actively adopting AI-based cybersecurity systems, then this social acceptance will likely enhance individual adoption intentions. In addition, society's emphasis on cybersecurity and the industry's acceptance of AI technology will also largely influence users' attitudes.

In addition, the results of this study indicate that resistance to change is one of the significant resistances that prevent UAE government workers from adopting AI-based cybersecurity systems. This finding is consistent with the studies of Tsai et al. (2020) and Guo et al. (2013), which showed that anxiety and fear of change can significantly hinder technology adoption. This resistance may stem from fear of the unknown, dependence on existing systems, or concerns about the cost of learning new technologies. To overcome this resistance, organizations need to adopt effective change management strategies such as providing the necessary support, communicating the importance of change, and demonstrating the potential benefits of the new technology. When users perceive that the change can bring significant efficiency gains and security, their willingness to resist may decrease, thus enhancing the adoption of AI cybersecurity systems. Furthermore, job insecurity strengthens employees' resistance to change. This is consistent with the findings of Eren et al. (2020) and Feng et al. (2023), who concluded that job insecurity is an important factor in employees' resistance to organizational change, including new technology implementation. This study adds to the existing literature by emphasizing the specific impact of job insecurity on the adoption of AI cybersecurity systems.

Overall, the empirical findings of this study reinforce the validity of the theoretical models used and hypotheses tested. Contributing to a broader understanding of the factors that influence the adoption of AI cybersecurity systems, these findings provide valuable insights for policymakers and practitioners aiming to enhance cybersecurity practices in their organizations.

CONCLUSION AND IMPLICATIONS

This study investigated the factors that influence UAE customers' intentions to use AI-based cybersecurity solutions. In order to better fit the research model to the context of this study, an extended model was constructed that incorporates the PMT and UTAUT2 components as well as two additional variables (job insecurity and resistance to change). The findings indicate that perceived vulnerability, facilitating conditions, perceived response efficacy, and social influence have a positive and significant impact on the intention to adopt AI-based cybersecurity solutions. Meanwhile, job insecurity enhanced employees' resistance to change, making resistance to change a major resistance to the intention to adopt AI-based cybersecurity systems.

In other words, if AI cybersecurity systems have the potential to induce job insecurity, their adoption will be limited owing to user reluctance. These findings suggest that organizations can improve AI-technology acceptance and adoption rates in their cybersecurity departments by investing in interventions to reduce job insecurity and resistance to change and improve users' knowledge of their susceptibility to cyber-attacks, threat severity, the ease of using AI technologies, and the ability of these technologies to address their issues effectively.

MANAGERIAL IMPLICATIONS

The findings of this study provide several managerial implications for organizations aiming to adopt AI-based cybersecurity systems. First, organizations should work with industry experts and reputable organizations to add credibility to the product through their endorsements and recommendations. Showcase examples of businesses or organizations that have successfully adopted AI cybersecurity systems, especially from companies in the same industry or of similar size, so that potential users can see the results in practice. Sharing user reviews and feedback on the adoption of AI systems through social media, online forums, blogs, and other channels to increase social acceptance.

Second, AI cybersecurity system providers should ensure that the system interface is simple and intuitive, lowering the technical threshold so that non-technical users can easily understand and operate the AI security system. The system should support seamless integration with existing IT infrastructure, reduce technical complexity in the deployment process, and provide users with detailed operation manuals, online tutorials, and technical support to help them quickly get started and solve problems encountered in use.

In addition, system providers should (i) demonstrate how AI network security systems can identify and respond to potential threats in a timely and effective manner through simulated attacks, penetration tests, and other means; (ii) provide users with data on the system's defense effectiveness under different attack scenarios to help them clearly understand the actual capabilities of the AI system; ensure that the AI system can provide real-time feedback and automatically fix identified vulnerabilities and threats to enhance users' trust in its effectiveness.

Finally, organizations must clearly articulate that AI systems are intended as an aid to human decision-makers, not a replacement. Highlighting the intelligent and automated nature of the system is meant to reduce repetitive, boring tasks and allow employees to focus on higher-value work. Provide employees with the necessary skills enhancement training on how to collaborate with AI systems and improve their personal technical skills to alleviate the fear of losing their jobs. Encourage employees to make finer decisions with the help of AI systems, proving that AI is a powerful tool for enhancing productivity, not a threat. Organizations should adopt an incremental approach to introduce AI systems gradually rather than rolling them out all at once. Allow users to initially feel the value of the system and gradually increase its application. During the design and implementation of the AI system, users are invited to participate in testing and feedback to feel part of the system improvement and reduce their resistance. Provide technical support, rewards, or incentives to early adopters to encourage them to become advocates of the AI system, thereby influencing more people to embrace the new technology.

LIMITATIONS AND FUTURE RESEARCH

This study has some limitations that should be noted. First, the use of a purposive sampling technique may limit the findings' generalizability to a larger population. Future studies could use random sampling methods to improve the sample's representativeness. Secondly, the study was conducted within the specific context of UAE government and semi-government organizations, which may not fully capture the complexity of AI adoption in different cultural or organizational settings. Future research should explore the adoption of AI-based cybersecurity systems in various industries and geographical regions to provide a more comprehensive understanding of the factors influencing adoption. Last, longitudinal studies could be conducted to examine how perceptions and adoption intentions evolve over time, particularly as organizations become more familiar with AI technologies and their potential benefits and challenges.

ACKNOWLEDGMENT

The authors express their sincere appreciation to the anonymous referees of the journal for their invaluable suggestions, which substantially enhanced the caliber of this paper. This article is supported by the Graduate on Time Grant (GOT) USM (No. R502-KR-GOT001-0000000151-K134). Disclaimers, as usual, apply.

REFERENCES

Addae, J. H., Sun, X., Towey, D., & Radenkovic, M. (2019). Exploring user behavioral data for adaptive cybersecurity. *User Modeling and User-Adapted Interaction, 29*, 701-750. https://doi.org/10.1007/s11257-019-09236-5

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179-211. https://doi.org/10.1016/0749-5978(91)90020-T

Ajzen, I., & Fishbein, M. (1975). A Bayesian analysis of attribution processes. *Psychological Bulletin, 82*(2), 261-277. https://doi.org/10.1037/h0076477

Al-Khater, W. A., Al-Maadeed, S., Ahmed, A. A., Sadiq, A. S., & Khan, M. K. (2020). Comprehensive review of cybercrime detection techniques. *IEEE Access*, *8*, 137293-137311. https://doi.org/10.1109/ACCESS.2020.3011259

Almansoori, A., Al-Emran, M., & Shaalan, K. (2023). Exploring the frontiers of cybersecurity behavior: A systematic review of studies and theories. *Applied Sciences, 13*(9), 5700. https://doi.org/10.3390/app13095700

Alneyadi, M. R. M. A. H., Kassim, N. Md., & Yin, T. S. (2022). Conceptual framework on the factors influencing users' intention to adopt ai-based cybersecurity systems at workplaces in the UAE. *Global Business & Management Research, 14*(3), 1053-1064. http://www.gbmrjournal.com/pdf/v14n3s/V14N3s-72.pdf

Alneyadi, M. R. M. A. H., & Normalini, M. K. (2023). Factors influencing user's intention to adopt AI-based cybersecurity systems in the UAE. *Interdisciplinary Journal of Information, Knowledge, and Management, 18,* 459-486. https://doi.org/10.28945/5166

Ameen, N., Tarhini, A., Shah, M. H., Madichie, N., Paul, J., & Choudrie, J. (2021). Keeping customers' data secure: A cross-cultural study of cybersecurity compliance among the Gen-Mobile workforce. *Computers in Human Behavior, 114*, 106531. https://doi.org/10.1016/j.chb.2020.106531

Baker, E. W., Al-Gahtani, S. S., & Hubona, G. S. (2007). The effects of gender and age on new technology implementation in a developing country: Testing the Theory of Planned Behavior (TPB). *Information Technology & People*, *20*(4), 352–375. https://doi.org/10.1108/09593840710839798

Bhargava, A., Bester, M., & Bolton, L. (2021). Employees' perceptions of the implementation of robotics, artificial intelligence, and automation (RAIA) on job satisfaction, job security, and employability. *Journal of Technology in Behavioral Science, 6*, 106-113. https://doi.org/10.1007/s41347-020-00153-8

Bhatele, K. R., Shrivastava, H., & Kumari, N. (2019). The role of artificial intelligence in cyber security. In S. Geetha & A. Phamila (Eds.), *Countering cyber attacks and preserving the integrity and availability of critical systems* (pp. 170-192). IGI Global. https://doi.org/10.4018/978-1-5225-8241-0.ch009

Brown, S. A., & Venkatesh, V. (2005). Model of adoption of technology in households: A baseline model test and extension incorporating household life cycle. *MIS Quarterly, 29*(3), 399-426. https://doi.org/10.2307/25148690

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*, *17*(5), 5-21

Champion, V. L., & Skinner, C. S. (2008). The health belief model. In K. Glanz, B. K. Rimer, & K. Viswanath (Eds.), *Health behavior and health education: Theory, research, and practice* (4th ed., pp. 45-65). Jossey-Bass.

Chin, W. W. (1998). The partial least squares approach for structural equation modeling. In G. A. Marcoulides (Ed.), *Modern methods for business research* (pp. 295-336). Lawrence Eribaum Associates Publishers. https://www.researchgate.net/publication/311766005_The_Partial_Least_Squares_Approach_to_Structural_Equation_Modeling

Cohen, J. (1988). *Statistical power analysis for the behavioral sciences* (2nd ed.). Routledge. https://doi.org/10.4324/9780203771587

Cohen, J. (2013). *Statistical power analysis for the behavioral sciences.* [ebook]. https://www.google.com/books/edition/_/2v9zDAsLvA0C?hl=en&sa=X&ved=2ahUKEwiB8_Lp6vCKAxU4CjQIHcJ2G_YQre8FegQIDRAJ

Craighead, C. W., Ketchen, D. J., Dunn, K. S., & Hult, G. T. M. (2011). Addressing common method variance: guidelines for survey research on information technology, operations, and supply chain management. *IEEE Transactions on Engineering Management*, *58*(3), 578–588. https://doi.org/10.1109/TEM.2011.2136437

Creswell, J. W., & Creswell, J. D. (2017). *Research design: Qualitative, quantitative, and mixed methods approaches* (4th ed.). Sage.

Dabbous, A., Aoun Barakat, K., & Merhej Sayegh, M. (2021). Enabling organizational use of artificial intelligence: An employee perspective. *Journal of Asia Business Studies, 16*(2), 245-266. https://doi.org/10.1108/JABS-09-2020-0372

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*(3), 319-340. https://doi.org/10.2307/249008

de Azambuja, A. J. G., Plesker, C., Schützer, K., Anderl, R., Schleich, B., & Almeida, V. R. (2023). Artificial intelligence-based cyber security in the context of industry 4.0: A survey. *Electronics, 12*(8), 1920. https://doi.org/10.3390/electronics12081920

Editor's Desk. (2020, March 27). UAE embraces blockchain technology and digital identity to fight Covid-19! *Blockchain Magazine.* https://blockchainmagazine.net/uae-embraces-blockchain-technology-and-digital-identity-to-fight-covid-19/

Eren, A. S., Ozyasar, K., & Taşliyan, M. (2020). The effect of technology adoption on job insecurity: A case study in Turkish textile sector. *Kahramanmaraş Sütçü İmam Üniversitesi Sosyal Bilimler Dergisi*, *17*(2), 1007-1023. https://doi.org/10.33437/ksusbd.706168

Feng, C., Cooper, B., & Zhu, C. J. (2023). How and when job security reduces resistance to change in the context of organizational change. *The Journal of Applied Behavioral Science*, *59*(3), 426-447. https://doi.org/10.1177/00218863211040613

Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A meta-analysis of research on protection motivation theory. *Journal of Applied Social Psychology, 30*(2), 407-429. https://doi.org/10.1111/j.1559-1816.2000.tb02323.x

Fornell, C., & Larcker, D. F. (1981). Structural equation models with unobservable variables and measurement error: Algebra and statistics. *Journal of Marketing Research*, *18*, 382-388. https://doi.org/10.2307/3150980

Goodhue, D. L., & Thompson, R. L. (1995). Task-technology fit and individual performance. *MIS Quarterly, 19*(2), 213-236. https://doi.org/10.2307/249689

Guo, X., Sun, Y., Wang, N., Peng, Z., & Yan, Z. (2013). The dark side of elderly acceptance of preventive mobile health services in China. *Electronic Markets*, *23*(1), 49-61. https://doi.org/10.1007/s12525-012-0112-4

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. https://doi.org/10.1016/j.ijinfomgt.2019.03.008

Guven, H. (2018). *The state of cyber (in)security in the United Arab Emirates.* https://www.cs.tufts.edu/comp/116/archive/spring2018/hguven.pdf

Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2016). *A primer on Partial Least Squares Structural Equation Modeling (PLS-SEM).* Sage.

Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2017). *A primer on Partial Least Squares Structural Equation Modeling* (2nd ed.). Sage. https://doi.org/10.15358/9783800653614

Hair, J. F., Hult, G. T. M., Ringle, C. M., Sarstedt, M., Danks, N. P., & Ray, S. (2021). Evaluation of reflective measurement models. *Partial Least Squares Structural Equation Modeling (PLS-SEM) Using R* (pp. 75-90). Springer. https://doi.org/10.1007/978-3-030-80519-7_4

Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report the results of PLS-SEM. *European Business Review*, *31*(1), 2-24. https://doi.org/10.1108/EBR-11-2018-0203

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. https://doi.org/10.1080/10580530.2015.1117842

Henseler, J., Ringle, C., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science*, *43*, 115-135. https://doi.org/10.1007/s11747-014-0403-8

Huang, C.-Y., & Kao, Y.-S. (2015). UTAUT2-based predictions of factors influencing the technology acceptance of phablets by DNP. *Mathematical Problems in Engineering, 2015,* Article 603747. https://doi.org/10.1155/2015/603747

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly*, *34*(3), 549-566. https://doi.org/10.2307/25750691

Krosnick, J. A. (2018). Questionnaire design. In D. Vannette, & J. Krosnick (Eds.), *The Palgrave handbook of survey research* (pp. 439-455). Palgrave Macmillan. https://doi.org/10.1007/978-3-319-54395-6_53

Lee, H. J., 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. https://doi.org/10.14257/ijast.2018.111.14

Lemos, R. (2024a, March 14). 150K+ UAE network devices & apps found exposed online. *Dark Reading.* https://www.darkreading.com/threat-intelligence/150kplus-uae-network-devices-apps-exposed-online

Lemos, R. (2024b, October 1). UAE, Saudi Arabia become plum cyberattack targets. *Dark Reading.* https://www.darkreading.com/cyberattacks-data-breaches/uae-saudi-arabia-cyberattack-targets

Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems*, *11*(7), 394-413. https://doi.org/10.17705/1jais.00232

Lin, T.-C., Huang, S.-L., & Hsu, C.-J. (2015). A dual-factor model of loyalty to IT product – The case of smartphones. *International Journal of Information Management, 35*(2), 215-228. https://doi.org/10.1016/j.ijinfomgt.2015.01.001

Lindell, M. K., & Whitney, D. J. (2001). Accounting for common method variance in cross-sectional research designs. *Journal of Applied Psychology, 86*(1), 114–121. https://doi.org/10.1037/0021-9010.86.1.114

Lu, L., Cai, R., & Gursoy, D. (2019). Developing and validating a service robot integration willingness scale. *International Journal of Hospitality Management, 80*, 36-51. https://doi.org/10.1016/j.ijhm.2019.01.005

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology, 19*(5), 469–479. https://doi.org/10.1016/0022-1031(83)90023-9

Malek, C. (2018, April 29). UAE embraces emerging technologies in education. *Arab Weekly*. https://thearabweekly.com/uae-embraces-emerging-technologies-education

MEIR Team. (2024, December 4). UAE: Cyber threats rise sharply in 2024, expected to worsen with new technologies. *Middle East Insurance Review*. https://meinsurancereview.com/News/View-NewsLetter-Article/id/90224/type/MiddleEast/UAE-Cyber-threats-rise-sharply-in-2024-expected-to-worsen-with-new-technologies

Morris, M. G., Venkatesh, V., & Ackerman, P. L. (2005). Gender and age differences in employee decisions about new technology: An extension to the theory of planned behavior. *IEEE Transactions on Engineering Management*, *52*(1), 69-84. https://doi.org/10.1109/TEM.2004.839967

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), 4-20.

Nam, K., Dutt, C. S., Chathoth, P., Daghfous, A., & Khan, M. S. (2021). The adoption of artificial intelligence and robotics in the hotel industry: Prospects and challenges. *Electronic Markets, 31*, 553-574. https://doi.org/10.1007/s12525-020-00442-3

Naranjo-Zolotov, M., Oliveira, T., Cruz-Jesus, F., Martins, J., Gonçalves, R., Branco, F., & Xavier, N. (2019). Examining social capital and individual motivators to explain the adoption of online citizen participation. *Future Generation Computer Systems*, *92*, 302-311. https://repositorio.inesctec.pt/server/api/core/bitstreams/c8aa61e6-69cb-4bf0-ae21-320b7b3c63a6/content

Nguyen, P. (2013). Mothers' perceived vulnerability, perceived threat and intention to administer preventive medication to their children. *Contemporary Management Research*, *9*(4), 399-418. https://doi.org/10.7903/cmr.11093

Park, C., & Lee, S.-W. (2014). A study of the user privacy protection behavior in the online environment: Based on protection motivation theory. *Journal of Internet Computing and Services*, *15*(2), 59-71. https://doi.org/10.7472/jksii.2014.15.2.59

PositiveTechnologies. (2024, September 18). GCC countries and the cybercriminal services market (2023–2024 report). https://global.ptsecurity.com/analytics/gulf-countries-as-a-commodity-in-the-market-on-criminal-cyber-services-2023-2024

Ramayah, T., Cheah, J., Chuah, F., Ting, H., & Memon, M. A. (2018). *Partial Least Squares Structural Equation Modeling (PLS-SEM) using SmartPLS 3.0: An updated guide and practical guide to statistical analysis* (2nd ed.). Pearson.

Regmi, P. R., Waithaka, E., Paudyal, A., Simkhada, P., & Van Teijlingen, E. (2016). Guide to the design and application of online questionnaire surveys. *Nepal Journal of Epidemiology, 6*(4), 640-644. https://doi.org/10.3126/nje.v6i4.17258

Rippetoe, P. A., & Rogers, R. W. (1987). Effects of components of protection-motivation theory on adaptive and maladaptive coping with a health threat. *Journal of Personality and Social Psychology, 52*(3), 596-604. https://doi.org/10.1037/0022-3514.52.3.596

Rizvi, M. (2023). Enhancing cybersecurity: The power of artificial intelligence in threat detection and prevention. *International Journal of Advanced Engineering Research and Science, 10*(5), 55-60. https://doi.org/10.22161/ijaers.105.8

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology, 91*(1), 93-114. https://doi.org/10.1080/00223980.1975.9915803

Rogers, R. W. (1983). Cognitive and psychological processes in fear appeals and attitude change: A revised protection motivation theory. In J. T. Cacioppo, & R. E. Petty (Eds.), *Social psychophysiology: A sourcebook* (pp. 153-176). Guilford.

Samtani, S., Kantarcıoğlu, M., & Chen, H. (2020). Trailblazing the artificial intelligence for cybersecurity discipline. *ACM Transactions on Management Information Systems*, *11*(4), Article 17. https://doi.org/10.1145/3430360

Sarker, I. H., Furhad, M. H., & Nowrozy, R. (2021). Ai-driven cybersecurity: An overview, security intelligence modeling and research directions. *SN Computer Science, 2*, Article173. https://doi.org/10.1007/s42979-021-00557-0

Selya, A. S., Rose, J. S., Dierker, L. C., Hedeker, D., & Mermelstein, R. J. (2012). A practical guide to calculating Cohen's f^2, a measure of local effect size, from PROC MIXED. *Frontiers in Psychology, 3*, 111. https://doi.org/10.3389/fpsyg.2012.00111

Shahbaznezhad, H., Kolini, F., & Rashidirad, M. (2021). Employees' behavior in phishing attacks: What individual, organizational, and technological factors matter? *Journal of Computer Information Systems, 61*(6), 539-550. https://doi.org/10.1080/08874417.2020.1812134

Shamiulla, A. M. (2019). Role of artificial intelligence in cyber security. *International Journal of Innovative Technology and Exploring Engineering, 9*(1), 4628-4630. https://doi.org/10.35940/ijitee.A6115.119119

Shmueli, G., & Koppius, O. R. (2011). Predictive analytics in information systems research. *MIS Quarterly, 35*(3), 553-572. https://doi.org/10.2307/23042796

Simonet, J., & Teufel, S. (2019). The influence of organizational, social and personal factors on cybersecurity awareness and behavior of home computer users. In G. Dhillon, F. Karlsson, K. Hedström, & A. Zúquete (Eds.), *ICT systems security and privacy protection* (pp. 194-208). Springer.

Sun, Y., Wang, N., Guo, X., & Peng, Z. (2013). Understanding the acceptance of mobile health services: A comparison and integration of alternative models. *Journal of Electronic Commerce Research, 14*(2), 183-200.

Tabrizi, B., Lam, E., Girard, K., & Irvin, V. (2019, March 14). Digital transformation is not about technology. *Harvard Business Review.* https://hbr.org/2019/03/digital-transformation-is-not-about-technology

Taylor, D. G., Voelker, T. A., & Pentina, I. (2011). *Mobile application adoption by young adults: A social network perspective.* WCBT Faculty Publications. https://digitalcommons.sacredheart.edu/wcob_fac/1/

Thompson, R. L., Higgins, C. A., & Howell, J. M. (1991). Personal computing: Toward a conceptual model of utilization. *MIS Quarterly*, *15*(1), 125-143. https://doi.org/10.2307/249443

Tsai, T.-H., Lin, W.-Y., Chang, Y.-S., Chang, P.-C., & Lee, M.-Y. (2020). Technology anxiety and resistance to change: a behavioural study of a wearable cardiac warming system using an extended TAM for older adults. *PLoS ONE*, *15*(1), e0227270. https://doi.org/10.1371/journal.pone.0227270

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly, 27*(3), 425-478. https://doi.org/10.2307/30036540

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*, *36*(1), 157-178. https://doi.org/10.2307/41410412

White, K. R. G., Kinney, D., Danek, R. H., Smith, B., & Harben, C. (2020). The Resistance to Change-Beliefs Scale: Validation of a new measure of conservative ideology. *Personality and Social Psychology Bulletin*, *46*(1), 20-35. https://doi.org/10.1177/0146167219841624

Wilson, G. (2020, June 25). Blue prism: UAE leaders embrace intelligent automation. *BusinessChief.* https://businesschief.eu/technology/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.

AUTHORS

Mohammed Rashed Mohammed Al Humaid Alneyadi is a Deputy Head of the Communications and IT Department at the Global Aerospace Logistics private company in UAE. He has 24 years of experience in the Communications and IT field. He obtained his first degree in Computer Engineering from the Florida Institute of Technology (FIT), USA, in 1999. He completed his first Master of Science in Computer Science from the New York Institute of Technology (NYIT) in UAE in 2008. He completed his second Master of Science in Information Technology (Specialization in Cyber Security) at Zayed University in UAE in 2012. He completed his PhD in Operations Management at the University of Science, Malaysia (2023). He has embarked on a mission to leverage Artificial Intelligence (AI) across all fields, aiming to maximize its potential to drive innovation, enhance efficiency, and unlock new opportunities that benefit industries and humanity as a whole.

Normalini Md Kassim is currently an associate professor at the School of Management at the Universiti Sains Malaysia and a visiting professor at the Management & Science University (Malaysia). She is a Technical Specialist with the Malaysian Board of Technologists. She is also a Chartered Member of the Chartered Institute of Logistics & Transport (CMILT). Her publications have appeared in IGI Global Handbook, Procedia-Social and Behavioral Sciences (Elsevier), International Journal of Productivity and Performance Management (Emerald), Global Business Review (SAGE), Taylor and Francis, Social Indicators Research, International Journal of Communication Systems, International Journal of Enterprise Information Systems, Industrial Engineering & Management Systems, Global Business and Management Research and Springer. She has experience with industries like Maybank Berhad as a system engineer for four years and Hewlett Packard Singapore as a Project Manager for the Asia Pacific Project for ten years. She completed her Master of Business Administration (MBA) at the University of Science, Malaysia (2005) and completed her PhD in Technology Management from the same university (2012). She has embarked on a new research area: smart community, smart cities, and business analytics. With experience in banking, manufacturing, communication, and the financial industry, she would like to collaborate and share her experience in technology management, business analytics, and risk management. Her full profile can be accessed at www.som.usm.my.