FACTORS INFLUENCING USERS' INTENTION TO ADOPT ARTIFICIAL INTELLIGENCE CYBERSECURITY SYSTEMS AT GOVERNMENT AND SEMI-GOVERNMENT ORGANIZATIONS IN THE UNITED ARAB EMIRATES

MOHAMMED RASHED MOHAMMED
AL HUMAID ALNEYADI

UNIVERSITI SAINS MALAYSIA

2023

FACTORS INFLUENCING USERS' INTENTION TO ADOPT ARTIFICIAL INTELLIGENCE CYBERSECURITY SYSTEMS AT GOVERNMENT AND SEMI-GOVERNMENT ORGANIZATIONS IN THE UNITED ARAB EMIRATES

by

MOHAMMED RASHED MOHAMMED
AL HUMAID ALNEYADI

Thesis submitted in fulfillment of the requirements
for the degree of
Doctor of Philosophy

September 2023

ACKNOWLEDGEMENT

I am forever thankful for many people who greatly contributed and supported me during this life-changing process. Writing the first three chapters of this research has been a difficult and demanding process, and it would not have been successful were it not for the people named below.

First, I appreciate and sincerely thank my supervisors, Ts. Dr. Normalini Md Kassim and Associate Professor Dr. Teh Sin Yin, for encouraging, advising and guiding me throughout this research. You played a significant role in alleviating fears that I initially had at the beginning of this research and believed in my ability to transform the research idea into a reality. Your encouragement and motivation during times when I felt giving up as well as your suggestions and feedback improved my confidence and ability to address challenges that I thought were beyond my capacity. I am grateful for your support, mentorship, and friendship which has developed during this research. I am privileged and honored to work with you.

Second, I wish to thank my fellow doctoral classmates for your friendship, support, and crucial insights during this doctoral program. Many thanks to Sultan, Majid, and Fayez for providing me with a shoulder to lean on as we shared our experiences and insights during this doctoral journey. Despite the challenges, your friendship and our experiences gave me a reason to work harder in this research. I am grateful for being part of my doctoral journey.

Last but not least, I wish to extend special thanks and appreciation to my family members and friends. Special thanks to my wife, sons and daughters, and my friends for encouraging me to keep going and bearing with me when I could not get adequate time for you as I had to focus on my research and writing. Even when things seemed tough, you encouraged me, expressed confidence in me and gave me a reason to try harder. I feel blessed to have such understanding family and friends.

TABLE OF CONTENTS

LIST OF TABLES

Page

LIST OF FIGURES

LIST OF ABBREVIATIONS

AI	Artificial Intelligence
AIS	Artificial Immune Systems
ANN	Artificial Neural Networks
CF	Collaborative Filtering
CI	Computational Intelligence
CPS	Cyber-Physical Systems
DDoS	Distributed Denial of Service
DL	Deep Learning
DoS	Denial-of-Service
EPAADPS	Efficient Proactive Artificial Immune System-based Anomaly Detection and Prevention System
EWMA	Exponentially Weighted Moving Average
FTC	Federal Trade Commission
GCC	Gulf Cooperation Council
HTMT	Heterotrait-Monotrait ratio of correlations
IDPS	Detection and Prevention System
IDT	Innovation Diffusion Theory
IoT	Internet of Things
IP	Internet Protocols
IPS	Intrusion Prevention System
IT	Information Technology
ML	Machine Learning
MM	Motivational Model
MOOC	Massive Open Online Courses
MPCU	Model of PC Utilisation
NESA	National Electronic Security Authority

NSA	Negative Selection Algorithm
OFD	Online Food Delivery
PBIL	Population-Based Incremental Learning
PLS-SEM	Partial Least Squares structural equation and Modelling
PMT	Protection Motivation Theory
RPA	Robotic Process Automation
RTC	Resistance to Change
SCT	Social Cognitive Theory
SPSS	Statistical Package for Social Sciences
TAM	Technology Acceptance Model
TPB	Theory Of Planned Behaviour
TPK	Technological Pedagogical Knowledge
TRA	Telecommunications Regulations Authority of the UAE
TTF	Task-Technology Fit
UTAUT	Unified Theory of Acceptance and Use of Technology
UTRA	UAE's Telecommunication Regulations Authority

LIST OF APPENDICES

FAKTOR-FAKTOR YANG MEMPENGARUHI NIAT PENGGUNA UNTUK MENERIMA PAKAI SISTEM KESELAMATAN SIBER KECERDASAN BUATAN DI ORGANISASI KERAJAAN DAN SEPARA KERAJAAN DI EMIRIAT ARAB BERSATU

ABSTRAK

Kajian bertujuan untuk mengkaji faktor-faktor yang mempengaruhi niat pengguna untuk mengambil sistem siber keselamatan AI di tempat kerja di UAE. Ini adalah sebagai tindak balas terhadap masalah penyelidikan yang diperhatikan mengenai penggunaan yang rendah dan niat untuk menggunakan sistem siber keselamatan berdasarkan AI di UAE, walaupun terdapat banyak manfaat yang berkaitan dengan teknologi tersebut. Oleh itu, kajian ini memperluas gabungan model Teori Penerimaan dan Penggunaan Teknologi (UTAUT) dan Teori Motivasi Perlindungan (PMT) dengan memperkenalkan hubungan dan pemboleh ubah baru (pengetahuan AI, rintangan kepada perubahan, dan ketidakstabilan pekerjaan). Berdasarkan analisis 340 soal selidik yang dijalankan kepada individu yang bekerja di pelbagai organisasi kerajaan dan separa-kerajaan di UAE menggunakan strategi PLS-SEM, didapati bahawa faktor-faktor seperti persepsi kerentanan, persepsi keberkesanan diri, persepsi keberkesanan tindak balas, jangkaan usaha, pengetahuan dalam AI, dan keadaan memfasilitasi mempengaruhi secara signifikan dan positif niat pengguna untuk mengambil sistem siber keselamatan berdasarkan AI. Walau bagaimanapun, didapati bahawa teknologi baru dikaitkan dengan ketidakstabilan pekerjaan dan rintangan kepada perubahan, yang boleh memberi kesan negatif secara signifikan terhadap niat pengguna untuk menerima dan mengambil teknologi siber keselamatan berdasarkan AI. Kajian ini tidak menemui hubungan yang signifikan antara pengaruh sosial dan niat untuk menggunakan sistem siber keselamatan berdasarkan AI. Oleh itu, kajian ini membantu untuk memahami beberapa faktor yang mungkin menyumbang kepada pengambilan yang lembap sistem siber keselamatan berdasarkan AI oleh organisasi di UAE. Ia bertindak sebagai penerang mata bagi organisasi-organisasi tersebut untuk menilai diri mereka sendiri secara kritikal dan menentukan tahap kecekapan mereka dalam mengambil sistem siber keselamatan berdasarkan AI dan membangunkan langkah-langkah dan pendekatan yang boleh mereka ambil untuk mengurangkan rintangan pekerja terhadap perubahan teknologi baru dalam sektor keselamatan siber.

FACTORS INFLUENCING USERS’ INTENTION TO ADOPT ARTIFICIAL INTELLIGENCE CYBERSECURITY SYSTEMS AT GOVERNMENT AND SEMI-GOVERNMENT ORGANIZATIONS IN THE UNITED ARAB EMIRATES

ABSTRACT

The revolutionising impacts of artificial intelligence (AI) on other fields have led to the realisation that the technology can improve cybersecurity and mitigate cybercrimes in both private and government organisations. However, this realisation has not contributed to the rapid adoption of cybersecurity systems in the UAE, despite the country being ranked as one of the nations that are quick to embrace emerging technologies. Against this background, this study investigated the factors that influence users' intention to adopt (ITA) AI cybersecurity systems at workplaces in the UAE. It drew upon a theoretical framework derived from the Protection Motivation Theory (PMT) and the Unified Theory of Acceptance and Use of Technology (UTAUT). This framework was extended by introducing new relationships and variables (AI knowledge, resistance to change, and job insecurity) to enhance its predictive power. A quantitative research approach and a correlational research design was adopted, whereby 340 questionnaires were administered to respondents chosen using the purposive sampling technique. These respondents comprised persons working in the IT department and/ or responsible for the cybersecurity of government and semi-government organisations in the UAE. The findings made from their responses indicated that factors such as perceived vulnerability (PV), perceived severity (PS), perceived self-efficacy (PSE), perceived response efficacy (PRE), attitude, effort expectancy (EE), knowledge in AI (AK), and facilitating conditions

(FC) significantly and positively influenced ITA. On the other hand, job insecurities (JI) and resistance to change (RC) had significant negative effects on ITA. The study found no significant relationship between social influence (SI) and ITA. Users' attitudes mediated the relationship between FC, AK, and ITA, but the construct's mediating effect on the relationship between SI and ITA was insignificant. The practical contributions of this study include promoting an understanding of some of the factors that could be contributing to the sluggish adoption of AI cybersecurity systems by organisations in the UAE. The study acts as an eye-opener for these organisations to critically evaluate themselves and establish their level of preparedness in terms of adopting AI-based cybersecurity systems and come up with measures and approaches they can adopt to minimise employees' resistance to new technological changes in cybersecurity sectors. The study's theoretical contributions include enriching the available literature concerning the intention to adopt new technologies such as AI cybersecurity systems. This study has also proposed a new research framework developed by integrating constructs of the PMT and UTAUT and extending it by introducing three new variables (AI knowledge, resistance to change, and job insecurity). This extension helps to improve the comprehensiveness and predictive power of the integrated model.

CHAPTER 1

INTRODUCTION

1.1 Introduction

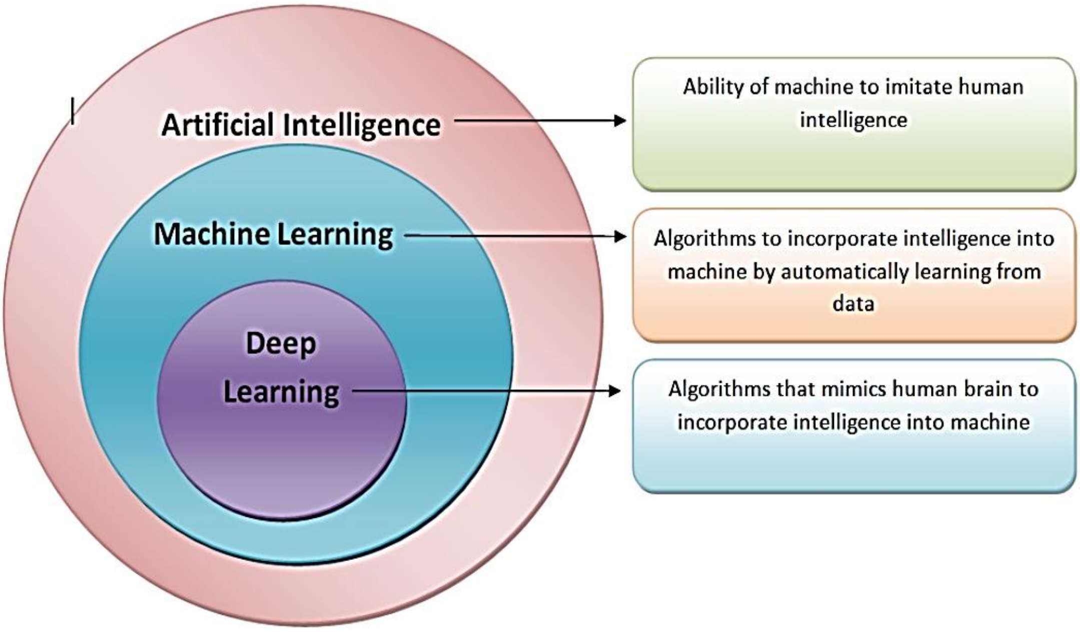
Cybersecurity refers to the protection of computer networks, hardware, and data against unauthorised/illegal access, usage, or damage. It also involves safeguarding information integrity, privacy, and availability (Zhang et al., 2022). Evidence suggests that cybersecurity attacks have grown significantly in terms of volume and complexity, thus making the traditional human-centric approaches increasingly less effective (Ramírez, 2017; Salloum et al., 2020). For this reason, artificial intelligence (AI) is seen as a more efficient approach that could help organisations avoid threats. Research further shows that AI technologies have revolutionised many other fields by assisting managers in deriving meaning from complex and enormous data (Patil, 2016; Taddeo, 2019). As such, they are identified as one of the tools that could revolutionise the cybersecurity field by gathering intelligence from millions of sources and using it to mitigate the identified threats in record time (Jakhar & Kaur, 2020; Patil, 2016).

Recent innovations such as machine learning (ML) and deep learning (DL) are, for instance, making it possible for people to build intelligent machines that can learn from past experiences and use them to address a problem in real-time. Typically, without AI techniques, computer programs are designed to depend on a pre-coded set of instructions to complete a task (Jakhar & Kaur, 2020; Paudel, 2016). If the input data is the same, then the program will always produce the same results regardless of the number of times it is run. In contrast, ML allows computers to complete tasks and gradually improve themselves as they come across more data (Anwar & Hassan, 2017;

Jakhar & Kaur, 2020; Salloum et al., 2020). It is, therefore, possible that the same inputs can generate different results as time progresses. The figure below illustrates the relationship between deep learning, machine learning, and artificial intelligence.

Figure 1.1

Relationship Between Artificial Intelligence, Machine Learning, and Deep Learning


Artificial Intelligence
Machine Learning
Deep Learning
Ability of machine to imitate human intelligence
Algorithms to incorporate intelligence into machine by automatically learning from data
Algorithms that mimics human brain to incorporate intelligence into machine

Source: Analytics Vidhya (2021)

One of the potential benefits of AI in the cybersecurity field is that it is more accurate and faster, which makes it more effective in providing real-time detection and neutralisation of threats (Taddeo, 2019). Cybersecurity threats have become more complicated and destructive, hence necessitating speedier responses because a single second can save an organisation from losing crucial information. AI can significantly help discover hidden and complex techniques and vulnerabilities to a system or network by analysing massive data and using the derived results to categorise various computer threats. According to Dilek et al. (2015), an AI system is capable of detecting malpractices such as intensive utilisation of network resources such as memory, processors and bandwidths, unusual and questionable traffic, and suspicious connections, among other suspicious activities on the network. The AI-based cybersecurity system then takes the appropriate immediate response, including prompting the administrators to take the appropriate actions.

Evidence further indicates that AI can be used in an Intrusion Prevention System (IPS) whereby it can actively neutralise the identified threats by stopping processes from running, blocking IP addresses, stopping suspicious transactions, and so on (Abdulqadder et al., 2020; Taddeo, 2019). Its ability to continually update itself with more input data also implies that it can evolve with cybercriminals techniques. All these capabilities point to AI's potential to positively impact efforts to improve cybersecurity. As observed by Mohammed (2020), AI is increasingly being integrated into business practices and systems, especially in the information technology and telecommunication sectors. He further established that “45% of big enterprises and 29% of small and medium-sized enterprises” have used AI in their operations (p. 172). These statistics indicate that AI’s importance is growing substantially. However, the fact that AI systems are also susceptible to cyber-attacks indicates that they could also have undesirable effects that could prevent their adoption/use in most organisations (Hartmann & Steup, 2020; Sedjelmaci et al., 2020). To this end, this study aims to comprehensively investigate the matter and shed light on the factors influencing the intention to adopt AI cybersecurity systems in the UAE at the individual level.

Generally, AI cybersecurity adoption is the process of integrating artificial intelligence (AI) into cybersecurity systems and processes. This can involve using AI to automate tasks, detect and respond to threats, and improve decision-making.

1.2 Background of the Study

The advent of automation technology in the early 20th century played a critical role in the emergence of the concept of artificial intelligence (AI) and AI theory in the mid-20th century. During this period, the term was primarily used to refer to the process through which a computer was used to build a sophisticated device that shared vital intelligence features with a human being (Chen, 2019). This definition has, however, evolved considerably over the years. For instance, Shenoy (1985) (as cited in Chen (2019) defined the term as “an obscure branch of computer science.” Others have described it as the act of making computers do things using intelligence like humans (Chen, 2019). These differences in perspectives indicate that a universal or precise definition of AI is still lacking. Nonetheless, there seems to be a consensus among scholars that the primary concern of AI is the development of machines that can carry out complex tasks that demand human intelligence (Gursoy et al., 2019). This observation implies that AI-based cybersecurity can be described as intelligent systems designed to safeguard computer networks, hardware, programs, and data from unauthorised access, usage, or damage. In this context, the word intelligence refers to the systems' humanlike ability to learn and improve their knowledge over time.

Over the past few years, AI usage has gained significant momentum due to the improvements it brings to the delivery of services and decision-making. Evidence suggests that about 20% of organisations globally have incorporated it in their day-to-day operations (Jakhar & Kaur, 2020; Thomas, 2020). It has been identified as one of the most transformative technologies due to its revolutionising effects on many sectors ranging from transport to manufacturing, government, and research. According to Chen (2019) and Gursoy et al. (2019), AI brings benefits such as improved decision-making and forecasting, as well as automation of tasks. Although other innovations have also played an essential role in the automation of functions since the Industrial Revolution, the incorporation of AI technologies such as machine learning (ML) and robotics has pushed automation to a new level (Gursoy et al., 2019; Jakhar & Kaur, 2020).

They have, for instance, brought the aspect of intelligence and enabled the analysis of voluminous data from multiple sources. These contributions have enabled organisations to improve efficiency, comprehensively view their businesses and the market, and predict growth prospects (Ibrahim et al., 2018). Predictive intelligence also allows organisations to scrutinise and improve processes, thus increasing efficiency, production, revenues, and value. According to Chen (2019), one of the most significant technological paradigms in the use/adoption of AI is the cross-enterprise capability, which connects all the functional entities in an organisation and enhances cross-functional activities to obtain new knowledge. Unlike the previous predictive tools, AI techniques have more predictive abilities, which allow them to get information from numerous sources and link organisational decision-making and dynamic relations with the markets (Chen, 2019).

Recently, organisations across the globe have been grappling with the problem of cybercrimes (offences committed over a network where a computer is used as a tool or is the target) (Gangwar & Narang, 2020; Lee et al., 2018). These offences are usually intended to cause reputational, physical, mental, or financial damages through unauthorised access to confidential data (Sikolia et al., 2018). In particular, crimes perpetuated over the internet have become rampant as organisations continue to rely heavily on computer technologies for different transactions and daily operations. Gangwar and Narang (2020) noted that new technologies have indeed brought new opportunities for cybercriminals to thrive, thus making computer crimes more sophisticated and unpredictable.

Most cybercrimes involve attacks on information related to individuals, organisations, or governments (Arora et al., 2014; Gangwar & Narang, 2020). Though they do not target the physical body, they focus on the individual or virtual organisational entity, including the informational characteristics that identify people on the internet. These identifiers play a critical role in the day-to-day provision of services because people's data are in many computer databases held by either government agencies or business organisations (Diorditsa, 2020; Gangwar & Narang, 2020). As such, while efficiency is enhanced, cybercriminals are also provided with an opportunity through which they can exploit the weaknesses generated by the centralisation of confidential information in networked computers to commit different kinds of crimes (Diorditsa, 2020; Gangwar & Narang, 2020; Lee et al., 2018).

Types of cybercrimes are many, and they evolve daily with technological advancement. Some of the most common types of cybercrimes include hacking (such as cross-site scripting, theft of FTP passwords, and SQL Injections), virus dissemination, logic bombs, denial-of-service (DoS) attacks, phishing, email bombing and spamming, web jacking, cyberstalking, and identity theft and credit card fraud (Group Pvt, 2021; Kumari, 2020). As Kumari (2020) notes, identity theft occurs when a cybercriminal steals the identity of a system user and pretends to be the legitimate user to access resources such as bank accounts and credit cards. The criminals may also use the stolen identity to commit other crimes. According to Group Pvt (2021), identity theft and credit card fraud are among the most common types of cybercrimes, where 4.8 million identity theft and credit card fraud cases were reported to the Federal Trade Commission (FTC) in the USA alone. These incidences led to an estimated loss of $4.5 Billion. Phishing attacks are also common at the corporate level, whereby a survey conducted in 2020 in the USA indicated that 74% of the surveyed organisations experienced a successful phishing attack. This type of cybercrime involves extracting confidential information such as usernames, passwords and credit card numbers while masquerading as a legitimate enterprise (Federal Trade Commission, 2021).

Some cybercrimes, such as breaches of individual or corporate privacy, have recently become common, with criminals seeking to destroy the integrity of information stored in digital databases or use it to blackmail the victims (Arora et al., 2014). The recent past has also witnessed an increase in cases related to identity theft. This kind of crime involves stealing personal identification details such as users' names, addresses, credit card/bank account numbers, passwords, and social security numbers, among other details, for use in an economic crime (Al-Khater et al., 2020; Diorditsa, 2020; Torten et al., 2018). A study conducted by McCoy and Hanel (2018) revealed that a total of 16.8 billion US dollars had been lost to identity theft crimes in 2017. It further established that over 16.7 million US consumers were victims of this vice (McCoy & Hanel, 2018).

The amount of money directed towards cybersecurity (protection of computer systems and data from cyber-attacks) has also increased considerably, with the available research indicating that organisations could be spending an average of $50,000 per attack (Bawany et al., 2017; Farahbod et al., 2020). What is worrying is that despite this considerable investment, the world is still witnessing a rapid increase in cybersecurity issues. This situation is forcing organisations worldwide to adopt human-centred measures, whereby the principal focus is placed on altering users' behaviours rather than the exponential number of increasing threats (Patil, 2016). While this approach can help create awareness and identify behavioural abnormalities, it leaves the organisation with no exclusive control of security. Therefore, a more efficient and robust cybersecurity approach is becoming a necessity rather than an option for organisations seeking to improve their cybersecurity (Farahbod et al., 2020; Johnson, 2020).

The ever-escalating threat of cybercrimes may call for mandatory adoption and use of cybersecurity systems, especially in government and semi-government organisations. As noted by Kaur et al. (2023), several approaches can be used to ensure organisations use AI cybersecurity systems instead of the traditional methods of curbing cybercrimes. One of the most notable approaches that may be used is reviewing security policies and documentation. This may involve examining an organisation's cybersecurity policies and making appropriate amendments to ensure that AI-powered cybersecurity systems are endorsed as the appropriate mechanisms for countering cybercrimes instead of the traditional methods. With the appropriate policies, Mijwil and Aljanabi (2023) suggest that enforcing AI cybersecurity systems in organisations would be easy. Another technique that may be used to enforce the use of AI cybersecurity systems in organisations is advocating for best cybersecurity practices, with adopting AI cybersecurity systems as one such practice. According to Mijwil and Aljanabi (2023), advocating for the best cybersecurity practices may involve sharing knowledge and resources with organisations to allow them to make informed decisions on countering cybercrimes (Kaur et al., 2023). These two measures, among others, may play a leading role in ensuring that organisations use AI cybersecurity systems instead of traditional ones.

1.3 Research Problem

As mentioned in the previous section, cybersecurity threats are one of the primary challenges affecting organisations across the globe (Gangwar & Narang, 2020; Lee et al., 2018). Despite the considerable investment directed at this field, the threats show no signs of slowing down. Instead, the threats are becoming more complex as technology advances (Steinbart et al., 2018; Tejada, 2020). As a result, businesses and government agencies are losing significant amounts of money to cyber criminals, hiring computer security professionals, and/ or implementing defensive measures to address the problem. For instance, efforts geared towards tightening cybersecurity were found to have cost businesses around the world an average of 3.8 to 16.8 million US dollars per organisation in 2017 (Taddeo, 2019). The situation, however, did not improve because, in 2018, more than 2.6 million people reported new types of cyber-attacks in their day-to-day activities (Farahbod et al., 2020; Taddeo, 2019).

In the UAE, research conducted by the DarkMatter Group in 2019 indicated that the country is a victim of about 5% of the entire world's cyber-attacks, with the past five years recording a 55% increase in such attacks (DarkMatter Group, 2019). It has also been established that the country suffers from several cybersecurity vulnerabilities, highlighting the need for concerted efforts to address the problem (DarkMatter Group, 2019; Guven, 2018). The findings by Guven and the DarkMatter Group indicated that cybersecurity threats in the UAE and other Middle Eastern countries have become both widespread and regularly undetected. Criminals have also been targeting the region's critical infrastructure, thus placing its security and that of the population at a much higher risk. The DarkMatter Group report further noted that most of these threats were intended to cause espionage or disruption of services, with spear-phishing being the principal tactic used to access the targets (DarkMatter Group, 2019).

A related study conducted by the UAE's Telecommunication Regulations Authority (UTRA) further established that more than 86 new cyber-attacks were encountered at the start of 2018, with the Careem data violation topping the list. The Careem cyber-attack is reported to have put the data of more than 14 million accounts to unauthorised users, thus placing them under significant threat (as cited by Chandra et al., 2019). Research also indicates that the UAE is among the top 20 countries at the highest risk of malware-class attacks through online infection (see Table 1.1). UAE is also a leading target for cybercriminals employing other techniques of cybercrime. Transaction-based offences such as credit/debit card fraud are also reported as the costliest techniques in the country, accounting for at least $1,000 per user (Chandra et al., 2019). However, individual customers were not the only victims because organisations were also found to have suffered, especially from denial-of-service (DDoS) and malicious software attacks (Chandra et al., 2019).

Table 1.1

Top 20 Countries at the Highest Risk of Malware-Class Attacks

Rank	Country	% of users attacked **
1	Algeria	11.2052
2	Mongolia	11.0337
3	Albania	9.8699
4	France	9.8668
5	Tunisia	9.6513
6	Bulgaria	9.5252
7	Libya	8.5995
8	Morocco	8.4784
9	Greece	8.3735
10	Vietnam	8.2298
11	Somalia	8.0938
12	Georgia	7.9888
13	Malaysia	7.9866
14	Latvia	7.8978
15	UAE	7.8675
16	Qatar	7.6820
17	Angola	7.5147
18	Réunion	7.4958
19	Laos	7.4757
20	Mozambique	7.4702

Source: Kaspersky (2020)

As the country transforms into a smart nation by integrating technologies such as the Internet of Things (IoT) and Cyber-Physical Systems (CPS), robust cybersecurity will increasingly become necessary. Expanding digital infrastructure will undoubtedly create more opportunities for cybercriminals to exploit and make UAE a significant target for cyber-attacks. What is worrying is that despite this realisation, there are still organisations with weak cybersecurity practices. For instance, some of the strategies adopted to combat the threats include human-centric efforts such as creating awareness, fostering cybersecurity research, and developing an incident report framework and international cooperation (Al-Khater et al., 2020; Guven, 2018). However, as indicated earlier in this chapter, the amount of data that must be analysed to detect threats has increased beyond human capacity to process, thus highlighting the need for intervention from intelligent machines.

The revolutionising effects of AI technologies in other fields are opening the eyes of both private and public organisations to the realisation that AI could improve cybersecurity and mitigate the impacts of cybercrimes. The sluggish adoption and use of AI cybersecurity systems is witnessed despite the fact that various reports have in the recent past ranked UAE (both in the private and public sectors) among the countries that have been quickly embracing emerging technological trends such as digital identity, robotic process automation (RPA), intelligent automation, and blockchain technology (Desk, 2020; The Arab Weekly, 2018; Wilson, 2020). For example, a recent report published by Datatechvibe indicated that 98% of UAE organisations consider AI vital to their resilience and ability to withstand economic uncertainties (Datatechvibe, 2023). To this end, they have invested heavily in the establishment of data science platforms for developing and maintaining AI models. The same report suggested that 68% of UAE organisations have invested almost 50% of their technology budget on programs related to AI. Some of the organisations that have embraced AI in their operations include Emirates NBD, Dubai Police, and Emirates Airlines. However, none of them has used AI in cybersecurity field. This selective adoption and use of technologies in particular sectors raise curiosity among scholars who want to understand what factors could be influencing such behaviours among Emiratis (Desk, 2020; The Arab Weekly, 2018; Wilson, 2020).

The slow rate of adoption and use of AI-based cybersecurity systems may emanate from employees' reservations about new semi-autonomous technologies with humanlike intelligence like AI. Various studies have indicated that employees consciously or unconsciously resist digital transformation, especially when they fear that the new technology will threaten their jobs (Bhargava et al., 2021; Nam et al., 2020; Tabrizi et al., 2019). According to Tabrizi et al. (2019), the fear of losing status or job security is one of the main factors that make employees consciously or unconsciously resist a technology that may appear to threaten their jobs. Similar sentiments were made by Nam and colleagues, who noted that employees might not be comfortable with a new technology or change because of perceived job insecurity. Though Bhargava et al. (2021) observed that humans and AI would have to work hand in hand and that "human touch" and "soft skills" cannot be replicated by AI and automation, the authors noted that most employees still perceived such technologies as a threat, not as an opportunity. As a result, they are likely to resist the adoption and use of such technologies.

The employees' reservations could also emanate from having a negative attitude towards the new technology. According to Losova (2014), users' intention to use a new system is significantly influenced by the extent to which they like or dislike the system based on their perceptions. In this regard, if a technology is perceived as beneficial, pleasant, or good, potential users will likely develop an interest in using it. When the new technology or system is perceived as harmful, bad, or unpleasant, potential users will likely dislike it and not develop an interest in using it. This observation implies that in the context of the present research, where users are supposed to accept AI cybersecurity systems voluntarily, users can only embrace and use the systems if they perceive them to be beneficial; hence, they have the right attitude towards them.

Past research on implementation of information technologies and systems has shown that users' acceptance and attitudes towards the system play an indispensable role in such a process (Chaudhry, 2018; Ngeno et al., 2021; Taherdoost (2019); Taherdoost et al., 2012); these studies have shown that factors such as subjective norms, self-efficacy, usefulness, and ease of use, among other factors can explain and predict user acceptance (Hoong et al., 2017; Lai, 2017; Ramayah et al., 2020). Indeed, scholars in the fields of sociology, psychology, and information systems have proposed numerous theoretical models for explaining and predicting user acceptance of a new technology or system. Some of the widely-cited theories include the technology acceptance model (TAM), the unified theory of acceptance and use of technology (UTAUT) model, the protection motivation theory (PMT), and the task-technology fit (TTF) model, among others. The majority of these theories have closely related features. For instance, TAM’s perceived usefulness, PMT’s perceived response efficacy, and UTAUT’s performance expectancy are closely related components (Chiyangwa & Alexander, 2016; Lee et al., 2018; Sari et al., 2018).

Though the above-stated theories have been widely used, their capability to explain and predict the acceptance of some modern technologies, such as AI, among organisations and individuals is still in doubt. According to Lu et al. (2019), some elements in the previous user acceptance and technological implementation models are irrelevant or inapplicable to the emerging smart technologies such as AI, which have humanlike intelligence; this is because the existing theories had initially been developed to adopt non-intelligent technologies. In their study, which investigated the factors influencing the adoption of AI devices in service delivery, the authors noted that some constructs of the existing theories, such as *perceived usefulness* and *ease of use*, were not relevant in predicting customers' willingness to accept AI devices. This is because AI devices are designed to interact with users like real humans (Lu et al., 2019; Gursoy et al., 2019).

The observations above imply that more research on modern intelligent technologies is needed in order to develop relevant, comprehensive models that explain and predict the psychological factors influencing users' intention to adopt such technologies. So far, there is limited research on the multifaceted smart/intelligent technology acceptance, while the available few studies in this area utilise the previous technology acceptance theoretical models, which contain some irrelevant elements. This makes it difficult for researchers to understand, explain, and predict the reasons behind the slower adoption of AI-based cybersecurity systems in the UAE public sector compared to other sectors that have registered significant growth in the adoption of emerging technologies. In this regard, there is a need to conduct more research to empirically determine the reasons behind such trends and developments.

Furthermore, while the available literature has attempted to shed some light on the impacts that some aspects of AI could have on cybersecurity, research on the factors influencing the Emiratis' intention to adopt/use AI cybersecurity systems is still lacking. Most of the studies conducted on artificial intelligence have focused on the potential of AI in the UAE (Singh & Shaurya, 2021), UAE's artificial intelligence strategies and pursuits (Chandra et al., 2019; Khan, 2019), and some of the measures that UAE is embracing to tackle cybersecurity threats (Al-Qudah, 2021; Almarzooqi, 2019). The present study, therefore, seeks to bridge this gap and promote an understanding of what ought to be done in the United Arab Emirates to enhance the acceptance of AI in the field. The problems that the study seeks to solve, therefore, include the following:

i) Apathy in adopting and using AI-based cybersecurity systems in the UAE (Azar & Haddad, 2019; De Bellis & Johar, 2020; Cherrayil, 2019; Dubai World Trade Centre, 2021; TahawulTech, 2019; Nhede, 2021).

ii) Lack of an empirical study that has examined why there is low user adoption/use of AI cybersecurity frameworks in the UAE.

Based on these problems or research gaps, the present study sought to partly adopt and extend the existing technology adoption models to develop a research framework that would help to investigate the factors influencing the intention to adopt AI-based cybersecurity systems in the UAE. In this case, several technology adoption models were explored (as discussed in the next chapter (section 2.5)), and constructs/variables deemed relevant to an AI-related technology were incorporated into the research framework. PMT and UTAUT emerged as the most suitable models for the present study, meaning that most of the constructs used were derived from them. The resulting framework included the intention to adopt/ accept AI cybersecurity systems as the dependent variable, while 12 variables derived from the protection motivation theory (perceived vulnerability, perceived severity, perceived response efficacy, and perceived self-efficacy), UTAUT (social influence, facilitating conditions, and effort expectancy), and the available literature (resistance to change, attitude towards AI security systems, AI knowledge, and job insecurity) as the independent variables. Besides serving as an independent variable, attitude towards AI security systems is anticipated to mediate the effect of the above-stated variables (social influence, facilitating conditions) on the users' intention to accept AI cybersecurity systems in the UAE. A thorough discussion of these variables and the reasons justifying their use are provided in chapter two.

1.4 Research Questions

To address the research problem highlighted above and bridge the identified literature gap, this study sought to investigate the factors influencing the intention to adopt AI cybersecurity systems in the UAE's workplace at the individual level. The following research questions guided the study:

i) What is the influence of PMT’s constructs (perceived vulnerability, perceived severity, perceived self-efficacy, and perceived response efficacy) on users' intention to use AI cybersecurity systems at workplaces in the UAE?

ii) What are the impacts of UTAUT’s constructs (social influence, facilitating conditions, and effort expectancy) on users' intention to use AI cybersecurity systems at workplaces in the UAE?

iii) What is the relationship between user attitudes toward AI cybersecurity systems and users’ intention to adopt AI cybersecurity systems?

iv) What is the relationship between AI knowledge, resistance to change, job insecurity, and users’ intention to adopt AI cybersecurity systems?

v) What is the mediating effect of users' attitudes on users' intention to adopt AI cybersecurity systems?

1.5 Research Objectives

In particular, the study sought to meet the following objectives:

i) To determine the influence of PMT’s constructs (perceived vulnerability, perceived severity, perceived self-efficacy, and perceived response efficacy) on users' intention to use AI cybersecurity systems at workplaces in the UAE.

ii) To assess the impacts of UTAUT’s constructs (social influence, facilitating conditions, and effort expectancy) on users' intention to use AI cybersecurity systems at workplaces in the UAE.

iii) To establish the relationship between user attitudes toward AI cybersecurity systems and users’ intention to adopt AI cybersecurity systems.

iv) To establish the relationship between AI knowledge, job insecurity, resistance to change, and users' intention to adopt AI cybersecurity systems.

v) To investigate the mediating effect of users' attitudes on users' intention to adopt AI cybersecurity systems.

1.6 Scope of the Study

This study's scope was limited to individuals working in UAE government and semi-government organisations, specifically in the information technology (IT) departments, in charge of organisations' cybersecurity. A limited scope was deemed necessary due to time and resource constraints, as well as the need to comprehensively investigate the subject matter. One of the principal reasons the study focused on individuals in charge of cybersecurity of UAE-based government and semi-government organisations was the increased attention the country has received from cyber-attackers. It is worth noting that using AI technology in such organisations is not mandatory, meaning employees are free to accept or not accept and use the technology. This made it necessary to assess the willingness of the employees in such organisations to embrace and use AI-based cybersecurity technology.

Research shows that the country's critical organisations have been the primary targets for cybercriminals in the recent past, and they have been incurring significant losses in terms of money and data due to cyber-attacks or investments in security measures (Azar & Haddad, 2019). For instance, inside knowledge from some companies suggests that ransomware attacks have increased considerably, but their details have yet to reach the public domain. It has also been established that the number of UAE organisations that have embraced AI in their cybersecurity framework is considerably low (Azar & Haddad, 2019), yet the government and semi-government organisations in the UAE are quick to embrace new technologies (Wilson, 2020; The Arab Weekly, 2018; Desk, 2020). All these findings highlighted the need for research that could get to the bottom of the matter and establish the factors that affect users' (IT personnel and persons in charge of protecting organisations from cyber threats) decisions regarding the incorporation of AI.

1.7 Significance of the Study

The results made in the present study may benefit society, considering that cybersecurity is one of the most critical aspects of the modern world, characterised by globalisation and the massive use of the internet. They are expected to help developers and organisations intending to adopt AI-based cybersecurity systems understand some of the critical factors or aspects to consider to encourage massive adoption of such systems in the fight against cybercrimes. The study could also be of great importance to proponents or researchers since it provides a foundation for studying factors influencing the adoption and use of semi or fully-autonomous technologies with humanlike intelligence, such as artificial intelligence. Further details about the present study's theoretical contribution and practical implications are provided in the subsections below.

1.7.1 Theoretical contributions

Apart from the benefits described in the problem justification section, the present study's findings are expected to make significant academic contributions. For instance, they could aid in developing a cybersecurity model that organisations could use when incorporating AI-related technologies into their information security systems to increase the probability of their employees' and other users' acceptance. To the best of the researcher's knowledge, there is currently no model/theory established to shed more light on the factors that influence the adoption of AI in cybersecurity measures, and there is scant literature concerning the adoption of AI technology and devices in general. The study could, therefore, lay the foundation from which such models can be developed. This study is also expected to contribute to theory development by introducing three new variables (AI knowledge, resistance to change, and job insecurity) to PMT and UTAUT. These variables have not been integrated before in the context of the two models which underlie the study.

With most of the reviewed studies deriving their findings from hypothetical situations and small samples, their reliability is questionable. This problem has been addressed by the present research, considering that it has enriched the existing body of literature regarding the factors influencing users' intention to adopt cybersecurity systems. The sample used during the survey was big enough to allow the generalisation of the results, while the reliability of the findings was enhanced by conducting the research in a practical setting. As such, the organisations involved could, therefore, adopt the recommendations given and use them to improve the acceptance and use of AI in their information security infrastructure. It has also been established that despite the realisation of AI's potential to revolutionise many industries, how it is used and what affects its acceptance and usage have not received sufficient attention from scholars. Therefore, insights gained from this study could create a basis from which further studies can be conducted in the future.

1.7.2 Practical implications

As previously indicated in this chapter, cybersecurity issues have emerged as one of the most significant concerns affecting individuals and organisations across the globe. Individuals, businesses, and government agencies are losing substantial amounts of money to cyber criminals or through investments in efforts meant to protect computer systems against cyber-attacks. Therefore, the results obtained from this study could go a long way in promoting an understanding of the status of cybersecurity in the UAE and the measures being implemented to curb cyber threats. They could also be an eye-opener to managers and government policymakers in terms of what they are supposed to do to ensure that AI is successfully integrated into cybersecurity at both the individual and organisational levels.

The study sheds light on the factors hindering/promoting the incorporation of AI into cybersecurity technologies, thus providing practitioners with new insights on how cybersecurity defence can be strengthened to save individuals, businesses, and the government billions of money. It has also been established that one of the challenges affecting the cybersecurity sector is the lack of enough qualified professionals to handle the threats (Furnell et al., 2017). As such, AI could help organisations in their efforts to bridge the skills gap. UAE organisations could use the findings presented to develop measures for enhancing the adoption and acceptance of AI cybersecurity systems in workplaces.

Evidence from the available body of knowledge suggests that AI technologies are yet to reach their full potential and that machine learning and deep learning techniques will continue, making them more powerful (Kaja, 2019). Also, society and cybercriminals are evolving rapidly, which implies that cybersecurity personnel cannot afford to be left behind. They must change their tactics to stay ahead of the threats, or else criminals will outsmart them. To this end, results obtained from this study could provide a wake-up call to realise the magnitude of the task ahead and how the acceptance of AI may help individuals and organisations improve their cybersecurity.

1.8 Definition of the Constructs and Key Terms Used

Cybersecurity – refers to the practice of protecting computers, mobile phones, networks, applications, and digital data from unauthorised access or exploitation by malicious people (Kansagra et al., 2016).

Behavioural intention- refers to the extent to which users intend to use technology (Gursoy et al., 2019).

Facilitating conditions- refer to the technical infrastructure and organisational resources necessary for the adoption and use of new technology (Gursoy et al., 2019).

Perceived vulnerability- refers to how susceptible an organisation or individual feels to a given threat/ risk (Wong et al., 2016).

Perceived severity- refers to the adverse consequences an organisation or individual links to an outcome or event, such as a security breach (Wong et al., 2016).

Effort expectancy- refers to how easy or difficult it is to use new technology (Chiyangwa & Alexander, 2016).

Social influence- refers to the extent to which other important organisations or individuals believe an individual or organisation should use a technology (Gursoy et al., 2019).

Subjective norm- refers to the perception of others' approval or disapproval of a behaviour (Bautista et al., 2018).

AI knowledge- Having a technical/ in-depth understanding of how it works and can even run an AI-based cybersecurity system (Safa et al., 2015).

Perceived response efficacy- The belief that specific processes (AI) will mitigate the threat. It assesses how effective an individual believes the coping response is in averting the threat (Sikolia et al., 2018).

Perceived self-efficacy- an individual's idea of their ability to implement the necessary actions to mitigate the threat. It assesses how confident an individual believes he/she can perform the coping response (Sikolia et al., 2018).

Job insecurity- An individual's fear/ uncertainty of losing their job due to being replaced by technology (Stettner, 2018).

Attitude towards AI security systems- An individual’s positive or negative feelings towards a behaviour (Jain, 2014).

Resistance to Change (RC)- generalised disapproval of change due to its suspected adverse effects (Bhattacherjee & Hikmet, 2007).

1.9 Structure of the Thesis

This thesis consists of five different chapters. The first chapter focuses on the introduction and background of the research topic. It includes the problem statement, research aim and objectives, research questions, research justification, study scope, theoretical implications, and the definition of the key terms used. The second chapter comprehensively reviews the existing body of knowledge regarding artificial intelligence and cybersecurity. The third chapter presents the methodology used to collect and analyse data, while chapter four offers an analysis and discussion of the findings obtained from the research, as well as the strengths and limitations of the study. Concluding remarks, recommendations, and directions for further studies are then provided in the final chapter (Chapter 5).