

LEVEL 7 ASSESSMENT SPECIFICATION

Student name:	Chiang Chun Wah	Student ID number:	2119645
Programme:	DBA		
Module:	Converting Research into Practice		
Module code:	HKBM7020	Contribution to Overall Module Assessment (%):	100%
Lecturer:	Dr Alice Te	Internal Verifier:	Prof. Eddie Yu
Assignment Title:	Impact of Machine Learning on Cybersecurity Operational Efficiency in Banking of Hong Kong – Moderating Role of Transformational Leadership	Word count (or equivalent):	7,500 words (+/-10%)
Submission deadline:	17 February 2025	Return date of provisional marks & written feedback:	17 March 2025 (Tentative)
Submission method:	All written assessments, where practical and possible, must be submitted via Turnitin unless otherwise instructed by the Lecturer. (Please DO NOT put this assessment specification into Turnitin or it will match many similarities with other students' submissions.) Alternative submission method (if applicable): Late submission of the assessment will result in a late penalty mark.: Work which is submitted up to 1 week late will be capped at 50% for the first attempt and will be awarded a mark of 0% for re-assessment. Late submission penalties may be lifted only if there is an approved extenuating circumstances claim. Work submitted more than 1 week late will be considered as a non-submission and will not be marked. The work may be considered as a submission for reassessment if offered by an Examining Board or if there is an approved extenuating circumstances claim.		
Academic honesty / referencing:	Academic honesty is required. In the main body of your submission you must give credit to authors on whose research and ideas your work is based. Append to your submission a reference list that indicates the books, articles, etc. that you have used, cited or quoted in order to complete this assessment.		

Research Proposal - Impact of Machine Learning on Cybersecurity Operational Efficiency in Banking of Hong Kong – Moderating Role of Transformational Leadership

Student Name (ID): Chiang Chun Wah, Ray (2119645)

Programme: University of Wales Trinity Saint David – DBA

Module: HKBM 7020 Assignment

Lecturer: Dr. Alice Te

Table of Contents

1. Introduction.....	4
1.1 Trend and Significance.....	5
Trend.....	5
Significance.....	7
1.2 Research Background.....	7
Research Aim	9
Research Objectives.....	9
2. Literature Review	11
2.1 Machine Learning Techniques	12
2.2 Machine Learning for Cybersecurity Applications	14
2.3 Transformational Leadership Style for Innovation.....	17
2.4 Theoretical Framework.....	18
2.4.1 Background Theory	18
2.4.2 Factors in Satisfaction of Machine Learning.....	22
2.4.3 Summary of Theoretical Framework.....	24
3. Research Design	26
3.1 Research Philosophy and Approach	27
3.2 Research Methodology	27
3.3 Summary of Research Design	29
4. Expected Result.....	30
5. Research Work Plan.....	31
Reference List.....	32

List of Tables

Table 2.1: Summary of Studies Analysis.....	19
Table 2.2: Summary of Hypothesis.....	25
Table 5.1: Timeline of Work Plan	31

List of Figures

Figure 1.1: Loss of Cyberattack from 2018 to 2028.....	6
Figure 2.1 Research Framework	22
Figure 3.1: Research Flow for this Research	26

1. Introduction

Considering ongoing technological advancements and the ever-evolving business environment, it is imperative for organizations to dynamically reassess and realign their business strategies to adapt to external changes. This adaptive process often involves integrating technology into various aspects of business operations and everyday tasks, unlocking new opportunities to sustain a competitive edge (Ancillai *et al.*, 2023). Over the past decade, breakthroughs in areas such as digitalization, cloud computing, and artificial intelligence (AI) have had a profound impact on enterprises, leading to significant transformations and presenting both challenges and a lot of opportunities for growth and innovation (Chen, Wu and Zhao, 2023). For instance, cloud computing achieved widespread adoption by businesses just five years after its introduction. Similarly, AI technologies, including image and speech recognition and chatbots, began to emerge in 2016, culminating in the launch of next-generation AI solutions, like ChatGPT, by 2022 (Leme Lopes, 2023). Considering rapid technological advancements, organizations must comprehend sustainable innovation and evaluate the relevance of these technologies within their respective industries. Understanding and exploiting technological capabilities is vital for contemporary enterprises to develop in a dynamic market. By integrating these advancements into their business strategies, organizations can better position themselves to seize opportunities and maintain their competitive edge; failure to do so may result in a loss of industry leadership. Ultimately, integrating these edge technologies is not operating with the trend but a critical strategy for enhancing operational capabilities and sustaining competitive advantage.

AI is set to be the disruptive technology with the force of the next decade, mainly due to its ability to enhance human capabilities at a low cost (Kelly, Kaye and Oviedo-Trespalcacios, 2023). Bogatinovski *et al.* (2021) pointed out this technological advancement that is anticipated to improve everyday life by advancing information technology, and Murphy *et al.* (2021) further determined it positively impacts critical sectors such as healthcare, customer service, education, and transportation. Following its popularity, generative AI (GenAI) has emerged as a significant player within the AI landscape, drawing considerable attention and study. Tools like ChatGPT and Copilot exemplify this innovation, using machine learning to generate text, video, and music by leveraging existing data (Alamleh, Alqahtani and Elsaid, 2023). Most organizations (71%) that have adopted AI solutions report substantial returns on investment within just 14 months (Korolov, 2024).

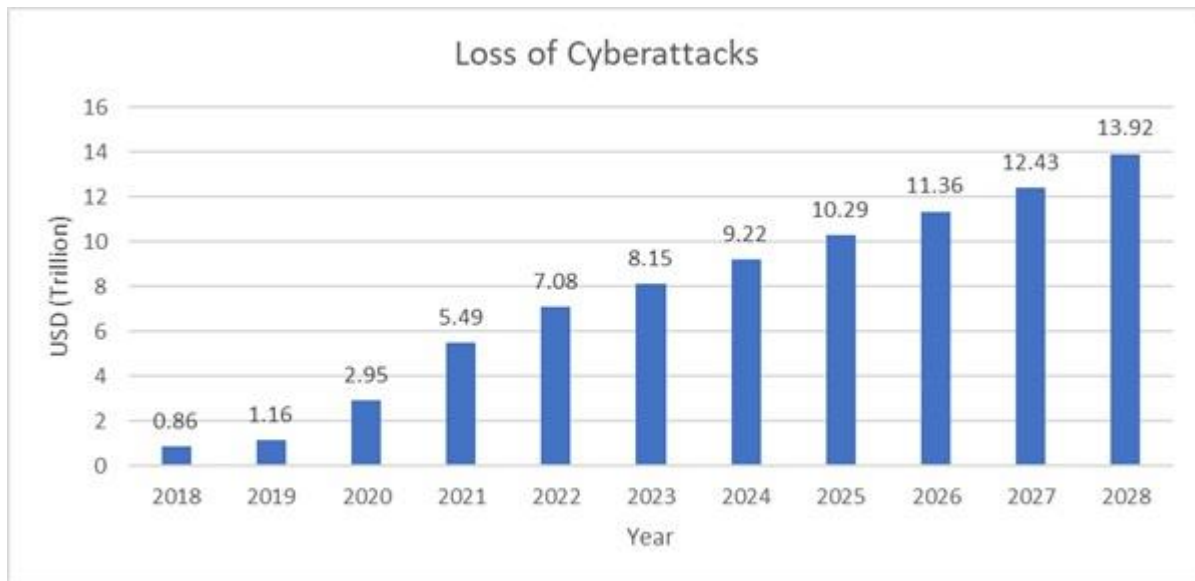
Furthermore, the previous study showed that workers who use AI tools have a 14% increase in productivity; specifically, less skilled and experienced employees have up to 35% gain. Conversely, seasoned professionals have demonstrated a 59% increase in efficiency when writing business documents per hour (Noy and Zhang, 2023), while coding software projects have seen a remarkable 126% efficiency improvement (Peng *et al.*, 2023). However, technology presents a dual challenge; while AI enhances organizational productivity, it can also be exploited for cyberattacks and criminal activities. According to Angela Romei (2024) surveys indicate that 37% of cyberattacks are attributed to AI-generated actions. Thus, while AI holds the potential to drive business growth when applied correctly, it also poses significant risks that could jeopardize organizational interests if mismanaged.

1.1 Trend and Significance

Trend

Cyberattacks can harm organizations, including data loss, financial repercussions, theft of intellectual property, system inaccessibility, leakage of personal and secret information, fraudulent transactions, interruption of business operations, and data and system recovery efforts. Additionally, such attacks can severely harm an organization's reputation. Since 2006, organizations have increasingly faced significant risks associated with cyberattacks (CSIS, 2024). Current estimates indicate that approximately 2,220 cyberattacks occur daily, culminating in over 800,000 incidents yearly (Charlton, 2024). The impact of these attacks can vary, ranging from minor disruptions in operations to substantial financial losses. Regardless of the nature of the cyberattack, each associated consequence incurs a specific cost, whether financial or otherwise. According to Statista (2024) report, they projected that the financial impact of cybercrime is expected to rise dramatically in coming four years, with losses anticipated to grow from around \$9 to \$14 trillion, that is shown in Figure 1.1. This trend underscores the importance of organizations developing a robust cybersecurity framework to mitigate security risks and safeguard their assets.

Figure 1.1: Loss of Cyberattack from 2018 to 2028



Technology has undeniably enhanced our lives and economic systems; however, it has also empowered hackers by providing them with advanced tools. Historically, cybercriminals relied on traditional phishing and social engineering techniques to deceive their targets. In recent years, artificial intelligence (AI) has allowed hackers to create convincing simulations of video and voice, thereby facilitating cyberattacks that effectively gain victims' trust. This trend poses an escalating threat as hackers increasingly adopt AI and machine learning (ML) technologies. The first instance of an AI-driven cyberattack was identified in 2017 (Yamin *et al.*, 2021), highlighting the growing sophistication of these threats. An organization in India had a security breach where basic pattern recognition methods were used to understand the behavior of standard users in the network (Rosenbush, 2017). The malware therefore was able to emulate the behavior of the users thus making it difficult for the security systems to detect the malware as an intruder. In general terms, a cyberattack is the deliberate and coordinated attempt by one party to gain access to the computer networks of another party. Presently, companies face various cyber incidents, for instance, ransomware attacks, phishing scams, viruses, application of weak passwords, and social engineering. These incidents can lead to severe consequences, causing operational disruptions and substantial financial losses. Notably, a cyberattack on China's Industrial and Commercial Bank of China (ICBC), the largest bank in the world, and a ransomware incident that impacted the U.S. Treasury markets underscore the potential risks (Kharpal, 2023). In a striking case from 2024, a victim in Hong Kong transferred HKD 200 million to attackers who had successfully used deepfake technology to impersonate the CFO

of the United Kingdom- based multinational company during a video conference (Hoi-ying, 2024). Such incidents highlight the urgent need for organizations to bolster their cybersecurity measures in response to evolving threats.

Significance

The increasing frequency and severity of cyberattacks each year pose significant challenges on a global scale, serving as a critical alert for cybersecurity professionals and organizations alike. This trend shows us the urgent necessity for effective measures to mitigate the threats within the cybersecurity landscape. As such, robust cybersecurity practices are essential for organizations, with effective defenses against cyberattacks vital to a business's overall success. Integrating artificial intelligence (AI) into cyberattacks has further complicated the situation, particularly within Hong Kong's banking sector, where security concerns have heightened (Farayola, 2024). Organizations in this industry are grappling with various cybersecurity challenges, including a shortage of skilled cybersecurity professionals in the labor market (Meineke, 2024). This makes it difficult to recruit experienced individuals to perform the routine security operations. Moreover, many organizations were still using legacy security systems and methods to analyze the threats; however, these approaches often fail to address the urgent external challenges they face effectively. Such outdated methods may prove inadequate against the sophisticated tactics employed in modern cyberattacks (Shwede, Malaka and Rwashdeh, 2023). As a response to this evolving threat landscape, leveraging AI technologies to combat AI-driven cyberattacks is emerging as a critical strategy for the future of cybersecurity (Sarker, Furhad and Nowrozy, 2021). Consequently, organizations must prioritize protecting their IT assets, especially internet-facing systems operating against cyberattacks. This issue must be addressed, and action must be taken immediately. This study explores how machine learning can address challenges and impact on the operation efficiency of cybersecurity.

1.2 Research Background

In the organizations, cybersecurity operations heavily depend on the effectiveness of security systems, employees' experience, and tools designed to quickly and intelligently detect and prevent security incidents. Given the large volume amounts of data handled by various entities, including government bodies, corporations, financial institutions, and healthcare providers,

there is a pressing need for comprehensive cybersecurity technologies and management tools. Cybersecurity encompasses governance, policy formulation, system design, procedural implementation, and ongoing monitoring to safeguard an organization's assets. Mohammadi et al. (2019) studied legacy security systems, such as antivirus, intrusion detection, firewalls, and antispam, are inadequate for addressing the evolving demands of today's security landscape. These systems identify the threats based on the pattern and highly rely on experience to analyze the case one by one. In contrast, artificial intelligence (AI) is an innovative technology with considerable advantages that enhance capabilities in cyber-defense and monitoring. Therefore, this study focuses on AI that integrates into cybersecurity operations, aiming to automate and improve the efficiency of the operations.

Integrating AI within banking operations demonstrates a comprehensive scope, encompassing customer-facing operations and internal processes (Fares, Butt and Lee, 2023). Research conducted by HKMA reveals that 89% of financial institutions have embraced AI technologies (HKMA, 2019). The banking sector appears to be experiencing unprecedented transformation through AI adoption, where approximately 94% of institutions implementing such systems declared strategic alignment with corporate objectives. The fundamental catalysts driving this technological revolution encompass superior customer engagement metrics, enhanced cybersecurity protection, operational cost optimization, and enhanced risk mitigation protocols. This study investigation is propelled by the accelerating digitization phenomena and evolving cybersecurity landscape in banking operations. Machine learning (ML) is a type of AI for use in cybersecurity in the market. Most researchers studied ML nature, but they do not describe how to integrate it into cybersecurity measures (Mohammadi *et al.*, 2019; Helm *et al.*, 2020; Gormont *et al.*, 2023). This research scrutinizes various barriers, privacy concerns, and system reliability while exploring viable solutions for precision and security measures within banking cybersecurity frameworks. Prior academic contributions have extensively documented AI's influence on service delivery optimization and cost reduction initiatives. Contemporary investigations by researchers, including Choithani et al. (2024) enhances customer service and reduce costs, AL-Dosari, Fetais and Kucukvar (2024) faced challenges when implementing it in the bank, and Mishra (2023)'s analytical framework provided a substantial theoretical foundation, Nevertheless, existing literature presents a notable gap regarding cybersecurity implications within Hong Kong's banking infrastructure.

Technology significantly boosts productivity and efficiency within organizations; however, effective leadership is crucial for maximizing the outcomes of technology implementation.

Yating, Sains Malaysia, and Mengjiao (2024) identified the importance of leadership in guiding employees and enhancing their performance within organizations. Leadership entails the ability to influence, motivate, and direct followers or teams toward the achievement of organizational goals and objectives. Consequently, the leadership style adopted is viewed as a moderating factor in this study, particularly in examining the impact of cybersecurity on operational efficiency. This perspective emphasizes the interplay between leadership dynamics and technological integration in fostering a secure and efficient organizational environment.

Research Aim

This research aims to identify ML's operational efficiency within Hong Kong's banking cybersecurity fabric. The usage of ML in cybersecurity frameworks has several implications, all of which are inseparable parts of the unpredictable in the actual situation. A wide range of operational consequences encompasses advantageous and disadvantageous outcomes affecting cybersecurity protocol implementation. Naturally, this will affect the implementation of security protocols. This investigation looks at diverse operational parameters, with security protocols intersecting privacy considerations and assessment frameworks' conformity degrees of accuracy. Through this comprehensive methodological approach, we will delve into an in-depth analysis of these interconnected variables that affect operational efficiency in cyber security.

Research Objectives

The study aims to identify the site where ML is used within the banking information environment and has its primary objectives accordingly. Firstly, an understanding of AI applications and banking information systems provides a broad framework from which we might consider the establishment of a robust security regime (Herrmann and Masawi, 2022). This vision makes it possible to prioritize cybersecurity initiatives and allocate resources effectively, in order that we might address the highest risk points. Second, the study focuses on the utility of machine learning capacity in enhancing the operational effectiveness of cyber-defenses for banks. ML algorithms can learn continuously from emerging trends and threats to provide advice or decisions based on what they have learned. Finally, through an inquiry into the role of machine learning in cybersecurity operations, this study hopes to demonstrate how

ML reduces human interaction time while accelerating detection rates and shortening response times. Ultimately, this reduces the overall costs of running a cybersecurity operation.

To fulfill these objectives, the study poses three research questions:

RQ1: Which capabilities of ML can be used in cybersecurity operations?

RQ2: How does ML affect cybersecurity operational efficiency in the banking industry?

RQ3: What leadership style is advantageous for innovation?

2. Literature Review

By offering in-depth analyses of current research, theories, and practical applications on the merger of Artificial Intelligence (AI), Machine Learning (ML), and Cybersecurity in the Financial Services Industry (FSI), an exhaustive review of literature represents a vital tool for decision-makers. In essence, this review critically evaluates the results and implications of various influential articles dealing with benefits to be obtained, areas of difficulty, and consequences involved in putting into action such integrated strategies. Researchers have seen these twin technologies “AI” and “ML” ushering in a new era for securing the FSI. They point out how these technologies can greatly enhance operational resilience against cyber threats.

The review includes three main areas: (1) an examination of the different machine learning techniques available, (2) how machine learning is applied in cybersecurity, and (3) how transformational leadership contributes to innovation. In order to study literature that makes clear both the advantages and pitfalls of adopting these integrated approaches, an overwhelming number of studies illustrate how AI and ML have revolutionized FSI security, showing their capabilities for automatic identification of conceivable threats, shortened response times to fraud control actions, all while actually improving their effectiveness through this increased automation which combined with real-time monitoring does much more than simply deter those involved in fraudulent activity from attempting to attack you again take pause before either slowly collecting and analyzing the entire vast protective umbrella cocoon will be removed from them.

The literature also reveals significant pitfalls to be avoided. These pitfalls include the need for careful data management, the risk of algorithmic bias in models built along incorrect assumptions, and the ongoing demand to train and refresh ML models to continue adjusting new conditions to emerging cyber threats. More generally, the review thus brings under the one that a number of concrete findings. It indicates chances for improved operational efficiency and, through collating findings like this, also clearly identifies issues that should be considered if AI and ML are to be properly knit into the fabric of cyber protection practices for that industry catchword.

This research was also deeply influenced by a variety of previous studies. These gave us the data needed to get a comprehensive understanding of present research and set the direction for future studies. We believe that understanding the types of threats now being posed will play an important role in guiding practitioners through this complex and rapidly changing digital

environment as it makes its way into an increasingly digital financial marketplace. The insights gained from this review are instrumental for stakeholders aiming to leverage technology for improved security while addressing the multifaceted challenges presented by the digital age.

2.1 Machine Learning Techniques

Machine Learning has different learning methods that the public calls "models." These models include a supervised model, an unsupervised model, a semi-supervised model, and a reinforcement learning model (Taha, 2023). Each of these models has distinct methodologies and approaches for developing algorithms that allow systems to extract insights from the data. This section will sort this out as well as record their application fields respectively.

Supervised Learning

The main objective of supervised learning is to formulate a model which refers to known datasets. In this methodology, the algorithm is designed in such a way as to portray the relationship between inputs and their corresponding output through a dataset that contains both input data that serves as inputs or independent variables and related targets (Sarker, 2021). The idea is to develop a model that understands the relationship between input and output data so that it may forecast the results for new data as well as ones never encountered before. This method is widespread across many fields; for example, it looks at the message content in an e-mail to classify the mail correctly.

Unsupervised Learning

In contrast to supervised learning, unsupervised learning concentrates on datasets without labels. This method tries to find significant patterns and structures in the data without any notion of what output categories there should be (Taha, 2023). The aim is to disclose meaningful groups and generative details from inside the entire dataset universe. Tasks accomplished by unsupervised learning can include clustering, such as likeminded data points together, feature learning, frequency analyses, dimensionality reduction, discovering correlation rules, and anomaly detection. It provides invaluable insight into the inherent structure of data and is often used for exploratory data analysis.

Semi-supervised Learning

Semi-supervised learning merges elements of various learning methodologies by leveraging labeled and unlabeled data (Taha, 2023). This method is most beneficial when there is a shortage of labeled data but an abundance of unlabeled information (Sarker, 2021). Semi-supervised learning uses both types of data to enhance predictability. When forecast accuracy is based on information from these two data sources, Semi-supervised learning is widely used in bioactivity, information classification, and machine translation. This hybrid method capitalizes on the strengths of supervised and unsupervised learning to provide a more robust model.

Reinforcement Learning

Reinforcement Learning focuses on training software agents or machines to make optimal decisions in each environment (Gormont *et al.*, 2023). The agent learns directly from feedback from the decision. Thus, its action will be rewarded based on whether it makes profitable decisions, regardless of whether these are positive or negative. Behind each action taken lies a decisive response from the environment, which allows for evaluation of the effectiveness of that deed considering its outcomes. Reinforcement learning has been widely successful in training AI models for intricate tasks, such as self-driving autos, robot automation in industry and commerce, and supply chain management. However, it is less effective when applied to simple problem scenarios.

In summary, there are several different methodologies within machine learning (ML):

- Supervised learning uses labeled data sets to find the relationship between input and output.
- Unsupervised learning focuses on unlabeled data sets to detect underlying patterns and structures.
- Semi-supervised learning strives to improve prediction accuracy by combining both labeled and unlabeled information.
- Reinforcement learning brings feedback regarding the success of actions taken or not taken into decision-making processes.

Each of these methods has unique characteristics, and each finds application throughout various domains. It is destined to play a significant role in furthering artificial intelligence and automation technology.

2.2 Machine Learning for Cybersecurity Applications

Cybersecurity operations include 3 fundamental sections: prevention, detection, and response (Li *et al.*, 2019). In practice, totally preventing cyber threats is not possible; for instance, one cannot completely stop a hacker developing malware or sending a phishing email. Many ML applications in cyber-defense focus on detection (Apruzzese *et al.*, 2023). According to Sarker (2023), two main approaches to cybersecurity threat identification are signature-based and behavior-based. Signature-based method based on patterns corresponding to known threats. In contrast, behavior-based approaches do not depend on fixed patterns. Instead, they establish a baseline of normal behavior and identify harmful activities that deviate from this norm, interpreting such deviations as potential security incidents. These two approaches are complementary: signature-based methods excel at accurately detecting known threats, while behavior-based methods, despite a higher likelihood of false positives, are more effective at identifying novel attacks. However, those methods cannot detect zero-day attacks effectively, as these attacks do not have historical information that can be referenced. This limitation has prompted the exploration of advanced detection methods. Cybersecurity professionals increasingly leverage AI capabilities, including ML and deep learning (DL) techniques, to identify unknown malware (Martínez Torres, Iglesias Comesaña and García-Nieto, 2019). Within the field of cybersecurity, various threat detection systems are employed to enhance protection measures.

Network Intrusion Detection

Network intrusion detection is used to inspect and analyze the operation of network traffic to determine abnormal traffic or suspicious activities. It operates by looking at all the data packets that are traveling across the network and continually seeks signs that may indicate an intrusion, suspicious behavior, or, indeed, attacks. In 2017, Apruzzese et al. (2017), in cybersecurity research, explored innovative uses of clustering approaches for the discovery of cyber-attacks. Their research included having NetFlow, which is data that encapsulates network traffic-

clustered by analysts looking for behavior over time that is similar to another. It identified hosts whose activities sounded alarms within the traditional network intrusion detection system (NIDS) that was based on human handwriting signatures for threats. Everybody hit heavy things at such times of collision. By including machine learning as a tool to aid in the process, the efficacy of NIDS was greatly advanced. Where the old signature-based system had been able to identify three paltry bad hosts, now, through integration with machine learning techniques, it was able to recognize an astonishingly diverse range of threats. This has expanded realms for detection in the ongoing war against cyber intrusions to previously unseen levels, bringing about greater possibilities and an unprecedented future unknown in other media.

However, Apruzzese's experimental setting is static, relying on the "VirusTotal" feed of samples for the system. VirusTotal is a free online website that allows visitors to submit suspicious files or URLs for analysis. It aggregates results from several antivirus engines and website scanners to obtain an overall appraisal of a file or link's safety. In real-world scenarios, attackers frequently use their wits about them to make disturbances. This makes it hard for technical means to detect their actions. They can completely undermine monitoring mechanisms, usher in the tragic condition of false negatives converting after prolonged incubation and pose dire dangers for entire organizations to slip away unpunished as malcontent. Then they force it from computing to storage mode &, increasingly sophisticated, users change behavior patterns to escape security measures.

Malware Detection

Malware detection is the discovery and analysis of computer viruses, worms, trojans, ransomware, or other malicious software that can harm computers/networks. Malware includes viruses, worms, trojans, ransomware, and spyware. Two basic approaches to malware detection can be discerned: static and dynamic analysis. The static analysis method involves examining a file to determine if it could be potential malware without running through the evaluation process (Gorment *et al.*, 2023). This strategy involves dabbling in the file's properties and putting them under machine learning (ML) models for detailed inspection. In contrast, the dynamic analysis method begins with the file's execution (Gorment *et al.*, 2023). This approach means the suspect file is run inside a controlled environment, known as a "Sandbox", Here, the ML model closely monitors the file's behavior and breaks it down. This twin approach allows organizations to boost their cybersecurity in several ways. Employing proactive detection

strategies. This approach further hardens an organization against potential threats, particularly when combined with proactive and reactive defenses.

Static analysis provides a simple and robust technique for finding known malware and is further enhanced by employing machine learning (ML). Li *et al.* (2017) observed that similar malware samples share common properties, helping to improve classification within the Android operating system. With labeled data, detection precision can be significantly improved. Kalash *et al.* (2018) demonstrated this by achieving an astonishing detection rate of over 99% for Windows malware.

However, a striking limitation of static analysis is its vulnerability to sophisticated attackers: they may change the malware's cover pattern while keeping the core logic intact, which in turn evades detection. Even more deviously, seasoned attackers often create malware capable of altering executable parameters automatically according to the system environment on which they're about to prey. This can set traditional detection methods at naught. This underscores the need for businesses in malware detection strategies to always carry out constant innovation and adaptation.

Phishing Detection

A phishing attack is a form of cybercrime. In this case, the attackers try to get someone to reveal their login name, passcode, and credit card information. The method of deception is usually a fraudulent e-mail, message, or website that looks like it is from another person. Therefore, phishing has become a major everlasting threat to computer security and is often used to break into the computer systems of specific organizations. Alhogail and Alsabih (2021) new classifier for phishing e-mail detection is going to use Graph Convolutional Network (GCN) methods and Natural Language Processing (NLP) on the text. Their paper points to the increasingly severe nature of phishing attacks today, explains why current detection methods are inadequate in this sort of fast-changing environment, and presents an algorithm capable of achieving a detection ratio (with e-mail text alone) higher than 98% with a low false-positive rate. This is powerful evidence of its own short-selling capability for correctly finding out misleading messages. By doing so, the research presents potential opportunities for improving the creation of such automatic systems and suggests how they could be applied in various media types based on text, thereby giving some larger implications within network safety.

However, Alhogail's study only focuses on the text contained within these malicious emails. It does not consider at all attacks that exploit attachments or Web link functions that are present in the email message. Phishing attacks frequently use these elements to trick their victims into opening attachments or clicking on links, thereby exposing sensitive information. According to Positive Technologies (2024) analysis, 56% of phishing emails will have something embedded with the email. This figure applies to URLs and attachments, meaning one in two phishing emails also contains a compromised link. By contrast, when the machine learning analysis excludes both attachments and URLs, the study does not provide any kind of overall strategy for detecting phishing, and this fails to cover some aspects of how these types of fraud operate. This may make it less likely that the study will be effective in identifying these threats, if at all. For a more comprehensive detection system, such as we are suggesting, then everything must be considered in a phishing e-mail, including not only the text at its heart but also the attachments and URLs.

2.3 Transformational Leadership Style for Innovation

Innovation is a key element in organizations that drive growth and sustain competitive advantage. A good leader plays a crucial role in the organization's achievement of innovative goals. The leader is like a coach who defines tactics, coordinates, and motivates the team members to achieve their goals. These behaviors refer to a leadership style, which is a classification of how leaders influence their subordinates or followers (Yating, Sains Malaysia and Mengjiao, 2024). In the early research, various leadership styles impact innovation performance, such as transformational, transactional, autocratic, and democratic leadership (Costa, Pádua and Moreira, 2023).

In this study, transformational leadership plays a moderating role in exploring the effect of the outcome of operational efficiency by using ML in cybersecurity operations. Transformational leadership leader has characters that encourage and inspire subordinates to reach their goal and exceed expectations (Korejan and Shahbazi, 2016). It involves a dynamic process in which leaders and subordinates engage in mutual influence, fostering collaboration and commitment to a shared vision. They encourage subordinates to have critical thinking and explore innovative ideas to foster an atmosphere for organizational development. This is precisely what organizations need to use innovative technology like ML. Tayal et al. (2018) identified that transformational leadership significantly impacts information technology innovation. It shapes

followers' satisfaction by aligning their beliefs and values and motivating them to accept change.

However, Tayal's study did not include risk appetite. Risk appetite is an essential element of leadership when adopting and implementing cutting-edge technologies in the organization. It is the leader's willingness to take a risk while initiating or adopting new technologies in the organization. It is a key factor that affects the implementation scope and impacts the innovation outcome.

2.4 Theoretical Framework

Organizations must proactively assess their influence on the company and its operations before integrating new technologies or innovations. These considerations can arise from both external and internal environments. Various models analyze adopter groups' characteristics based on psychological and demographic factors, regardless of whether they pertain to individuals or organizations. Understanding these dynamics is essential for gauging the willingness to embrace technology or innovation effectively (van Oorschot, Hofman and Halman, 2018).

2.4.1 Background Theory

Several research models and theoretical frameworks have been developed investigating how the adoption of new technologies is affected (Hasani *et al.*, 2023). The Technology Acceptance Model (TAM) focuses on user acceptance of technology (Alneyadi, Md Kassim and Yin, 2022). Protection Motivation Theory (PMT) examines how individuals are motivated to defend themselves from threats (Al-Kumaim and Alshamsi, 2023). The Diffusion of Innovation Theory (DOI) looks at how innovations spread through populations within and between them (Shaikh *et al.*, 2023). The Unified Theory of Acceptance and Use of Technology (UTAUT) integrates various acceptance models to yield a comprehensive understanding of technology use (Alneyadi, Md Kassim and Yin, 2022). Each of these theories provides valuable insights into factors that drive adoption (or its converse) in different spheres of technology. These models and frameworks all throw light on the processes of technology adoption. There is a large body of research on adopting new technologies in the context of cybersecurity within the financial services industry. Table 2.1 summarizes the main themes of existing studies and expands on each framework as follows.

Table 2.1: Summary of Studies Analysis

Theme Analysed	Studies	Theoretical Framework	Research Objective through the Framework
This study investigates factors influencing users' intention to adopt AI-based cybersecurity systems in the UAE.	Alneyadi et al. (2022)	Protection Motivation Theory (PMT)	- Perceived vulnerability, perceived severity, perceived response efficacy, perceived self-efficacy, job insecurity, and resistance to change all significantly influenced the intention to adopt AI-based cybersecurity systems in the UAE. - The findings provide insights into measures that can boost the acceptability and use of cybersecurity systems in the UAE. - Perceived self-efficacy and perceived response efficacy were found to be positively related to the intention to adopt AI-based cybersecurity systems, suggesting practitioners should focus on these factors.
This study explores the factors that predict the social sustainability of AI chatbots, using an enhanced model based on the Protection Motivation Theory and finding that PMT factors and cybersecurity concerns, particularly confidentiality and privacy, significantly predict the sustainable use of AI chatbots.	Arpaci (2024)	Protection Motivation Theory (PMT)	- PMT factors, including perceived severity, perceived vulnerability, self-efficacy, response efficacy, and response costs, significantly predict the sustainable use of AI chatbots. - Cybersecurity factors, such as confidentiality and privacy, also significantly impact the sustainable use of AI chatbots, which in turn affects their social sustainability. - The study's model explained a substantial portion of the variance in both sustainable use (70%) and social sustainability (74%), with confidentiality being the most influential predictor of sustainable use.
This study explores the role of cybersecurity leadership and other factors in preventing cyberattacks in financial organizations in the UAE, finding that cybersecurity leadership mediates the relationship between various factors and cyberattack prevention.	Al-Kumaim & Alshamsi (2023)	Protection Motivation Theory (PMT)	- cybersecurity leadership is an important factor in preventing cyberattacks in financial organizations in the UAE. - Greater success in cybersecurity leadership leads to increased implementation of cyberattack prevention measures. - the study emphasizes the importance of cybersecurity leadership in protecting against cyberattacks and promoting cybersecurity awareness within financial organizations and UAE society.
This paper presents a quantitative, correlational study investigating the factors that influence users' intention to adopt AI-based cybersecurity systems in the UAE, with the aim of helping organizations adopt these systems more successfully and contributing to the academic literature on AI-based cybersecurity systems.	Alneyadi et al. (2022)	Protection Motivation Theory (PMT) and Unified Theory of Acceptance and Use of Technology (UTAUT2)	- The main findings of the study are expected to help organizations adopting AI-based cybersecurity systems make informed decisions about the functionality and design of such systems to enhance user acceptance and minimize resistance. - The findings are also expected to help developers of AI-based cybersecurity systems understand the key factors to consider when designing such systems to improve their adoption and use rate.
This study proposes a comprehensive framework to identify the key factors impacting cybersecurity technology adoption by SMEs in the UK and its positive impact on organizational performance.	Hasani et al. (2023)	Technology-Organization-Environment (TOE) framework, Diffusion of Innovation (DOI) theory, Technology Acceptance Model (TAM), Institutional theory	- Compatibility, observability, and perceived ease of use are important factors that influence the adoption of cybersecurity technologies. - Organizational characteristics such as top management support, IT modularity, organizational flexibility, and collaborative board oversight impact a firm's readiness to adopt cybersecurity technologies. - Cybersecurity technology adoption has a significant positive impact on the performance of SMEs.
This paper examines the factors that drive non-users of digital banking services rendered by Pakistani Islamic banks to adopt digital banking, finding that adoption is largely determined by relative advantage, technology self-efficacy, and complexity.	Shaikh et al. (2023)	Diffusion of Innovation (DOI) theory	- Adoption of digital banking services by non-users of Islamic banks in Pakistan is influenced by perceived relative advantage, technology self-efficacy, and perceived complexity. - Technology self-efficacy is the most influential factor in determining digital banking adoption. - The findings provide essential insights for banks and policymakers to increase the adoption of digital banking services among Islamic bank customers.

Protection Motivation Theory (PMT)

This theory is well-regarded for its insights into user behavior regarding technology acceptance (Al-Kumaim and Alshamsi, 2023). It focuses on individuals' motivations to protect themselves from perceived threats. The framework is built around two key elements: threat appraisal and coping appraisal (Alneyadi, Md Kassim and Yin, 2022). Threat appraisal involves an individual's evaluation of the likelihood and seriousness of potential harm. Specifically, perceived severity relates to the expected negative consequences of not adopting the recommended seriousness, while the vulnerability reflects the individual's awareness of the chances of encountering such harm (Farooq, Ndiege and Isoaho, 2019). On the other hand, coping appraisal includes factors like self-efficacy, response efficacy, and response costs. It signifies the belief that the recommended actions can effectively reduce harm, the individual's confidence in their capability to carry out the suggested behaviors, and the costs associated with implementing these behaviors.

Unified Theory of Acceptance and Use of Technology (UTAUT2)

The UTAUT2 model has been developed to extend the UTAUT model that was proposed by Venkatesh, Morris, Davis, and Davis in 2003 (Al-Okaily *et al.*, 2020). This revised framework identifies two primary outcomes, behavioral intention, and usage behavior, alongside seven key predictors. These factors influence the user to accept and adopt new information technology (IT) systems. Effort expectancy, performance expectancy, and social influence variables directly affect users who are willing to accept and their behaviors. At the same time, the other factors are also strong predictors that predict the individual behavioral responses (Alneyadi, Md Kassim and Yin, 2022).

Technology Acceptance Model (TAM)

The Technology Acceptance Model (TAM) has garnered recent attention in studying the acceptance and use of newly devised technology. It accurately mirrors users' aspirations to adopt and use new technology in different settings (Hasani *et al.*, 2023). TAM is a framework that is widely used to understand and explain technology acceptance and its integration into organizational contexts, as well as the factors that influence the adoption of technology (Chen, Wu and Zhao, 2023). TAM is essentially designed to explain the relationship between the

acceptance of new technology, the intention to use it, and, ultimately, the actual use of the technology (Putri, Widagdo and Setiawan, 2023).

Diffusion of Innovation (DOI)

This theory serves as a vital framework for guiding technology progress by skillfully customizing and presenting innovations to suit various adoption stages. It emphasizes the influence of peer interactions and communication along the adoption journey (Hasani *et al.*, 2023). It explores how people adopt new technologies, processes, and ideas and classifies them into five groups: innovators, early adopters, early majority, late majority, and laggards. Each constitutes a way of behaving and believing that is particular to those joined by common socialization and communication, which have their own respective presentations of what new advances are and what is required (Shaikh *et al.*, 2023).

Innovators are excited by technology, learn fast, and are willing to take risks. They usually have deep technical knowledge and are not overly concerned about the outcomes, which makes them eager to adopt new innovations. Application of and acceptance of innovation happens in 2 stages, which are initiation and implementation, wherein initiation is the previous step towards implementation, which is completion (Hasani *et al.*, 2023). Challenges serve as an impetus for organizations to adopt and spread new processes or creative ideas. Realization leads toward searching for creative solutions which can better fit the problem. Hence, individuals go through five phases of an innovation-based decision-making framework (Shaikh *et al.*, 2023): knowledge, persuasion, decision, implementation, and confirmation.

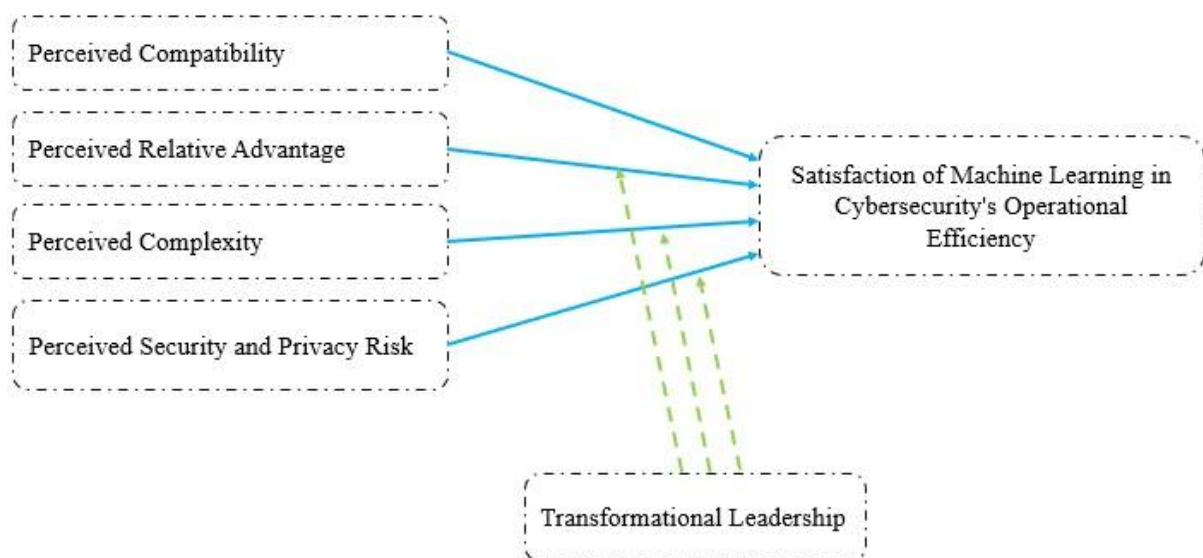
Summary of Theory

This study aims to evaluate the impact of ML on efficiency in cybersecurity operations. It is driven by different factors and adopts ML. Several theories were studied in the above section, and assessing the users' intentions, accepting new technology and adaptation, the Diffusion of Innovations (DOI) theory is more appropriate framework for this study.

2.4.2 Factors in Satisfaction of Machine Learning

In section 2.4.1, a range of theories was explored. This study adopted DOI theory and integrated constructs associated with new technology, including complexity, relative advantage, and compatibility. Papernot et al. (2018) noted concerns regarding information security and data privacy risks in machine learning are significant. Training ML models can involve retaining sensitive data, which may render that data vulnerable to membership inference attacks. These considerations are critical in evaluating their impact on adopting this technology. Moreover, the transformational leadership variable is moderating to determine the interaction with the independence variables. Consequently, this research builds on the DOI theory and integrates perceived security and privacy risk with transformational leadership as vital factors for investigation, as illustrated in Figure 2.1.

Figure 2.1 Research Framework



2.4.2.1 Perceived Compatibility

Perceived compatibility refers to the new technologies and how difficult it is to integrate with existing systems, reflecting the awareness of the effort that the latest technologies can be seamlessly integrated (Charlton and Cornwell, 2019). According to Shaikh et al. (2023), perceived compatibility describes a system that adheres to widely accepted standards, user experiences, and requirements. Thus, this concept is influenced by the resources available within an organization that facilitates implementing ML and the degree of integration of ML

and cyber-defense systems. Traditional banks often face historical and reputational challenges that differentiate them from emerging digital banks when adopting new technologies (Ya. A. Shmuratko and S. A. Sheludko, 2021). These institutions may struggle to adapt to technological advancements due to entrenched practices that obstruct the adoption of innovative solutions. Such resistance can lead to heightened security risks because their legacy cyber-defense systems may not be compatible with new technological advancements. Consequently, the following hypothesis is proposed:

H1: The compatibility of machine learning is significantly associated with cybersecurity's efficiency.

2.4.2.2 Perceived Relative Advantage

Relative advantage is the perception that an innovation has relative benefits over existing methods. These benefits encompass economic benefits, increased status, and efficiency (Shaikh *et al.*, 2023). When transformation has a collaborative form, making it into a sustainable practice and increasing employee risk appetite for new features by the critics (Wipulanusat, Panuwatwanich and Stewart, 2017). By adopting new solutions, people will be able to gain from these advantages and get the best results in various functions. Thus, the following hypothesis is proposed:

H2: The integration of machine learning, guided by transformational leadership, significantly enhances the efficiency of cybersecurity practices.

2.4.2.3 Perceived Complexity

By the definition of Mohd Amir *et al.* (2020), complexity refers to the challenges and clarity involved in innovation. According to research to research by Izuagbe *et al.* (2019), the streamlined routine reduction can enhance new technologies' adoption, while an increase in routine discretion can negatively affect the new technologies' adoption process. However, transformational leaders inspire subordinates to achieve tasks and overcome challenges successfully (Wipulanusat, Panuwatwanich and Stewart, 2017). Considering this, we need to consider whether machine learning (ML) can provide a net positive impact on the efficiency of cybersecurity operations. Thus, we propose the following hypothesis:

H3: The complexity of machine learning can be reduced by transformational leadership leaders, with a significantly positive impact on the efficiency of cybersecurity.

2.4.2.4 Perceived Security and Privacy Risk

ML models are designed to detect patterns from training data, which allows them to forecast the patterns on new datasets (Strobel and Shokri, 2022). Machine learning engages with various elements of sensitive organizational data during the model training process. The risk of data leakage arises when unauthorized individuals get this data in training or inference. It is a crucial consideration for cybersecurity operations. Adopting ML facilitates using cutting-edge tools and fosters innovative business solutions. Banks must implement comprehensive security strategies and controls to protect information assets (Lukonga, 2018). Transformational leaders are prepared to accept risks and inspire their followers to navigate the challenges of implementing innovation (Wipulanusat, Panuwatwanich and Stewart, 2017). Therefore, we propose the following hypothesis:

H4: Perceived security and privacy risk with transformational leadership positively impact cybersecurity operational efficiency.

2.4.3 Summary of Theoretical Framework

Machine learning can potentially raise significant concerns regarding data security and privacy within various processes. Furthermore, the preceding literature review primarily emphasizes quantitative approaches while neglecting professional opinions. IT expertise and professionals' opinions are important inputs to studies in specific domain, like cybersecurity. Addressing these gaps is vital as organizations consider integrating machine learning into their cybersecurity frameworks. To lay the groundwork for this study, the DOI framework's construct and "perceived security and privacy risk" construct are determined in this studies. Four hypotheses were developed by understanding the contextual elements, summarized in Table 2.2.

Table 2.2: Summary of Hypothesis

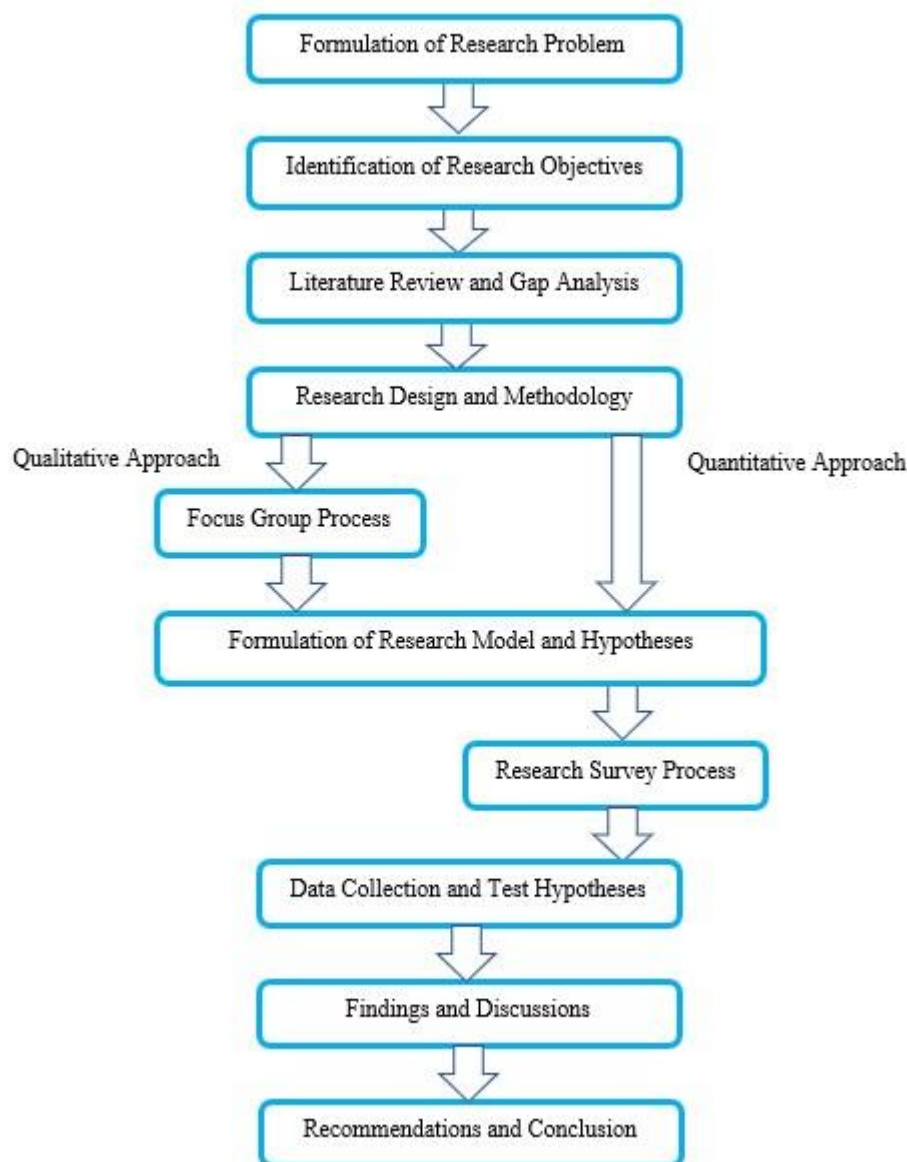
#	Hypothesis
H1	The compatibility of machine learning is significantly associated with cybersecurity's efficiency.
H2	The integration of machine learning, guided by transformational leadership, significantly enhances the efficiency of cybersecurity practices.
H3	The complexity of machine learning can be reduced by transformational leadership leaders, with a significantly positive impact on the efficiency of cybersecurity.
H4	Perceived security and privacy risk with transformational leadership positively impact cybersecurity operational efficiency.

Integrating machine learning (ML) within the banking sector facilitates using sophisticated analytical tools and implementing innovative business solutions. Banks must establish robust security measures and adopt forward-thinking strategies to protect customer information and fulfill client expectations (Lukonga, 2018). Traditional banks often encounter more challenges than emerging digital banks when adopting new technologies. Adaptation to these changes can be complicated by existing practices that obstruct the implementation of innovative solutions. As a result, this situation may introduce security and privacy vulnerabilities into legacy financial and security systems, as new technologies might not be compatible with older infrastructures.

3. Research Design

This research embraces a pragmatic philosophical approach, leveraging existing theories, concepts, and empirical findings to address the identified research problem while offering actionable solutions (Saunders, Lewis and Thornhill, 2023). This could have both highly theoretical and practical dimensions and utilizes a diversity of methodologies and perspectives to engage with the specific research questions being addressed. We used an abductive reasoning approach extending DOI theory, bringing forth a novel factor that has been empirically validated via observational methods.

Figure 3.1: Research Flow for this Research



3.1 Research Philosophy and Approach

This research embraces a pragmatic philosophical approach, leveraging existing theories, concepts, and empirical findings to address the identified research problem while offering actionable solutions (Saunders, Lewis and Thornhill, 2023). It combines both theoretical and practical dimensions, employing a diverse array of methodologies and viewpoints to explore the research questions at hand. The study adopts an abductive reasoning strategy that extends the DOI theory, simultaneously introducing a novel factor that has been empirically validated through observational methods.

3.2 Research Methodology

Data collection methods are an important means of gathering the information required by analysis objectives. In qualitative research, researchers are question-marked, or quantifier points are discussed from a variety of angles. This method encompasses collecting participants' opinions and insights or descriptive insights through interviews and focus groups (Rosenthal, 2016). On the other hand, quantitative research is characteristic of collecting and analyzing numbers, making it possible for researchers to describe, predict or control various factors of concern (Goertzen, 2017). This method usually uses tools such as questionnaires or polls to obtain data that can be analyzed statistically (Kelley-Quon, 2018).

This study uses a mixed methods approach, combining both quantitative and qualitative methodologies. This approach, by combining the strengths of each, further validates the research findings. It allows qualitative data to be analyzed within a quantitative framework, and vice versa, quantitative results can confirm qualitative conclusions (dos Santos *et al.*, 2017). Throughout the research, both primary data obtained in real-time by the researcher and secondary data from existing literature are used. In this way, the results will be comprehensive and authentic (Ajayi, 2023).

Qualitative methodologies look at recording the views, recommendations, and experiences of the research topic from participants (Hammarberg, Kirkman and De Lacey, 2016). To improve data collection and bring about an interactive situation where participants could learn from sharing their insights with researchers, focus group discussions were coherent, in-depth exchanges of views among the participants. This group interview format sharpens insights from many people (Abraham *et al.*, 2022), making the data collection process efficient and productive.

By contrast, quantitative methods are an objective way to obtain and analyze numerical data--an essential condition for verifying hypotheses and measuring many factors (Apuke, 2017). This research, which uses questionnaires as their main channel for collecting data, is limited to employees in Hong Kong's financial services industry (including the IT sector). Unlike the prior section, these mixed methods both deepens understanding of the research topic and simultaneously allows for the comparison of data collected from different sources, thus producing multiple insights that are complimentary rather than conflicting.

Comprehensive Understanding:

In this method, we can combine both methods, allowing the research subject matter to be as broad as possible (Dawadi, Shrestha and Giri, 2021). Therefore, qualitative methods capture an individual's views and allow elaborately detailed explanations. The same technique serves for information being completed into greater depth: cortex but not depth. Conversely, quantitative techniques provide statistical statements that enhance the tendency for independent prediction and help us to see how a series of variables are related to one another so that any arrival on this new planet must ipso facto abide by rules in a similar way.

Cross-verifying:

This method also enhances the cross-check of data obtained from sources, strengthening the research's reliability and validity (Ijadi Maghsoodi *et al.*, 2024). By corroborating findings derived from both methods, researchers can reinforce the base of their conclusions, reducing unconscious bias.

Complementary Insights:

Qualitative approaches emphasize that the richness and depth of inquiries may evolve from research that enlists human subjects. One direction to take is contextual factors, while another entail carrying out open-ended interviews with participants to talk about their experiences themselves: a practice known as meaning-making. This builds up thick narratives. Contradictory as it may seem, quantitative methods cannot be omitted because of the demand for objectivity: precise, unambiguous measurement and general populations as soon as those

which shall also be studied through a mixed-method approach (Dawadi, Shrestha and Giri, 2021).

Flexibility:

Researchers can be flexible in designing the research and using the data collection techniques in mixed method. They can combine both methods to align with research questions and objectives (Dawadi, Shrestha and Giri, 2021).

3.3 Summary of Research Design

This research utilizes a mix-method that merges both qualitative and quantitative methods. This approach leverages the strengths of both methods, facilitating a more detailed understanding of the study, cross-checking the findings, and producing fruitful and solid conclusions. It complements both methods perfectly. Combining qualitative methods (such as large group discussions or interviews) and quantitative methods (statistical algorithms, modeling) provides a deep stockpile of information, allowing researchers to look at patterns and predict the likely future trends using the actual data itself. This design is more comprehensive and looks more deeply into the issue. In sum, the research is steadied and backed up.

4. Expected Result

The foreseeable results of this study include its findings on the outer perimeters of the Hong Kong banking sector's cyber-defense, specifically on how to incorporate machine learning technologies into effective practice. Describing these outer perimeters will show that machine learning can be employed to strengthen measures against cyberterrorism of all kinds, thus raising the overall security level maintained throughout the entire series of banking establishments.

Along the same line, the research wishes to consider the delightful results brought about by installing machine learning in running a business organization and focus particularly on transformational leadership. This is important because transformational leaders have moral values and can make the team enter new dimensions of security practice; not only that, but they will also urge people to continue trying new things constantly. By inserting machine learning into whole systems for security, the research will discover where time is being wasted and how processes can be simplified so that organizations move more smoothly.

By contrast, the study will also study the potential negative effects of machine learning adopted in security. Such risks may include increased system complexity, possible over-reliance on automated processes and new vulnerabilities that can pop up. As the research uncovers these drawbacks, it will explain in a general all-round way how banking institutions implementing avant-garde technologies meet with greater resistance. After these findings are confirmed, the research will propose strategies to reinforce the positive effects identified and further enhance operational efficiency. This may include optimizing the present machine learning applications, promoting staff training to inspire employees to display these high technologies fully, and joining up the work of cybersecurity teams with company leaders so that their strategic goals are aligned.

The insights of this study will be invaluable for banking institutions' key stakeholders, such as top executives, the Chief Information Officer (CIO), the Chief Information Security Officer (CISO), and other security stakeholders. With authoritative and operable findings being thrown up, this research will give these leaders at various significantly different levels of guidance they need to decide on introducing machine learning in their enterprise infosec strategies and, hence, produce a more secure and more efficient banking environment.

5. Research Work Plan

For guidance the research in these 3 years, the research work plan is developed and shows in Figure 3.1. The plan activities are listed in table 5.1 with high-level timeline.

Table 5.1: Timeline of Work Plan

#	Activities	Start-Time	Finish-Time	Deliverable
1	Formulate Research Problem	Jul 2025	Sep 2025	
2	Identify Research Objectives	Jul 2025	Sep 2025	
3	Literature Review	Jul 2025	May 2027	
4	Research Design and Methodology	Nov 2025	Dec 2025	
5	Focus Group Processes	Jan 2026	Feb 2026	1. Interview Questions 2. Interview Result
6	Formulation of Research Model and Hypotheses	Feb 2026	Feb 2026	1. Conceptual Framework 2. Hypotheses
7	Research Survey Process	Feb 2026	Apr 2026	Questionnaire Statement
8	Data Collection and Test Hypotheses	Apr 2026	May 2026	Respondents Feedback
9	Findings and Discussions	May 2026	May 2027	
10	Recommendations and Conclusion	May 2026	May 2027	

Reference List

- Abraham, M. *et al.* (2022) 'Implications of XR on Privacy, Security and Behaviour: Insights from Experts', *ACM International Conference Proceeding Series* [Preprint]. Available at: <https://doi.org/10.1145/3546155.3546691>.
- Ajayi, V.O. (2023) *A Review on Primary Sources of Data and Secondary Sources of Data*. Available at: https://www.researchgate.net/publication/370608670_A_Review_on_Primary_Sources_of_Data_and_Secondary_Sources_of_Data (Accessed: 8 February 2025).
- Alamleh, H., Alqahtani, A.A.S. and Elsaid, A. (2023) 'Distinguishing Human-Written and ChatGPT-Generated Text Using Machine Learning', *2023 Systems and Information Engineering Design Symposium, SIEDS 2023*, pp. 154–158. Available at: <https://doi.org/10.1109/SIEDS58326.2023.10137767>.
- AL-Dosari, K., Fetais, N. and Kucukvar, M. (2024) 'Artificial Intelligence and Cyber Defense System for Banking Industry: A Qualitative Study of AI Applications and Challenges', *Cybernetics and Systems*, 55(2), pp. 302–330. Available at: <https://doi.org/10.1080/01969722.2022.2112539>.
- Alhogail, A. and Alsabih, A. (2021) 'Applying machine learning and natural language processing to detect phishing email', *Computers & Security*, 110, p. 102414. Available at: <https://doi.org/10.1016/j.cose.2021.102414>.
- Al-Kumaim, N.H. and Alshamsi, S.K. (2023) 'Determinants of Cyberattack Prevention in UAE Financial Organizations: Assessing the Mediating Role of Cybersecurity Leadership', *Applied Sciences* 2023, Vol. 13, Page 5839, 13(10), p. 5839. Available at: <https://doi.org/10.3390/APP13105839>.
- Alneyadi, M.R.M.A.H., Md Kassim, N. and 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, pp. 1053–1064. Available at: <https://openurl.ebsco.com/contentitem/bth:160657561?sid=ebsco:plink:crawler&id=ebsco:bth:160657561&crl=c> (Accessed: 6 February 2025).
- Al-Okaily, M. *et al.* (2020) 'An empirical investigation on acceptance of mobile payment system services in Jordan: extending UTAUT2 model with security and privacy', *International Journal of Business Information Systems*, 42(1), pp. 123–152. Available at: <https://doi.org/10.1504/IJBIS.2020.10036883>.
- Ancillai, C. *et al.* (2023) 'Digital technology and business model innovation: A systematic literature review and future research agenda', *Technological Forecasting & Social Change*, 188, p. 122307. Available at: <https://doi.org/10.1016/j.techfore.2022.122307>.
- Angela Romei (2024) *Soaring Scam and Fraud Sophistication Remains Top Challenge Threatening to Overwhelm the Global Financial Services Sector* | Mitek Systems, Inc. Available at: <https://investors.miteksystems.com/news-releases/news-release-details/soaring-scam-and-fraud-sophistication-remains-top-challenge> (Accessed: 26 January 2025).
- Apruzzese, G. *et al.* (2017) 'Identifying malicious hosts involved in periodic communications', *2017 IEEE 16th International Symposium on Network Computing and Applications, NCA 2017*, 2017-January, pp. 1–8. Available at: <https://doi.org/10.1109/NCA.2017.8171326>.
- Apruzzese, G. *et al.* (2023) 'The Role of Machine Learning in Cybersecurity', *Digital Threats: Research and Practice*, 4(1). Available at: <https://doi.org/10.1145/3545574/ASSET/C4586A69-4437-435A-9DE6-E5F12828847D/ASSETS/GRAPHIC/DTRAP-2021-0064-F15.JPG>.

- Apuke, O.D. (2017) 'Quantitative Research Methods : A Synopsis Approach', *Kuwait Chapter of Arabian Journal of Business and Management Review*, 6(11), pp. 40–47. Available at: <https://doi.org/10.12816/0040336>.
- Bogatinovski, J. *et al.* (2021) 'Artificial Intelligence for IT Operations (AIOps) Workshop White Paper'. Available at: <https://arxiv.org/abs/2101.06054v1> (Accessed: 26 January 2025).
- Charlton, A.B. and Cornwell, T.B. (2019) 'Authenticity in horizontal marketing partnerships: A better measure of brand compatibility', *Journal of Business Research*, 100, pp. 279–298. Available at: <https://doi.org/10.1016/J.JBUSRES.2019.03.054>.
- Charlton, E. (2024) *2023 was a big year for cybercrime – here's how we can make our systems safer* | *World Economic Forum*. Available at: <https://www.weforum.org/stories/2024/01/cybersecurity-cybercrime-system-safety/> (Accessed: 26 January 2025).
- Chen, B., Wu, Z. and Zhao, R. (2023) 'From fiction to fact: the growing role of generative AI in business and finance', *Journal of Chinese Economic and Business Studies*, 21(4), pp. 471–496. Available at: https://doi.org/10.1080/14765284.2023.2245279/ASSET/30F057BF-2635-4362-A5A5-9CFAE6E3A590/ASSETS/GRAPHIC/RCEA_A_2245279_F0006_OC.JPG.
- Choithani, T. *et al.* (2024) 'A Comprehensive Study of Artificial Intelligence and Cybersecurity on Bitcoin, Crypto Currency and Banking System', *Annals of Data Science*, 11(1), pp. 103–135. Available at: <https://doi.org/10.1007/S40745-022-00433-5/TABLES/2>.
- Costa, J., Pádua, M. and Moreira, A.C. (2023) 'Leadership Styles and Innovation Management: What Is the Role of Human Capital?', *Administrative Sciences* 2023, Vol. 13, Page 47, 13(2), p. 47. Available at: <https://doi.org/10.3390/ADMSCI13020047>.
- CSIS (2024) *Significant Cyber Incidents | Strategic Technologies Program | CSIS*. Available at: <https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents> (Accessed: 26 January 2025).
- Dawadi, S., Shrestha, S. and Giri, R.A. (2021) 'Mixed-Methods Research: A Discussion on its Types, Challenges, and Criticisms', *Journal of Practical Studies in Education*, 2(2), pp. 25–36. Available at: <https://doi.org/10.46809/jpse.v2i2.20>.
- Farayola, O.A. (2024) 'REVOLUTIONIZING BANKING SECURITY: INTEGRATING ARTIFICIAL INTELLIGENCE, BLOCKCHAIN, AND BUSINESS INTELLIGENCE FOR ENHANCED CYBERSECURITY', *Finance & Accounting Research Journal*, 6(4), pp. 501–514. Available at: <https://doi.org/10.51594/FARJ.V6I4.990>.
- Fares, O.H., Butt, I. and Lee, S.H.M. (2023) 'Utilization of artificial intelligence in the banking sector: a systematic literature review', *Journal of Financial Services Marketing*, 28(4), pp. 835–852. Available at: <https://doi.org/10.1057/S41264-022-00176-7/TABLES/4>.
- Farooq, A., Ndiege, J.R.A. and Isoaho, J. (2019) 'Factors Affecting Security Behavior of Kenyan Students: An Integration of Protection Motivation Theory and Theory of Planned Behavior', *IEEE AFRICON Conference*, 2019-September. Available at: <https://doi.org/10.1109/AFRICON46755.2019.9133764>.
- Goertzen, M.J. (2017) 'Chapter 3. Introduction to Quantitative Research and Data', *Library Technology Reports*, 53(4), pp. 12–18. Available at: <https://journals.ala.org/index.php/ltr/article/view/6325/8275> (Accessed: 8 February 2025).

- Gorment, N.Z. *et al.* (2023) ‘Machine Learning Algorithm for Malware Detection: Taxonomy, Current Challenges, and Future Directions’, *IEEE Access*, 11, pp. 141045–141089. Available at: <https://doi.org/10.1109/ACCESS.2023.3256979>.
- Hammarberg, K., Kirkman, M. and De Lacey, S. (2016) ‘Qualitative research methods: when to use them and how to judge them’, *Human Reproduction*, 31(3), pp. 498–501. Available at: <https://doi.org/10.1093/HUMREP/DEV334>.
- Hasani, T. *et al.* (2023) ‘Evaluating the adoption of cybersecurity and its influence on organizational performance’, *SN Business & Economics* 2023 3:5, 3(5), pp. 1–38. Available at: <https://doi.org/10.1007/S43546-023-00477-6>.
- Helm, J.M. *et al.* (2020) ‘Machine Learning and Artificial Intelligence: Definitions, Applications, and Future Directions’, *Current Reviews in Musculoskeletal Medicine*, 13(1), pp. 69–76. Available at: <https://doi.org/10.1007/S12178-020-09600-8/FIGURES/1>.
- Herrmann, H. and Masawi, B. (2022) ‘Three and a half decades of artificial intelligence in banking, financial services, and insurance: A systematic evolutionary review’, *Strategic Change*, 31(6), pp. 549–569. Available at: <https://doi.org/10.1002/JSC.2525>.
- HKMA (2019) ‘Reshaping Banking with Artificial Intelligence’.
- Hoi-ying, L. (2024) *UK multinational Arup confirmed as victim of HK\$200 million deepfake scam that used digital version of CFO to dupe Hong Kong employee | South China Morning Post*. Available at: <https://www.scmp.com/news/hong-kong/law-and-crime/article/3263151/uk-multinational-arup-confirmed-victim-hk200-million-deepfake-scam-used-digital-version-cfo-dupe> (Accessed: 26 January 2025).
- Ijadi Maghsoodi, A. *et al.* (2024) ‘What Makes Effective Acute Geriatric Care? - A mixed Methods Study From Aotearoa New Zealand’, *Ageing International*, 49(3), pp. 660–683. Available at: <https://doi.org/10.1007/S12126-024-09568-7/FIGURES/1>.
- Izuagbe, R. *et al.* (2019) ‘Effect of perceived ease of use on librarians’ e-skills: Basis for library technology acceptance intention’, *Library & Information Science Research*, 41(3), p. 100969. Available at: <https://doi.org/10.1016/J.LISR.2019.100969>.
- Kalash, M. *et al.* (2018) ‘Malware Classification with Deep Convolutional Neural Networks’, *2018 9th IFIP International Conference on New Technologies, Mobility and Security, NTMS 2018 - Proceedings*, 2018-January, pp. 1–5. Available at: <https://doi.org/10.1109/NTMS.2018.8328749>.
- Kelley-Quon, L.I. (2018) ‘Surveys: Merging qualitative and quantitative research methods’, *Seminars in pediatric surgery*, 27(6), pp. 361–366. Available at: <https://doi.org/10.1053/J.SEMPEDSURG.2018.10.007>.
- Kelly, S., Kaye, S.A. and Oviedo-Trespalacios, O. (2023) ‘What factors contribute to the acceptance of artificial intelligence? A systematic review’, *Telematics and Informatics*, 77, p. 101925. Available at: <https://doi.org/10.1016/J.TELE.2022.101925>.
- Kharpal, A. (2023) *ICBC, the world’s biggest bank, hit by ransomware cyberattack*. Available at: <https://www.cnn.com/2023/11/10/icbc-the-worlds-biggest-bank-hit-by-ransomware-cyberattack.html> (Accessed: 26 January 2025).
- Korejan, M.M. and Shahbazi, H. (2016) ‘An analysis of the transformational leadership theory’, *Journal of Fundamental and Applied Sciences*, 8(3), pp. 452–461. Available at: <https://doi.org/10.4314/JFAS.V8I3S.192>.

Korolov, M. (2024) *3 areas where gen AI improves productivity — until its limits are exceeded* | CIO. Available at: <https://www.cio.com/article/1312721/3-areas-where-gen-ai-improves-productivity-until-its-limits-are-exceeded.html> (Accessed: 31 January 2025).

Leme Lopes, A.P. (2023) 'Artificial history? Inquiring ChatGPT on historiography', *Rethinking History*, 27(4), pp. 709–749. Available at: <https://doi.org/10.1080/13642529.2023.2234227>.

Li, J. *et al.* (2019) 'The Approaches of Prevention, Detection, and Response for Cybersecurity of I&C Systems in NPPs', *Lecture Notes in Electrical Engineering*, 507, pp. 283–290. Available at: https://doi.org/10.1007/978-981-13-3113-8_33.

Li, Y. *et al.* (2017) 'Android Malware Clustering through Malicious Payload Mining', *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 10453 LNCS, pp. 192–214. Available at: https://doi.org/10.1007/978-3-319-66332-6_9.

Lukonga, I. (2018) *Fintech, Inclusive Growth and Cyber Risks: Focus on the MENAP and CCA Regions by Inutu Lukonga :: SSRN*. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3267228 (Accessed: 8 February 2025).

Martínez Torres, J., Iglesias Comesaña, C. and García-Nieto, P.J. (2019) 'Review: machine learning techniques applied to cybersecurity', *International Journal of Machine Learning and Cybernetics*, 10(10), pp. 2823–2836. Available at: <https://doi.org/10.1007/S13042-018-00906-1/FIGURES/1>.

Meineke, M. (2024) *Tackling cybersecurity's global talent shortage: Report* | World Economic Forum. Available at: <https://www.weforum.org/stories/2024/04/cybersecurity-industry-talent-shortage-new-report/> (Accessed: 26 January 2025).

Mishra, S. (2023) 'Exploring the Impact of AI-Based Cyber Security Financial Sector Management', *Applied Sciences* 2023, Vol. 13, Page 5875, 13(10), p. 5875. Available at: <https://doi.org/10.3390/APP13105875>.

Mohammadi, S. *et al.* (2019) 'Cyber intrusion detection by combined feature selection algorithm', *Journal of Information Security and Applications*, 44, pp. 80–88. Available at: <https://doi.org/10.1016/j.jisa.2018.11.007>.

Murphy, K. *et al.* (2021) 'Artificial intelligence for good health: a scoping review of the ethics literature', *BMC Medical Ethics*, 22(1), pp. 1–17. Available at: <https://doi.org/10.1186/S12910-021-00577-8/FIGURES/4>.

Noy, S. and Zhang, W. (2023) 'Experimental Evidence on the Productivity Effects of Generative Artificial Intelligence', *SSRN Electronic Journal* [Preprint]. Available at: <https://doi.org/10.2139/SSRN.4375283>.

van Oorschot, J.A.W.H., Hofman, E. and Halman, J.I.M. (2018) 'A bibliometric review of the innovation adoption literature', *Technological Forecasting and Social Change*, 134, pp. 1–21. Available at: <https://doi.org/10.1016/J.TECHFORE.2018.04.032>.

Papernot, N. *et al.* (2018) 'SoK: Security and Privacy in Machine Learning', *Proceedings - 3rd IEEE European Symposium on Security and Privacy, EURO S and P 2018*, pp. 399–414. Available at: <https://doi.org/10.1109/EUROSP.2018.00035>.

Peng, S. *et al.* (2023) 'The Impact of AI on Developer Productivity: Evidence from GitHub Copilot'. Available at: <https://arxiv.org/abs/2302.06590v1> (Accessed: 26 January 2025).

Positive Technologies (2024) *Trends in phishing attacks on organizations in 2022–2023*. Available at: <https://global.ptsecurity.com/analytics/trends-in-phishing-attacks-on-organizations-in-2022-2023#What%20are%20the%20dangers%20of%20phishing%20messages?> (Accessed: 1 February 2025).

Putri, G.A., Widagdo, A.K. and Setiawan, D. (2023) ‘Analysis of financial technology acceptance of peer to peer lending (P2P lending) using extended technology acceptance model (TAM)’, *Journal of Open Innovation: Technology, Market, and Complexity*, 9(1), p. 100027. Available at: <https://doi.org/10.1016/J.JOITMC.2023.100027>.

Rosenbush, S. (2017) *The Morning Download: First AI-Powered Cyberattacks Are Detected* - WSJ. Available at: <https://www.wsj.com/articles/the-morning-download-first-ai-powered-cyberattacks-are-detected-1510839203> (Accessed: 26 January 2025).

Rosenthal, M. (2016) ‘Qualitative research methods: Why, when, and how to conduct interviews and focus groups in pharmacy research’, *Currents in Pharmacy Teaching and Learning*, 8(4), pp. 509–516. Available at: <https://doi.org/10.1016/J.CPTL.2016.03.021>.

dos Santos, J.L.G. *et al.* (2017) ‘INTEGRATING QUANTITATIVE AND QUALITATIVE DATA IN MIXED METHODS RESEARCH’, *Texto & Contexto - Enfermagem*, 26(3), p. e1590016. Available at: <https://doi.org/10.1590/0104-07072017001590016>.

Sarker, I.H. (2021) ‘Machine Learning: Algorithms, Real-World Applications and Research Directions’, *SN Computer Science*, 2(3), pp. 1–21. Available at: <https://doi.org/10.1007/S42979-021-00592-X/FIGURES/11>.

Sarker, I.H. (2023) ‘Machine Learning for Intelligent Data Analysis and Automation in Cybersecurity: Current and Future Prospects’, *Annals of Data Science*, 10(6), pp. 1473–1498. Available at: <https://doi.org/10.1007/S40745-022-00444-2/FIGURES/6>.

Sarker, I.H., Furhad, M.H. and Nowrozy, R. (2021) ‘AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions’, *SN Computer Science*, 2(3), pp. 1–18. Available at: <https://doi.org/10.1007/S42979-021-00557-0/FIGURES/5>.

Saunders, M., Lewis, P. and Thornhill, A. (2023) ‘2023 Research methods for business students Preface and Chapter 4’, *Research Methods for Business Students*, (February), pp. 128, i–xxvii. Available at: https://www.researchgate.net/publication/240218229_Research_Methods_for_Business_Students (Accessed: 8 February 2025).

Shaikh, I.M. *et al.* (2023) ‘ISLAMIC BANK CUSTOMERS’ ADOPTION OF DIGITAL BANKING SERVICES: EXTENDING DIFFUSION THEORY OF INNOVATION’, *Journal of Islamic Monetary Economics and Finance*, 9(1), pp. 57–70. Available at: <https://doi.org/10.21098/JIMF.V9I1.1545>.

Shwede, F., Malaka, S. and Rwashdeh, B. (2023) ‘The Moderation Effect of Artificial Intelligent Hackers on the Relationship between Cyber Security Conducts and the Sustainability of Software Protection: A Comprehensive Review’, *Migration Letters*, 20. Available at: <https://doi.org/10.59670/ML.V20IS9.4947>.

Statista (2024) *Cybersecurity - Worldwide | Statista Market Forecast*. Available at: <https://www.statista.com/outlook/tmo/cybersecurity/worldwide> (Accessed: 26 January 2025).

Strobel, M. and Shokri, R. (2022) ‘Data Privacy and Trustworthy Machine Learning’, *IEEE Security and Privacy*, 20(5), pp. 44–49. Available at: <https://doi.org/10.1109/MSEC.2022.3178187>.

Taha, K. (2023) 'Semi-supervised and un-supervised clustering: A review and experimental evaluation', *Information Systems*, 114, p. 102178. Available at: <https://doi.org/10.1016/j.is.2023.102178>.

Tayal, R. *et al.* (2018) 'The impact of transformational leadership on employees' acceptance to change: Mediating effects of innovative behaviour and moderating effect of the use of information technology', *VINE Journal of Information and Knowledge Management Systems*, 48(4), pp. 559–578. Available at: <https://doi.org/10.1108/VJIKMS-05-2018-0039>.

Wipulanusat, W., Panuwatwanich, K. and Stewart, R.A. (2017) 'Exploring leadership styles for innovation: An exploratory factor analysis', *Engineering Management in Production and Services*, 9(1), pp. 7–17. Available at: <https://doi.org/10.1515/EMJ-2017-0001>.

Ya. A. Shmuratko and S. A. Sheludko (2021) 'FINANCIAL TECHNOLOGIES' IMPACT ON THE DEVELOPMENT OF BANKING', *Financial and credit activity problems of theory and practice*, 4(31), pp. 61–69. Available at: <https://doi.org/10.18371/FCAPTP.V4I31.190792>.

Yamin, M.M. *et al.* (2021) 'Weaponized AI for cyber attacks', *Journal of Information Security and Applications*, 57, p. 102722. Available at: <https://doi.org/10.1016/J.JISA.2020.102722>.

Yating, L., Sains Malaysia, U. and Mengjiao, Z. (2024) 'A Review of the Impact of Leadership Styles on Employee Innovation Performance AP Dr Mohd Anuar bin Arshad', 14(1). Available at: <https://doi.org/10.6007/IJARBSS/v14-i1/20050>.