

LEVEL 7 ASSESSMENT SPECIFICATION

Student name:	Chiang Chun Wah	Student ID number:	2119645
Programme:	DBA		
Module:	Research Principles and Philosophy		
Module code:	HKBM7017	Contribution to Overall Module Assessment (%):	100%
Lecturer:	Dr Chammy Lau	Internal Verifier:	Prof Peter Fong
Assignment Title:	Report (Research Proposal)	Word count (or equivalent):	7500 words (+/-10%)
Submission deadline:	22 July 2024	Return date of provisional marks & written feedback:	23 August 2024
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. Penalties for late submission: Up to one week late, maximum mark of 50%. Over one week late, 0%. Only the Extenuating Circumstances Panel may approve a change to submission dates.		
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**

Abstract

Purpose

AI technology is popular worldwide and Machine Learning (ML) is one of technology which is discussed on commercial and personal levels by everyone. ML is gradually integrating into our daily lives, and various industries plan to incorporate it into their operations, either to expand business opportunities or optimize internal processes. ML has started to be used in cybersecurity defense because cyberattacks are more complicated and leverage AI to launch attacks. Using AI against AI is the trend in the cybersecurity landscape. However, the organizations do not clearly understand the trade-offs of using ML, such as complexity, resources, and privacy. Significantly, there is a privacy risk when it is implemented in the banking industry. The aims of this research is to analyze the effects of machine learning (ML) on cybersecurity operations within the banking sector of Hong Kong. The study aims to identify both positive and negative impacts and propose practical recommendations to maximize the positive effects while mitigating any potential adverse consequences.

Design/Methodology/Approach - To comprehensively examine the variables and their interrelationships, a hybrid methodology incorporating both qualitative and quantitative approaches was employed. A focus group was formed to engage in discussions regarding the capabilities of machine learning, concerns surrounding it, and potential applications in cybersecurity defense. Additionally, a survey is conducted to gather representative responses for analyzing the data subsequently.

Expected Results - The results of this study are expected to identify which Hong Kong banking cybersecurity defense can utilize machine learning, the positive impacts that can increase operational efficiency, and the negative impacts that pose risks to operations. Upon confirming these results, the positive impacts will be leveraged or strengthened to increase operational efficiency further, while the negative impacts will be mitigated.

Originality/Value - This paper takes a comprehensive approach to determine various factors that impact the operational efficiency of cybersecurity in the banking sector in Hong Kong. Moreover, it presents practical recommendations aimed at mitigating these negative impacts and ultimately enhancing the overall operational efficiency of cybersecurity measures.

Keywords – Machine Learning (ML), Cybersecurity Operations, DOI, Hong Kong.

Table of Contents

1. Introduction.....	5
1.1 Trend and Significance.....	6
Trend.....	6
Significance.....	8
1.2 Research Background.....	8
Research Aim	9
Research Objectives.....	9
2. Literature Review	11
2.1 Definition of ML.....	11
2.2 Machine Learning Techniques	12
2.3 Machine Learning for Cybersecurity Applications	14
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	25
3.1 Research Philosophy and Approach	26
3.2 Research Methodology	26
3.3 Summary of Research Design	28
Reference List.....	29

List of Tables

Table-2.1: ML Definition.....	11
Table-2.2: Summary of Studies Analysis	19
Table-2.3: Summary of Hypothesis	24

List of Figures

Figure-1.1: Loss of Cyberattack from 2018 to 2028.....	7
Figure-2.2: Research Framework.....	22
Figure-3.1: Research Flow for this Research.....	25

1. Introduction

As technology continues to advance and the business environment undergoes constant evolution, organizations are continuously adapting their business strategies in response to external changes. This adaptation involves integrating technology into various aspects of business operations or daily activities to foster new business opportunities for maintaining competitiveness and foster new business opportunities (Ancillai et al., 2023). Over the past decade, technological advancements in digitalization, cloud computing, and artificial intelligence (AI) have significantly impacted enterprises. These advancements have brought about substantial changes and challenges, while simultaneously presenting numerous opportunities for growth and innovation (Chen, Wu, and Zhao, 2023). The second generation of cloud computing took only five years from its introduction to widespread adoption by enterprises (Varghese, 2019). AI technologies, such as image and speech recognition, chatbots have been rolled out since 2016. Until 2022, next generation AI (GenAI) was launched in the world, such as ChatGPT (Leme Lopes, 2023). Organizations should understand and assess these technologies for their industry in advance in the context of rapid technological development. Understanding and leveraging technology's capabilities is essential for modern enterprises to navigate and succeed in a dynamic business landscape. Organizations should incorporate these technological advancements into their business strategies in time. By doing so, they can better position themselves to capitalize on opportunities and sustain competitiveness. Otherwise, organizations may lose competitiveness or leading edge in the industry. Integrating these technologies is not merely a trend but a necessary strategy to enhance operational capabilities and maintain a competitive edge.

AI is poised to be the transformative technology of the coming decade, primarily because it can augment human abilities at a minimal cost (Kelly, Kaye, and Oviedo-Trespalcacios, 2023). This technological support is expected to improve daily life by advancing IT operations (Bogatinovski et al., 2021), as well as enhancing sectors such as healthcare, customer service, education, and transportation (Murphy et al., 2021). After AI became popular in the world in several years, GenAI emerges as a transformative force and has garnered significant attention and analysis within the field of AI. Widely used tools like ChatGPT and Copilot exemplify this technology. According to AlQahtani, A. A. S. and ElSaid, A. (2023), these tools utilize a form of Machine Learning (ML) to produce outputs such as text, video, and music by leveraging existing data. According to Korolov (2024), a substantial majority of companies (71%) that have already implemented AI solutions experience significant returns on their investments

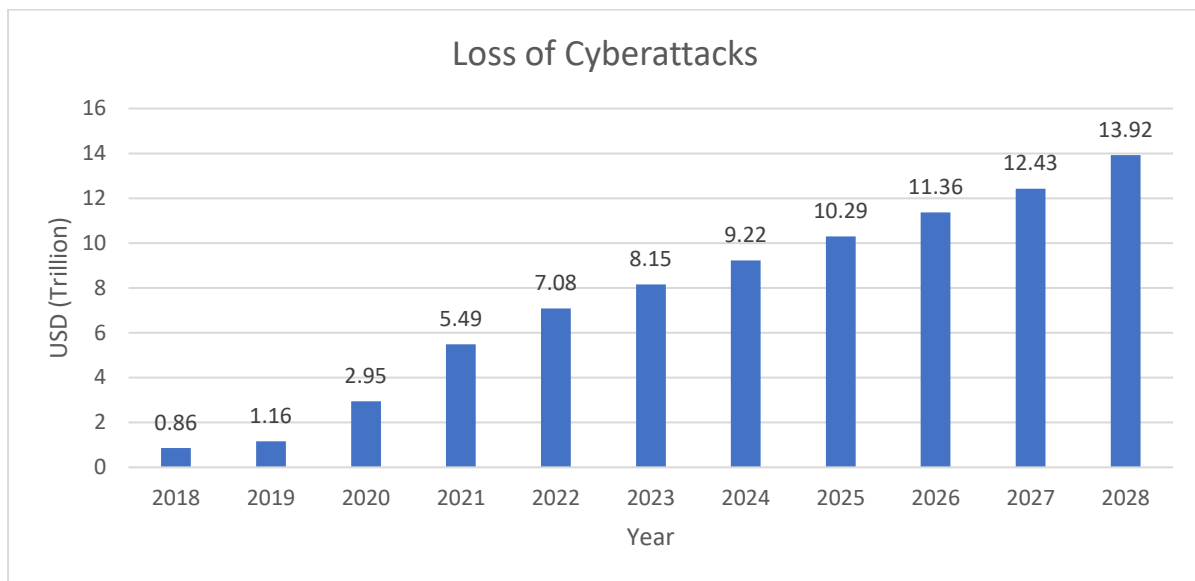
within a span of 14 months. Additionally, Brynjolfsson, Li, and Raymond (2023) found that workers utilizing GenAI tools were 14% more productive, with the most significant productivity gains of up to 35% observed among the least skilled and least experienced workers. Noy, S. and Zhang, W. (2023) determined that experienced business professionals increased their 59% efficiency in writing business documents per hour. 126% of efficiency improvement for coding a software project in the other researcher (Peng et al., 2023). There are elements of light and dark in AI technologies. If AI is used correctly, it can facilitate organizations' business growth. If not, it is a terrible technology that threatens organizations' interests.

1.1 Trend and Significance

Trend

A cyberattack encompasses a range of negative outcomes, including but not limited to data loss, financial setbacks, intellectual property theft, system unusable, personal and confidential information leakage, fraudulent activities, disruptions to business operations, the need for forensic investigations, data and system recovery processes, and damage to reputation. Since 2006, organizations have encountered significant risks from cyberattacks (Csis, 2024). Every day, approximately 2,220 cyberattacks take place, resulting in over 800,000 attacks annually (Charlton, 2024). Cyberattacks have the potential to affect organizations in various ways, ranging from minor operational disruptions to significant financial losses. Regardless of the specific type of cyberattack, each consequence incurred carries a certain cost, whether it be monetary or in other forms. According to Statista Market Insights (2024), they projected cybercrime will cause the loss and are anticipated to experience a substantial increase over the next four years. It is estimated to rise from around \$9 trillion in 2024 to \$14 trillion by 2028, that is shown in Figure 1.1.

Figure-1.1: Loss of Cyberattack from 2018 to 2028



Technology has been the development that facilitates our life and economy but strengthens the capabilities of hackers. In the past, hackers used traditional phishing and social engineering methods to cheat the victims. In recent years, they have been using AI to simulate video and voice to launch cyberattacks. This method easily gains the trust of victims. The threat is expected to escalate as hackers increasingly utilize AI and ML technologies. The first AI cyberattack has been detected in 2017 (Yamin et al., 2021). In India, a company detected an attack where rudimentary machine learning was employed to observe and understand typical user behavior patterns within a network (Rosenbush, 2017). Subsequently, the software started imitating this behavior, seamlessly blending into the network's background and evading detection by security tools. Broadly speaking, a cyberattack refers to a deliberate and organized effort made by an individual or a collective entity to undermine the information system of another individual or organization. Currently, various types of security incidents or cybercrimes, including ransomware, phishing email, malware, web application attack, social engineering, etc., have become prevalent. These incidents can have serious repercussions, affecting both organizations and individuals by causing operational disruptions and significant financial losses. For instance, a cyberattack targeted China's ICBC, the world's largest bank, and a ransomware attack reportedly disrupted the US Treasury markets (Kharpal, 2023). In 2024, the victim in Hong Kong transferred HKD 200 million in funds to attackers who used video conferences with a deep fake impersonation of the CFO of a multinational company based in the United Kingdom (Hoi-ying, 2024).

Significance

The frequency and severity of cyberattacks are on the rise each year, presenting significant challenges. This serves as a warning for cybersecurity professionals and organizations, emphasizing the urgent need to address and mitigate the growing threats in the field. Thus, cybersecurity is extremely important to organizations, and defending against cyberattacks is crucial to a business's success. Cyberattack is becoming more common and complicated after integrating AI into the attack chain. However, the traditional protection methods may not be enough to protect from the new generation's cyberattack (Shwedeh, Malaka and Rwashdeh, 2023). Technology should address the problem, so using AI against AI's cyberattacks is the cybersecurity landscape in the future (Sarker, Furhad and Nowrozy, 2021). Therefore, it is crucial to prioritize the protection of IT applications and systems, particularly those connected to the Internet, from a wide range of unauthorized access, cyberattacks, and potential damage. This issue demands immediate attention and action. This paper focuses on addressing this crucial issue by exploring the impact of machine learning on practical and intelligent protection methods.

1.2 Research Background

In practice, the security of businesses, government agencies, organizations, and individuals largely rely on the efficiency of security systems or tools to promptly and intelligently identify and prevent security incidents. With the immense volume of data managed by government bodies, military sectors, corporations, financial entities, healthcare institutions, and others, comprehensive cybersecurity technology and management tools are necessary. Cybersecurity involves governance, policy, systems and design, procedures, and monitoring to protect organization's assets that includes tangible and intangible. Traditional security measures, such as anti-malware software, intrusion detection systems, firewalls, and anti-spam systems, may no longer be enough to protect the organization from today's evolving requirements (Mohammadi et al., 2019). The primary limitation of these conventional systems lies in their reliance on the expertise of a limited number of security professionals. Conversely, Artificial Intelligence (AI), recognized as the essential technology in Industry 4.0, offers substantial benefits for brilliant cybersecurity defense and monitoring due to its powerful capabilities and flexible extension. Therefore, we focus on integrating cybersecurity and AI, which ultimately automates and enhances cybersecurity defense with intelligence surpassing traditional security systems.

The utilization of AI in banking is extensive, spanning various areas including the front-desk functions, and back-end departments (Fares, Butt, and Lee, 2023). According to a survey conducted by HKMA (2019), 89% of banks have either already implemented or are planning to implement AI applications. Moreover, most banks, precisely 94% of those that have adopted AI, express their intention to leverage this technology in shaping their corporate strategies. The motivations behind this increasing adoption are centered around enhancing customer experience, maintaining cost-effectiveness, improving efficiency, and effectively managing risks. The primary driver behind this research is the growing trend of digitization and automation in the banking industry, and global cybersecurity posture. This research focuses on analyzing and addressing the challenges (such as privacy and trustworthiness) and potential solutions (such as accuracy and safety) concerning the operational efficiency of cybersecurity within the banking sector. Earlier studies have examined AI's role in enhancing customer service and reducing costs in the banking industry (Choithani et al., 2024), the obstacles faced when implementing AI in this sector (AL-Dosari, Fetais, and Kucukvar, 2024), and the types of AI algorithms suitable for financial management (Mishra, 2023). However, there is a need for research to address the impact of cybersecurity on the banking sector in Hong Kong.

Research Aim

This research aims to identify AI's impact on cybersecurity operational efficiency in the Hong Kong banking sector. Due to its unpredictable nature, using AI in cybersecurity raises different impacts. These impacts include positive and negative ones on cybersecurity operations. They may relate to privacy, security, risk, accuracy, trustworthiness, and regulations.

Research Objectives

In addition to identifying the areas where AI is being applied in the cybersecurity of the banking sector, this study has three objectives. Firstly, comprehensively understanding the applications of AI in banking cybersecurity provides a holistic view of the areas that require focus and attention to ensure robust protection of sensitive customer data (Herrmann and Masawi, 2022). This understanding helps prioritize cybersecurity efforts and resource allocation to address the most critical areas and potential vulnerabilities. Secondly, it emphasizes the importance of machine learning capabilities in driving operational efficiency in cyber defense within the banking sector. Machine learning algorithms can continuously learn from the patterns and new threats that cause damage and make decisions. Finally, by exploring machine learning's impacts on cybersecurity operations, the research aims to shed light on how these technologies can

streamline and optimize defense mechanisms, enhance detection and response capabilities, and ultimately strengthen banks' overall capabilities of cybersecurity.

Thus, there are 3 research questions to achieve the above objectives.

RQ1: What is AI's dominant and emerging applications in the banking sector's cybersecurity?

RQ2: What are the capabilities of machine learning in cybersecurity operations?

RQ3: What is machine learning's positive and negative impacts on cybersecurity's operational efficiency?

2. Literature Review

Several areas are included in the literature review of this study: (1) the definition of machine learning, (2) machine learning techniques, (3) machine learning for cybersecurity applications, and (4) theoretical framework.

2.1 Definition of ML

Coming up with a precise definition of AI proves challenging as there is no universally agreed-upon concept. AI comprises multiple components and processes, ultimately leading to outcomes that can be unpredictable. AI covered various techniques and methodologies for mimicking complex human capabilities, such as independent decision-making and simulated human language (Truby, Brown, and Dahdal 2020). Within AI, machine learning (ML) deals explicitly with identifying data patterns and decision-making based on those recognized patterns.

Table-2.1: ML Definition

Theme Analysed	Studies	ML Definition
The paper aims to provide a unified or general definition of deep learning and outline a general methodology for learning and deep learning, as there is currently a lack of a unified definition in the literature.	Zhang, W. J. et al. (2018)	definition of machine learning that involves employing a sequential arrangement of nonlinear processing units to extract and transform features.
The introduction provides an overview of data drift, which refers to differences between the training data and real-world data used by medical machine learning models, and establishes it as a significant challenge in the deployment of such models.	Sahiner, B. et al. (2023)	The paper does not provide a formal definition of machine learning or artificial intelligence, but describes various applications of these techniques in medical imaging and therapy, such as disease detection, diagnosis, segmentation, image reconstruction, and autonomous decision-making.
The introduction provides background on the challenge of real-world systems changing over time, leading to performance degradation of machine learning models, and the need to identify and address these changes, referred to as "concept drift", while noting the lack of unified terminology in the literature.	Bayram, F., Ahmed, B. S. and Kassler, A. (2022)	A modification in the connection between the input data and the target variables within supervised learning models
The introduction provides an overview of how AI and machine learning are transforming the practice of medicine, particularly in the field of orthopedics, and the purpose of the paper is to critically evaluate the recent literature on machine learning in orthopedics and discuss its potential impact on the future of musculoskeletal care.	Helm, J. M. et al. (2020)	Artificial intelligence (AI) is defined as the theory of human intelligence being exhibited by machines. Machine learning (ML) is a subset of AI that exhibits the "learning" associated with human intelligence, using computational algorithms to recognize patterns and make predictions. Deep neural networks are more complex ML models that use hierarchical tiers to process inputs and generate outputs, without explicit programming.

There are several definitions of ML in previous research, as shown in Table 2.1:

(1) According to Bayram, Ahmed, and Kassler (2022), the definition of the term refers to a modification in the connection between the input and output data within supervised learning models.

(2) On the other hand, Sahiner et al. (2023) defined it as the specific functional relationship that a learning model establishes based on the training data, linking the input to the target variable.

(3) Helm et al. (2020), the definition encompasses the processes related to human intelligence and the ability to enhance analysis through computational algorithms. These algorithms utilize extensive datasets to identify patterns and train the system to autonomously provide recommendations or make decisions.

(4) In their work, Zhang et al. (2018) embraced a definition of machine learning that involves employing a sequential arrangement of nonlinear processing units to extract and transform features. Each subsequent round in this arrangement takes the output from the preceding round as input and learns various representations corresponding to distinct rounds of abstraction. These levels collectively form a hierarchical structure of concepts.

In this research, ML is defined as the simulation of human thinking to process input data and output target variables based on the cumulative experience of previous responses.

2.2 Machine Learning Techniques

Taha (2023) categorizes machine learning (ML) clustering techniques into four categories: supervised, unsupervised, semi-supervised, and reinforcement learning. The following section offers an overview of each of these categories:

Supervised Learning

The primary goal is to acquire knowledge of a function that can effectively associate input data with corresponding output values by utilizing labeled training examples (Sarker, 2021). Supervised learning algorithms utilize the provided input and output data to deduce the underlying function and subsequently generate predictions for new, unseen data. This learning approach is frequently utilized in classification tasks, where data samples are assigned to predefined classes, and in return tasks, where the goal continuously forecasts values based on

the data. For example, it can be used to classify emails by predicting the class based on the given text.

Unsupervised Learning

It operates on unlabeled datasets, extracting patterns and structures without predefined output labels (Taha, 2023). Unsupervised learning is a data-driven approach focused on uncovering significant patterns, groupings, and generative features within a dataset. Unsupervised learning encompasses various tasks, such as clustering, grouping similar data samples, characteristic learning, frequency, dimensionality reduction, discovering correlation rules, and abnormal detection. This approach provides valuable insights into the data's inherent structure and is commonly employed for exploratory analysis purposes.

Semi-supervised Learning

It integrates aspects of previous learning methods by utilizing both data types (Taha, 2023). This method is used when labeled data is limited but unlabeled data is plentiful (Sarker, 2021). The key objective of semi-supervised learning is to improve prediction accuracy by incorporating information from both types of data. It is widely used in fraud risk detection, text and data classification, and machine translation.

Reinforcement Learning

It focused on training software agents or machines to make optimal decisions within a given environment (Gorment et al., 2023). There is interaction between the learning environment and the software agent, and the agent learns from the feedback in the environment based on whether it receives true or false. The goal is to maximize cumulative rewards or minimize risks by taking actions informed by environmental feedback. Reinforcement learning is especially effective for training AI models to perform complex tasks, including self-driving vehicles, manufacturing automation, robotics, and supply chain management. However, solving simple problems is not suitable for using reinforcement learning.

To summarize, ML encompasses a range of learning methodologies. Supervised learning uses labeled data to understand input-output relationships, whereas unsupervised learning analyzes unlabeled data to uncover patterns and structures. Semi-supervised learning enhances predictions by leveraging both data types, while reinforcement learning enhances the decision process through the use of receiving true or false. Each of these learning approaches has unique

strengths and is applied across various domains, contributing significantly to the progress of artificial intelligence and automation technologies.

2.3 Machine Learning for Cybersecurity Applications

Cybersecurity generally includes three areas: prevention, detection, and response (Li et al., 2019). In the real world, 100% prevention is impossible. For example, it is not possible to prevent an attacker from creating malware or phishing emails. Most ML in cybersecurity focuses on threat detection (Apruzzese et al., 2023). According to Sarker, I. H. (2023), cybersecurity threat identification employs two primary approaches: signature-based and behavior-based. Signature-based approaches are based on specific patterns that match known threats, assuming that future threats will exhibit similar patterns. Conversely, the behavior-based approach is not based on patterns. It establishes a baseline of normal behavior and identifies harmful activities that deviate from it, interpreting such deviations as potential security incidents. Both approaches complement each other: signature-based approaches are highly precise in identifying known threats, while behavior-based approaches, though prone to more false alarms, are adept at detecting novel attacks. However, both methods have limitations in detecting zero-day attacks. This is because there is no pattern, and behavior can be referenced. This type of threat led to the adoption of advanced methods. Cybersecurity professionals consider AI's capabilities to detect unknown malware, such as ML or deep learning (DL) techniques (Martínez Torres, Iglesias Comesaña and García-Nieto, 2019). There are different threat detection systems in cybersecurity.

Network Intrusion Detection

Unsupervised learning techniques play a crucial role in scenarios where obtaining labeled data for an entire network is challenging. These methods allow us to discover patterns and anomalies without relying on explicit supervision. Within this category, clustering methods have shown promising results. Let's break down the key points from the paragraphs you provided:

Clustering for Intrusion Detection:

- Researchers like Apruzzese et al. (2017) have explored using clustering techniques for detecting attacks. In their study, they clustered NetFlows (network flow data) based on similar temporal behavior. By doing so, they identified victim's hosts that triggered

alarms from a network intrusion detection system (NIDS) that relied on manual signatures.

- The integration of machine learning (ML) techniques significantly improved the NIDS's detection performance. While the traditional signature-based NIDS detected only three malicious hosts, incorporating ML allowed for the identification of a higher number of threats.

Supporting Rule Generation for NIDS:

- Unsupervised methods have also been leveraged to generate rules for misuse-based NIDS. These rules help identify abnormal behavior or potential attacks within the network.
- Researchers have successfully employed unsupervised approaches to counter lateral movement—instances where attackers move laterally within a network. By minimizing false positives, these methods enhance the effectiveness of NIDS.

Deep Learning and PCAP Analysis:

- Deep, unsupervised algorithms have proven beneficial for NIDS. For example, Mirsky et al. (2018) used DL techniques to analyze data.
- Their approach maintains a low false positive rate but significantly improved the detection rate from less than 1% to over 95%. This is a significant leap in accuracy and reliability.

These methods can enhance threat detection, reduce false positives, and adapt to evolving attack patterns.

Malware Detection

There is a different level detection in malware detection.

Malware Detection and Host-Level Analysis:

- Malware detection is a critical challenge in cybersecurity. Since malware primarily affects specific devices, we analyze data at the host level.

- Windows OS has been the primary target for malware attacks due to its widespread usage. However, attackers are increasingly focusing on mobile devices running Android OS.
- There are two main types of analyses for detecting malware:
 - Static Analysis: This approach identifies malware by examining a file without executing any code. It extracts properties from the file and analyzes them using machine learning (ML) models.
 - Dynamic Analysis: It analyses the software behavior during execution. The suspicious file is executed in an isolation environment sandbox, and ML models capture and analyze its process behaviors.

Static Analysis and ML Techniques:

- Static analyses are straightforward and effective against known malware. They can be further improved using various ML approaches.
- Clustering is one such technique. Researchers like Li et al. (2017) have used clustering to enhance Android malware detection. By identifying shared properties among similar malware samples, they achieved higher detection rates.
- When labeled data is available, static analyses can be even more accurate. Additionally, DL can perform detection after converting executable files into images. Kalash et al. (2018) impressively identified over 99% of Windows malware using this method.
- However, static detection approaches have limitations. Malware executables can be modified without altering their underlying logic, allowing them to evade static methods. Advanced malware can modify its executables automatically based on the victim's system to reduce the static detection rate.

Dynamic Analysis and ML Solutions:

- ML combines dynamic analysis to provide practical solutions against different types of malware (malware that constantly changes its appearance).
- Clustering is again valuable here. The malware has similar behaviors that are grouped, and ML solutions can tailor for previously unseen clusters.
- Amer and Zelinka (2020) concentrated on Windows malware. They used ML's Natural Language Processing (NLP) techniques with graph analysis, which they then fed into dynamic API calls to achieve an impressive 99.9% accuracy.

- Liu et al. (2021) proposed DL for grouping Android malware. Their deep neural networks extracted relevant dynamic features, resulting in nearly 80% accuracy.
- Another study tackled Windows ransomware using deep learning, achieving high detection rates (93%) and precision (97%) (Al-Hawawreh and Sitnikova, 2019).

Phishing Detection

Phishing remains a common and persistent threat in the cybersecurity landscape. It is a common method to be used for infiltrating target networks (Kettani and Wainwright, 2019).

Phishing Websites Detection:

- Phishing websites are cleverly disguised to resemble legitimate sites, making them a potent vector for infiltrating target networks.
- ML can help detect these malicious sites. There are two primary approaches:
- URL-Based Analysis: In this method, the URL or visual representation of the webpage is analyzed. Researchers like Tian et al. (2018) have explored this avenue.
- Blacklists: Traditionally, blacklists have been used to block known phishing sites. However, these lists become unreliable as attackers constantly shift their tactics across multiple sites. Sophisticated adversaries often create “squatting” phishing websites that mimic legitimate domains but subtly alter the URL.
- ML as an Alternative: ML provides an alternative method to maintain the phishing blacklist instead of manually. Modern web browsers already leverage ML techniques to assess the trustworthiness of websites dynamically (Alsaedi et al., 2024).

Phishing Email Detection:

- Detecting phishing emails is equally critical. These emails either direct users to compromised websites or manipulate them into sharing sensitive information.
- ML and Natural Language Processing (NLP) play a key role in analyzing email content. Researchers like Alhogail and Alsabih (2021) have explored this avenue.
- Unsupervised ML Techniques: Diale, Celik, and Van Der Walt (2019) achieved impressive results by using unsupervised ML techniques. Their approach achieved a detection rate of over 95%.

- Challenges with Ground-Truth Labels: Obtaining reliable ground-truth labels for email classification can be challenging. Similar to phishing website detection, this challenge has led email providers to adopt supervised ML techniques, enhancing their automatic filters (Karim et al., 2019).

2.4 Theoretical Framework

Organizations should understand their impact on the company and business in advance to adopt new technology or innovation. These factors may come from the external or internal environment. Different models that consider the proportions adopter groups of psychological and demographic, whether they are individuals or organizations, willing to use technology or innovation (van Oorschot, Hofman, and Halman, 2018).

2.4.1 Background Theory

Different research models and theoretical frameworks have been developed to understand the factors that influence the adoption of new technology (Hasani et al., 2023). These include theories such as the technology acceptance model (Alneyadi, Md Kassim, and Yin, 2022), the protection motivation theory (Al-Kumaim and Alshamsi, 2023), the diffusion of innovation theory (Shaikh et al., 2023), and the unified theory of acceptance and use of technology (Alneyadi, Md Kassim, and Yin, 2022), each employed to clarify the adoption processes. Numerous studies have investigated the adoption of new technologies within cybersecurity in the financial services sector. Table 2.2 provides a synthesis of the primary areas covered in prior research.

Table-2.2: Summary of Studies Analysis

Theme Analysed	Studies	Theoretical Framework	Main Findings	Methodology	Conclusions
This study investigates factors influencing users' intention to adopt AI-based cybersecurity systems in the UAE.	Rashed Mohamed Al Humaid Alneyadi, M. and Kassim Nommalini, M. (2023)	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.	- The study used a quantitative approach guided by the positivist research philosophy. - It employed a correlational research design to test an extended Protection Motivation Theory (PMT) model. - Data was collected through online questionnaires from a purposive sample of participants working in IT and cybersecurity roles in UAE government and semi-government organizations. - The data was analyzed using the PLS-SEM strategy with SmartPLS software, with two phases: (1) assessing the measurement model and (2) assessing the structural model.	The main conclusions of the study are: 1. The study investigated factors influencing the intention to adopt AI-based cybersecurity systems in the UAE. 2. The study used a quantitative approach, which limited the ability to provide unique insights, and the authors recommend using a mixed-method approach in future research. 3. The study's scope was limited to individuals working in government and semi-government organizations in Abu Dhabi, and the authors recommend expanding the scope in future studies and testing more constructs beyond the ones used in the extended PMT model.
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, I. (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.	- Survey methodology with 1,741 participants with prior chatbot experience - Convenience sampling with informed consent - 8-factor, 34-item scale with 5-point Likert scale - Multianalytical approach using Structural Equation Modeling (SEM) and Artificial Neural Network (ANN) analyses	The key conclusions of the study are: 1) Factors related to the Protection Motivation Theory, such as perceived vulnerability, perceived severity, self-efficacy, response efficacy, and response costs, positively predict the sustainable use of AI chatbots; 2) Confidentiality emerged as the most influential predictor of sustainable use of AI chatbots; 3) The study developed a comprehensive model that integrates cybersecurity factors (confidentiality and privacy) with the Protection Motivation Theory, providing a holistic framework for understanding the social sustainability of AI chatbots; 4) To maintain confidentiality in AI chatbots, service providers should implement measures such as encryption, robust data protection policies, and user control over personal data; 5) The findings indicate that users' perceptions of threats and efficacy of AI chatbots, as well as cybersecurity concerns about confidentiality and privacy, play a crucial role in the sustainable use and social sustainability of AI chatbots.
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, N. H. and Alshamsi, S. K. (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.	Quantitative research method - Questionnaire survey of 310 financial executive officers in UAE banks - Probability random sampling to select the sample - 368 questionnaires distributed, 310 used for analysis after discarding 58 incomplete responses	The study investigated factors that contribute to cyberattack prevention in financial organizations in the UAE, proposed a research framework using Protection Motivation Theory and new variables like cybersecurity leadership, organization frequent training, and government frequent alerting, and provided managerial and theoretical implications, emphasizing the importance of cybersecurity leadership, government frequent alerting, and organization cybersecurity frequent training in practice.
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, M. R. M. A. H., Md Kassim, N. and Yin, T. S. (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.	- Quantitative, cross-sectional research methodology - Correlational research design - Web-based survey questionnaire - Sample size of 178 respondents, selected using purposive sampling - Data cleaned and prepared using SPSS - Data analyzed using PLS-SEM	The study is expected to contribute to the available body of knowledge by enriching the literature on adopting and using autonomous or semi-autonomous technologies like AI-based cybersecurity systems. It is also expected to contribute to theory development by introducing a new variable to a hybrid of PMT and UTAUT2 models. The findings are expected to help decision-makers in organizations choose AI-based cybersecurity systems whose design and functionality match the factors found to positively impact users' intention to use them, in order to minimize resistance and facilitate smooth adoption. The findings may also help developers of AI-based cybersecurity systems understand the parameters they should consider when designing such systems to enhance 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, T. 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.	- Quantitative survey methodology - Survey distributed to around 190 IT experts from UK organizations - Survey delivered electronically using Google Forms - SPSS and AMOS used for Confirmatory Factor Analysis and Structural Equation Modeling	Organizations must be prepared to respond as cyberattacks increase in frequency. This study has proposed a comprehensive framework that incorporates the TOE framework, TAM, DOI, and the balanced scorecard to identify the factors that impact cybersecurity technologies adoption by SMEs in the UK and their impact on organizational performance. The key factors with the highest impact on cybersecurity technology adoption were organizational flexibility, collaborative board oversight, and vendor support. The study makes theoretical contributions by integrating multiple frameworks to develop a comprehensive model for cybersecurity technology adoption, and practical contributions by providing empirical evidence on the factors impacting cybersecurity technology adoption and organizational performance.
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, I. M. 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.	- Data was collected through an online survey of 208 Islamic bank customers in Karachi, Pakistan who were non-users of digital banking services. - A filter question was used to ensure only non-users participated. - Validated and modified instruments from prior research were used to measure the key constructs. - The data was analyzed using the partial least squares (PLS) technique with SmartPLS software.	The key conclusions from the paper are that regulators and central banks should understand the barriers preventing non-users from adopting digital banking services and embrace new technology channels that customers want to use. Policymakers and Islamic bank management should investigate the key factors influencing digital banking adoption, such as technology self-efficacy, perceived relative advantage, perceived complexity, and perceived compatibility. There may be additional variables beyond the ones studied that could drive digital banking adoption. Policymakers may need to make modifications to digital policymaking to gain the support of non-users, and central bankers should consider the findings to persuade clients to use available digital services.

Protection Motivation Theory (PMT)

It is a widely used theory that explains users' behavior in accepting technology (Al-Kumaim and Alshamsi, 2023). This theory focuses on individuals' motivation to protect themselves from perceived threats. The model consists of two key components: threat appraisal and coping appraisal (Alneyadi, Md Kassim, and Yin, 2022). Threat assessment includes an individual's evaluation of the likelihood and severity of potential damage. Perceived severity reflects the perceived negative consequences of not adopting the recommended behavior, while perceived vulnerability captures the individual's perception of the likelihood of experiencing harm (Farooq, Ndiege, and Isoaho, 2019). On the other hand, copying appraisal includes self-efficacy, response efficacy, and response costs. They believed the recommended actions could avoid harm, their confidence in implementing the behavior successfully, and the costs associated with adopting the recommended behavior.

Unified Theory of Acceptance and Use of Technology (UTAUT2)

It was formulated as a revision of the original UTAUT model by Venkatesh, Morris, Davis, and Davis in 2003 (Abu Shanab et al., 2020). UTAUT2 introduces two main outcomes: behavioral intention and use behavior, along with seven predictors that include social influence, price value, hedonic motivation, facilitating conditions, habit, performance expectancy, and effort expectancy. These variables are pivotal in shaping user acceptance and adoption behaviors towards information technology (IT) solutions. Notably, the initial trio (effort expectancy, performance expectancy, and social influence) directly impact user intentions and behaviors, while the remaining factors are identified as robust predictors of individual behaviors (Alneyadi, Md Kassim, and Yin, 2022).

Technology Acceptance Model (TAM)

It has garnered considerable acclaim for its effectiveness in explaining the adoption and utilization of information technology. This model adeptly captures a significant portion of the variability in users' intentions to adopt and use technology across diverse settings (Hasani et al., 2023). TAM offers valuable insights into technology acceptance, its integration in the workplace, and the factors influencing user adoption (Chen, 2023). The core aim of TAM is to clarify the connection between technological acceptance, adoption, and, finally, the willingness to use the technology. It identifies usefulness and ease of use as essential factors that profoundly influence new technology adoption (Putri, Widagdo, and Setiawan, 2023).

Diffusion of Innovation (DOI)

This theory is a significant model for guiding technological advancements by effectively modifying and presenting innovations to accommodate different levels of adoption. It recognizes the crucial role of peer networking and communication in the adoption process (Hasani et al., 2023). This theory pertains to individuals adapting to new products, processes, ideas, and philosophies. It categorizes adopters into five groups: innovators, early adopters, early majority, late majority, and laggards (Shaikh et al., 2023). Innovators are enthusiastic about technology, quick to adapt, and willing to take risks. They possess in-depth technical knowledge and embrace uncertainty regarding outcomes. They are motivated and eager to embrace new technologies. Early adopters are visionaries and opinion leaders. They strive to be trendsetters, aiming to revolutionize competitive rules within their industries. They also serve as role models in their social circles. The early majority consists of pragmatists who value peer interaction, prefer proven applications, and prioritize reliable services. The late majority represents conservatives who respond to peer pressure and economic necessity in adopting new technology, primarily driven by the need to keep up with competitors. Lastly, laggards are skeptics who remain isolated from opinion leaders. They view technology as an operational obstacle, harbor suspicions toward innovations and the decision-making process, and perceive it as a limited resource. The utilization and acceptance of innovation can be divided into two stages: implementation and initiation (Hasani et al., 2023). The recognition of a problem serves as the catalyst for the adoption and diffusion process, as it is perceived as a requirement for an innovative product or idea. This recognition prompts the search for innovative solutions that can address the identified issue. Consequently, individuals go through five distinct phases within the innovation-based decision-making system (Shaikh et al., 2023): the knowledge, persuasion, decision, implementation, and confirmation stage.

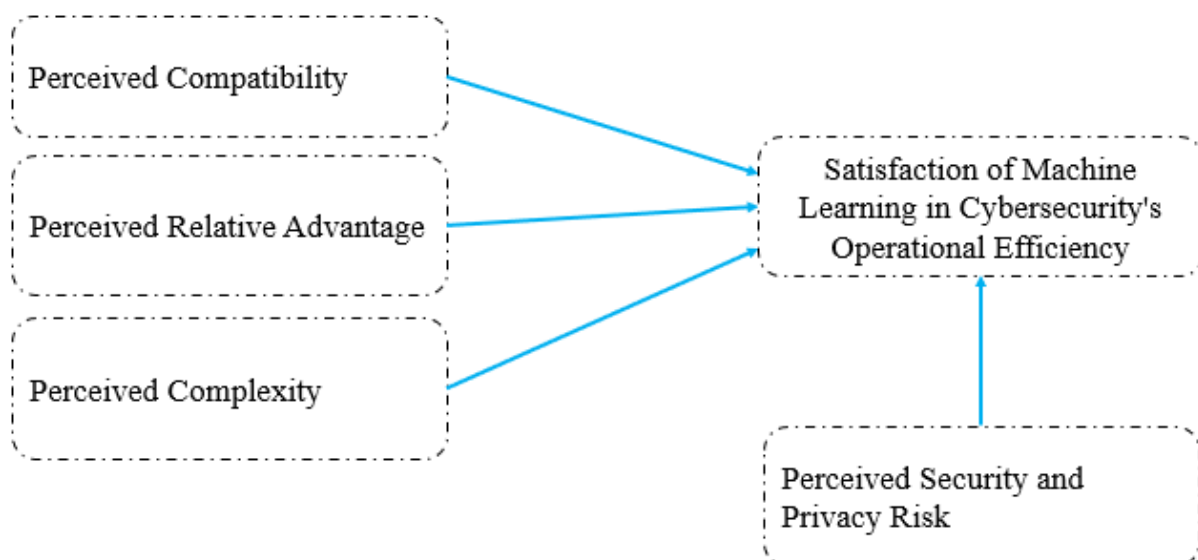
Summary of Theory

This study's objective is to assess the effects of using machine learning on operational efficiency in cybersecurity. The adoption of ML in the banking sector is primarily driven by these factors. In terms of determining the technology acceptance and implementation, the DOI theory is considered the most suitable compared to the aforementioned theories (Shaikh et al., 2023).

2.4.2 Factors in Satisfaction of Machine Learning

In section 2.4.1, various theories were examined. This study is grounded in the DOI theory and incorporates perception factors related to new technology, such as complexity, relative advantage, compatibility. According to Papernot et al. (2018), security and privacy risks concern in ML are important. Machine learning's model training has the potential to store sensitive data, making them susceptible to membership inference attacks. These factors play a crucial role in assessing the extent of their influence on the adoption of this technology. Therefore, this study builds upon the Diffusion of Innovation (DOI) theory and incorporates perceived security and privacy risks as essential factors to investigate in the research and illustrates in Figure 2.1.

Figure-2.2: Research Framework



2.4.2.1 Perceived Compatibility

It represents compatibility between innovation or new technologies and existing technology, indicating the belief that the latest technology is compatible (Charlton and Cornwell, 2019). Perceived compatibility, as defined by Shaikh et al. (2023), refers to a system that aligns with widely accepted standards, user experiences, and requirements. Consequently, perceived compatibility is characterized by the organization's resources that support the implementation of ML and the level of integration between ML and the cybersecurity system. Traditional banks have historical and reputation burdens compared to emerging digital banks in adopting new technologies (Shmuratko and Sheludko, 2021). Banks may encounter challenges in adapting to these changes due to existing practices that hinder the implementation of new technologies.

This can potentially introduce additional security risks as legacy financial and security software systems may not be compatible with innovative solutions. Thus, the below hypothesis is made:

H1: The compatibility of machine learning positively affects cybersecurity's efficiency.

2.4.2.2 Perceived Relative Advantage

Relative advantage pertains to how individuals perceive an innovation as more advantageous than traditional methods. It encompasses benefits such as economic gains, improved status, and increased efficiency (Shaikh et al., 2023). By embracing innovation, individuals can reap these advantages and experience positive outcomes in various endeavors. Thus, the below hypothesis is made:

H2: The Advantage of machine learning positively affects cybersecurity's efficiency.

2.4.2.3 Perceived Complexity

The level of difficulty and comprehensibility associated with an innovation is referred to as complexity, as defined by Mohd Amir et al. (2020). Higher complexity has been found to negatively influence new technology adoption (Izuagbe et al., 2019). It is essential to investigate whether machine learning (ML) has a detrimental effect on the efficiency of cybersecurity operations. Therefore, we propose the following hypothesis:

H3: The complexity of machine learning has a negative impact on the efficiency of cybersecurity.

2.4.2.4 Perceived Security and Privacy Risk

ML algorithms aim to identify patterns within training data, enabling ML to make predictions on new data (Strobel and Shokri, 2022). In training the model, machine learning interacts with various aspects of sensitive data within an organization. Data leakage can occur when an unauthorized entity gains access to the data while training or inference models, making it a critical factor to consider in cybersecurity operations. The implementation of AI in the banking sector enables the utilization of advanced analytical tools and the adoption of innovative business solutions. Banks are required to adopt effective security measures and innovative

solutions to safeguard customer information and meet customer expectations (Lukonga, 2018). Thus, the below hypothesis is made:

H4: Security and Privacy Risks negatively impact cybersecurity operational efficiency.

2.4.3 Summary of Theoretical Framework

Machine learning possesses significant capabilities that can introduce data security and privacy concerns into processes. Additionally, the literature review mentioned above primarily focuses on quantitative methods and lacks qualitative methods. Given the rapid development of AI technology, it becomes crucial to consider the perspectives of IT or cybersecurity professionals, especially considering the emphasis on AI over the years. These gaps should be addressed when organizations contemplate incorporating machine learning into their cybersecurity operations.

To establish a foundation, the independent variables in the Diffusion of Innovation (DOI) model were identified, and subsequently, the factor of "perceived security and privacy risk" was introduced in this study. By comprehending the contextual factors, four hypotheses were formulated, and they are summarized in Table 2.3.

Table-2.3: Summary of Hypothesis

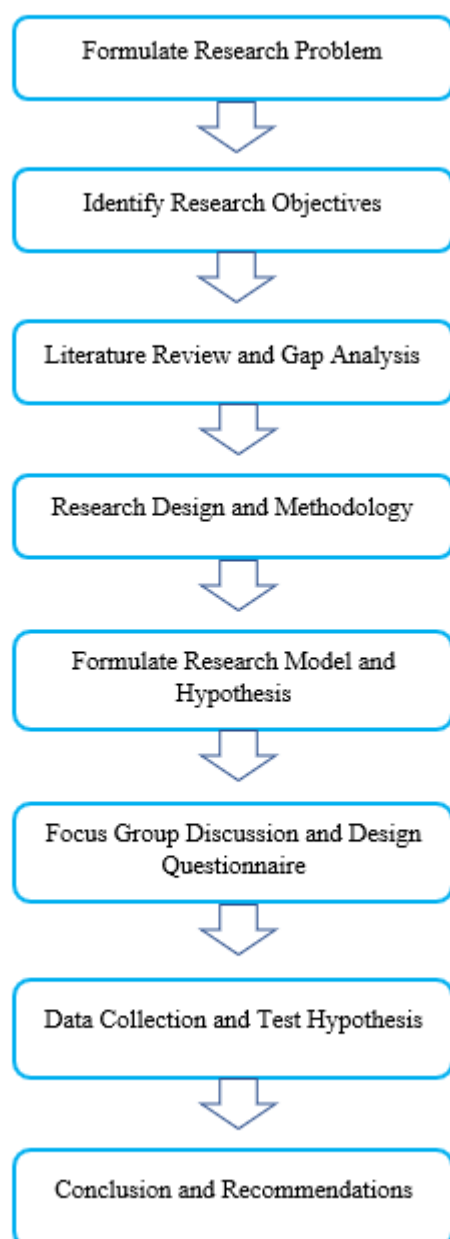
#	Hypothesis
H1	The compatibility of machine learning positively affects cybersecurity's efficiency.
H2	The Advantage of machine learning positively affects cybersecurity's efficiency.
H3	The complexity of machine learning has a negative impact on the efficiency of cybersecurity.
H4	Security and Privacy Risks negatively impact cybersecurity operational efficiency.

The innovation of ML in the banking sector enables the utilization of advanced analytical tools and the adoption of innovative business solutions. Banks are required to adopt effective security measures and innovative solutions to safeguard customer information and meet customer expectations (Lukonga, 2018). Traditional banks have burdens compared to emerging digital banks in adopting new technologies. Banks may face different challenges in adapting to these changes because of existing practices that hinder the implementation of new technologies. This can bring security and privacy risks into legacy financial and security systems because innovative solutions may not be compatible.

3. Research Design

This section outlines the study's methods to ensure a systematic approach to analyzing research actions and addressing research inquiries. It provides comprehensive information on the study, including data collection and evaluation methods, the utilization of various tools and techniques, and the rationale behind the chosen methods (Bouchrika, 2024). The research approach and activities were designed to address the research questions presented in Section 1. The flow of this research is shown in Figure 3.1.

Figure-3.1: Research Flow for this Research



3.1 Research Philosophy and Approach

This study utilizes the pragmatism philosophy as it applies theories, concepts, and findings to tackle the research problem and offer practical solutions (Saunders, Lewis and Thornhill, 2023). It combines theoretical and practical aspects and employs various methods and viewpoints to address research inquiries. The research adopts the abduction approach, which builds upon the DOI theory and introduces a new factor that is empirically tested through observation.

3.2 Research Methodology

Data collection methods serve as techniques for acquiring information for analysis purposes. Qualitative research is commonly utilized to answer the research questions after categories and analyzed factual data or descriptive data (Hammarberg, Kirkman, & de Lacey, 2016). It involves collecting, examining, and interpreting opinions or descriptive data from targeted populations, such as interviews or focus groups (Rosenthal, 2016). Conversely, quantitative method focuses on gathering and analyzing numerical data (Goertzen, 2017). This involves using polls or survey methods to gather the information that can be used for analyses and predictions after conducted statistical algorithm (Kelley-Quon, 2018).

The combined qualitative and quantitative methods are used in this research. This approach helps validate research findings by utilizing both types of data, examining qualitative data in quantitative and quantitative results to validate the qualitative insights (Santos et al., 2017). The analysis uses both primary and secondary data to achieve objective outcomes and results. The real-time data collected by the researcher is classified as primary data, and the researchers provide past data from articles and journals as secondary data (Ajayi, 2023).

Qualitative research methods collect the research topic's opinions, suggestions, and perspectives of participants (Hammarberg, Kirkman, & de Lacey, 2016). To facilitate the effectiveness of collecting data and interaction between researcher and participants, focus group discussions were conducted to encourage in-depth conversations. Focus groups involve group interviews that promote information exchange among participants to generate data, allowing efficient gathering of information from multiple participants simultaneously (Abraham et al., 2022). In the discussion, the researcher encourages participants to ask, share experiences, and provide feedback on others' experiences and viewpoints in response to the researcher's inquiries. This approach effectively leveraged participants' knowledge and experiences.

Conversely, quantitative research methods aim to objectively collect and analyze numerical data to describe, predict, or control factors of interest (Apuke, 2017). This method facilitates testing hypotheses by using collected and analyzed data. Therefore, this research also adopts this method of using a questionnaire to collect data from IT industry employees, particularly those currently or formerly employed in Hong Kong's financial services sector. This approach utilizes the advantages of both methods. It includes a comprehensive understanding of the study, cross-verifying data from multiple sources, complementary insights, flexibility, and validity.

Comprehensive Understanding:

The hybrid approach employs both qualitative and quantitative methods, enabling a thorough comprehension of the research topic (Dawadi, Shrestha, and Giri, 2021). Qualitative methods delve into participants' perspectives, capturing intricate and nuanced data for in-depth insights. On the other hand, quantitative methods provide statistical analysis and generalizability, facilitating examining patterns and relationships among variables.

Cross-verifying:

The hybrid methodology facilitates the cross-verification of data from multiple sources, enhancing the credibility and validity of the research (Ijadi Maghsoodi et al., 2024). By cross-verifying findings obtained through different methods, researchers can bolster the robustness of their conclusions, mitigating biases and increasing confidence in the results.

Complementary Insights:

Qualitative and quantitative methods offer complementary insights. Qualitative methods focus on subjective experiences, constructing meaning and contextual factors, yielding rich narratives and in-depth understanding (Dawadi, Shrestha, and Giri, 2021). Quantitative methods, on the other hand, emphasize objective measurements, statistical analysis, and generalizability, enabling broader conclusions. The hybrid methodology allows researchers to leverage the strengths of both approaches, providing a more holistic and well-balanced perspective on the research topic.

Flexibility:

The hybrid approach provides flexibility in research design and data collection methods. Dawadi, Shrestha, and Giri (2021) can combine qualitative and quantitative methods to align

with specific research questions and objectives. This flexibility enhances adaptability and responsiveness to the research context and participant needs.

Validity:

The hybrid approach supports the validation of research result by incorporating diverse collected data and statistical analysis (Rahman, 2016). It addresses potential biases, increases the reliability of the results, and offers a more comprehensive and well-rounded interpretation of the study.

3.3 Summary of Research Design

In this research, a hybrid methodology is employed, which combines both qualitative and quantitative methods. This approach capitalizes on the strengths of each method, leading to achieve a more comprehensive comprehension of the study, bolstering the validity of the findings, and yielding nuanced and robust conclusions. By integrating qualitative techniques such as interviews or observations with quantitative approaches like statistical analysis or data modeling, researchers can capture rich contextual information while also uncovering patterns and trends within the data. This blending of methods allows for a more holistic and in-depth exploration of the research topic, resulting in more reliable and meaningful outcomes.

Reference List

- Abraham, M. *et al.* (2022) “Implications of XR on privacy, security and behaviour: Insights from experts,” in *Nordic Human-Computer Interaction Conference*. New York, NY, USA: ACM.
- Abu Shanab, E. *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*, 1(1), p. 1. doi: 10.1504/ijbis.2020.10036883.
- Ajayi, V. O. (2023) *A Review on Primary Sources of Data and Secondary Sources of Data*, *Researchgate.net*. Available at: https://www.researchgate.net/publication/370608670_A_Review_on_Primary_Sources_of_Data_and_Secondary_Sources_of_Data (Accessed: July 13, 2024).
- Alamleh, H., AlQahtani, A. A. S. and ElSaid, A. (2023) “Distinguishing human-written and ChatGPT-generated text using machine learning,” in *2023 Systems and Information Engineering Design Symposium (SIEDS)*. IEEE, pp. 154–158.
- 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. doi: 10.1080/01969722.2022.2112539.
- Al-Hawawreh, M. and Sitnikova, E. (2019) “Leveraging deep learning models for ransomware detection in the industrial internet of things environment,” in *2019 Military Communications and Information Systems Conference (MilCIS)*. IEEE.
- Alhogail, A. and Alsabih, A. (2021) “Applying machine learning and natural language processing to detect phishing email,” *Computers & security*, 110(102414), p. 102414. doi: 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 (Basel, Switzerland)*, 13(10), p. 5839. doi: 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*, *Ebscohost.com*. Available at: <https://web.p.ebscohost.com/ehost/detail/detail?vid=0&sid=b78aa9ef-3557-478b-aa6f-8b5c6f57e303%40redis&bdata=JnNpdGU9ZWWhvc3QtbGl2ZQ%3d%3d> (Accessed: July 7, 2024).

- Alsaedi, M. *et al.* (2024) “Multi-modal features representation-based convolutional neural network model for malicious website detection,” *IEEE access: practical innovations, open solutions*, 12, pp. 7271–7284. doi: 10.1109/access.2023.3348071.
- Amer, E. and Zelinka, I. (2020) “A dynamic Windows malware detection and prediction method based on contextual understanding of API call sequence,” *Computers & security*, 92(101760), p. 101760. doi: 10.1016/j.cose.2020.101760.
- Ancillai, C. *et al.* (2023) “Digital technology and business model innovation: A systematic literature review and future research agenda,” *Technological forecasting and social change*, 188(122307), p. 122307. doi: 10.1016/j.techfore.2022.122307.
- Apruzzese, G. *et al.* (2017) “Identifying malicious hosts involved in periodic communications,” in *2017 IEEE 16th International Symposium on Network Computing and Applications (NCA)*. IEEE.
- Apruzzese, G. *et al.* (2020) “Hardening random forest cyber detectors against adversarial attacks,” *IEEE transactions on emerging topics in computational intelligence*, 4(4), pp. 427–439. doi: 10.1109/tetci.2019.2961157.
- Apruzzese, G. *et al.* (2023) “The role of machine Learning in cybersecurity,” *Digital threats: research and practice*, 4(1), pp. 1–38. doi: 10.1145/3545574.
- 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. doi: 10.12816/0040336.
- Arpaci, I. (2024) “A multianalytical SEM-ANN approach to investigate the social sustainability of AI chatbots based on cybersecurity and protection motivation theory,” *IEEE transactions on engineering management*, 71, pp. 1714–1725. doi: 10.1109/tem.2023.3339578.
- Bayram, F., Ahmed, B. S. and Kessler, A. (2022) “From concept drift to model degradation: An overview on performance-aware drift detectors,” *Knowledge-based systems*, 245(108632), p. 108632. doi: 10.1016/j.knosys.2022.108632.
- Bogatinovski, J. *et al.* (2021) “Artificial Intelligence for IT operations (AIOPS) workshop white paper.” doi: 10.48550/ARXIV.2101.06054.
- Bouchrika, I. (2024) *How to Write Research Methodology: Overview, Tips, and Techniques*, *Research.com*. Available at: <https://research.com/research/how-to-write-research-methodology> (Accessed: July 13, 2024).
- Brynjolfsson, E., Li, D. and Raymond, L. (2023) *Generative AI at Work*. Cambridge, MA: National Bureau of Economic Research.
- Caldwell, M. *et al.* (2020) “AI-enabled future crime,” *Crime science*, 9(1). doi: 10.1186/s40163-020-00123-8.

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. doi: 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/agenda/2024/01/cybersecurity-cybercrime-system-safety/> (Accessed: June 29, 2024).

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. doi: 10.1080/14765284.2023.2245279.

Chen, C.-H. (2023) “Extending the technology acceptance model: A new perspective on the adoption of blockchain technology,” *Human behavior and emerging technologies*, 2023, pp. 1–14. doi: 10.1155/2023/4835896.

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. doi: 10.1007/s40745-022-00433-5.

CISA (2024) *Incident detection, response, and prevention*, *Cisa.gov*. Available at: <https://www.cisa.gov/topics/cyber-threats-and-advisories/incident-detection-response-and-prevention> (Accessed: July 6, 2024).

Corsini, A., Yang, S. J. and Apruzzese, G. (2021) “On the evaluation of sequential machine learning for network intrusion detection,” in *Proceedings of the 16th International Conference on Availability, Reliability and Security*. New York, NY, USA: ACM.

Csis (2024) *Significant cyber incidents*, *Csis.org*. Available at: <https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents> (Accessed: June 26, 2024).

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. doi: 10.46809/jpse.v2i2.20.

Diale, M., Celik, T. and Van Der Walt, C. (2019) “Unsupervised feature learning for spam email filtering,” *Computers & electrical engineering: an international journal*, 74, pp. 89–104. doi: 10.1016/j.compeleceng.2019.01.004.

Díaz-Verdejo, J. E. *et al.* (2020) “A methodology for conducting efficient sanitization of HTTP training datasets,” *Future generations computer systems: FGCS*, 109, pp. 67–82. doi: 10.1016/j.future.2020.03.033.

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. doi: 10.1057/s41264-022-00176-7.

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,” in *2019 IEEE AFRICON*. IEEE.

Fleck, A. (2022) *Cybercrime expected to skyrocket in coming years*, Statista. Available at: <https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/> (Accessed: June 29, 2024).

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/6325/8274> (Accessed: July 13, 2024).

Gorment, N. Z. *et al.* (2023) “Machine learning algorithm for malware detection: Taxonomy, current challenges, and future directions,” *IEEE access: practical innovations, open solutions*, 11, pp. 141045–141089. doi: 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 (Oxford, England)*, 31(3), pp. 498–501. doi: 10.1093/humrep/dev334.

Hasani, T. *et al.* (2023) “Evaluating the adoption of cybersecurity and its influence on organizational performance,” *SN business & economics*, 3(5). doi: 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. doi: 10.1007/s12178-020-09600-8.

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. doi: 10.1002/jsc.2525.

HKMA (2019) *Reshaping Banking with Artificial Intelligence*, Hong Kong Monetary Authority. Available at: https://www.hkma.gov.hk/media/eng/doc/key-functions/financial-infrastructure/Whitepaper_on_AI.pdf (Accessed: June 30, 2024).

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: June 29, 2024).

IDC (2023) *IDC FutureScape, IDC: The premier global market intelligence company*. Available at: <https://www.idc.com/getdoc.jsp?containerId=prUS51366723> (Accessed: June 19, 2024).

Ijadi Maghsoodi, A. *et al.* (2024) “What makes effective acute geriatric care? - A mixed methods study from aotearoa New Zealand,” *Ageing international*. doi: 10.1007/s12126-024-09568-7.

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. doi: 10.1016/j.lisr.2019.100969.

Jan, Z. *et al.* (2023) “Artificial intelligence for industry 4.0: Systematic review of applications, challenges, and opportunities,” *Expert systems with applications*, 216(119456), p. 119456. doi: 10.1016/j.eswa.2022.119456.

Javaid, A. *et al.* (2016) “A deep learning approach for network intrusion detection system,” in *Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies (formerly BIONETICS)*. ACM.

Kalash, M. *et al.* (2018) “Malware classification with deep convolutional neural networks,” in *2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*. IEEE.

Karim, A. *et al.* (2019) “A comprehensive survey for intelligent spam email detection,” *IEEE access: practical innovations, open solutions*, 7, pp. 168261–168295. doi: 10.1109/access.2019.2954791.

Kelley-Quon, L. I. (2018) “Surveys: Merging qualitative and quantitative research methods,” *Seminars in pediatric surgery*, 27(6), pp. 361–366. doi: 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(101925), p. 101925. doi: 10.1016/j.tele.2022.101925.

Kettani, H. and Wainwright, P. (2019) “On the top threats to cyber systems,” in *2019 IEEE 2nd International Conference on Information and Computer Technologies (ICICT)*. IEEE.

Kharpal, A. (2023) *China’s ICBC, the world’s biggest bank, hit by cyberattack that reportedly disrupted Treasury markets*, CNBC. Available at: <https://www.cnbc.com/2023/11/10/icbc-the-worlds-biggest-bank-hit-by-ransomware-cyberattack.html> (Accessed: June 29, 2024).

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: June 19, 2024).

Leme Lopes, A. P. (2023) “Artificial history? Inquiring ChatGPT on historiography,” *Rethinking history*, 27(4), pp. 709–749. doi: 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,” in *Lecture Notes in Electrical Engineering*. Singapore: Springer Singapore, pp. 283–290.

Li, Y. *et al.* (2017) “Android malware clustering through malicious payload mining.” doi: 10.48550/ARXIV.1707.04795.

Liang, X.-R. *et al.* (2023) “Outlier-based anomaly detection in firewall logs,” in *2023 International Conference on Communications, Computing, Cybersecurity, and Informatics (CCCI)*. IEEE.

Liu, Z. *et al.* (2021) “Research on unsupervised feature learning for Android malware detection based on Restricted Boltzmann Machines,” *Future generations computer systems: FGCS*, 120, pp. 91–108. doi: 10.1016/j.future.2021.02.015.

Lukonga, I. (2018) *Fintech, Inclusive Growth and Cyber Risks: Focus on the MENAP and CCA Regions*, *Ssrn.com*. Available at: <https://ssrn.com/abstract=3267228> (Accessed: July 3, 2024).

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. doi: 10.1007/s13042-018-00906-1.

Mirsky, Y. *et al.* (2018) “Kitsune: An ensemble of autoencoders for online network intrusion detection.” doi: 10.48550/ARXIV.1802.09089.

Mishra, S. (2023) “Exploring the impact of AI-based cyber security financial sector management,” *Applied sciences (Basel, Switzerland)*, 13(10), p. 5875. doi: 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. doi: 10.1016/j.jisa.2018.11.007.

Mohd Amir, R. I. *et al.* (2020) “Perceived ease of use, perceived usefulness, and behavioral intention: The acceptance of crowdsourcing platform by using technology acceptance model (TAM),” in *Charting a Sustainable Future of ASEAN in Business and Social Sciences*. Singapore: Springer Singapore, pp. 403–410.

Murphy, K. *et al.* (2021) “Artificial intelligence for good health: a scoping review of the ethics literature,” *BMC medical ethics*, 22(1). doi: 10.1186/s12910-021-00577-8.

Noy, S. and Zhang, W. (2023) “Experimental evidence on the productivity effects of generative artificial intelligence,” *SSRN Electronic Journal*. doi: 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. doi: 10.1016/j.techfore.2018.04.032.

Papernot, N. *et al.* (2018) “SoK: Security and privacy in machine learning,” in *2018 IEEE European Symposium on Security and Privacy (EuroS&P)*. IEEE.

Peng, S. *et al.* (2023) “The impact of AI on developer productivity: Evidence from GitHub Copilot.” doi: 10.48550/ARXIV.2302.06590.

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. doi: 10.1016/j.joitmc.2023.100027.

Rahman, M. S. (2016) “The advantages and disadvantages of using qualitative and quantitative approaches and methods in language ‘testing and assessment’ research: A literature review,” *Journal of education and learning*, 6(1), p. 102. doi: 10.5539/jel.v6n1p102.

Rashed Mohamed Al Humaid Alneyadi, M. and Kassim Normalini, M. (2023) “Factors influencing user’s intention to adopt AI-based cybersecurity systems in the UAE,” *Interdisciplinary Journal of Information Knowledge and Management*, 18, pp. 459–486. doi: 10.28945/5166.

Rosenbush, S. (2017) *First AI-Powered Cyberattacks Are Detected*, *Wsj.com*. Available at: <https://www.wsj.com/articles/the-morning-download-first-ai-powered-cyberattacks-are-detected-1510839203> (Accessed: June 27, 2024).

Rosenthal, M. (2016) “Qualitative research methods: Why, when, and how to conduct interviews and focus groups in pharmacy research,” *Currents in pharmacy teaching & learning*, 8(4), pp. 509–516. doi: 10.1016/j.cptl.2016.03.021.

Roser, M. (2022) *The brief history of artificial intelligence: the world has changed fast — what might be next?*, *Ourworldindata.org*. Available at: <https://ourworldindata.org/brief-history-of-ai> (Accessed: June 17, 2024).

Sahiner, B. *et al.* (2023) “Data drift in medical machine learning: implications and potential remedies,” *The British journal of radiology*, 96(1150). doi: 10.1259/bjr.20220878.

Sahu, S. K., Mokhade, A. and Bokde, N. D. (2023) “An overview of Machine Learning, Deep Learning, and Reinforcement Learning-based techniques in Quantitative Finance: Recent progress and challenges,” *Applied sciences (Basel, Switzerland)*, 13(3), p. 1956. doi: 10.3390/app13031956.

Santos, J. L. G. dos *et al.* (2017) “INTEGRAÇÃO ENTRE DADOS QUANTITATIVOS E QUALITATIVOS EM UMA PESQUISA DE MÉTODOS MISTOS,” *Texto & contexto enfermagem*, 26(3). doi: 10.1590/0104-07072017001590016.

Sarker, I. H. *et al.* (2020) “Cybersecurity data science: an overview from machine learning perspective,” *Journal of big data*, 7(1). doi: 10.1186/s40537-020-00318-5.

Sarker, I. H. (2021) "Machine learning: Algorithms, real-world applications and research directions," *SN computer science*, 2(3). doi: 10.1007/s42979-021-00592-x.

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. doi: 10.1007/s40745-022-00444-2.

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). doi: 10.1007/s42979-021-00557-0.

Saunders, M., Lewis, P. and Thornhill, A. (2023) *Research methods for business students*. 8th ed. London, England: Pearson Education.

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). doi: 10.21098/jimf.v9i1.1545.

Shmuratko, Y. A. 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. doi: 10.18371/fcaptp.v4i31.190792.

Shwedeh, 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*, *Researchgate.net*. Available at: <https://www.researchgate.net/publication/376450709> (Accessed: June 29, 2024).

Statista Market Insights (2024) *Cybersecurity - worldwide*, Statista. Available at: <https://www.statista.com/outlook/tmo/cybersecurity/worldwide> (Accessed: June 29, 2024).

Strobel, M. and Shokri, R. (2022) "Data privacy and trustworthy machine learning," *IEEE security & privacy*, 20(5), pp. 44–49. doi: 10.1109/msec.2022.3178187.

Taha, K. (2023) "Semi-supervised and un-supervised clustering: A review and experimental evaluation," *Information systems*, 114(102178), p. 102178. doi: 10.1016/j.is.2023.102178.

Tian, K. *et al.* (2018) "Needle in a haystack: Tracking down elite phishing domains in the wild," in *Proceedings of the Internet Measurement Conference 2018*. New York, NY, USA: ACM.

Varghese, B. (2019) "A history of the cloud," *ITNOW*, 61(2), pp. 46–48. doi: 10.1093/itnow/bwz049.

Yamin, M. M. *et al.* (2021) "Weaponized AI for cyber attacks," *Journal of information security and applications*, 57(102722), p. 102722. doi: 10.1016/j.jisa.2020.102722.

Zhang, W. J. *et al.* (2018) "On definition of deep learning," in *2018 World Automation Congress (WAC)*. IEEE.