Heliyon 10 (2024) e37571

Contents lists available at ScienceDirect

Heliyon

journal homepage: www.cell.com/heliyon

Research article

Integrating machine learning for sustaining cybersecurity in digital banks

Muath Asmar [a,*], Alia Tuqan [b]

[a] Department of Finance, Faculty of Business and Communication, An-Najah National University, Nablus, Palestine
[b] Master of Business Administration, Faculty of Graduate Studies, An-Najah National University, Nablus, Palestine

ARTICLE INFO

Keywords:
Cybersecurity
Digital banking
Machine learning
Fraud detection
Security measures
Phishing attacks

ABSTRACT

Cybersecurity continues to be an important concern for financial institutions given the technology's rapid development and increasing adoption of digital services. Effective safety measures must be adopted to safeguard sensitive financial data and protect clients from potential harm due to the rise in cyber threats that target digital organizations. The aim of this study is to investigates how machine learning algorithms are integrated into cyber security measures in the context of digital banking and its benefits and drawbacks. We initially provide a general overview of digital banks and the particular security concerns that differentiate them from conventional banks. Then, we explore the value of machine learning in strengthening cybersecurity defenses. We revealed that insider threats, distributed denial of service (DDoS) assaults, ransomware, phishing attacks, and social engineering are main cyberthreats that are digital banks exposed. We identify the appropriate machine learning algorithms such as support vector machines (SVM), recurrent neural networks (RNN), hidden markov models (HMM), and local outlier factor (LOF) that are used for detection and prevention cyberthreats. In addition, we provide a model that considers ethical concerns while constructing a cybersecurity framework to address potential vulnerabilities in digital banking systems. The advantages and disadvantages of incorporating machine learning into the cybersecurity strategy of digital banks are outlined using strengths, weaknesses, opportunities, threats (SWOT) analysis. This study seeks to provide a thorough knowledge of how machine learning may strengthen cybersecurity procedures, protect digital banks, and maintain customer trust in the ecosystem of digital banking.

1. Introduction

Banking has seen a significant shift in the contemporary digital era, moving from traditional brick-and-mortar facilities to the internet and mobile platforms. At present, customers may conduct transactions from almost anywhere and at any time owing to the expansion of digital banking and the convenience it offers [1]. In addition, customers are able to manage accounts, transfer funds, and pay bills online as a result of this modification, which has radically altered how people interact with their financial institutions [2].The provision of financial services via digital platforms, such as mobile applications, websites, and other technological tools, is referred to as digital banking, sometimes known as Neobanks or Virtual Banks [3]. Currently, the majority of conventional banks offer digital services, and the government is actively promoting the use of cashless payments in daily life, especially during the Covid-19 pandemic

* Corresponding author.
E-mail addresses: asmar@najah.edu (M. Asmar), aliatuqan@stunajah.edu (A. Tuqan).

https://doi.org/10.1016/j.heliyon.2024.e37571
Received 20 December 2023; Received in revised form 4 September 2024; Accepted 5 September 2024
Available online 6 September 2024

when there is a greater need to minimize physical interactions [4].

Digital banking not only offers convenience, but also introduces new threats and concerns. The increased threat of Cyberattacks is one of the main issues with digital banking [5]. The digital banking sector, which is made up of various businesses, faces Cybersecurity and data breach issues [6]. Recently, the potential of security breaches and data theft has greatly increased, as the use of digital channels for banking services increases [7]. Cybercriminals always come up with new tactics, such as phishing scams, malware attacks, and identity theft, to take advantage of weaknesses in financial systems. These dangers have become a very critical concern that needs the attention of organizations to confidentially ensure the protection and security of information systems [8]. Thus, banks have invested significantly in cybersecurity tools, such as firewalls, encryption, and intrusion detection systems, to reduce these risks [9]. Thus, due to the constantly changing threat landscape, digital banks must maintain their systems updated to prevent cyberattacks. An emerging phenomenon in the banking industry is the rise of digital banks, which are totally virtual institutions that lack physical offices and conduct all banking operations only through mobile applications. The complete digitization of operations alters the way consumers perceive the service, and thus, impacts their patterns of consumption and financial behavior [4].

Cybersecurity in digital banking must include intrusion detection systems (IDS) and intrusion prevention systems (IPS) [10]. IDS track network activity and warn security personnel for additional investigation when they spot potential security lapses or illegal activity. IPS, on the contrary, employ methods, such as firewall rules and behavior analysis, to stop harmful actions before they cause harm. They actively prevent and mitigate cyber threats in real-time. Digital Banks may strengthen their security protocols, safeguard their networks, systems, and invaluable customer data, as well as actively defend against developing cyberattacks by deploying IDS and IPS [11]. However, implementing technology solutions cannot sufficiently address the complex issues of cybersecurity. A thorough comprehension of the underlying dangers and the capacity to foresee and react to developing prospective dangers are required. Here, machine learning has a key role to play [12]. Machine learning is a subset of artificial intelligence that enables the system to learn from their previous performance and advance naturally. Machine learning can be used in the context of cybersecurity to identify and stop cyberattacks by analyzing massive amounts of data, identifying patterns, and detecting anomalies that could be signs of a possible danger [13]. Furthermore, artificial intelligence and machine learning have served as the primary tools used by banks in their credit card fraud detection systems. These tools can detect and stop fraudulent transactions with speed and accuracy by analyzing the transaction histories, user behavior patterns, and external data sources [14]. A lot of recent attention has been paid to machine learning in the banking industry [15]. Banks are investigating how this technology may increase the protection of their assets and boost the effectiveness of their entire operations. However, incorporating machine learning in digital banking encounters challenges, such as concerns with data quality and privacy [16].

Maintaining customer confidence and trust is a major problem for digital banking [17]. When customers trust digital banking systems with their personal and financial information, they require a high level of safety and reliability. Any violation of that trust, such as a system failure or data breach, can negatively affect the financial institution's reputation and customer base [18]. In addition, given the rapid improvements in technology, financial institutions must continually spend in the modernization of their digital banking systems to stay up to date with changing customer expectations and industry norms [19]. In today's digital settings, cyber threats are becoming more and more dynamic, which drives the need for automated and intelligent cyber solutions [20]. Indeed, several studies have explored machine learning for enhanced cybersecurity in different applications and contexts [e.g., 21,22–24]. These extensive surveys and reviews demonstrate how machine learning improved cybersecurity in various applications and scenarios. However, the use of machine learning for enhancing and sustaining cybersecurity in digital banking is incomprehensively examined in the existing literature, and there remains a research gap in comprehensively assessing their combined effectiveness in digital banks. Thus, this study aims to focus on the interaction between cybersecurity and machine learning in digital banking.

The rationale for combining machine learning and cybersecurity in digital banking is based on the fact that digital banks are more vulnerable to cyberthreats than conventional banks. Unlike conventional banks, digital banks are unable to recover in the case of a network or system failure [25]. Some digital banks have failed in the U.S. and Japan, while others have suffered losses from significant data breaches [26]. Financial technology development has amplified cybercrime, prompting trust and security concerns in banking [6]. Traditional security techniques, such as statistical and rule-based methods, often struggle to adapt to the changing nature of new threats [25]. Thus, it is a sine qua non to employ machine learning that have the capability to recognize and react to intricate, unfamiliar dangers in real-time by examining extensive quantities of data and recognizing patterns that suggest harmful behavior.

A comprehensive analysis of a state-of-the-art machine learning in the cybersecurity of digital bank is introduced. Through this approach, we aim to address the following important queries.

1. What are the cybersecurity attacks that digital banks are exposed?
2. What are the cutting-edge machine learning algorithms significant to sustain the cybersecurity of digital bank?
3. How can cyber analysts, researchers, or engineers integrate machine learning to sustain the cybersecurity of digital banks?
4. What are the strengths, weaknesses, opportunities, and threats of integrating machine learning into cybersecurity of digital banks?

In this light, we aim to explore how machine learning can be used to improve and sustain digital banking industry cybersecurity and its associated challenges. Accordingly, in an effort to provide an even clearer analysis of machine learning applications on cybersecurity of digital banking, our primary contributions in this extensive review-based study are thus outlined as follows. First, this study provides an extensive analysis of current developments and cutting-edge machine learning techniques in a cybersecurity application for digital banks. Second, a flowchart is designed to explain the sequential steps and decision-making points involved in using machine learning for reliable cybersecurity, and a model for integrating cybersecurity with machine learning in digital banks is developed. Third, this study summarizes advantages, disadvantages, challenges, and drawbacks of integrating cybersecurity with machine

learning in digital banking using SWOT analysis. Finally, the current challenges and open issues of integrating machine learning for cybersecurity in digital banks are highlighted, and possible research routes are suggested. Implementing machine learning techniques to enhance cybersecurity measures in the digital banking presents practical implications that stimulate innovation, enhance security results, improved operational efficiency, ensuring the integrity of services and encourage cooperation between cybersecurity firms, digital banks, and regulators to build a safe and stable financial ecosystem.

The remainder of this paper is organized as follows. The next section provides a detailed literature review process methodology. Then, the literature pertaining to digital banks was examined to comprehend their functions, how they differ from traditional banks, and the potential advantages of technological adoption in the banking sector. Subsequently, the literature on the importance of cybersecurity has been investigated to determine the main cybersecurity attacks to which digital banks are exposed. Thereafter, to comprehend how machine learning may support the sustainability of cybersecurity in digital banks, the literature on the significance of machine learning and the integration of cybersecurity and machine learning in the context of digital banks has been investigated. This approach includes the introduction of machine learning and cybersecurity integration model and SWOT analysis of integrating machine learning into cybersecurity in digital banks. Finally, we conclude the study by highlighting the limitation, future research direction, and recommendations to banks, regulatory bodies, and government agencies.

2. Methodology

The present study endeavors to investigate how machine learning may support and improve the cybersecurity of digital banks using an approach based on the results of previous literature. This method allows for a comprehensive analysis of existing research in order to answer the research questions presented in this study. The literature review was conducted using reliable academic databases and search engines to ensure a broad and relevant collection of academic articles based on related search keywords. The selection of articles for the review was based on criteria related to article relevance, recency, peer review, and language. Key information from each article was extracted, including the specific cybersecurity challenges addressed and machine learning techniques used. The subsequent step involved conducting a critical review and thematic analysis of the content of each article. We then combined and synthesized the insights from this process to provide a methodical and structured investigation of how machine learning can sustain cybersecurity in digital banks.

2.1. Literature search methodology

We investigated academic publishing archives (such as Google Scholar, Web of Science, Dimensions, and IEEE Xplore) to identify any similar studies on incorporating machine learning for cybersecurity of digital banks. We discovered a number of machine learning-based cybersecurity applications with a large body of work [e.g., 23, 27, 28]. We discovered an abundance of studies that investigate the integration of machine learning for sustaining cybersecurity in digital banks. In the present study, we shed light on this significant subject by examining several up-to-date and carefully selected works at the cutting edge of this study field [e.g., 5, 29, 30]. This study will be beneficial to scholars and professionals interested in understanding the role of machine learning integration in maintaining cybersecurity within digital banks. The multidisciplinary nature of integrating machine learning to maintain cybersecurity in digital banking prompted us to synthesize three primary study areas to explore pertinent topics and identify innovative research directions.

2.2. Selection process

To obtain sufficient information on these subjects, pertinent and well-cited publications were searched from various journals utilizing online databases including Springer Link, Science Direct, IEEE digital library, Taylor and Francis, and Emerald Insights (Emerald). The first step to find relevant research publications includes the identification of search keywords. In this step, several keywords related to digital banks, cybersecurity, and machine learning were used. The second step involves construction of search strings using Boolean Operators. Table 1 presents the primary study areas, searched fields, and search keyword. We utilized the logical operator “OR” to distinguish synonyms, alternate spellings, or abbreviations, allowing results that include any of these terms to be displayed. We employed the logical operator “AND” to connect phrases, guaranteeing that we obtained results that included all of the given terms that represent the study areas, including digital banks and cybersecurity, machine learning and cybersecurity, and digital banks and machine learning.

Table 2 presents the criteria for including or excluding search results derived from the search strings created.

Table 1
Primary study areas, searched fields, and search string.

Primary Study Areas	Searched fields	Search keyword
Cybersecurity	Title, Abstract, Keywords	Cyber, Threat, Attack, Crime, Fraud
Machine Learning	Title, Abstract, Keywords	Machine Learning, Artificial Intelligence, Deep Learning
Digital banks	Title, Abstract, Keywords	Finance, Bank

A list of highly referenced, peer-reviewed publications was sorted and thoroughly examined (initial abstract examination), with the articles selected based on how well they addressed and contributed to the research question of this study. Subsequently, the selected articles underwent another screening to exclude unrelated studies that produced redundant findings and to establish connections between the various articles and the research topics in this investigation. In Fig. 1, the main steps of the research methodology are visually represented for each step of the literature selection process via the databases.

3. Literature review

The technology's quick development has completely transformed the banking sector, bringing development to digital banks that provide various financial services via digital platforms [31]. Understanding each of the cybersecurity threats and opportunities that face digital banks is crucial because they continue to grow in popularity and transform the banking industry [31]. In this literature review, we examine the key features of digital banks and how they differ from traditional banks. We explore the value of cybersecurity generally and specifically in the context of digital banking, considering several security protocols that have been implemented to protect confidential financial data. We also examine the significance of machine learning and how it could enhance cybersecurity measures in the world of digital banking. This review attempts to provide a thorough knowledge of the connection of cybersecurity, machine learning, and digital banks by combining previous study findings. It also offers helpful insights for researchers as well as professionals in the field.

3.1. Digital banks and traditional banks

The banking sector has transitioned from traditional brick-and-mortar branches to digital platforms due to technological improvements, encompassing customer preferences and competitive forces. This transition has significantly altered the way banks engage with consumers, provide services, and oversee operations, resulting in substantial changes in the banking industry. The transition from physical to digital platforms in the banking sector has extensive effects, altering banks' operations, customer interactions, and competitive strategies. Digitalization provides advantages in efficiency, innovation, and market growth, but it also introduces issues in cybersecurity, regulatory compliance, and people management. Banks can leverage the digital transition to achieve sustainable development and provide value to customers by proactively addressing these possibilities and obstacles. Digital banks have emerged as revolutionary organizations, transforming the way financial services are provided in the banking industry's rapidly changing market [32]. Digital banks typically employ online platforms to operate, utilizing technological improvements to provide customers easy access to various banking services [33]. The spread of internet access and the widespread use of mobile devices serve as contributing factors to the emergence of digital banks [34]. Without being restricted by physical branch locations, these digital-first institutions allow their customers the freedom to manage their financial affairs anytime, from almost anywhere [35].

The operational infrastructure of digital and traditional banks differs substantially in several important ways [33]. While digital banks use digital channels as their main form of interaction, traditional banks still significantly rely on their physical branch networks to provide services. Digital banks can provide various benefits, including greater accessibility, 24/7 availability, and streamlined processes, attributable to this fundamental transformation [36]. Customers no longer have to visit physical branches during business hours to perform basic transactions. Instead, customers may easily complete tasks, such as checking account balances, transferring money, paying bills, or even applying for loans by navigating through user-friendly mobile applications or web-based platforms [37]. Digital banks have also completely redesigned the consumer experience by prioritizing customization and user-centric design [38]. These banks are able to personalize their services to correspond to particular preferences and financial objectives via sophisticated data analytics and consumer insights. Digital banks provide their customers a more personalized and engaging banking experience, from targeted product recommendations to personalized financial management tools [39]. Nevertheless, the switch to digital banking still has limitations. Customer concerns about data security and privacy are becoming increasingly common because they depend increasingly on digital platforms for their banking needs. The huge volumes of private information that are communicated and the digital nature of transactions introduce a special set of hazards that must be handled carefully [40]. Digital banks must adopt cybersecurity measures to safeguard customer data, secure digital channels, and cease unauthorized access or fraudulent activities [41]. A proactive approach to cybersecurity is required given the ongoing evolution of cyber threats. Hence, digital banks should invest in advanced encryption methods, multi-factor authentication, and real-time monitoring systems to guarantee the integrity and confidentiality of customer information [42]. The significance of cybersecurity, the function of machine learning, and how these fields intersect in the context of digital banking will be explored as we delve into this literature review.

Table 2
Inclusion/Exclusion criteria for selecting related literature.

Inclusion/Exclusion criteria Rationale	Rationale
Studies related to digital banks and cybersecurity, machine learning and cybersecurity, and digital banks and machine learning were included	To guarantee that the literature includes pertinent studies that address the research questions.
Only studies that are published in reputable scientific databases were included.	To guarantee the precision, dependability, and scholarly integrity of the literature review.
Duration of publication.	To ensure that the information is current, studies published between 2010 and 2024 ware used.
Language of the papers.	Only English studies ware included.

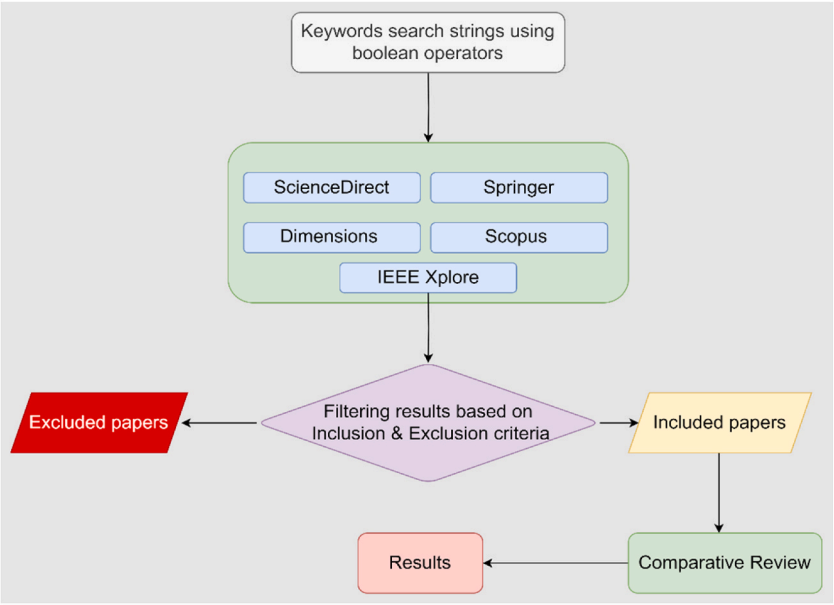

Fig. 1. The main steps of the research methodology.

3.2. Importance of cybersecurity

Cybersecurity is crucial in the linked world we live in today, where digital transactions are an essential element of our daily lives. The practices, technologies, and security measures used to protect computer systems, networks, and data from unwanted access, exploitation, or damage are referred to as cybersecurity [43]. Although it is significant in many different fields, digital banking, where the security of private financial data is crucial, is particularly significant [44]. Robust cybersecurity protocols must be prioritized by digital banks in their efforts to deliver seamless and secure banking services. Financial institutions should constantly adjust to new threats due to the rapid improvements in technology and the sophistication of cyber threats [45]. Cybercriminals use diverse strategies, including phishing attacks, malware injections, and identity theft, to target weaknesses and obtain illegal access to confidential consumer information [46].

The consequences of a successful cyberattack on digital banks can be severe, including financial losses, harm to the bank's reputation, and a decline in customers' satisfaction and even some legal penalties [47]. Digital banks use various cybersecurity methods to secure their systems and safeguard client information to reduce these threats [5]. These protocols employ a multi-layered approach and include measures, such as network firewalls, encryption algorithms, secure authentication protocols, and intrusion detection, and prevention systems [48]. Access control protocols prevent unauthorized access to critical information and resources, whereas authentication protocols guarantee that only authorized users can access and conduct transactions within the digital banking system [49].The security team at the bank must be aware of any potential dangers or unusual activity within the system by employing intrusion detection measures. Intrusion detection systems can rapidly identify and respond to unusual activities by monitoring network traffic and evaluating patterns, thereby reducing the impact of a cyberattack [50]. Moreover, in recent years, machine learning-based intrusion detection methods have become increasingly popular. These techniques use algorithms that can adapt to dynamic circumstances and learn from massive amounts of data to detect new and evolving threats [51].

Key management protocols are also vital to guarantee safe data transfer and communication inside digital banking systems. These protocols handle secure generation, distribution, and revocation of cryptographic keys used in encryption and decryption processes [52]. Digital banks can create secure communication channels and shield sensitive data from prohibited interception or tampering by utilizing effective key management protocols [53].

3.3. Cybersecurity attacks of digital banks

Macas, Wu [23] examined several types of cyberattacks. In this study we discussed the most common major cybersecurity threats to which digital banks are vulnerable, highlighting their potential consequences, the challenges they create, and the machine learning approaches employed to detect and prevent these threats. Table 3 provides a summary of the major cybersecurity threats to which digital banks are vulnerable, as well as the machine learning approaches employed to detect and prevent these threats.

3.3.1. Phishing attacks

Phishing attacks are social engineering strategies used by malicious individuals to trick people and obtain sensitive data, including login credentials and financial information [54]. These types of attacks frequently use phishing emails, spoofed websites, or text

Table 3
Major cybersecurity threats and machine learning approaches for detecting and preventing threats.

Cyber Threat	Category	Machine Learning Algorithms
Phishing Attacks	Supervised Learning Algorithms	Logistic Regression
		Support Vector Machines (SVM)
		Random Forests
	NLP Techniques	Sentiment Analysis
		Text Classification
		Keyword Extraction
	Ensemble Learning Techniques	AdaBoost
		Gradient Boosting
	Deep Learning Approaches	Convolutional Neural Networks (CNN)
		Recurrent Neural Networks (RNN)
Malware and Ransomware	Anomaly Detection Algorithms	Isolation Forest
		One-Class SVM
		Autoencoders
	Behavior-based Detection	Hidden Markov Models (HMM)
		Decision Trees
	Deep Learning Approaches	Convolutional Neural Networks (CNN)
		Recurrent Neural Networks (RNN)
Distributed Denial of Service (DDoS) Attacks	Traffic Analysis and Classification	Decision Trees
		Random Forests
	Anomaly Detection	Support Vector Machines (SVM)
		Gaussian Mixture Models (GMM)
		Autoencoders
	Deep Learning Approaches	Recurrent Neural Networks (RNN)
		Convolutional Neural Networks (CNN)
Insider Threats	User Behavior Analytics	Clustering
		Sequence Mining
	Anomaly Detection	Isolation Forest
		Local Outlier Factor (LOF)
		Autoencoders
	Contextual Analysis	Decision Trees
		Random Forests
		Support Vector Machines (SVM)
Social Engineering	Email Phishing Detection	Naive Bayes
		Random Forests
		Recurrent Neural Networks (RNNs)
	User Behavior Modeling	Hidden Markov Models (HMM)
		Long Short-Term Memory (LSTM)
	NLP for Social Engineering Detection	Sentiment Analysis
		Named Entity Recognition
		Intent Detection

messages to deceive people into revealing private information [55]. A targeted variation known as spear phishing focuses on specific individuals or organizations with the attack [56]. Machine learning algorithms and natural language processing (NLP) approaches can analyze text to identify signs of phishing [57]. For instance, phishing attempts can be detected using supervised learning techniques, such as logistic regression, support vector machines (SVM), and random forests. These algorithms gain knowledge from labelled datasets, which include features from legitimate and phishing emails or webpages. The algorithms can find patterns and indications that distinguish attempts at phishing from legitimate communications by training on such data [58]. Furthermore, to identify suspicious patterns, malicious URLs, or phishing email content, NLP techniques including sentiment analysis, text classification, and keyword extraction can be used [57]. Recurrent neural networks (RNN) and long short-term memory (LSTM) networks are examples of algorithms that can efficiently handle sequential data and capture contextual information in textual content, improving the precision of phishing detection systems [59]. Furthermore, by integrating several weak classifiers into a strong classifier, ensemble learning techniques, such as AdaBoost and gradient boosting, can enhance the performance of phishing detection models [60]. Ensemble methods increase the reliability and precision of the detection process by leveraging the collective wisdom of several models [61]. Ensemble learning techniques, which combine the predictions of different classifiers, can manage complicated and dynamic phishing attack patterns, resulting in a more dependable defense against phishing threats [62]. In addition, two types of deep learning algorithms, namely, convolutional neural networks (CNN) and RNN, have demonstrated promising results in a number of cybersecurity domains [63]. Deep learning models can learn complex feature representations from raw data, including photos or email content, in the context of phishing attack detection [64].

3.3.2. Malware and ransomware

Malware refers to malicious software, including viruses, worms, and Trojans, which can exploit vulnerabilities to obtain unauthorized access or steal sensitive information [65]. Ransomware encrypts files and demands ransom to decrypt those files and then redeliver them back to the users [66]. By detecting deviations from normal system behavior, malware and ransomware can be successfully identified using anomaly detection techniques, such as Isolation Forest, One-Class SVM, and Autoencoders [67]. These

algorithms provide a baseline of normal behavior by learning from historical data. Every deviation from this standard is marked as a potential malware or ransomware attack [68]. Furthermore, to distinguish between legal and malicious behavior, algorithms, such as Hidden Markov Models (HMM) and Decision Trees, can capture sequential patterns and dependencies [69]. These algorithms can identify anomalies and possibly harmful behavior linked to malware or ransomware by focusing on the execution of applications, system calls, network connections, and file operations [70,71]. Furthermore, CNNs and RNNs, two deep learning algorithms, have demonstrated potential in the detection of malware and ransomware [72]. While RNNs may capture temporal dependencies in the behavior of processes or network connections, CNNs can analyze the content of files or network traffic data [73].

3.3.3. Distributed denial of service (DDoS) attacks

DDoS attacks disrupts the availability of digital banking services by flooding network infrastructure or applications with traffic [74]. Attackers generate high volumes of traffic by using botnets or amplified reflection techniques, which prevent legitimate users from using services [74]. Decision trees and random forests are a few examples of machine learning algorithms used to analyze network traffic and classify it as legitimate or malicious [75]. Moreover, support vector machines (SVM), Gaussian mixture models (GMM), and autoencoders are three excellent anomaly detection techniques for spotting anomalous network activity indicating DDoS attacks [76]. These algorithms learn normal network traffic patterns and identify deviations from the established baseline as probable DDoS attacks. Anomaly detection algorithms can detect anomalous activities and initiate prompt mitigation measures by monitoring features, such as traffic volume, packet rates, or communication patterns [77]. Furthermore, RNNs and CNNs, two examples of deep learning algorithms, have shown potential in the detection and mitigation of DDoS attacks [78–80].

3.3.4. Insider threats

The greatest cybersecurity risk to businesses and organizations, especially the banks, arises from insider threats. Insider threats involve authorized individuals who maliciously use their access privileges or unintentionally cause security incidents, such as employees or privileged users [81]. These threats can result in unauthorized data access, data leakage, fraud, or the introduction of vulnerabilities [82]. User behavior analytics (UBA) uses machine learning techniques to examine user behavior patterns and detect deviations from the usual. These algorithms, which include clustering, sequence mining, and anomaly detection, learn from prior data to create baseline user profiles and identify suspicious behavior [83,84]. UBA algorithms can identify anomalies that could be signs of insider threats by keeping track of user behavior, access patterns, data transfers, and system interactions, allowing for rapid detection and mitigation [85]. In addition, unusual behavior that could be signs of insider threats can be determined using anomaly detection algorithms, such as unsupervised learning approaches, such as isolation forest, local outlier factor (LOF), or autoencoders. These algorithms can capture subtle anomalies that might not be clearly described in the training data because they learn from unlabeled data and search for deviations from normal patterns. Anomaly detection algorithms can detect possible malicious actions carried out by insiders by tracking numerous data sources, such as log files, system events, or user activity logs [86]. Furthermore, contextual analysis enhances the detection of insider threats by combining machine learning techniques with contextual data. Decision trees, random forests, and SVMs are a few examples of algorithms that may analyze user behavior in the context of their roles, privileges, and work environments. These algorithms can discriminate between legitimate and suspicious activities by considering contextual elements, such as time of day, location, data sensitivity, or psychological factors, improving the accuracy of insider threat detection [87,88].

3.3.5. Social engineering

Social engineering attacks use psychological manipulation to deceive people into divulging private information or carrying out unauthorized actions [89]. Techniques including pretexting, baiting, and phishing are used to deceive staff or consumers and acquire unauthorized access to digital financial systems [90]. Email phishing, a commonly used social engineering technique, involves sending fraudulent emails to users in an effort to deceive them into disclosing sensitive information or clicking on malicious links [91]. To identify phishing attempts, machine learning algorithms may analyze email content, sender information, and user behavior. Examples include Naive Bayes, random forests, and RNNs [92]. Moreover, algorithms, such as hidden Markov models (HMMs) and long short-term memory (LSTM) networks can capture sequential dependencies and spot anomalous behavior related to social engineering by keeping track of user interactions, access patterns, and system behavior [93]. In addition, to identify social engineering attempts, text-based interactions, such as chat conversations or social media interactions, can be analyzed using natural language processing (NLP) techniques and machine learning algorithms [94,95]. Manipulative language, suspicious requests, and unauthorized information disclosure can be detected using NLP techniques, such as sentiment analysis, named entity recognition, or intent detection [95, 96].

3.4. Machine learning

Machine learning, a branch of artificial intelligence, has become a significant tool in the fields of cybersecurity and digital banking, with its increased capabilities for threat detection, anomaly detection, and fraud prevention [97]. In the context of digital banking, machine learning algorithms play a crucial role in enhancing security measures by utilizing their capacity to rapidly and accurately process and analyze massive amounts of data [98]. Traditional rule-based approaches, which rely on predetermined rules and signatures, frequently struggle to cope with the evolving nature of cyber threats [28]. On the contrary, machine learning uses complicated algorithms that can adapt to and learn from data, allowing systems to detect and respond to new threats in real-time [99]. In digital banking, machine learning is primarily used for anomaly detection. Banks can establish baseline behavior patterns for their systems and detect anomalies that can point to a security breach by training machine learning models on large datasets [100]. SVM or deep

neural networks (DNN) are examples of machine learning algorithms that can efficiently identify anomalous network traffic, user behavior, or transaction patterns. This approach enables security teams to take immediate action and stop potential cyber threats from causing significant harm [101]. In addition, machine learning is essential for detecting fraud in digital banking. Machine learning models are used to identify complex patterns and signs of fraudulent behavior by analyzing user profiles, historical transaction data, and other relevant characteristics [102]. An effective model for classification tasks can be produced by random forests, an ensemble learning technique that incorporates various decision trees [103]. In the context of fraud detection, a random forest model is trained on a dataset including features obtained from historical transactions, such as transaction amount, location, time, and user behavior patterns. Each decision tree in the random forest is trained using a different feature combination and a random subset of the data to produce predictions. The random forest approach can offer a more precise and trustworthy evaluation of whether a transaction is fraudulent or legal by combining the predictions collected from different trees [104].

Gradient boosting is another ensemble learning strategy that creates a powerful predictive model by gradually including weak learners (decision trees) into the ensemble. Contrary to random forests, which produce independent trees simultaneously, gradient boosting builds trees sequentially, with each tree aiming to correct errors caused by the preceding ones [105]. Classification algorithms, such as random forests and gradient boosting, can distinguish between genuine and fraudulent transactions. Thus, banks are better equipped to proactively spot and stop fraud, protecting the financial institution and its clients [106,107]. In the event of a security breach, machine learning algorithms also improve the effectiveness and efficiency of incident response. Clustering algorithms, such as k-means or hierarchical clustering can prioritize and categorize occurrences by utilizing historical data and real-time monitoring, offering valuable information to incident response teams, which can act instantly [108].

Machine learning techniques also enhance the processes of user authentication and identity verification. Machine learning models may build comprehensive user profiles that enable accurate secure authentication by examining a number of variables, such as biometric data, behavioral patterns, and device information [109]. CNN, RNN, and decision trees are examples of deep learning architectures that can reduce the risks of identity theft, password theft, and unauthorized access to digital banking platforms [110–112]. We can conclude that machine learning plays a crucial role in enhancing and sustaining cybersecurity measures in the digital banking industry by utilizing efficient algorithms and data analytics skills.

Machine learning algorithms serve as the cornerstone of advancements in artificial intelligence and have revolutionized multiple industries by enabling computers to learn from data and make predictions or decisions on their own [113]. In this section, we present a technical overview of the main machine learning algorithms, highlighting their fundamental principles and characteristics. The supervised learning algorithms, based on labelled training data, attempt to learn a mapping function from input features to target outputs. They employ two types of models, such as regression and classification, to represent the relationships between inputs and outputs [114]. Contrary to logistic regression, which is frequently used for binary classification tasks, linear regression employs linear models to estimate continuous target variables [104]. Decision trees enable complex decision boundaries by recursively partitioning the input space using feature values [115]. While neural networks use interconnected layers of artificial neurons to capture nonlinear interactions [116], SVMs seek out the best hyperplanes to separate different classes [117].

Unsupervised learning algorithms search for inherent patterns or structures in unlabeled data [118]. Clustering algorithms group similar data points together based on similarity measures [119]. *K*-means clustering partitions the data into *K* clusters by minimizing the sum of squares within each cluster [120]. Data points are organized into clusters using hierarchical clustering, which produces a tree-like structure containing different granularity levels [121]. Dimensionality reduction techniques are intended to reduce the dimensionality of data while retaining the most significant data [122].

Principal component analysis (PCA) identifies orthogonal directions for the maximum variance [123], whereas t-distributed stochastic neighbor embedding (t-SNE) maintains local neighborhood relationships while visualizing high-dimensional data in lower dimensions [124]. Reinforcement learning algorithms, through interactions with the environment, focus on learning optimal decision-making policies. They use a machine-learning agent that selects actions based on observed states and receives feedback in the form of rewards [125]. Q-learning is a well-known technique that uses a value function to estimate the potential future rewards of adopting particular policies in specified states [126]. Policy gradients optimize the parameters of a policy network to maximize cumulative rewards [127]. Deep Q-Networks (DQNs) combine deep neural networks and Q-learning to manage complex environments with high-dimensional state spaces [128].

Deep learning algorithms use artificial neural networks with multiple layers of interconnected nodes to learn hierarchical data representations [129]. CNNs excel in analyzing images and videos because they utilize pooling layers to extract local features to capture spatial correlations [130]. Recurrent connections in RNNs, which are intended for sequential data processing, enable information persistence through time steps [131]. Generative adversarial networks (GANs) match a discriminator network against a generator network in a competitive environment to generate realistic synthetic data samples [132].

4. Integrating cybersecurity and machine learning in digital banks

The rapid growth of machine learning techniques has created new opportunities for enhancing cybersecurity in digital banking. Machine learning algorithms are essential tools for detecting and preventing cyberattacks because they can scan enormous volumes of information, identify patterns, and generate precise predictions [27]. Digital banks can improve their security procedures and keep up with cybercriminals by utilizing machine learning [133].

Anomalies and possible intrusions in digital banking systems are efficiently detected by machine learning algorithms [134]. These algorithms can recognize deviations from typical user behavior, network traffic, or system activity patterns by learning from prior data [135]. Machine learning models can raise alerts and initiate preventive actions in real-time, reducing potential security breaches, by

establishing baselines and continuously monitoring the anomalies [136]. In addition, user behavior patterns can be examined by machine learning algorithms to determine shady activities and potential risks [137]. These models can spot deviations or anomalies that can indicate fraudulent activities or unauthorized access by analyzing parameters, such as login times, transaction patterns, and device usage [138]. Large-scale threat intelligence data can be used to train machine learning algorithms to recognize new cyber-threats and foresee attack tactics [139]. Machine learning models are trained to detect patterns and indicators of known attacks by examining historical attack data, security logs, and external threat feeds [140].

Digital banking systems can become more adaptable and self-learning in their security measures with the help of machine learning [141]. Machine learning models can upgrade their algorithms and boost their performance over time by continuously assessing new data and adjusting to shifting threat environments [142]. Digital banks, which are highly flexible, are better prepared to counteract

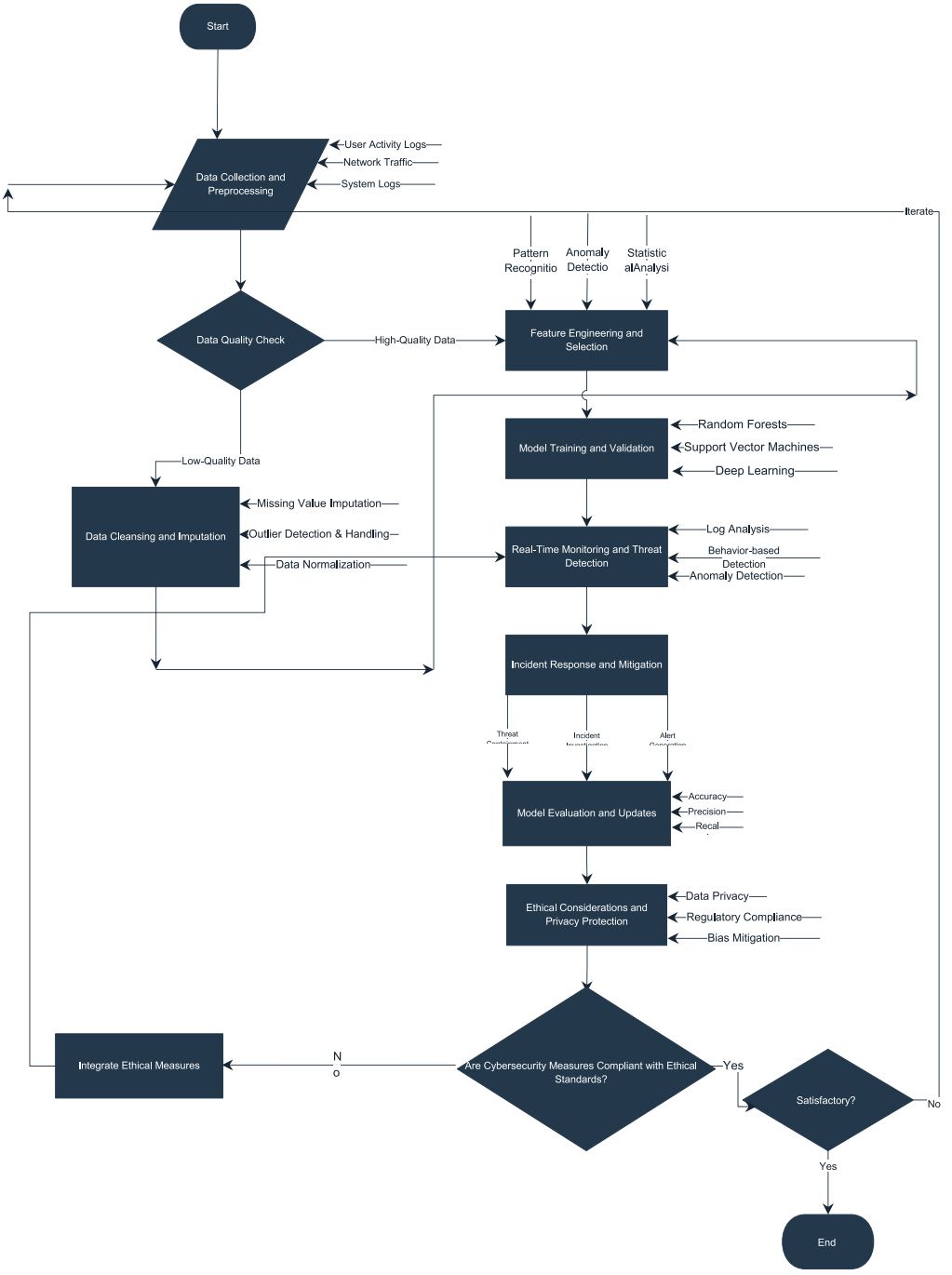

Fig. 2. Machine learning and cybersecurity integration model.

emerging and complex cyberthreats, assuring the continuous security of critical consumer data and financial assets [143].

In summary, for digital banks, implementing machine learning methods into cybersecurity procedures has many benefits. Financial institutions may improve their security protocols, quickly identify and address cyberthreats, and guarantee the security of customer assets and information by utilizing machine learning. However, considering the difficulties and ethical issues that come with deploying machine learning-based cybersecurity solutions in digital banking is highly important. A research gap in terms of addressing the integration of cybersecurity and machine learning in the context of digital banking still exists, despite the significant progress in both fields. The existing literature has mainly concentrated on either machine learning applications in different industries or cybersecurity in conventional banking. Studies explicitly examining how machine learning can be integrated into cybersecurity procedures in the special context of digital banks are limited. This gap offers an opportunity to address the specific challenges and opportunities of the digital banking industry.

Digital banks start to recognize the possibility of integrating machine learning techniques into their cybersecurity procedures to strengthen their defensive measures against developing cyberthreats [144]. Advanced capabilities for threat detection, anomaly identification, and pro-active incident response may be made available through this integration [145]. In this section, we discuss the concept of incorporating machine learning into digital banks' cybersecurity and present a model to accomplish this objective. We also perform a SWOT analysis to explore the benefits and drawbacks of this integration in the context of digital banking.

4.1. Machine learning and cybersecurity integration model

The integration of machine learning techniques into cybersecurity practices has emerged as an effective approach to increase the effectiveness and efficiency of bank security systems [146]. In the context of digital banks, this section presents a machine learning and cybersecurity integration model that illustrates the sequential procedures and decision-making points involved in utilizing machine learning for robust cybersecurity. The model presented in Fig. 2 includes a number of stages. Following this model will enable digital banks to efficiently use machine learning to detect and combat cyberthreats, protect confidential data, and guarantee system security in general.

A rigorous and systematic approach is required to integrate machine learning into security procedures in digital banks. The accompanying flowchart visually illustrates the integration process, providing a comprehensive overview of the interconnected steps and their relationships within the model.

The major processes included in the model are as follows.

- Data Collection and Preprocessing

Digital banks obtain enormous volumes of data from various sources, such as customer transactions, network logs, and system events [147]. The data are gathered and preprocessed to clean, standardize, and transform them into a format that can be used by machine learning algorithms [148]. Contextual data, such as customer behavior patterns, transaction history, and access logs, are also included.

- **Feature Engineering and Selection**

Feature engineering is the extraction of helpful and relevant characteristics from the preprocessed data [149]. These elements can include transaction amounts, timestamps, user locations, device information, and access patterns in the context of digital banking [30]. Then, feature selection approaches determine which features are most important and discriminative for the machine learning model.

- **Model** Training **and Validation**

The preprocessed data and selected features are used to train machine learning models, such as random forests or gradient boosting [150]. The model picks up on trends and connections between certain traits and cybersecurity concerns. Different techniques are used for training, and hyperparameter tuning is conducted to enhance model performance [151]. Cross-validation techniques evaluate the model's resilience and generalizability [152].

- **Real-time** Monitoring **and Threat Detection**

The digital banking system uses the trained machine learning model to continually monitor incoming data streams. Real-time transactions, network traffic, user activities, and system logs are examined to identify unusual activity, suspicious patterns, or potential cyber threats [153]. Contextual information is used to distinguish between legitimate and dangerous behavior, such as the customer's transaction history and typical behavior [154].

- **Incident** Response **and Mitigation**

The machine learning model activates immediate incident response mechanisms when a possible threat is identified, including initiating user authentication challenges, banning suspicious transactions, issuing alarms, or contacting security personnel [155]. The significance and urgency of the response are determined by contextual information from the model, such as the level of risk connected

to a certain transaction or user [156].

- **Model** Evaluation **and Updates**

The performance of the machine learning model must be continuously evaluated. Evaluation measures for precision, recall, and F1 score evaluate how well the model works to identify and manage cyber threats [157]. The model is regularly updated depending on newly gathered data, emerging threat intelligence, and input from security analysts [158]. The model's accuracy and adaptability are improved by retraining with more recent data [159].

- **Ethical** Considerations **and Privacy Protection**

The integration process incorporates ethical considerations and privacy protection safeguards at every step. Data anonymization techniques are used to protect client privacy [160], and strict access controls guarantee that only authorized employees have access to sensitive data [161]. Regulatory framework adherence is a top priority to maintain compliance and trust; examples include general data protection regulation (GDPR) and CCPA [162]. The challenges related to the digital banking environment are addressed by interpreting the incorporation of machine learning into cybersecurity in digital banks using this model. Real-time monitoring, advanced feature engineering, contextual data, and incident response mechanisms are included in the model. They are specially designed to consider the specifics of digital banking operations. Digital banks may strengthen their cybersecurity defenses, identify new threats, and safeguard consumer assets and sensitive data by utilizing machine learning techniques inside this framework.

4.2. SWOT analysis of integrating machine learning into cybersecurity in digital banks

A SWOT analysis can be helpful in determining the benefits and drawbacks of integrating machine learning into cybersecurity in digital banks [163]. This review shows the possible advantages and difficulties of this strategy while considering the internal and external factors, which affect integration. Table 4 presents the SWOT analysis for integrating machine learning into cybersecurity in digital banks.

4.2.1. Strengths

- Enhanced threat detection as machine learning algorithms can analyze enormous volumes of data in real-time, enabling the early identification of potential cyberthreats and enhancing the general safety condition of digital banks [164].
- Machine learning models can identify patterns and anomalies with greater accuracy by employing advanced algorithms, which reduce the rate of false positives and false negatives in security measures [165].
- Machine learning algorithms evolve and adapt to new data and emerging threats [166]. As a result, digital banks remain proactive against changing cyber threats and effectively combat new attacks.
- Automated incident response is made possible by the integration of machine learning, which simplifies the processes of rapidly identifying, limiting, and recovering from cyberattacks [140].

4.2.2. Weaknesses

- For efficient training, machine learning models primarily depend on reliable diverse datasets. In addition to maintaining data privacy and regulatory compliance, digital banks may encounter difficulties obtaining appropriate and representative data [167].
- Model interpretability is also a problem due to the complex internal mechanisms. Some machine learning algorithms, such as deep learning neural networks, are frequently referred to as "black boxes" given the difficulty to comprehend their decision-making process and produce understood outcomes [168,169].
- Machine learning models are vulnerable to adversarial attacks, in which malicious actors intentionally modify input data to deceive the model [170,171]. In this scenario, the security of digital banking systems may be endangered.

Table 4
SWOT analysis for the integration model.

Strengths	Weaknesses
● Enhanced Threat Detection ● Improved Accuracy ● Adaptive Defense Mechanisms ● Efficient Incident Response	● Data Complexity and Quality ● Model Interpretability ● Vulnerability to Adversarial Attacks
Opportunities	**Threats**
● Advanced Fraud Detection ● Behavioral Analysis ● Predictive Threat Intelligence	● Rapidly Evolving Cyber Landscape ● Resource and Expertise Requirements ● Regulatory and Ethical Considerations

4.2.3. Opportunities

- Machine learning integration can increase fraud detection capabilities in digital banks by recognizing unusual patterns, suspicious transactions, and fraudulent activity in real-time, thereby minimizing financial losses and boosting client confidence [29,172].
- A proactive approach to identifying potential cyber threats or unauthorized access attempts is made possible by machine learning's analysis of user behavioral patterns to create baseline profiles and spot abnormal activity [173].
- Massive amounts of threat intelligence data, including indicators of compromise, vulnerabilities, and attack patterns, can be analyzed by machine learning algorithms to provide anticipated insights that promote proactive threat mitigation [174].

4.2.4. Threats

- Machine learning models must be constantly monitored and updated to stay effective because adversaries continuously modify their methods of attack [175].
- Some institutions may face financial and managerial challenges as a result of the significant expenditures necessary for successful implementation of machine learning into the cybersecurity of digital banks [157].
- Concerns about privacy, data protection, and regulatory compliance arise by the integration of machine learning. Digital banks must ensure that their machine learning procedures comply with ethical and legal standards to secure customer data and maintain public trust [176].

5. Recommendations and implications

Several recommendations to various stakeholders involved in the integration of machine learning into cybersecurity in digital banks are based on the SWOT analysis.

Cybersecurity companies are required to protect digital financial institutions from expanding cyber threats. These companies must work closely with digital banks to strengthen their partnership. The collaboration should be defined by a thorough comprehension of the specific security requirements of financial institutions, leading to the creation of customized machine learning-based solutions. This approach could include working on joint research initiatives, exchanging threat intelligence, and developing cutting-edge machine learning-based security solutions together. In addition, cybersecurity firms must proactively invest in R&D to stay ahead of new cyber hazards. This technique will update their tools and approaches. Providing a full range of cybersecurity services is crucial; it involves efficient incident response procedures, frequent security audits, and extensive personnel training programs in addition to strong threat detection and prevention methods. Cybersecurity companies can assist digital banks to adopt and maintain highly effective cybersecurity measures by giving them ongoing assistance and guidance. As a result, the entire digital banking ecosystem is strengthened against possible cyber threats.

Protecting customer data integrity and privacy is a top priority in digital banking. Digital banks are required to adhere to strict data governance regulations given that machine learning primarily depends on high-quality data. Employing cutting-edge data anonymization techniques and closely following the data protection regulations are required to secure the privacy of sensitive consumer information. Effectively strengthening cybersecurity measures entails considerable costs. Digital banks should invest in cutting-edge machine learning-based cybersecurity technologies, hire qualified professionals, and carry out regular security assessments to stay ahead of potential attacks. A multi-layered security approach that incorporates technologies, such as firewalls, intrusion detection systems, encryption, and enhanced user authentication techniques, should be implemented to develop a strong defense against cyberattacks [177].

Digital banks should develop a culture of continual training and monitoring among their personnel given the constantly evolving nature of cyber threats. This strategy's key elements include regular vulnerability assessments, frequent protocol upgrades, and in-depth cybersecurity training for staff employees. Collaboration with cybersecurity companies and active engagement in industry-wide information-sharing initiatives enable the exchange of threat intelligence and best practices, warranting a coordinated response to cyber threats. Pertinent cybersecurity regulations and guidelines including the GDPR and the Payment Card Industry Data Security Standard (PCI DSS) should be complied. Adherence increases confidence and trust within the digital banking ecosystem and guarantees the protection of customer information [178]. Digital banks must also invest in extending research and development projects that keep up with technical improvements and the changing threat landscape to proactively strengthen their cybersecurity posture.

The strengthening of the cybersecurity environment for digital banking depends heavily on regulatory authorities and governmental organizations. Regulatory agencies must proactively establish and implement cybersecurity policies and regulations that are customized to the digital banking industry to reinforce the resilience of digital banks against changing cyber threats. These rules should include strict standards for compliance, incident reporting procedures, and data protection safeguards. These organizations establish a consistent and strong cybersecurity framework throughout the digital banking industry by enacting clear and precise laws.

In addition, encouraging collaboration is crucial. Regulators should actively encourage cooperation among digital banks, prestigious academic institutes, and cybersecurity companies. These partnerships can act as incubators for new ideas and the sharing of knowledge. Research organizations supply the most recent academic insights, cybersecurity corporations contribute cutting-edge technologies and skills, and digital banks provide real-world difficulties and scenarios. This trilateral partnership can spur the creation of cutting-edge cybersecurity solutions. Regulatory bodies and government organizations can empower the digital banking industry to leverage collective intelligence, enabling rapid response to new cyber threats and maintaining the overall security of digital

banking ecosystems by encouraging synergy among these entities.

The findings of this study have practical implications for digital banks, they can use the study's findings to improve their cybersecurity procedures by incorporating machine learning algorithms into digital banks cybersecurity infrastructure. The proposed model for integrating machine learning algorithms outlines a systematic approach for using machine learning algorithms to identify, detect, and mitigate cybersecurity threats in real-time by digital banks. The results of this study also point to a number of practical implications for regulatory organizations that should concentrate on ensuring strong cybersecurity procedures while encouraging innovation in the financial industry. Furthermore, the study's findings can also have significant practical implications for cybersecurity companies. These firm can strengthen collaboration with digital banks and fostering the development of cutting-edge cybersecurity solutions based on machine learning algorithms, In addition, the findings of this study have practical implications for cybersecurity companies, they can be essential to the efforts of integrating machine learning for sustain digital bank cybersecurity by enhancing collaboration with digital banks and development of advanced cybersecurity solutions based on machine learning algorithms.

6. Conclusion

The integration of cybersecurity and machine learning in digital banks has been addressed in this study. The literature review highlighted the value of cybersecurity safety measures and emphasized how vulnerable digital banks are to cyberattacks. Machine learning has been recognized as an effective approach for fraud prevention and detection. The connections between cybersecurity protocols and machine learning methods in digital banks are complex and ever-changing, with machine learning being essential for improving cybersecurity practices. Several key conceptual relationships between cybersecurity procedures and machine learning techniques in the context of digital banks emerged in this study. First, machine learning algorithms can evaluate extensive data in real-time to detect and prevent many cyber risks, including malware, phishing attacks, and insider threats. Machine learning models can detect abnormal patterns that may indicate security breaches by monitoring network traffic, user behavior, and system records, allowing for proactive risk mitigation. Second, machine learning methods, such as anomaly detection algorithms, can recognize unusual behavior or departures from anticipated trends in digital financial systems. These algorithms can analyze historical data to identify new and complex cyber threats that conventional rule-based systems could miss, thereby improving the efficiency of cybersecurity protocols. Third, machine learning models can be used to examine transactional data and user behavior to identify fraudulent behavior, including unauthorized transactions, account takeovers, and identity theft. Machine learning techniques can detect fraudulent transactions in real-time using advanced analytics and pattern recognition algorithms, allowing digital banks to respond immediately and reduce financial losses. Forth, machine learning may help digital banks detect and prioritize security vulnerabilities in their IT infrastructure and software applications, aiding in vulnerability management and patch management. Machine learning models can forecast potential attack vectors by studying historical vulnerability data and threat intelligence feeds. They can advocate preemptive measures, such as patching susceptible systems or applying compensating controls to limit exposure to cyber threats. Fifth, machine learning techniques can improve user authentication and access control in digital banking systems. Behavioral biometrics, such keyboard dynamics and mouse movements, can be used to verify individuals by their distinct behavioral patterns, providing extra security compared with standard password-based authentication approaches. Finally, machine learning algorithms can scan extensive threat intelligence feeds and security event data to detect new cyber threats, trends, and attack patterns in cybersecurity analytics. These algorithms allow digital banks to analyze many sources of information to identify useful insights to anticipate and counter changing cyber threats by adjusting their cybersecurity protocols.

Therefore, the link between cybersecurity processes and machine learning techniques in digital banks focuses on using sophisticated analytics, automation, and predictive capabilities to improve threat detection, prevention, and response. Digital banks may effectively reduce cyber threats, protect consumer assets, and retain trust in the digital banking ecosystem by incorporating machine learning into their cybersecurity policies. The proposed model demonstrated how different components of integrating machine learning into cybersecurity in digital banks are interconnected. The advantages, disadvantages, opportunities, and risks of this integration were determined through a SWOT analysis. The research concludes that enhancing cybersecurity defenses and reducing threats in digital banks requires the integration of machine learning. To secure a robust security framework for the future of digital banking, ongoing research and collaboration are required.

This study has revealed the significant impact of incorporating machine learning into cybersecurity practices in digital banking. By conducting a thorough examination of current literature. The study emphasizes the crucial importance of machine learning approaches in enhancing cybersecurity measures, safeguarding digital banking, and upholding client confidence. Machine learning algorithms, such as anomaly detection models and behavioral analytics, provide improved features for detecting threats, assessing vulnerabilities, and responding to incidents. This approach ultimately strengthens the resilience of digital banking systems against changing cyber threats. This study also highlights distinctive contributions to the sector, including understanding the synergistic connection between machine learning and cybersecurity, the significance of adaptive security controls, and the opportunity for data-driven decision-making in risk management. The study provides a detailed knowledge of the opportunities and limitations of using machine learning in digital bank cybersecurity by combining theoretical principles with empirical evidence. Digital banks may anticipate and address security threats, improve operational effectiveness, and provide exceptional customer service by incorporating machine learning techniques into cybersecurity protocols. Digital banks can enhance their security measures against cyberattacks, protect consumer data, and ensure compliance with regulations by using advanced analytics and automation in a digitalized environment. The SWOT analysis in this study identifies the strengths, weaknesses, opportunities, and threats related to implementing machine learning in digital bank cybersecurity. Key strengths include the ability to adapt to evolving threats and improve threat detection capabilities, whereas the weaknesses revolve around challenges related to data complexity and quality, as well as model interpretability.

Opportunities lie in the potential for advanced fraud detection, whereas threats include rapidly evolving cyber landscape, regulatory scrutiny, and ethical concerns.

The limitations of this study are mainly related to publication bias. This study might have ignored the findings of some most recent works given that the literature on AI applications in cybersecurity has grown at an exponential rate. Moreover, not all field studies may be represented because unindexed conference papers, books, and essays were excluded from this review. Unpublished studies or non-English studies may lead to a biased representation of the research landscape. Furthermore, the literature search was limited to certain databases and keyword combinations. Relevant papers in less common databases or with different terminology may have been missed. The proposed conceptual integration model has not been empirically validated with real-world case studies of machine learning cybersecurity implementations in digital banking. In addition, the SWOT analysis draws mostly from academic literature. Validating perceptions by surveying industry security professionals could provide substantial context.

Future research should employ longitudinal designs to better understand the changes and trends in the application of machine learning in cybersecurity over time, accounting for technological advancements and evolving threat landscapes. Future researchers in the field of cybersecurity for digital banks are provided a compelling mission to investigate new cyberthreats and vulnerabilities designed to affect these institutions. A thorough investigation of these particular challenges present innovative solutions, particularly when machine learning techniques are applied. The resilience of digital financial systems is ensured by these techniques, which are essential for understanding complex risks and creating targeted solutions. Furthermore, investigating the ethical implications of using machine learning in the field of digital bank cybersecurity is crucial. To ensure the ethical and responsible use of these cutting-edge tools, consideration must be given to potential biases, privacy issues, and questions of fairness. Future academics can perform a substantial contribution to the creation of policies and frameworks that support the moral application of machine learning in digital bank cybersecurity by critically analyzing these ethical issues. Future research projects should also focus on comparing various machine learning-based cybersecurity methods. Researchers can identify the benefits and disadvantages of each approach by methodically contrasting several approaches. More research needs to be done to examine in details the application of integrating machine learning in cybersecurity in the context of digital banking with real-world examples or case studies. Best practices should be recognized while implementing machine learning-based cybersecurity solutions. Such comparison studies offer insightful guidance for digital bank deployment methods and ensure the best application of machine learning tools for effective cyber defense.

Data availability statement

No additional data was used for the research described in the article.

Funding statement

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

CRediT authorship contribution statement

Muath Asmar: Writing – review & editing, Supervision, Project administration, Methodology, Investigation. **Alia Tuqan:** Writing – review & editing, Writing – original draft, Project administration, Methodology, Investigation, Funding acquisition, Formal analysis, Conceptualization.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgement

The authors would like to thank the anonymous reviewers for their valuable comments and suggestions.

References

[1] L.K. Osei, Y. Cherkasova, K.M. Oware, Unlocking the full potential of digital transformation in banking: a bibliometric review and emerging trend, Future Business Journal 9 (1) (2023) 30.
[2] A.A. Isa, A. Hamdan, B. Alareeni, The impact of digital banking on the bank operation and financial performance, in: Innovation of Businesses, and Digitalization during Covid-19 Pandemic, Springer International Publishing, Cham, 2023.
[3] A. Bastari, et al., Digitalization in banking sector: the role of intrinsic motivation, Heliyon 6 (12) (2020) e05801.
[4] N.A. Windasari, et al., Digital-only banking experience: insights from gen Y and gen Z, Journal of Innovation & Knowledge 7 (2) (2022) 100170.
[5] H.M. Alzoubi, et al., Cyber security threats on digital banking, in: 2022 1st International Conference on AI in Cybersecurity (ICAIC), 2022.
[6] J.A. Jafri, et al., A systematic literature review of the role of trust and security on Fintech adoption in banking, Heliyon 10 (1) (2024) e22980.
[7] B. Chaimaa, E. Najib, H. Rachid, E-Banking overview: concepts, challenges and solutions, Wireless Pers. Commun. 117 (2) (2021) 1059–1078.
[8] W.S. Admass, Y.Y. Munaye, A.A. Diro, Cyber security: state of the art, challenges and future directions, Cyber Security and Applications 2 (2024) 100031.
[9] B. Panja, et al., Cybersecurity in banking and financial sector: security analysis of a mobile banking application, in: 2013 International Conference on Collaboration Technologies and Systems (CTS), 2013.

[10] A.Q. Stanikzai, M.A. Shah, Evaluation of cyber security threats in banking systems, in: 2021 IEEE Symposium Series on Computational Intelligence (SSCI), 2021.
[11] Y. Liu, X. Sun, X. Mao, Security problems and countermeasures with commercial banking computer networks, in: 2011 Seventh International Conference on Computational Intelligence and Security, 2011.
[12] G. Apruzzese, et al., The role of machine learning in cybersecurity, Digital Threats: Research and Practice 4 (1) (2023) 1–38.
[13] T. Mazhar, et al., Analysis of cyber security attacks and its solutions for the smart grid using machine learning and blockchain methods, Future Internet 15 (2) (2023) 83.
[14] M. Asmar, B.Y. Aqel, Analysis of credit cards fraud detection: process and techniques perspective, in: B.A.M. Alareeni, I. Elgedawy (Eds.), Artificial Intelligence (AI) and Finance, Springer Nature Switzerland, Cham, 2023, pp. 899–911.
[15] A.M. Ozbayoglu, M.U. Gudelek, O.B. Sezer, Deep learning for financial applications : a survey, Appl. Soft Comput. 93 (2020) 106384.
[16] O.H. Fares, I. Butt, S.H.M. Lee, Utilization of artificial intelligence in the banking sector: a systematic literature review, J. Financ. Serv. Market. 28 (4) (2023) 835–852.
[17] W.A. Alkhowaiter, Digital payment and banking adoption research in Gulf countries: a systematic literature review, Int. J. Inf. Manag. 53 (2020) 102102.
[18] K. Walker, A systematic review of the corporate reputation literature: definition, measurement, and theory, Corp. Reput. Rev. 12 (4) (2010) 357–387.
[19] A. Naimi-Sadigh, T. Asgari, M. Rabiei, Digital transformation in the value chain disruption of banking services, Journal of the Knowledge Economy 13 (2) (2022) 1212–1242.
[20] I.H. Sarker, et al., Explainable AI for cybersecurity automation, intelligence and trustworthiness in digital twin: methods, taxonomy, challenges and prospects, ICT Express (2024).
[21] M. Ahsan, et al., Enhancing machine learning prediction in cybersecurity using dynamic feature selector, Journal of Cybersecurity and Privacy 1 (1) (2021) 199–218.
[22] T. Berghout, M. Benbouzid, S.M. Muyeen, Machine learning for cybersecurity in smart grids: a comprehensive review-based study on methods, solutions, and prospects, International Journal of Critical Infrastructure Protection 38 (2022) 100547.
[23] M. Macas, C. Wu, W. Fuertes, A survey on deep learning for cybersecurity: progress, challenges, and opportunities, Comput. Network. 212 (2022) 109032.
[24] M. Nanda, M. Saraswat, P.K. Sharma, Enhancing cybersecurity: a review and comparative analysis of convolutional neural network approaches for detecting URL-based phishing attacks, e-Prime - Advances in Electrical Engineering, Electronics and Energy 8 (2024) 100533.
[25] M.M. Inuwa, R. Das, A comparative analysis of various machine learning methods for anomaly detection in cyber attacks on IoT networks, Internet of Things 26 (2024) 101162.
[26] M.A.M. Saif, et al., Determinants of the intention to adopt digital-only banks in Malaysia: the extension of environmental concern, Sustainability 14 (17) (2022) 11043.
[27] M. Ahsan, et al., Cybersecurity threats and their mitigation approaches using machine learning—a review, Journal of Cybersecurity and Privacy 2 (3) (2022) 527–555.
[28] G. Apruzzese, et al., On the effectiveness of machine and deep learning for cyber security, in: 2018 10th International Conference on Cyber Conflict (CyCon), 2018.
[29] Z. Chen, et al., Machine learning techniques for anti-money laundering (AML) solutions in suspicious transaction detection: a review, Knowl. Inf. Syst. 57 (2) (2018) 245–285.
[30] A. Dhoot, A.N. Nazarov, A.N.A. Koupaei, A security risk model for online banking system, in: 2020 Systems of Signals Generating and Processing in the Field of on Board Communications, 2020.
[31] V. Murinde, E. Rizopoulos, M. Zachariadis, The impact of the FinTech revolution on the future of banking: opportunities and risks, Int. Rev. Financ. Anal. 81 (2022) 102103.
[32] M. Barroso, J. Laborda, Digital transformation and the emergence of the Fintech sector: systematic literature review, Digital Business 2 (2) (2022) 100028.
[33] R. Alt, T. Puschmann, The rise of customer-oriented banking - electronic markets are paving the way for change in the financial industry, Electron. Mark. 22 (4) (2012) 203–215.
[34] C. Martins, T. Oliveira, A. Popovič, Understanding the Internet banking adoption: a unified theory of acceptance and use of technology and perceived risk application, Int. J. Inf. Manag. 34 (1) (2014) 1–13.
[35] S. Chauhan, A. Akhtar, A. Gupta, Customer experience in digital banking: a review and future research directions, International Journal of Quality and Service Sciences 14 (2) (2022) 311–348.
[36] M. Maiti, U. Ghosh, Next-generation internet of things in fintech ecosystem, IEEE Internet Things J. 10 (3) (2023) 2104–2111.
[37] S.J. Kaur, et al., Adoption of digital banking channels in an emerging economy: exploring the role of in-branch efforts, J. Financ. Serv. Market. 26 (2) (2021) 107–121.
[38] F.M. Alnaser, et al., Does artificial intelligence (AI) boost digital banking user satisfaction? Integration of expectation confirmation model and antecedents of artificial intelligence enabled digital banking, Heliyon 9 (8) (2023) e18930.
[39] E. Indriasari, F.L. Gaol, T. Matsuo, Digital banking transformation: application of artificial intelligence and big data analytics for leveraging customer experience in the Indonesia banking sector, in: 2019 8th International Congress on Advanced Applied Informatics (IIAI-AAI), 2019.
[40] T.M. Choi, H.K. Chan, X. Yue, Recent development in big data analytics for business operations and risk management, IEEE Trans. Cybern. 47 (1) (2017) 81–92.
[41] B. Vishnuvardhan, B. Manjula, R. Lakshman Naik, A study of digital banking: security issues and challenges, in: Proceedings of the Third International Conference on Computational Intelligence and Informatics, Springer Singapore, Singapore, 2020.
[42] W. Ahmed, et al., Security in next generation mobile payment systems: a comprehensive survey, IEEE Access 9 (2021) 115932–115950.
[43] M. Lezzi, M. Lazoi, A. Corallo, Cybersecurity for Industry 4.0 in the current literature: a reference framework, Comput. Ind. 103 (2018) 97–110.
[44] L.V. Casaló, C. Flavián, M. Guinalíu, The role of security, privacy, usability and reputation in the development of online banking, Online Inf. Rev. 31 (5) (2007) 583–603.
[45] J. Jang-Jaccard, S. Nepal, A survey of emerging threats in cybersecurity, J. Comput. Syst. Sci. 80 (5) (2014) 973–993.
[46] R. Sabillon, et al., Cybercriminals, cyberattacks and cybercrime, in: 2016 IEEE International Conference on Cybercrime and Computer Forensic (ICCCF), 2016.
[47] M. Lagazio, N. Sherif, M. Cushman, A multi-level approach to understanding the impact of cyber crime on the financial sector, Comput. Secur. 45 (2014) 58–74.
[48] S. Ramesh, et al., An adaptive multi-layered approach for DoS detection and mitigation, in: Computational Science and its Applications – ICCSA 2021, Springer International Publishing, Cham, 2021.
[49] G. Thawre, N. Bahekar, B.R. Chandavarkar, Use cases of authentication protocols in the context of digital payment system, in: 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT), 2020.
[50] S. Eswaran, et al., An enhanced network intrusion detection system for malicious crawler detection and security event correlations in ubiquitous banking infrastructure, Int. J. Pervasive Comput. Commun. 18 (1) (2022) 59–78.
[51] G. Kocher, G. Kumar, Machine learning and deep learning methods for intrusion detection systems: recent developments and challenges, Soft Comput. 25 (15) (2021) 9731–9763.
[52] S.K. Mousavi, et al., Security of internet of things based on cryptographic algorithms: a survey, Wireless Network 27 (2) (2021) 1515–1555.
[53] N.P. Rana, S. Luthra, H.R. Rao, Key challenges to digital financial services in emerging economies: the Indian context, Inf. Technol. People 33 (1) (2020) 198–229.
[54] J.A. Jafri, et al., A systematic literature review of the role of trust and security on Fintech adoption in banking, Heliyon 10 (1) (2024) 563059.
[55] Z. Alkhalil, et al., Phishing attacks: a recent comprehensive study and a new anatomy, Front. Comput. Sci. 3 (2021) 563060.
[56] B. Parmar, Protecting against spear-phishing, Comput. Fraud Secur. 2012 (1) (2012) 8–11.

[57] E. Benavides-Astudillo, et al., A phishing-attack-detection model using natural language processing and deep learning, Appl. Sci. 13 (2023), https://doi.org/10.3390/app13095275.
[58] P. Singh, Y.P.S. Maravi, S. Sharma, Phishing websites detection through supervised learning networks, in: 2015 International Conference on Computing and Communications Technologies (ICCCT), 2015.
[59] Y. Su, Research on website phishing detection based on LSTM RNN, in: 2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference, ITNEC), 2020.
[60] A. Maini, et al., Improving the performance of semantic-based phishing detection system through ensemble learning method, in: 2021 IEEE Mysore Sub Section International Conference (MysuruCon), 2021.
[61] O. Sagi, L. Rokach, Ensemble learning: a survey, Wiley Interdisciplinary Reviews: Data Min. Knowl. Discov. 8 (4) (2018) e1249.
[62] P.L. Indrasiri, M.N. Halgamuge, A. Mohammad, Robust ensemble machine learning model for filtering phishing URLs: expandable random gradient stacked voting classifier (ERG-SVC), IEEE Access 9 (2021) 150142–150161.
[63] I.H. Sarker, Deep cybersecurity: a comprehensive overview from neural network and deep learning perspective, SN Computer Science 2 (3) (2021) 154.
[64] C. Opara, B. Wei, Y. Chen, HTMLPhish: enabling phishing web page detection by applying deep learning techniques on HTML analysis, in: 2020 International Joint Conference on Neural Networks (IJCNN), 2020.
[65] G. Suarez-Tangil, et al., Evolution, detection and analysis of malware for smart devices, IEEE Communications Surveys & Tutorials 16 (2) (2014) 961–987.
[66] I.A. Chesti, et al., Evolution, mitigation, and prevention of ransomware, in: 2020 2nd International Conference on Computer and Information Sciences (ICCIS), 2020.
[67] Y. Guo, A review of Machine Learning-based zero-day attack detection: challenges and future directions, Comput. Commun. 198 (2023) 175–185.
[68] M. Rhode, P. Burnap, K. Jones, Early-stage malware prediction using recurrent neural networks, Comput. Secur. 77 (2018) 578–594.
[69] H.S. Galal, Y.B. Mahdy, M.A. Atiea, Behavior-based features model for malware detection, Journal of Computer Virology and Hacking Techniques 12 (2) (2016) 59–67.
[70] A.H. Celdrán, et al., Intelligent and behavioral-based detection of malware in IoT spectrum sensors, Int. J. Inf. Secur. 22 (3) (2023) 541–561.
[71] J. Singh, J. Singh, A survey on machine learning-based malware detection in executable files, J. Syst. Architect. 112 (2021) 101861.
[72] T. Bhardwaj, H. Upadhyay, L. Lagos, Deep learning-based cyber security solutions for smart-city: application and review, in: S.L. Fernandes, T.K. Sharma (Eds.), Artificial Intelligence in Industrial Applications: Approaches to Solve the Intrinsic Industrial Optimization Problems, Springer International Publishing, Cham, 2022, pp. 175–192.
[73] R. Vinayakumar, K.P. Soman, P. Poornachandran, Applying convolutional neural network for network intrusion detection, in: 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2017.
[74] S. Kumar, K.M. Carley, DDoS cyber-attacks network: who's attacking whom, in: 2016 IEEE Conference on Intelligence and Security Informatics (ISI), 2016.
[75] N. Farnaaz, M.A. Jabbar, Random forest modeling for network intrusion detection system, Procedia Computer Science 89 (2016) 213–217.
[76] C.-S. Shieh, et al., Detection of unknown DDoS attacks with deep learning and Gaussian mixture model, Appl. Sci. 11 (2021), https://doi.org/10.3390/app11115213.
[77] A. Valdes, S. Cheung, Communication pattern anomaly detection in process control systems, in: 2009 IEEE Conference on Technologies for Homeland Security, 2009.
[78] O. Yousuf, R.N. Mir, DDoS attack detection in Internet of Things using recurrent neural network, Comput. Electr. Eng. 101 (2022) 108034.
[79] K. Kumar Meenakshi, S. Behal, Distributed denial of service attack detection using deep learning approaches, in: 2021 8th International Conference on Computing for Sustainable Global Development (INDIACom), 2021.
[80] A. Mustapha, et al., Detecting DDoS attacks using adversarial neural network, Comput. Secur. 127 (2023) 103117.
[81] J.R.C. Nurse, et al., Understanding insider threat: a framework for characterising attacks, in: 2014 IEEE Security and Privacy Workshops, 2014.
[82] L. Xiangyu, L. Qiuyang, S. Chandel, Social engineering and insider threats, in: 2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), 2017.
[83] G. Martín, A, et al., A survey for user behavior analysis based on machine learning techniques: current models and applications, Appl. Intell. 51 (8) (2021) 6029–6055.
[84] P.H. Nguyen, et al., VASABI: hierarchical user profiles for interactive visual user behaviour analytics, IEEE Trans. Visual. Comput. Graph. 26 (1) (2020) 77–86.
[85] R.A. Alsowail, T. Al-Shehari, Techniques and countermeasures for preventing insider threats, PeerJ Computer Science 8 (2022) e938.
[86] D.C. Le, N. Zincir-Heywood, Anomaly detection for insider threats using unsupervised ensembles, IEEE Transactions on Network and Service Management 18 (2) (2021) 1152–1164.
[87] R.A. Alsowail, T. Al-Shehari, A multi-tiered framework for insider threat prevention, Electronics 10 (2021), https://doi.org/10.3390/electronics10091005.
[88] O. Brdiczka, et al., Proactive insider threat detection through graph learning and psychological context, in: 2012 IEEE Symposium on Security and Privacy Workshops, 2012.
[89] F. Salahdine, N. Kaabouch *social engineering attacks: a survey*, Future Internet 11 (2019), https://doi.org/10.3390/fi11040089.
[90] M. Adil, R. Khan, M.A.N.U. Ghani, Preventive techniques of phishing attacks in networks, in: 2020 3rd International Conference on Advancements in Computational Sciences (ICACS), 2020.
[91] S. Gupta, A. Singhal, A. Kapoor, A literature survey on social engineering attacks: phishing attack, in: 2016 International Conference on Computing, Communication and Automation (ICCCA), 2016.
[92] R. Abdulraheem, et al., Efficient Email phishing detection using Machine learning, in: 2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC), 2022.
[93] G. M, S.C. Sethuraman, A comprehensive survey on deep learning based malware detection techniques, Computer Science Review 47 (2023) 100529.
[94] Y. Sawa, et al., Detection of social engineering attacks through natural language processing of conversations, in: 2016 IEEE Tenth International Conference on Semantic Computing (ICSC), 2016.
[95] M. Lansley, et al., SEADer++: social engineering attack detection in online environments using machine learning, Journal of Information and Telecommunication 4 (3) (2020) 346–362.
[96] N. Tsinganos, I. Mavridis, D. Gritzalis, Utilizing convolutional neural networks and word embeddings for early-stage recognition of persuasion in chat-based social engineering attacks, IEEE Access 10 (2022) 108517–108529.
[97] B.B. Jayasingh, G.B. Sri, Online transaction anomaly detection model for credit card usage using machine learning classifiers, in: 2023 International Conference on Emerging Smart Computing and Informatics (ESCI), 2023.
[98] I.H. Sarker, Machine learning: algorithms, real-world applications and research directions, SN Computer Science 2 (3) (2021) 160.
[99] S. Soni, B. Bhushan, Use of Machine Learning algorithms for designing efficient cyber security solutions, in: 2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT), 2019.
[100] D. Dasgupta, Z. Akhtar, S. Sen, Machine learning in cybersecurity: a comprehensive survey, The Journal of Defense Modeling and Simulation 19 (1) (2022) 57–106.
[101] L.M. Ibrahim, Anomaly network intrusion detection system based on distributed time-delay neural network (DTDNN), J. Eng. Sci. Technol. 5 (4) (2010) 457–471.
[102] O. Kolodiziev, et al., Automatic machine learning algorithms for fraud detection in digital payment systems, Восточно-Европейский Журнал передовых технологий 5 (9–107) (2020) 14–26.
[103] D. Kocev, et al., Tree ensembles for predicting structured outputs, Pattern Recogn. 46 (3) (2013) 817–833.
[104] P.K. Sadineni, Detection of fraudulent transactions in credit card using machine learning algorithms, in: 2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2020.
[105] C. Bentéjac, A. Csörgő, G. Martínez-Muñoz, A comparative analysis of gradient boosting algorithms, Artif. Intell. Rev. 54 (2021) 1937–1967.

[106] A.A. Taha, S.J. Malebary, An intelligent approach to credit card fraud detection using an optimized light gradient boosting machine, IEEE Access 8 (2020) 25579–25587.
[107] S. Xuan, et al., Random forest for credit card fraud detection, in: 2018 IEEE 15th International Conference on Networking, Sensing and Control (ICNSC), 2018.
[108] D. Xu, Y. Tian, A comprehensive survey of clustering algorithms, Annals of Data Science 2 (2) (2015) 165–193.
[109] Z.T. Pritee, et al., Machine learning and deep learning for user authentication and authorization in cybersecurity: a state-of-the-art review, Comput. Secur. 140 (2024) 103747.
[110] N.K. Gyamfi, J.D. Abdulai, Bank fraud detection using support vector machine, in: 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference, IEMCON), 2018.
[111] K. Fu, et al., Credit card fraud detection using convolutional neural networks, in: Neural Information Processing, Springer International Publishing, Cham, 2016.
[112] Kanika, J. Singla, A survey of deep learning based online transactions fraud detection systems, in: 2020 International Conference on Intelligent Engineering and Management (ICIEM), 2020.
[113] D. Pattnaik, S. Ray, R. Raman, Applications of artificial intelligence and machine learning in the financial services industry: a bibliometric review, Heliyon (2024) e23492.
[114] P.C. Sen, M. Hajra, M. Ghosh, Supervised classification algorithms in machine learning: a survey and review, in: Emerging Technology in Modelling and Graphics: Proceedings of IEM Graph 2018, Springer, 2020.
[115] L. Rokach, Decision forest: twenty years of research, Inf. Fusion 27 (2016) 111–125.
[116] H.-G. Han, L.-D. Wang, J.-F. Qiao, Efficient self-organizing multilayer neural network for nonlinear system modeling, Neural Network. 43 (2013) 22–32.
[117] H. Cevikalp, Best fitting hyperplanes for classification, IEEE Trans. Pattern Anal. Mach. Intell. 39 (6) (2017) 1076–1088.
[118] H.U. Dike, et al., Unsupervised learning based on artificial neural network: a review, in: 2018 IEEE International Conference on Cyborg and Bionic Systems, CBS), 2018.
[119] D.T. Nguyen, L. Chen, C.K. Chan, Clustering with multiviewpoint-based similarity measure, IEEE Trans. Knowl. Data Eng. 24 (6) (2011) 988–1001.
[120] N. Ganganath, C.T. Cheng, C.K. Tse, Data clustering with cluster size constraints using a modified K-means algorithm, in: 2014 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, 2014.
[121] Maigha, M.L. Crow, Clustering-based methodology for optimal residential time of use design structure, in: 2014 North American Power Symposium (NAPS), 2014.
[122] L. Rashid, et al., Analysis of dimensionality reduction techniques on Internet of Things data using machine learning, Sustain. Energy Technol. Assessments 52 (2022) 102304.
[123] F.L. Gewers, et al., Principal component analysis: a natural approach to data exploration, ACM Comput. Surv. 54 (4) (2021) 1–34.
[124] W. Zhu, et al., A deep learning approach for process data visualization using t-distributed stochastic neighbor embedding, Ind. Eng. Chem. Res. 58 (22) (2019) 9564–9575.
[125] M. Van Otterlo, M. Wiering, Reinforcement learning and markov decision processes, in: Reinforcement Learning: State-Of-The-Art, Springer, 2012, pp. 3–42.
[126] B. Jang, et al., Q-learning algorithms: a comprehensive classification and applications, IEEE Access 7 (2019) 133653–133667.
[127] Z. Zhang, et al., A collaborative multiagent reinforcement learning method based on policy gradient potential, IEEE Trans. Cybern. 51 (2) (2019) 1015–1027.
[128] T.T. Nguyen, N.D. Nguyen, S. Nahavandi, Deep reinforcement learning for multiagent systems: a review of challenges, solutions, and applications, IEEE Trans. Cybern. 50 (9) (2020) 3826–3839.
[129] S.S. Tirumala, A. Narayanan, Hierarchical data classification using deep neural networks, in: Neural Information Processing, Springer International Publishing, Cham, 2015.
[130] A. Karpathy, et al., Large-scale video classification with convolutional neural networks, in: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 2014.
[131] K. Bandara, C. Bergmeir, S. Smyl, Forecasting across time series databases using recurrent neural networks on groups of similar series: a clustering approach, Expert Syst. Appl. 140 (2020) 112896.
[132] A. Creswell, et al., Generative adversarial networks: an overview, IEEE Signal Process. Mag. 35 (1) (2018) 53–65.
[133] A. Bilen, A.B. Özer, Cyber-attack method and perpetrator prediction using machine learning algorithms, PeerJ Computer Science 7 (2021) e475.
[134] H. Alqahtani, et al., Cyber intrusion detection using machine learning classification techniques, in: Computing Science, Communication and Security, Springer Singapore, Singapore, 2020.
[135] A.B. Nassif, et al., Machine learning for anomaly detection: a systematic review, IEEE Access 9 (2021) 78658–78700.
[136] B. Böse, et al., Detecting insider threats using radish: a system for real-time anomaly detection in heterogeneous data streams, IEEE Syst. J. 11 (2) (2017) 471–482.
[137] M. Leo, S. Sharma, K. Maddulety, Machine learning in banking risk management: a literature review, Risks 7 (1) (2019) 29.
[138] M. Ahmed, A.N. Mahmood, M.R. Islam, A survey of anomaly detection techniques in financial domain, Future Generat. Comput. Syst. 55 (2016) 278–288.
[139] S. Samtani, et al., Cybersecurity as an industry: a cyber threat intelligence perspective, The Palgrave Handbook of International Cybercrime and Cyberdeviance (2020) 135–154.
[140] I.H. Sarker, et al., Cybersecurity data science: an overview from machine learning perspective, Journal of Big data 7 (2020) 1–29.
[141] M. Tabiaa, A. Madani, The deployment of machine learning in eBanking: a survey, in: 2019 Third International Conference on Intelligent Computing in Data Sciences (ICDS), 2019.
[142] S.S. Gill, et al., AI for next generation computing: emerging trends and future directions, Internet of Things 19 (2022) 100514.
[143] E. Hossain, et al., Application of big data and machine learning in smart grid, and associated security concerns: a review, IEEE Access 7 (2019) 13960–13988.
[144] S. Mishra, Exploring the impact of AI-based cyber security financial sector management, Appl. Sci. 13 (10) (2023) 5875.
[145] I.H. Sarker, Machine learning for intelligent data analysis and automation in cybersecurity: current and future prospects, Annals of Data Science (2022) 1–26.
[146] K. Shaukat, et al., A survey on machine learning techniques for cyber security in the last decade, IEEE Access 8 (2020) 222310–222354.
[147] R.A. Ariyaluran Habeeb, et al., Real-time big data processing for anomaly detection: a Survey, Int. J. Inf. Manag. 45 (2019) 289–307.
[148] K. Maharana, S. Mondal, B. Nemade, A review: data pre-processing and data augmentation techniques, Global Transitions Proceedings 3 (1) (2022) 91–99.
[149] R. Punmiya, S. Choe, Energy theft detection using gradient boosting theft detector with feature engineering-based preprocessing, IEEE Trans. Smart Grid 10 (2) (2019) 2326–2329.
[150] D.A. Otchere, et al., Application of gradient boosting regression model for the evaluation of feature selection techniques in improving reservoir characterisation predictions, J. Petrol. Sci. Eng. 208 (2022) 109244.
[151] J.L. Leevy, et al., Detecting cybersecurity attacks across different network features and learners, Journal of Big Data 8 (1) (2021) 38.
[152] S.Z.H. Shoumo, et al., Application of machine learning in credit risk assessment: a prelude to smart banking, in: TENCON 2019 - 2019 IEEE Region 10 Conference (TENCON), 2019.
[153] T. Mahmood, U. Afzal, Security Analytics: big Data Analytics for cybersecurity: a review of trends, techniques and tools, in: 2013 2nd National Conference on Information Assurance (NCIA), 2013.
[154] F.N. Ogwueleka, et al., Neural network and classification approach in identifying customer behavior in the banking sector: a case study of an international bank, Human factors and ergonomics in manufacturing & service industries 25 (1) (2015) 28–42.
[155] Y. Mehmood, et al., Intrusion Detection System in Cloud Computing: Challenges and Opportunities, 2013, pp. 59–66.
[156] N.H. Ab Rahman, K.-K.R. Choo, A survey of information security incident handling in the cloud, Comput. Secur. 49 (2015) 45–69.
[157] X. Gao, et al., An adaptive ensemble machine learning model for intrusion detection, IEEE Access 7 (2019) 82512–82521.
[158] S. Brown, J. Gommers, O. Serrano, From cyber security information sharing to threat management, in: Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security, Association for Computing Machinery, Denver, Colorado, USA, 2015, pp. 43–49.

[159] A. Shrestha, A. Mahmood, Review of deep learning algorithms and architectures, IEEE Access 7 (2019) 53040–53065.
[160] M. Binjubeir, et al., Comprehensive survey on big data privacy protection, IEEE Access 8 (2020) 20067–20079.
[161] P. Samarati, S.C. de Vimercati, Access control: policies, models, and mechanisms, in: International School on Foundations of Security Analysis and Design, Springer, 2000, pp. 137–196.
[162] A. Aljeraisy, et al., Privacy laws and privacy by design schemes for the internet of things: a developer's perspective, ACM Comput. Surv. 54 (5) (2021) 1–38.
[163] I. Palomares, et al., A panoramic view and swot analysis of artificial intelligence for achieving the sustainable development goals by 2030: progress and prospects, Appl. Intell. 51 (9) (2021) 6497–6527.
[164] P.U. Chinedu, et al., Cybercrime detection and prevention efforts in the last decade: an overview of the possibilities of machine learning models, Review of International Geographical Education Online 11 (7) (2021).
[165] P. Dixit, S. Silakari, Deep learning algorithms for cybersecurity applications: a technological and status review, Computer Science Review 39 (2021) 100317.
[166] Q. Liu, et al., A survey on security threats and defensive techniques of machine learning: a data driven view, IEEE Access 6 (2018) 12103–12117.
[167] L. Zhou, et al., Machine learning on big data: opportunities and challenges, Neurocomputing 237 (2017) 350–361.
[168] Z.C. Lipton, The mythos of model interpretability: in machine learning, the concept of interpretability is both important and slippery, Queue 16 (3) (2018) 31–57.
[169] S. Chakraborty, et al., Interpretability of deep learning models: a survey of results, in: 2017 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation, 2017. *SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)*.
[170] E. Alhajjar, P. Maxwell, N. Bastian, Adversarial machine learning in network intrusion detection systems, Expert Syst. Appl. 186 (2021) 115782.
[171] F. Kreuk, et al., Deceiving end-to-end deep learning malware detectors using adversarial examples, arXiv preprint arXiv:1802.04528 (2018).
[172] G.A. Susto, et al., A fraud detection decision support system via human on-line behavior characterization and machine learning, in: 2018 First International Conference on Artificial Intelligence for Industries (AI4I), 2018.
[173] M. Shashanka, M.Y. Shen, J. Wang, User and entity behavior analytics for enterprise security, in: 2016 IEEE International Conference on Big Data (Big Data), 2016.
[174] Y. Shen, et al., Tiresias: predicting security events through deep learning, in: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, Association for Computing Machinery, Toronto, Canada, 2018, pp. 592–605.
[175] S. Zeadally, et al., Harnessing artificial intelligence capabilities to improve cybersecurity, IEEE Access 8 (2020) 23817–23837.
[176] A. Jobin, M. Ienca, E. Vayena, The global landscape of AI ethics guidelines, Nat. Mach. Intell. 1 (9) (2019) 389–399.
[177] S. Denman, Why multi-layered security is still the best defence, Netw. Secur. 2012 (3) (2012) 5–7.
[178] S. Rizvi, S. Campbell, K. Alden, Why compliance is needed for internet of things?, in: 2020 International Conference on Software Security and Assurance (ICSSA), 2020.