Educational Administration: Theory and Practice
2023, 29(1) 357-368
ISSN: 2148-2403
https://kuey.net/

Research Article

AI-Enhanced Detection and Mitigation of Cybersecurity Threats in Digital Banking

Suri babu Nuthalapati

*Cloudera, Santa Clara, California, United States 95054suri@cloudera.com

Citation: Suri babu Nuthalapati (2023), AI-Enhanced Detection and Mitigation of Cybersecurity Threats in Digital Banking *Educational Administration: Theoryand Practice*, *29(1)* 357-368, Doi: 10.53555/kuey.v29i1.6908

ARTICLE INFO

ABSTRACT

The rapid evolution of digital technologies has revolutionized the banking sector, making financial services more accessible and convenient through digital channels. However, this digital transformation has also introduced significant cybersecurity challenges, exposing financial institutions to a range of threats including fraud, data breaches, and malicious attacks. In response to these challenges, this research proposes an advanced AI-enhanced framework designed specifically for detecting and mitigating cybersecurity threats within the realm of digital banking. This research introduces an AI-enhanced framework for detecting and mitigating these threats in digital banking. Our solution includes a web application utilizing machine learning models to predict loan acceptance and detect fraudulent credit card transactions. Employing a Random Forest algorithm for loan prediction and a Support Vector Machine (SVM) for fraud detection, our models achieve precision rates of 92% and 90%, respectively. The system preprocesses datasets, splits them for training and validation, and generates pickle files for real-time predictions via the web application. An adaptive Class Incremental Learning Framework supports continuous improvement in threat detection. This framework enhances digital banking security by enabling real-time monitoring and proactive threat mitigation, thereby safeguarding sensitive financial information and preserving customer trust.

Keywords: Class Incremental Learning, Cyber security framework, Digital payment security, AI-enhanced cyber security, Real-time monitoring

INTRODUCTION

The rapid advancement of digital technologies has significantly transformed the banking sector, leading to the emergence of digital banking as a pivotal component of modern financial services. Over the past two decades, the proliferation of the internet, smartphones, and communication technologies has revolutionized the way banking services are delivered, making them more user-friendly, efficient, and accessible[1] [2]. Digital banking encompasses a wide range of financial activities conducted through digital platforms, including online banking, mobile banking, and the use of digital wallets, which have become integral to the daily lives of consumers [3][4].

The importance of digital banking has been further underscored by the economic disruptions caused by the COVID-19 pandemic. As traditional banking operations faced unprecedented challenges, digital banking emerged as a crucial enabler of cashless transactions, ensuring the continuity of financial services while adhering to social distancing norms [1]. This shift has not only highlighted the resilience of digital banking but also accelerated its adoption across various demographics and regions [5][6].

Moreover, the integration of innovative financial technologies such as blockchain, artificial intelligence, and big data analytics has enhanced the capabilities of digital banking, offering personalized and efficient services to customers [7]. These technologies have enabled banks to optimize their operations, reduce costs, and improve customer satisfaction by providing real-time, tailored financial solutions[2][8]. However, the rapid digital transformation also brings forth challenges related to data security, privacy, and regulatory compliance, which need to be addressed to ensure the sustainable growth of digital banking [7] [9].

Digital banking represents a significant evolution in the financial sector, driven by technological advancements and changing consumer preferences. Its growing importance is evident in its ability to provide seamless, efficient, and secure financial services, making it an indispensable part of the modern economy. As

digital banking continues to evolve, it is imperative for banks to navigate the associated challenges and leverage emerging technologies to stay competitive and meet the dynamic needs of their customers [8][10].

Digital banking, also known as internet or online banking, has revolutionized the financial sector by enabling customers to perform banking activities entirely online without the need for physical documents or visits to bank branches. This transformation is driven by the exponential growth of the internet, smartphones, and communication technologies over the past two decades, making financial transactions more user-friendly, efficient, and fast[11][12]. The Digital India initiative, launched by the Government of India, aims to transform the country into a digitally empowered society and knowledge economy, significantly boosting the adoption of digital banking [13]. The initiative has been instrumental in addressing the challenges of a large unbanked population and outdated banking technologies, which previously hindered the growth of digital banking in India [14]. The COVID-19 pandemic further accelerated the shift towards digital banking, as it enabled cashless transactions and minimized physical contact, thereby ensuring safety and convenience for users [15]. Digital banking offers numerous advantages, including 24/7 access to banking services, reduced operational costs for banks, and enhanced customer satisfaction through improved service quality and faster transaction processing [16] [17] [18]. It also plays a crucial role in enhancing economic transparency and reducing crime and corruption by providing a secure platform for financial transactions [19]. The integration of advanced technologies in digital banking has led to the automation and optimization of business processes, allowing banks to allocate resources more efficiently and improve service quality. Despite its benefits, digital banking faces challenges such as internet availability, low technological exposure in rural areas, and cybersecurity risk. However, the continuous advancements in technology and the growing importance of digital marketing strategies are expected to drive further growth and innovation in the digital banking sector [20]. The increasing use of digital payment services, driven by government initiatives and changing consumer behavior, highlights the significant and positive impact of digital banking on the financial landscape. As digital banking continues to evolve, it is poised to play an even more critical role in shaping the future of the global financial environment, making banking more accessible, efficient, and secure for users worldwide.

The digital banking sector has revolutionized the way financial transactions are conducted, offering unprecedented convenience and accessibility to users worldwide. However, this transformation has also introduced a myriad of cybersecurity threats that pose significant risks to both financial institutions and their customers. The increasing reliance on internet and mobile applications for banking activities has made the sector a prime target for cybercriminals, who employ sophisticated techniques to exploit vulnerabilities and steal sensitive information.

Cybersecurity threats in digital banking are multifaceted, encompassing a range of malicious activities such as phishing, malware, ransomware, and zero-click attacks. These threats have escalated in frequency and complexity, leading to substantial financial losses and reputational damage for banks. For instance, the number of data breaches in the banking sector has surged, with a notable increase in blackmail virus attacks by 1318% in the first half of 2021 alone [21]. This alarming trend underscores the urgent need for robust cybersecurity measures to protect digital banking systems from evolving cyber threats.

The banking sector's exposure to cyber-attacks is further exacerbated by the rapid digitization of financial services. As banks continue to adopt advanced technologies to enhance their operations, they inadvertently create new potential attack surfaces for cybercriminals. This dynamic environment necessitates continuous vigilance and adaptation of cybersecurity strategies to mitigate risks effectively. Financial institutions must invest in sophisticated technologies and security measures to safeguard against cyber-attacks, which have become an integral part of their business models[22].

Moreover, the human factor remains a critical vulnerability in the cybersecurity landscape. Despite the implementation of standard security protocols, the lack of awareness and vigilance among users can lead to successful cyber-attacks. For example, phishing attacks, which exploit human error, continue to be a major contributor to malicious activities in the e-banking sector[23]. As attackers develop more advanced methods, such as zero-click attacks that require no user interaction, the challenge of securing digital banking systems becomes even more daunting.

In response to these threats, financial institutions must adopt a comprehensive approach to cybersecurity that includes multiple layers of defense, continuous monitoring, and user education. By understanding the nature and classification of cyber threats, banks can develop targeted countermeasures to mitigate risks and enhance their overall security posture [24]. Additionally, leveraging emerging technologies such as Artificial Intelligence (AI) can provide real-time solutions to detect and prevent cyber-attacks, thereby strengthening the resilience of digital banking systems [25].

The rising threat of cyber-attacks in the digital banking sector demands a proactive and multifaceted approach to cybersecurity. As cybercriminals continue to evolve their tactics, financial institutions must remain vigilant and adaptive, employing advanced technologies and comprehensive security strategies to protect their assets and maintain customer trust. The ongoing battle between cybersecurity experts and cybercriminals highlights the critical importance of staying ahead of emerging threats to ensure the safety and integrity of digital banking services.

The digital banking sector has undergone a significant transformation in recent years, driven by the rapid adoption of online and mobile banking technologies. This shift has brought about numerous benefits,

including increased convenience, efficiency, and accessibility for customers. However, it has also introduced a new array of cybersecurity challenges that threaten the integrity and security of financial institutions. The rise in cyber-attacks targeting the banking sector is alarming, with incidents such as data breaches, ransomware, and fraud becoming increasingly prevalent. In 2021 alone, the number of data breaches surpassed the total number of events in 2020 by 17%, marking another "worst year ever" for cyber-attacks in the banking industry [26] [27]. The complexity and sophistication of these attacks have escalated, with cybercriminals leveraging advanced technologies such as artificial intelligence (AI) and machine learning to enhance their malicious activities [28]. The financial repercussions of these breaches are substantial, affecting not only the financial assets of institutions but also eroding customer trust and confidence. The banking sector is disproportionately affected by cyber threats compared to other industries, with a significant portion of cybercrimes related to ATM, debit card, and net banking fraud [29]. To combat these threats, it is imperative for banks to adopt a holistic and adaptive approach to cybersecurity, integrating advanced technologies like Big Data analytics, AI, and continuous risk assessment methodologies. Preventive measures such as multi-factor authentication, encryption techniques, and anomaly detection algorithms are crucial in safeguarding against cyber fraud. Additionally, collaboration between banks, law enforcement agencies, and cybersecurity organizations is essential to enhance information sharing and response to cyber threats. The digital payment ecosystem, which has seen a manifold increase in usage, is particularly vulnerable to cyber-attacks, necessitating robust security measures to protect against online fraud, identity theft, and spyware or virus attacks [30]. The introduction of innovative technologies such as the Internet of Things (IoT), cloud computing, and AI in the financial sector has further expanded the potential attack surfaces, making cybersecurity a top priority for financial institutions [31]. Despite the advancements in cybersecurity measures, the continuous evolution of cyber threats requires ongoing vigilance and adaptation. Educating customers and bank employees about cyber fraud risks and promoting a culture of cybersecurity awareness are also critical components in mitigating these risks [32]. As the digital banking landscape continues to evolve, the importance of robust cybersecurity frameworks cannot be overstated, underscoring the need for strategic investments in technology, education, and collaboration to safeguard financial assets and maintain customer trust in the digital age.

The rapid evolution of cyber threats has necessitated the development of advanced cybersecurity measures. Traditional cybersecurity solutions are increasingly proving inadequate in the face of sophisticated cyber-attacks, which have become more frequent and complex over the years. In this context, Artificial Intelligence (AI) has emerged as a promising tool to enhance cybersecurity measures. AI's capabilities in data analysis, pattern recognition, and predictive modeling offer significant potential to improve the detection, prevention, and response to cyber threats.

AI techniques, particularly machine learning and deep learning, have shown promise in enabling cybersecurity experts to counter the ever-evolving threats posed by cyber adversaries[33]. These techniques can analyze vast amounts of data in real-time, identify patterns and anomalies in network traffic, and predict potential cyber-attacks before they occur. This proactive approach allows for quicker and more effective responses to threats, thereby minimizing damage and disruption.

The integration of AI in cybersecurity is not without its challenges. There are concerns about the reliability of AI systems and the potential for AI to be used maliciously[34]. Additionally, the implementation of AI in cybersecurity requires significant resources, including large datasets for training AI models and skilled professionals to manage and interpret AI-generated insights[35]. Despite these challenges, the benefits of AI in enhancing cybersecurity are substantial. AI can significantly improve the speed and accuracy of threat detection and response, making it a valuable asset in the fight against cybercrime.

Moreover, the application of AI in specific sectors, such as power generation and distribution, has demonstrated its potential to enhance cybersecurity measures significantly[36]. AI's ability to continuously monitor and analyze data can help organizations stay ahead of evolving threats and ensure the security of critical infrastructure.

In conclusion, the potential of AI to enhance cybersecurity measures is immense. By leveraging AI's advanced capabilities, organizations can improve their defenses against cyber threats, ensuring the protection of valuable data and maintaining the integrity of their operations. However, it is crucial to address the associated challenges and risks to fully realize the benefits of AI in cybersecurity. As the field continues to evolve, ongoing research and development will be essential to harness the full potential of AI in enhancing cybersecurity measures[37].

The rapid evolution of the digital landscape has brought about a surge in cybersecurity threats, necessitating advanced measures to protect sensitive data and infrastructure. Traditional security methods are increasingly struggling to keep pace with the volume and complexity of these threats, making the integration of Artificial Intelligence (AI) into cybersecurity a promising solution. AI technologies, particularly machine learning algorithms, empower security systems to dynamically adapt to emerging threats by analyzing vast datasets in real-time, identifying anomalous patterns, and potential vulnerabilities, thus enabling proactive threat mitigation and rapid response capabilities. The potential of AI in enhancing cybersecurity is further underscored by its ability to automate routine security tasks, thereby reducing the burden on human operators and minimizing the likelihood of human error. AI's role in cybersecurity extends to the realm of Cyber Threat Intelligence (CTI), where it can automate and enhance various tasks, from data ingestion to

resilience verification, and provide real-time, contextual, and predictive insights for mitigation recommendations. Additionally, AI-based systems leverage machine learning, natural language processing, and other methods to enhance threat identification, response, and mitigation, offering strategies such as anomaly detection, behavior analysis, and predictive modeling. Generative AI, a form of AI that creates new data without relying on existing data or expert knowledge, further enhances threat intelligence by quickly identifying threats and vulnerabilities within an organization's infrastructure, providing an additional layer of defense against sophisticated attacks. The integration of AI into cybersecurity is not without challenges, including ethical dilemmas, potential biases, and the need for transparency in AI-driven decisions. However, the potential benefits of AI in fortifying cybersecurity measures are significant, offering innovative approaches to countering cybersecurity threats and addressing the complexities of modern systems [38]. As such, AI emerges as a potent tool in the ongoing battle to safeguard digital ecosystems against an increasingly sophisticated array of cyber threats.

LITERATURE REVIEW

The integration of Artificial Intelligence (AI) in cybersecurity has become a pivotal aspect of digital banking. As financial institutions increasingly adopt digital platforms, the need for robust cybersecurity measures has grown exponentially. This literature review explores the existing research on the application of AI in enhancing cybersecurity within the digital banking sector, highlighting key findings, methodologies, and future directions.

AI Applications in Cybersecurity for Digital Banking

AI has been instrumental in addressing various cybersecurity challenges in digital banking. Traditional methods have often fallen short in protecting client assets and ensuring data privacy. AI-powered solutions, such as chatbots, smart virtual assistants, and biometric user authentication, have been developed to tackle these issues effectively[39]. These technologies not only enhance security but also improve customer experience by providing seamless and secure banking services.

Biometric Authentication

Biometric authentication systems have gained significant traction in the banking sector due to their reliability and effectiveness in verifying user identities. These systems utilize physical and behavioral traits to authenticate users, thereby reducing the risk of unauthorized access and cyber threats [40]. The implementation of biometric security measures has been shown to provide high levels of safety and security, making them a preferred choice for many financial institutions.

Ethical Considerations and Trust in AI

The ethical implications of AI in cybersecurity are a critical area of concern. The interaction between humans and AI systems necessitates the establishment of ethical standards to ensure responsible use. Trust in AI is a double-edged sword; while it can enhance cybersecurity practices, it also poses risks if the AI systems themselves are compromised[41][42]. Therefore, continuous monitoring and the development of reliable AI systems are essential to mitigate these risks.

Impact of Digital Skills and Cybersecurity Awareness

The readiness for change in digital banking is influenced by the level of cybersecurity awareness and digital skills among banking professionals. Studies have shown that while cybersecurity awareness alone may not significantly impact readiness for change, digital skills play a crucial role in adapting to new technologies and cybersecurity measures [43]. This highlights the importance of incorporating digital intelligence and cybersecurity training in banking curricula.

Technological Advancements and Risk Management

The advent of Industry 4.0 technologies, including Big Data, Cloud Computing, Machine Learning, IoT, and Blockchain, has revolutionized cybersecurity in banking. These technologies enable the development of advanced security procedures and risk management strategies [44]. However, the rapid evolution of these technologies also introduces new vulnerabilities, necessitating continuous investment in cybersecurity infrastructure and practices.

Future research should focus on developing standards and certification procedures for AI in cybersecurity to ensure reliability and trustworthiness. Additionally, exploring the potential of AI in various application domains within cybersecurity can provide valuable insights into its strengths and weaknesses [45]. Addressing the limitations of AI, such as data quality and hidden biases, will be crucial in advancing its application in digital banking cybersecurity. The integration of AI in cybersecurity for digital banking presents both opportunities and challenges. While AI technologies offer promising solutions to enhance security and protect client assets, ethical considerations and the need for reliable systems cannot be overlooked. Continuous research and development, along with the implementation of robust standards, will be essential in harnessing the full potential of AI in this critical domain.

The integration of Artificial Intelligence (AI) in cybersecurity for digital banking has garnered significant attention in recent years, driven by the increasing sophistication and frequency of cyberattacks. Traditional cybersecurity measures are often inadequate in addressing the dynamic and complex nature of modern cyber threats, necessitating the adoption of AI-based solutions. AI's role in enhancing cybersecurity is multifaceted, encompassing threat detection, prediction, and response. AI techniques, such as machine learning (ML) and

deep learning (DL), have been instrumental in developing robust cybersecurity systems capable of identifying and mitigating threats in real-time [46][47]. For instance, AI-driven models like the Bayesian network-based prediction model and the Apriori Viterbi model have shown promise in predicting and detecting various types of cyber-attacks, including Distributed Denial of Service (DDoS) and socio-technical attacks [48]. Despite these advancements, the adoption of AI in cybersecurity is not without challenges. One significant issue is the "black-box" nature of many AI algorithms, which can make their decision-making processes opaque and difficult to interpret. This has led to the emergence of Explainable AI (XAI), which aims to make AI models more transparent and understandable to human operators, thereby enhancing trust and usability in cybersecurity applications [49] [50] [51]. The banking sector, in particular, stands to benefit immensely from AI-driven cybersecurity solutions. AI can help banks build resilient cyber-defense systems that limit unauthorized access and protect sensitive financial data [52]. However, the implementation of AI in banking cybersecurity is still in its nascent stages in many regions, with limited studies focusing on its application in African banks. Moreover, the rapid evolution of cyber threats necessitates continuous research and development to keep pace with emerging challenges. Researchers have highlighted the need for hybrid AI techniques that combine various AI subfields, such as Artificial Neural Networks (ANNs) and fuzzy systems, to enhance the effectiveness of cybersecurity measures. Additionally, the intersection of AI and cybersecurity extends beyond traditional banking to areas like investigative journalism, where AI technologies are used to detect and debunk deepfakes, thereby safeguarding the integrity of journalistic work. Overall, the literature underscores the transformative potential of AI in cybersecurity for digital banking, while also emphasizing the need for ongoing research to address existing challenges and explore new applications. The systematic literature reviews conducted in various studies provide a comprehensive overview of the current state of AI in cybersecurity, identifying key areas for future research and development [53] [54]. This body of work contributes to the advancement of knowledge in the field and aids in the development of more effective AI-driven cybersecurity solutions to combat evolving cyber threats.

The digital transformation of the banking sector has brought about significant advancements in service delivery and operational efficiency. However, this shift has also exposed banks to a myriad of cybersecurity threats. This literature review aims to synthesize existing research on the types of cybersecurity threats faced by digital banking institutions, highlighting the evolving nature of these threats and the measures being taken to mitigate them.

Types of Cybersecurity Threats

Phishing and Social Engineering

Phishing and social engineering attacks are among the most prevalent cybersecurity threats in the banking sector. These attacks exploit human vulnerabilities to gain unauthorized access to sensitive information. According to a study, phishing attacks have become a major threat due to the widespread digitization in the financial sector [55]. The increasing sophistication of these attacks makes them particularly challenging to defend against.

Malware and Ransomware

Malware, including ransomware, poses a significant threat to digital banking. These malicious software programs can disrupt operations, steal sensitive data, and demand ransom payments. The banking sector has seen a dramatic increase in ransomware attacks, with a 1318% year-over-year increase in blackmail virus attacks reported in the first half of 2021[56]. This trend underscores the urgent need for robust cybersecurity measures.

Distributed Denial of Service (DDoS) Attacks

DDoS attacks aim to overwhelm banking systems with a flood of traffic, rendering them unavailable to legitimate users. These attacks can cause significant financial and reputational damage. Research highlights that DDoS attacks are becoming more sophisticated, making it increasingly difficult for banks to defend against them [57].

Web Application Attacks

Web application attacks target vulnerabilities in online banking platforms. These attacks can lead to unauthorized access to customer accounts and financial data. The complexity and frequency of web application attacks have increased, necessitating advanced security measures to protect online banking services [58].

Impact on the Banking Sector

Financial and Reputational Damage

Cybersecurity threats can lead to substantial financial losses and damage to a bank's reputation. The direct costs include financial theft and fraud, while indirect costs encompass loss of customer trust and regulatory fines. A comprehensive analysis of cyber threats in the banking sector emphasizes the critical nature of these impacts and the need for effective risk management strategies [59]. Creating prediction models to forecast power usage in areas with multiple sectors can significantly enhance the efficiency of energy consumption and decision-making for energy management [60] [61]. Similarly, AI-enhanced detection and mitigation of cybersecurity threats in digital banking can improve the security and reliability of financial transactions.

Regulatory and Compliance Challenges

Banks must navigate a complex landscape of regulatory and compliance requirements to protect against cybersecurity threats. International and national regulatory bodies provide guidelines to help banks manage cyber risk exposure. However, the rapidly evolving nature of cyber threats presents ongoing challenges for compliance [62].

Mitigation Strategies

Technological and Organizational Measures

To combat cybersecurity threats, banks are investing in sophisticated technologies and implementing organizational measures. These include advanced encryption, multi-factor authentication, and continuous monitoring of network activity. A study on cyber risk management in banks highlights the importance of these measures in safeguarding against cyber-attacks [59].

Collaboration with Fintech Firms

The collaboration between banks and fintech firms has introduced new cybersecurity risks. However, this partnership also offers opportunities for enhanced security through shared resources and expertise. Creating prediction models to forecast power usage in areas with multiple sectors, aiming to optimize energy consumption and improve decision-making for energy management. Research suggests that a collaborative approach to cybersecurity can yield significant benefits, provided that both parties work together to mitigate risks [60].

The digital banking sector faces a diverse array of cybersecurity threats, ranging from phishing and malware to DDoS and web application attacks. These threats pose significant financial, reputational, and regulatory challenges. Effective mitigation strategies, including technological investments and collaborative efforts with fintech firms, are essential to safeguarding the banking sector against these evolving threats. Continued research and adaptation are crucial to staying ahead of cybercriminals and ensuring the security of digital banking services.

METHODOLOGY

The solution that is being suggested is comprised of a web application that makes use of a machine learning model in order to forecast the acceptance of loans. A number of different machine learning techniques are utilised in order to train the model, which is subsequently implemented into the web application. In order to train the model, the user is required to fill out a form that consists of eleven fields, which corresponds to the eleven attributes that were employed. Prior to the training of the model, the dataset is subjected to pre-processing, which includes the restoration of missing values through the use of the mean and mode technique and the conversion of string values to binary by the utilisation of label encoding. The dataset that has been preprocessed is divided into two halves, with eighty percent being used for training and twenty percent being used for validating the validity of the model using a variety of methods. After the dataset was divided into sections, the Random Forest algorithm was utilised, which resulted in a precision rate of 92%. Following the completion of the training process, the model will generate a pickle file. The user must first fill out the form that is provided on the web application, and then click the "MAKE PREDICTION" button in order to make a prediction regarding the acceptance of the loan. The trained model or pickle file is utilised by the system in order to generate predictions regarding the determination of whether or not the loan will be accepted. It is possible for banks and businesses to improve their loan approval procedure by utilising this technology.

The solution that is being proposed is an online application that makes use of an algorithm for machine learning in order to identify instances of fraudulent payments made with credit cards. Through the use of Kaggle, a data analysis platform that offers datasets, the dataset that was required for this research was acquired. For the purpose of training the model, the dataset was comprised of thirty thousand records of client credit card transaction histories that were collected over the course of the previous six months. The web application requires users to fill out a form in order to forecast instances of credit card theft. This is done in order to collect information. Subsequently, the dataset was treated to pre-processing and divided into two parts. Ninety percent of the dataset was designated for training, and the remaining ten percent was specifically saved for assessing the correctness of the model using a variety of approaches. An accuracy rate of 90% was achieved by the utilisation of the Support Vector Machine technique, which was implemented following the completion of dataset splitting. Following the completion of the training process, a pickle file is generated. This file is then utilised to make predictions regarding instances of fraudulent credit card transactions. The user is required to fill out the web application form and then click the "MAKE PREDICTION" button in order to make a prediction regarding a fraudulent transaction. Following this, the trained model is utilised to ascertain whether or not the transaction in question is fraudulent.

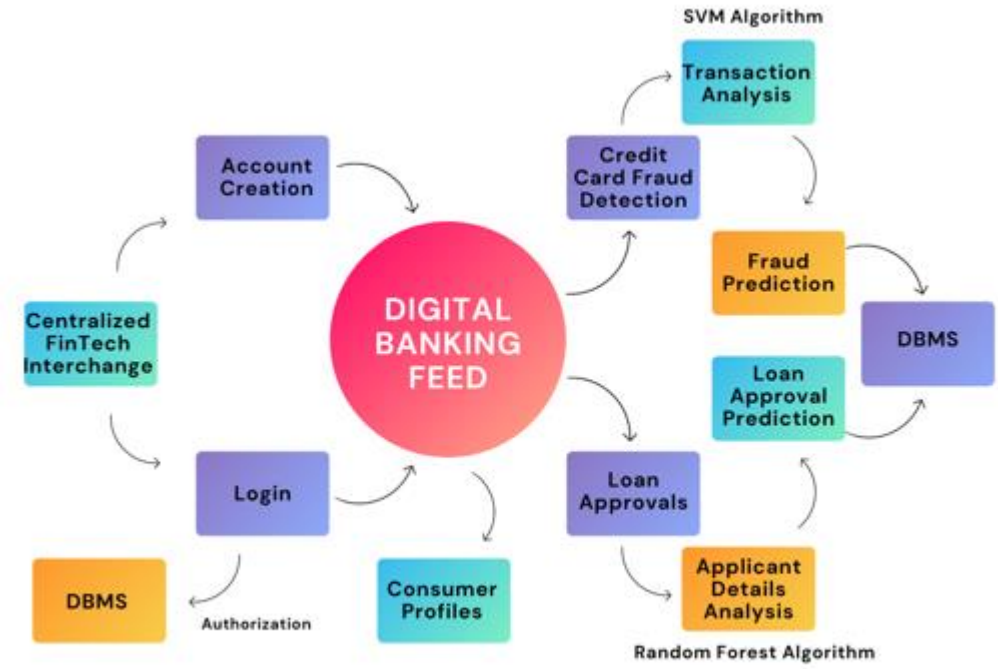


Figure.1 Proposed framework for Autonomic digital banking operations

The methodology known as Random Forest refers to a classifier technique that is widely used in the field of machine learning and is known for its high level of efficiency. The system is made up of a number of different decision trees that are independent of one another and collaborate in order to make decisions. The straightforwardness and versatility of this strategy, which enables it to handle classification and regression tasks in an efficient manner, has garnered widespread recognition.

Creating a large number of decision trees is how the Random Forest algorithm accomplishes its tasks. The majority of the trees that were chosen as a result of random selection will determine the final conclusion regarding the outcome of the tree. The selection of the most advantageous course of action can be accomplished by the utilisation of a decision tree, which is a graphical representation. Each individual branch of the tree represents a different option, occurrence, or response that could take place. This tactic is employed in situations when there are several subtrees in the forest in order to ensure that the model does not get overfit and to cut down on the amount of time required for training. In addition to this, it delivers results that are extremely precise and allows efficient management of big databases by predicting data that is absent. In order to complete the Random Forest Algorithm, the following steps are required:

The first step is to choose a subset of N records from the collection at random.

The second step is to construct a decision tree by making use of the existing N data.

Before proceeding with stages 1 and 2, it is necessary to specify the proper amount of trees that will be incorporated into the algorithm.

During the course of a regression challenge, each individual tree in the forest is responsible for producing a prediction for the output variable Y. This is done in an effort to establish a new record.

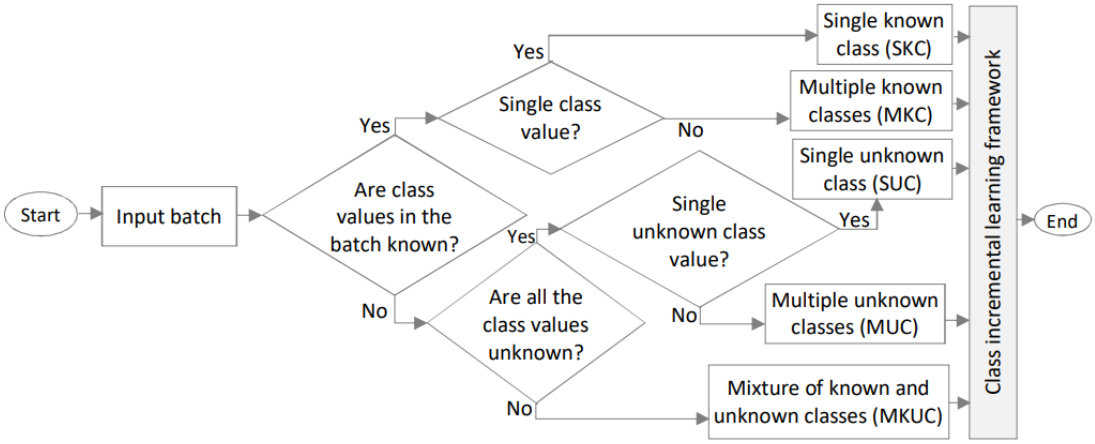
The Support Vector Machine is the name of the algorithm that is being discussed here. In the realm of machine learning, the Support Vector Machine (SVM) is a technique that is supervised and has the capability to solve classification and regression issues. In order to solve tough problems, the algorithm is frequently utilised in academic research because of its high rate of effectiveness. A hyperplane that effectively divides the data into a number of different categories is the fundamental goal of Support Vector Machines (SVM), which are a type of machine learning technique. The hyperplane is selected in order to get the best possible margin, which is defined as the greatest distance that exists between the hyperplane and the points that are closest to each class. In order to explain the reasoning behind the name of the procedure, the data points that are located in the closest proximity to the hyperplane are referred to as support vectors.

In order to perform its functions, the Support Vector Machine (SVM) algorithm makes use of a kernel function to convert the input into a space that has a greater number of dimensions. Because of this, the algorithm is able to choose a hyperplane that is capable of successfully separating the data in a manner that is devoid of linearity. The linear, polynomial, and radial basis function (RBF) kernel functions are the ones that are utilised most frequently.

In order to train the Support Vector Machine (SVM) model, the training procedure entails decreasing a loss function that imposes penalties for incorrect classifications while simultaneously raising the margin. In order to complete the method, you will need to find a solution to a quadratic optimisation problem, which might result in a significant amount of computer work when dealing with huge datasets. In spite of this, there are other optimisation strategies that can be implemented in order to enhance the speed of the process. Some examples of these strategies include sequential minimum optimisation and stochastic gradient descent.
After it has been trained, the support vector machine (SVM) model can be utilised to make predictions regarding the category of new data points by determining how close they are to the hyperplane. In the event that the distance is greater than a certain threshold, the data point is identified as belonging to one of the two categories; otherwise, it is classed as belonging to the other group.
The support vector machine (SVM) has been extensively utilised in the field of academic research for the purpose of resolving classification issues, such as the classification of images and texts, as well as regression tasks, such as the prediction of stock prices and property values. In order to improve the accuracy and efficiency of the model, support vector machines (SVM) have been used in conjunction with other methods, such as ensemble techniques and feature selection.
Support Vector Machines, often known as SVM, are a method that is both strong and versatile, making it an excellent choice for a variety of machine learning problems. The capacity of this method to properly examine both linear and nonlinear data, while also exhibiting extraordinary precision and adaptability, is the primary reason for its popularity among academics and professionals.

RESULTS & DISCUSSION

The purpose of this research study is to provide a novel web application that makes use of machine learning algorithms to forecast the acceptance of loans and identify fraudulent transactions that are performed using credit cards. The user provides the system with input data, which is then evaluated by the system in order to determine the status of the loan approval and identify any possible instances of fraud. A training dataset with 615 rows was used to evaluate the system, and the results showed that it had an accuracy rate of 92% when it came to predicting whether or not a loan would be approved. An evaluation of the system was carried out with the use of a training dataset that had thirty thousand customers. According to the findings of the test, the accuracy rate for identifying fraudulent credit card activity was 94%.



The diagram in Fig.2 represents a decision-making flowchart for classifying input batches in an AI-enhanced detection and mitigation framework for cybersecurity threats in digital banking. The framework is designed to handle different types of class values in the input data, which can be known or unknown. Here's a step-by-step explanation of the diagram:
1. Start: The process begins.
2. Input Batch: The system receives an input batch of data that needs to be classified.
3. Are class values in the batch known?
- Yes: If the class values in the batch are known, proceed to the next decision point.
- No: If the class values are not known, proceed to the decision point about unknown class values.
4. Single class value?
- Yes: If there is a single class value in the batch, it is classified as a Single Known Class (SKC).
- No: If there are multiple class values, proceed to the next decision point.
5. Single unknown class value?
- Yes: If there is a single unknown class value, it is classified as a Single Unknown Class (SUC).
- No: If there are multiple unknown class values, proceed to the next decision point.
6. Are all the class values unknown?
- Yes: If all the class values are unknown, it is classified as Multiple Unknown Classes (MUC).

- No: If there is a mixture of known and unknown class values, it is classified as Mixture of Known and Unknown Classes (MKUC).
7. Multiple known classes (MKC): If there are multiple known class values, it is classified as Multiple Known Classes (MKC).
8. Class Incremental Learning Framework: All classified batches (SKC, MKC, SUC, MUC, MKUC) are then processed by the Class Incremental Learning Framework, which is designed to handle and learn from these different types of class values incrementally.
9. End: The process concludes.
This flowchart helps in systematically categorizing the input data based on the known and unknown class values, which is crucial for the AI system to effectively detect and mitigate cybersecurity threats in digital banking operations.

To further elaborate on how this proposed framework for Autonomic digital banking operations with AI-Enhanced Detection and Mitigation of Cybersecurity Threats can be utilized in cybersecurity threat mitigation, the practical application of the decision-making flowchart is described as:
1. Input Data Classification: The framework's ability to classify input data into different categories (Single Known Class, Multiple Known Classes, Single Unknown Class, Multiple Unknown Classes, Mixture of Known and Unknown Classes) is crucial for understanding the nature of the cybersecurity threats present in the digital banking environment.
2. Adaptive Learning: By utilizing the Class Incremental Learning Framework, the system can continuously adapt and learn from the classified data batches. This adaptive learning approach enables the AI system to enhance its threat detection capabilities over time by incorporating new information and patterns.
3. Threat Detection: The framework can leverage the classified data to identify potential cybersecurity threats within the digital banking operations. By analyzing patterns and anomalies in the data, the system can proactively detect suspicious activities such as unauthorized access attempts, malware infections, or fraudulent transactions.
4. Threat Mitigation: Once a cybersecurity threat is detected, the framework can initiate mitigation strategies based on the type of threat identified. This may involve isolating affected systems, blocking malicious activities, alerting security teams, or implementing automated responses to prevent further damage.
5. Real-time Monitoring: The framework can be integrated into the digital banking infrastructure to provide real-time monitoring of security events and activities. By continuously analyzing incoming data and classifying potential threats, the system can respond promptly to emerging cybersecurity incidents.
6. Enhanced Security Posture: Through the intelligent classification and analysis of data batches, the framework contributes to strengthening the overall security posture of digital banking operations. By leveraging AI-enhanced detection capabilities, organizations can better protect sensitive customer information, financial transactions, and digital assets from cyber threats.

In summary, the proposed framework for Autonomic digital banking operations with AI-Enhanced Detection and Mitigation of Cybersecurity Threats offers a structured approach to classifying data, enabling adaptive learning, enhancing threat detection, implementing effective mitigation strategies, enabling real-time monitoring, and ultimately bolstering the security defenses of digital banking systems against evolving cyber threats.

CONCLUSION

The rapid digital transformation of the banking sector has brought unparalleled convenience and efficiency to financial services, but it has also introduced significant cybersecurity challenges. This research presents an innovative approach to enhancing digital banking security through the integration of AI and machine learning techniques. By developing web applications that utilize machine learning models for loan acceptance prediction and credit card fraud detection, we have demonstrated the potential of AI to improve decision-making processes and enhance security measures in digital banking.
The use of the Random Forest algorithm in loan prediction achieved a precision rate of 92%, indicating a robust capability to forecast loan approvals accurately. Similarly, the Support Vector Machine (SVM) algorithm for fraud detection achieved a 90% accuracy rate, showcasing its effectiveness in identifying fraudulent transactions. These results underscore the viability of machine learning algorithms in addressing key operational challenges in digital banking.
Our proposed AI-enhanced detection and mitigation framework for cybersecurity threats leverages the classification and adaptive learning capabilities of machine learning models to provide real-time, contextual threat detection and response. By systematically classifying input data and continuously learning from new data, the framework enhances the resilience of digital banking systems against evolving cyber threats.
The implementation of advanced AI techniques, such as Random Forest and SVM, in our web applications has proven to be effective in improving the accuracy and efficiency of loan approval processes and fraud detection mechanisms. Furthermore, the framework's adaptive learning approach ensures that the system remains robust against new and emerging threats, thereby safeguarding digital banking operations.

In conclusion, the integration of AI and machine learning into digital banking security offers a promising path forward for financial institutions. By adopting these advanced technologies, banks can enhance their operational efficiency, improve customer trust, and ensure the security of financial transactions. Future research should focus on refining these models, exploring new machine learning techniques, and addressing the challenges associated with AI implementation to further strengthen digital banking security.

REFERENCES

1. E. Indriasari, H. Prabowo, F. Gaol, and B. Purwandari, "Digital Banking: Challenges, Emerging Technology Trends, and Future Research Agenda," *Int. J. E Bus. Res.*, vol. 18, pp. 1-20, 2022, doi: 10.4018/ijebr.309398.
2. B. Balkan, "Impacts of Digitalization on Banks and Banking," in *Digital Transformation in Industry*, pp. 33-50, 2021, doi: 10.1007/978-981-33-6811-8_3.
3. V. Sardana and S. Singhania, "Digital technology in the realm of banking: A review of literature," *International Journal of Research in Finance and Management*, 2018, doi: 10.33545/26175754.2018.v1.i2a.12.
4. C. Shah and D. Naikwadi, "Trends and Encounters of Digital Banking in India," *International Journal of Advanced Research in Science, Communication and Technology*, 2023, doi: 10.48175/ijarsct-12990.
5. I. Journal, "IMPACT OF DIGITAL WORLD ON BANKING," *INTERANTIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT*, 2022, doi: 10.55041/ijsrem14266.
6. N. Kholiavko and O. Kozlianchenko, "Global Trends in the Banking Sector Digitalization," *THE PROBLEMS OF ECONOMY*, 2021, doi: 10.32983/2222-0712-2021-2-217-224.
7. M. Tashtamirov, "Financial Innovation and Digital Technology in the Banking System: An Institutional Perspective," *SHS Web of Conferences*, 2023, doi: 10.1051/shsconf/202317202004.
8. L. Wewege, J. Lee, and M. Thomsett, "Disruptions and Digital Banking Trends," *Journal of Applied Finance and Banking*, vol. 10, pp. 1-2, 2020.
9. R. Sebti, "BANKING IN THE DIGITAL AGE: ISSUES AND CHALLENGES," *RIMAK International Journal of Humanities and Social Sciences*, 2022, doi: 10.47832/2717-8293.18.12.
10. D. Broby, "Financial technology and the future of banking," *Financial Innovation*, vol. 7, pp. 1-19, 2021, doi: 10.1186/s40854-021-00264-y.
11. E. Indriasari, H. Prabowo, F. Gaol, and B. Purwandari, "Digital Banking," *International Journal of E-business Research*, 2022, doi: 10.4018/ijebr.309398.
12. S. Pranay, D. Adarsh, S. Shandilya, and P. Deshmukh, "Digital Banking in India- Prospects and Constraints," *International Journal of Advanced Research in Science, Communication and Technology*, 2022, doi: 10.48175/ijarsct-7819.
13. "Growth in use of digital banking in India," 2022, doi: 10.58260/j.mas.2202.0102.
14. "Acceleration of Digital Banking in India," *International Journal For Multidisciplinary Research*, 2023, doi: 10.36948/ijfmr.2023.v05i02.2307.
15. N. Todua and N. Gogitidze, "Features of the use of digital marketing in the banking sector," *Axali Ekonomisti*, 2022, doi: 10.36962/nec62-6303-042021-07.
16. R. Singhal, "Impact and importance of digital payment in India," *Social Science Research Network*, 2021, doi: 10.2139/SSRN.3947792.
17. J. Bishop and L. Turova, "The role of modern digital technologies in the functioning of the banking system," 2021, doi: 10.32782/2524-0072/2021-25-21.
18. P. Bijendra and A. Gupta, "Impact of E-Banking Its Growth and Future in India," *Social Science Research Network*, 2019, doi: 10.2139/SSRN.3308577.
19. A. Jaganathan, "Digitization in banking in India," 2020.
20. S. Rose and T. G.S., "A study on digital banking in India," 2019.
21. O. Gulyas and G. Kiss, "Cybersecurity threats in the banking sector," in *2022 8th International Conference on Control, Decision and Information Technologies (CoDIT)*, vol. 1, pp. 1070-1075, 2022, doi: 10.1109/CoDIT55151.2022.9804140.
22. W. Haruna, T. Aremu, and Y. Modupe, "Defending against cybersecurity threats to the payments and banking system," *ArXiv*, abs/2212.12307, 2022, doi: 10.48550/arXiv.2212.12307.
23. N. Tn and M. Kulkarni, "Zero click attacks – a new cyber threat for the e-banking sector," *Journal of Financial Crime*, 2022, doi: 10.1108/jfc-06-2022-0140.
24. A. Darem, A. Alhashmi, T. Alkhaldi, A. Alashjaee, S. Alanazi, and S. Ebad, "Cyber Threats Classifications and Countermeasures in Banking and Financial Sector," *IEEE Access*, vol. 11, pp. 125138-125158, 2023, doi: 10.1109/ACCESS.2023.3327016.
25. G. Lakshmi, S. Ovia, and A. Sre, "THE IMPACT OF CYBER CRIME AND SECURITY IN ONLINE BANKING TRANSACTION," *INTERNATIONAL JOURNAL OF MANAGEMENT AND SOCIAL SCIENCES*, vol. 8, pp. 28-31, 2018.
26. "Cybersecurity threats in the banking sector," 2022, doi: 10.1109/codit55151.2022.9804140.
27. O. Gulyas and G. P. Kiss, "Cybersecurity threats in the banking sector," 2022, doi:

10.1109/CoDIT55151.2022.9804140.
28. S. Mishra, "Exploring the Impact of AI-Based Cyber Security Financial Sector Management," *Applied Sciences*, 2023, doi: 10.3390/app13105875.
29. C. Sekhar and R. Kumar, "An Overview of Cyber Security in Digital Banking Sector," *East Asian Journal of Multidisciplinary Research*, 2023, doi: 10.55927/eajmr.v2i1.1671.
30. "Mounting Cases of Cyber-Attacks and Digital Payment," *Advances in information security, privacy, and ethics book series*, 2022, doi: 10.4018/978-1-6684-5827-3.ch005.
31. B. Jae Kwon and H. Gwang, "A Study on Digital Financial Security Threats and Cybersecurity Policies," *Global Management Journal*, 2023, doi: 10.38115/asgba.2023.20.6.133.
32. M. H. Alzoubi, T. M. Ghazal, M. Z. Hasan, A. AlKetbi, R. Kamran, N. A. Al-Dmour, and S. Islam, "Cyber Security Threats on Digital Banking," 2022, doi: 10.1109/ICAIC53980.2022.9896966.
33. S. Zeadally, E. Adi, Z. Baig, and I. Khan, "Harnessing Artificial Intelligence Capabilities to Improve Cybersecurity," *IEEE Access*, vol. 8, pp. 23817-23837, 2020, doi: 10.1109/ACCESS.2020.2968045.
34. M. Taddeo, T. McCutcheon, and L. Floridi, "Trusting artificial intelligence in cybersecurity is a double-edged sword," *Nature Machine Intelligence*, pp. 1-4, 2019, doi: 10.1038/s42256-019-0109-1.
35. X. Cao, "The application of artificial intelligence in internet security," *Applied and Computational Engineering*, 2023, doi: 10.54254/2755-2721/18/20230995.
36. N. Mohamed, A. Oubelaid, and S. Almazrouei, "Staying Ahead of Threats: A Review of AI and Cyber Security in Power Generation and Distribution," *International Journal of Electrical and Electronics Research*, 2023, doi: 10.37391/ijeer.110120.
37. M. Akhtar and T. Feng, "An overview of the applications of Artificial Intelligence in Cybersecurity," *EAI Endorsed Trans. Creative Technol.*, vol. 8, p. e4, 2021, doi: 10.4108/eai.23-11-2021.172218.
38. M. Vasupalli, "Utilizing Artificial Intelligence for Enhancing Cyber Security: Applications and Methodologies," *International Journal on Recent and Innovation Trends in Computing and Communication*, 2023, doi: 10.17762/ijritcc.v11i9.9346.
39. M. Thisarani and S. Fernando, "Artificial Intelligence for Futuristic Banking," in *2021 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC)*, pp. 1-13, 2021, doi: 10.1109/ice/itmc52061.2021.9570253.
40. H. Khan, M. Malik, S. Nazir, and F. Khan, "Utilizing Bio Metric System for Enhancing Cyber Security in Banking Sector: A Systematic Analysis," *IEEE Access*, vol. 11, pp. 80181-80198, 2023, doi: 10.1109/ACCESS.2023.3298824.
41. A. Popova, "CYBERSECURITY OF THE BANKING SYSTEM AND ETHICAL RULES OF THE INTERACTION BETWEEN A MAN AND ARTIFICIAL INTELLIGENCE: ON THE NEED FOR CO-EXISTENCE," 2021, vol. 1, pp. 47-62, doi: 10.18572/1812-3945-2021-1-47-62.
42. M. Taddeo, T. McCutcheon, and L. Floridi, "Trusting artificial intelligence in cybersecurity is a double-edged sword," *Nature Machine Intelligence*, pp. 1-4, 2019, doi: 10.1038/s42256-019-0109-1.
43. M. Zahiroh, "Cybersecurity Awareness and Digital Skills on Readiness For Change in Digital Banking," *Li Falah: Jurnal Studi Ekonomi dan Bisnis Islam*, 2020, doi: 10.31332/lifalah.v5i2.2271.
44. N. Thach, H. Hanh, D. Huy, S. Gwoździewicz, L. Nga, L. Huong, and V. Nam, "TECHNOLOGY QUALITY MANAGEMENT OF THE INDUSTRY 4.0 AND CYBERSECURITY RISK MANAGEMENT ON CURRENT BANKING ACTIVITIES IN EMERGING MARKETS - THE CASE IN VIETNAM," *International Journal for Quality Research*, 2021, doi: 10.24874/ijqr15.03-10.
45. S. Zeadally, E. Adi, Z. Baig, and I. Khan, "Harnessing Artificial Intelligence Capabilities to Improve Cybersecurity," *IEEE Access*, vol. 8, pp. 23817-23837, 2020, doi: 10.1109/ACCESS.2020.2968045.
46. U. U. Ibekwe, M. N. Mbanaso, and A. N. Nnanna, "A Critical Review of The Intersection of Artificial Intelligence and Cybersecurity," 2023, doi: 10.1109/icmeas58693.2023.10379362.
47. "A Comprehensive Study on Review of AI Techniques to Provide Security in the Digital World," 2022, doi: 10.1109/icicict54557.2022.9917931.
48. "Analysing Cyber Threats: A Comprehensive Literature Review on Data-Driven Approaches," *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 2023, doi: 10.32628/cseit2390351.
49. "Explainable Artificial Intelligence and Cybersecurity: A Systematic Literature Review," 2023, doi: 10.48550/arxiv.2303.01259.
50. C. Mendes and T. Nogueira Rios, "Explainable Artificial Intelligence and Cybersecurity: A Systematic Literature Review," *arXiv.org*, 2023, doi: 10.48550/arXiv.2303.01259.
51. F. Charmet, H. C. Tanuwidjaja, S. Ayoubi, P.-F. Gimenez, Y. Han, H. Jmila, G. Blanc, T. Takahashi, and Z. Zhang, "Explainable artificial intelligence for cybersecurity: a literature survey," *Annales Des Télécommunications*, 2022, doi: 10.1007/s12243-022-00926-7.
52. E. R. Ndukwe and B. B. Baridam, "A Graphical and Qualitative Review of Literature on AI-based Cyber-Threat Intelligence (CTI) in Banking Sector," 2023, doi: 10.24018/ejeng.2023.8.5.3103.
53. I. Tabassum, S. U. Bazai, Z. Zaland, I. M. Shah, M. Z. Khan, and M. I. Ghafoor, "Cyber Security's Silver Bullet - A Systematic Literature Review of AI-Powered Security," 2022, doi: 10.1109/IISEC56263.2022.9998305.
54. "Cyber Security's Silver Bullet - A Systematic Literature Review of AI-Powered Security," 2022, doi:

10.1109/iisec56263.2022.9998305.
55. P. Dzhaparov, "Cyber risks – the big challenge facing banks," *Ikonomika i Kompût"rni Nauki*, vol. 6, pp. 6-18, 2020.
56. O. Gulyas and G. Kiss, "Cybersecurity threats in the banking sector," in *2022 8th International Conference on Control, Decision and Information Technologies (CoDIT)*, vol. 1, pp. 1070-1075, 2022, doi: 10.1109/CoDIT55151.2022.9804140.
57. A. Darem, A. Alhashmi, T. Alkhaldi, A. Alashjaee, S. Alanazi, and S. Ebad, "Cyber Threats Classifications and Countermeasures in Banking and Financial Sector," *IEEE Access*, vol. 11, pp. 125138-125158, 2023, doi: 10.1109/ACCESS.2023.3327016.
58. M. Uddin, M. Ali, and M. Hassan, "Cybersecurity hazards and financial system vulnerability: a synthesis of literature," *Risk Management*, vol. 22, pp. 239-309, 2020, doi: 10.1057/s41283-020-00063-2.
59. I. Yildirim, "Cyber Risk Management in Banks," *Global Cyber Security Labor Shortage and International Business Risk*, 2019, doi: 10.4018/978-1-5225-5927-6.CH003.
60. J. I. Janjua, A. Sabir, T. Abbas, S. Q. Abbas, and M. Saleem, "Predictive Analytics and Machine Learning for Electricity Consumption Resilience in Wholesale Power Markets," in *2024 2nd International Conference on Cyber Resilience (ICCR)*, Dubai, United Arab Emirates, 2024, pp. 1-7, doi: 10.1109/ICCR61006.2024.10533004.
61. W. Alomoush, T. A. Khan, M. Nadeem, J. I. Janjua, A. Saeed and A. Athar, "Residential Power Load Prediction in Smart Cities using Machine Learning Approaches," *2022 International Conference on Business Analytics for Technology and Security (ICBATS)*, Dubai, United Arab Emirates, 2022, pp. 1-8, doi: 10.1109/ICBATS54253.2022.9759024.
62. K. Najaf, I. Mostafiz, and R. Najaf, "Fintech firms and banks sustainability: Why cybersecurity risk matters?" 2021, doi: 10.1142/S2424786321500195.