The Role Artificial Intelligence in Modern Banking: An Exploration of AI-Driven Approaches for Enhanced Fraud Prevention, Risk Management, and Regulatory Compliance

Layla Abdel-Rahman Aziz
Department of Economics and Finance, Aswan Institute of Technology
Yuli Andriansyah
Universitas Islam Indonesia; Department of Islamic Economics
https://orcid.org/0000-0003-3394-5222

Abstract

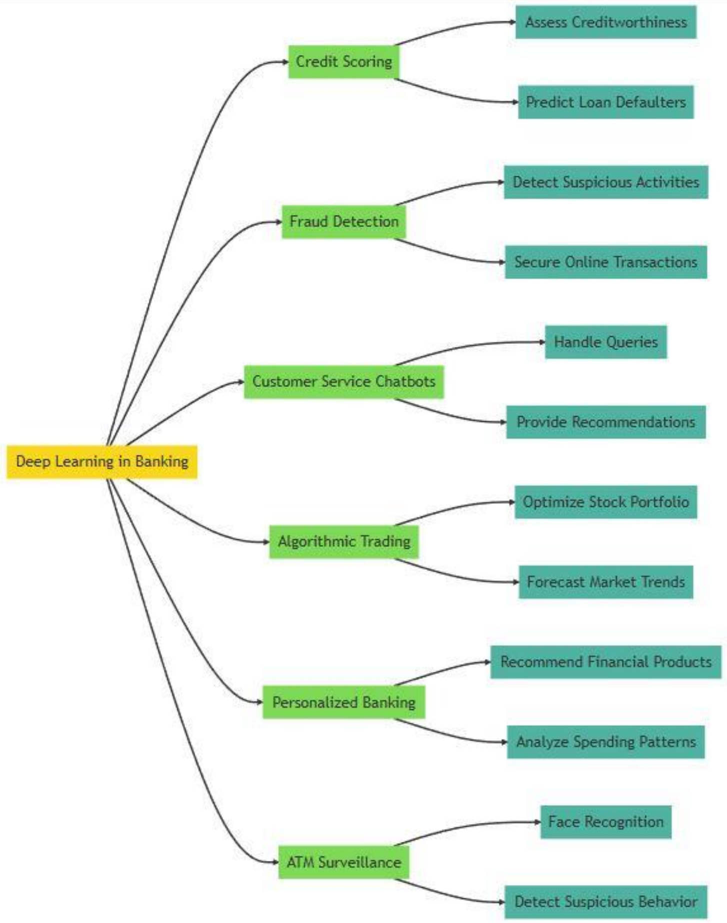
Banking fraud prevention and risk management are paramount in the modern financial landscape, and the integration of Artificial Intelligence (AI) offers a promising avenue for advancements in these areas. This research delves into the multifaceted applications of AI in detecting, preventing, and managing fraudulent activities within the banking sector. Traditional fraud detection systems, predominantly rule-based, often fall short in real-time detection capabilities. In contrast, AI can swiftly analyze extensive transactional data, pinpointing anomalies and potentially fraudulent activities as they transpire. One of the standout methodologies includes the use of deep learning, particularly neural networks, which, when trained on historical fraud data, can discern intricate patterns and predict fraudulent transactions with remarkable precision. Furthermore, the enhancement of Know Your Customer (KYC) processes is achievable through Natural Language Processing (NLP), where AI scrutinizes textual data from various sources, ensuring customer authenticity. Graph analytics offers a unique perspective by visualizing transactional relationships, potentially highlighting suspicious activities such as rapid fund transfers indicative of money laundering. Predictive analytics, transcending traditional credit scoring methods, incorporates a diverse data set, offering a more comprehensive insight into a customer's creditworthiness. The research also underscores the importance of user-friendly interfaces like AI-powered chatbots for immediate reporting of suspicious activities and the integration of advanced biometric verifications, including facial and voice recognition. Geospatial analysis and behavioral biometrics further bolster security by analyzing transaction locations and user interaction patterns, respectively. A significant advantage of AI lies in its adaptability. Self-learning systems ensure that as fraudulent tactics evolve, the AI mechanisms remain updated, maintaining their efficacy. This adaptability extends to phishing detection, IoT integration, and cross-channel analysis, providing a comprehensive defense against multifaceted fraudulent attempts. Moreover, AI's capability to simulate economic scenarios aids in proactive risk management, while its ability to ensure regulatory compliance automates and streamlines a traditionally cumbersome process.

Keywords: *Artificial Intelligence, Fraud Prevention, Risk Management, Banking Innovations, Regulatory Compliance*

Introduction

The modern banking system, a cornerstone of global economies, is a complex web of institutions, instruments, and processes that facilitate the movement and storage of money. Historically, banks began as places where individuals could safely store their wealth, usually in the form of gold or silver. Over time, these institutions evolved, offering loans to businesses and consumers, thereby playing a pivotal role in the expansion of trade and the growth of economies.

Figure 1. Deep learning in modern banking and finance



Today, the definition of a bank has expanded beyond brick-and-mortar establishments to include digital and online platforms, reflecting the rapid technological advancements and changing consumer preferences [1], [2].

At the heart of the banking system are several core components. Firstly, there are the central banks, which are typically state-owned entities responsible for issuing the national currency, setting monetary policy, and overseeing the stability of the financial system. Commercial banks, on the other hand, are what most people commonly interact with. They offer a wide range of services, from accepting deposits to providing loans. Investment banks focus on assisting companies in raising capital, mergers and acquisitions, and other complex financial transactions. Additionally, there are specialized banks, like savings banks and credit unions, which cater to specific needs or communities [3]–[5].

The advent of technology has dramatically reshaped the banking landscape. Digital banking, a subset of the broader financial technology (FinTech) movement, refers to the use of electronic platforms to conduct banking activities. This can range from online banking websites to mobile apps. These digital platforms allow consumers to perform a myriad of tasks, from checking account balances to transferring funds internationally, all at their fingertips. Moreover, the rise of blockchain technology and cryptocurrencies has introduced a new dimension to the banking world, challenging traditional notions of currency and transaction processing [6]–[8].

Given the critical role banks play in the economy, a robust regulatory framework is essential to ensure their stability and integrity. Regulatory bodies, often at the national level, set guidelines and standards that banks must adhere to. These regulations cover a wide spectrum of areas, from capital adequacy requirements to consumer protection measures. Compliance with these regulations is paramount, not only to ensure the smooth functioning of the banking system but also to instill confidence among the public. In the wake of financial crises, these regulations are often revisited and revised to address systemic vulnerabilities [9].

While the modern banking system has brought about numerous benefits, it is not without its challenges. Cybersecurity threats loom large as digital transactions become the norm. The traditional banking model is also under threat from disruptive FinTech startups that offer niche services at a fraction of the cost. Moreover, as global economies become more interconnected, the banking system must grapple with geopolitical uncertainties and cross-border regulatory complexities. However, with challenges come opportunities. The future of banking lies in its ability to adapt, innovate, and cater to the ever-evolving needs of consumers and businesses alike [10].

In the intricate world of banking, fraud prevention and risk management are paramount to maintaining the integrity and trustworthiness of financial institutions. Banking fraud encompasses a wide range of malicious activities, from identity theft to sophisticated cyber-attacks. As the banking sector evolves, especially with the rise of digital banking, the methods employed by fraudsters become increasingly sophisticated. Consequently, risk management strategies have had to adapt and innovate to counter these threats, ensuring that both the bank's assets and its customers' funds are protected [11].

Fraud prevention in banking is a multi-faceted endeavor. It begins with robust authentication processes, ensuring that only legitimate account holders can access their funds. This often involves multi-factor authentication, combining something the user knows (like a password), something the user has (like a physical token or a phone), and something the user is (biometrics like fingerprints or facial recognition). Additionally, continuous transaction monitoring is crucial. Advanced algorithms and artificial intelligence can detect unusual transaction patterns, flagging them for review. Employee training is also vital, as human error or oversight can often be a weak link in the security chain [12]–[15]. Risk management in banking goes beyond just fraud prevention. It encompasses a broader strategy to identify, assess, and prioritize risks. Once these risks are identified, appropriate measures are taken to mitigate them. This might involve diversifying investments, setting limits on loan exposures, or hedging against potential losses. Regular audits, both internal and external, play a crucial role in risk management, ensuring that all processes are up to standard and that any potential vulnerabilities are addressed promptly. Furthermore, contingency planning ensures that, should a risk materialize, the bank has a clear plan of action to minimize damage [16]–[19].

Given the potential systemic implications of banking failures, regulatory bodies worldwide have established stringent guidelines for risk management. These regulations ensure that banks maintain adequate capital reserves, follow best practices in their operations, and remain transparent in their dealings. Basel III, for instance, is a global regulatory standard on bank capital adequacy, stress testing, and market liquidity risk. Adherence to such standards is not just about compliance; it's about ensuring the stability of the global financial system. Banks that fail to comply face hefty penalties, reputational damage, and, in extreme cases, the risk of license revocation [20]–[23].

As technology continues to advance, the tools and strategies used in fraud prevention and risk management will need to evolve. The integration of machine learning and AI in transaction monitoring can lead to quicker detection of fraudulent activities [24]. Blockchain technology, with its emphasis on transparency and security, might also play a role in future risk management strategies. However, with every technological advancement, new vulnerabilities may emerge. The challenge for banks will be to stay one step ahead, continuously innovating, and adapting to ensure the safety and security of their operations and their customers' assets.

Figure 1. Modern Banking and Traditional Banking

Criteria	Traditional Banking	Modern Banking
Mode of Operation	Primarily brick-and-mortar branches.	Digital platforms, online, mobile apps.

Accessibility	Limited to branch timings.	24/7 access through online platforms.
Services	Basic banking services.	Wide range of services including digital wallets, P2P transfers, etc.
Customer Interaction	Face-to-face interactions.	Chatbots, emails, online support.
Transaction Speed	Can be slower due to manual processes.	Instant or near-instant.
Geographical Reach	Limited to branch locations.	Global access through the internet.
Documentation	Paper-based.	Electronic and digital documentation.
Security	Physical vaults, guards.	Encryption, multi-factor authentication, biometrics.
Flexibility	Fixed processes and offerings.	Customizable user experiences, dynamic product offerings [25].
Cost Efficiency	Higher overhead due to physical infrastructure.	Lower overhead, often leading to fewer fees for customers.
Innovation	Slower to adopt new technologies.	Rapid adoption of fintech solutions.
Customer Experience	Standardized experience.	Personalized based on user behavior and preferences.
Environmental Impact	Paper-intensive, physical infrastructure.	Reduced paper use, digital operations.

Modern banking and traditional banking represent two distinct approaches to financial services, each shaped by the evolution of technology and customer expectations. Traditional banking relies on brick-and-mortar branches as its primary mode of operation. Customers must adhere to branch timings, limiting their accessibility to physical locations. In contrast, modern banking operates through digital platforms and mobile apps, offering customers the convenience of 24/7 access to their financial accounts and services. This shift in accessibility has transformed the way people interact with their finances, allowing them to manage transactions and accounts on their own schedules [26]–[29].

Services offered by traditional banks were once limited to basic banking functions, in post pandemic era [30]–[32]. These institutions focused on account management, loans, and standard transactions. On the other hand, modern banking has revolutionized the financial landscape by expanding its services to encompass a wide array of options. These offerings include digital wallets, peer-to-peer (P2P) transfers, investment platforms, and more [33]–[35]. This increased diversity of services empowers customers with greater control over their financial activities and investments, catering to a diverse range of needs and preferences [36]–[39].

The customer interaction experience has also undergone a significant transformation. Traditional banking relied heavily on face-to-face interactions, with customers visiting physical branches for inquiries or transactions. Modern banking, however, has integrated technological advancements such as chatbots, emails, and online support to facilitate customer interactions. These digital channels enable real-time assistance, streamlined query resolution, and immediate access to information, reducing the need for customers to physically visit a branch [29], [40], [41].

The speed of transactions is another key differentiator between the two banking models. Traditional banking processes were often hindered by manual procedures, leading to slower transaction speeds. In contrast, modern banking leverages automation, real-time processing, and instant transfer methods to ensure transactions are executed swiftly or even instantaneously. This acceleration in transaction speed has contributed to the efficiency and effectiveness of financial operations for customers. Furthermore, modern banking's geographical reach far surpasses that of traditional banking. While traditional banks were confined to their physical branch locations, modern banking harnesses the power of the internet to offer global access to financial services. Customers can perform transactions, manage accounts, and access information from anywhere in the world, bridging geographical boundaries and facilitating international financial activities.

In terms of security, traditional banking relied on physical vaults and guards to protect physical assets. In modern banking, security measures have shifted towards encryption, multi-factor authentication, and biometric technologies to safeguard digital assets and information [42]–[44]. These advanced security protocols provide customers with enhanced protection against cyber threats and unauthorized access, contributing to a higher level of trust in digital financial operations.

The innovation pace between traditional and modern banking models also stands in stark contrast. Traditional banking was often hesitant to adopt new technologies, leading to slower advancements in the sector [45]. In contrast, modern banking has embraced fintech solutions and rapidly incorporated technological innovations to improve services, enhance customer experiences, and adapt to changing market dynamics [46].

Ultimately, the customer experience has been profoundly impacted by the shift from traditional to modern banking. Traditional banking offered a standardized experience with limited customization. Modern banking, however, prioritizes personalization based on user behavior and preferences. This tailored approach enhances customer satisfaction, engagement, and loyalty by catering to individual financial goals and needs [47]–[49]. Finally, the environmental impact of these banking models is noteworthy. Traditional banking, with its paper-intensive processes and physical infrastructure, contributed to a significant environmental footprint. In contrast, modern banking has adopted digital operations, reduced paper usage and minimizing the environmental impact associated with physical infrastructure [50]–[53].

AI-Driven Approaches for Enhanced Fraud Prevention, Risk Management, and Regulatory Compliance

Traditional fraud detection systems predominantly rely on rule-based methods, where a set of predefined rules are established to identify suspicious transactions. For instance, if a transaction exceeds a certain limit or occurs from an unfamiliar geographic location, it's flagged for further investigation. However, these methods often lag in accuracy and speed, given the dynamic nature of fraud tactics. With the advent of Artificial Intelligence (AI), the landscape of fraud detection is witnessing a paradigm shift. AI can seamlessly process and analyze vast volumes of transaction data in real-time, spotlighting any anomalies or unexpected patterns that could indicate fraudulent activity. Unlike traditional systems, which rely on static rules, AI continually adapts to evolving fraud tactics by learning from new data, making it significantly more efficient in pinpointing and preventing fraud as it unfolds.

At the heart of many AI solutions lies deep learning—a subset of machine learning that utilizes neural networks to model and process complex datasets. Deep learning shines in its ability to recognize intricate patterns that might be imperceptible to other algorithms or the human eye [31], [54]–[56]. In the context of fraud detection, neural networks can be trained on vast repositories of historical fraud data. As the model trains, it begins to understand the nuances and subtleties associated with potentially fraudulent transactions. The beauty of deep learning is its ability to discern patterns even in noisy datasets and differentiate between legitimate and suspicious activities. Consequently, when such a model is presented with a new transaction, it can evaluate its characteristics in comparison to learned patterns and predict with high accuracy if the transaction is potentially fraudulent [44], [57], [58].

Deep learning is a subset of machine learning that employs neural networks with many layers, typically referred to as deep neural networks. The basic unit of these networks is the neuron, which is inspired by the biological neurons found in the human brain. Each neuron in a neural network receives input [59]–[61], processes it, and sends output to the subsequent layer [62]. These neurons are interconnected, and as data traverses through the layers, each neuron learns to transform the data in a manner that the final output layer can make an accurate prediction or classification [63]–[65]. The depth of these networks, which often consists of hundreds or thousands of layers, allows them to model and comprehend intricate patterns in the data. This is achieved through a process called backpropagation, where the model's prediction is compared to the actual output, and the error is propagated backwards to adjust the weights and biases of the neurons. This iterative learning process enables the deep learning model to refine its understanding of the data and its predictions over time [61], [66], [67].

The strength of deep learning lies in its ability to automatically learn representations from raw data without much manual feature engineering. For fraud detection, this means that instead of just relying on manually predefined rules or set indicators, the model can sift through vast amounts of raw data to discover potentially suspicious patterns by itself [68]–[70]. Features or patterns that might appear benign or inconspicuous in isolation can, in combination, indicate fraudulent activity. For instance, a series of transactions that individually seem legitimate could, when seen as a sequence, suggest a fraud pattern. By learning from the data, deep learning models can uncover these complex interdependencies. They're especially adept at identifying non-linear relationships, which are often the hallmarks of sophisticated fraud schemes [71].

Furthermore, deep learning models are adaptive and scalable. As new data flows in, the model can adjust and refine its understanding, making it adept at catching new and evolving types of fraud. This adaptability is crucial in the ever-evolving landscape of cyber threats and fraudulent tactics. Traditional rule-based systems, as effective as they may be for known patterns, may not adapt quickly to novel threats. In contrast, a well-designed and regularly trained deep learning model can recognize and respond to such novel patterns faster. It's this combination of depth, adaptability, and the ability to understand vast amounts of varied data that makes deep learning a formidable tool in the fight against fraud [72].

The Know Your Customer (KYC) procedure is a cornerstone in the banking and financial sectors, ensuring that institutions know the true identities and intents of their customers, thereby preventing money laundering or other illicit activities. Traditionally, KYC processes involve manual verification of customer documents, a labor-intensive and time-consuming endeavor. Enter Natural Language Processing (NLP)—a branch of AI that deals with the interaction between computers and human language. NLP can be used to automate and enhance the KYC process by analyzing the textual information present in customer documents, digital communications, social media activity, and other digital traces. Beyond mere textual matching, NLP algorithms can understand context, sentiment, and even identify attempts at deception. By leveraging NLP, financial institutions can not only streamline their KYC processes but also achieve a higher degree of accuracy in verifying the authenticity of their customers [73]–[75].

In the realm of fraud detection, representing transactions in a visual form can provide unique insights that are not immediately evident in tabular or textual data [76]. Graph analytics harnesses this visualization power by mapping transactions onto a network or graph structure. In such a graph, nodes typically represent entities like individual accounts, while edges represent transactions or relationships between these accounts. AI-driven algorithms can then scour this graph for suspicious patterns [77]. For instance, if there's a rapid succession of funds moving between closely interconnected accounts, it might be indicative of money laundering schemes or layered transactions meant to obscure the original source of funds. Graph analytics, aided by AI, offers the advantage of spotting these anomalies in a holistic context, considering the entire network of transactions rather than isolated events, thus enhancing the accuracy and comprehensiveness of fraud detection [78].

Traditional credit scoring models have primarily focused on a narrow set of parameters such as past loan histories, current debts, and income levels. However, with the vast amount of data now available from diverse sources, AI's predictive analytics offers a more nuanced and comprehensive assessment of a borrower's creditworthiness. By analyzing non-traditional data points, like timely utility payments, online shopping behavior, or even social media activity, AI can glean insights into a person's financial habits, responsibility, and reliability [79] . This broader dataset provides a more holistic view of a potential borrower and helps in predicting the likelihood of them defaulting on a loan. Thus, financial institutions can make more informed lending decisions, possibly extending credit to deserving individuals who might have been overlooked by traditional scoring methods [80].

In an era where immediacy is prized, waiting in long phone queues or navigating cumbersome online interfaces to report suspicious financial activities can be discouraging for customers. AI-powered chatbots, integrated within banking platforms, offer an expedited and user-friendly solution. These chatbots are designed to intuitively understand customer queries, gather essential details about the suspicious activity, and then instantaneously trigger an internal investigation or alert relevant authorities. Not only does this speed up the reporting process, but the real-time nature of these interactions also means that potentially fraudulent activities can be halted or investigated more swiftly. Additionally, the data collected by these chatbots can be fed back into the system, further refining the AI's understanding of emerging fraud patterns and tactics [81].

The realm of biometric systems has long been seen as the future of secure authentication, but the integration of AI supercharges its efficacy. Facial recognition systems, for instance, can be enhanced to discern minute differences in facial structures, or even determine if a face presented is live or a photograph. Fingerprint scanners can be optimized to analyze the intricate whirls and ridges of a person's fingerprint at an unprecedented level of detail. Voice recognition systems, backed by AI, can detect not only the tonal quality of a person's voice but also their speech patterns, rhythm, and other subtle vocal attributes [82], [83]. These AI-augmented biometric verification systems significantly reduce the chances of false positives, ensuring that banking services remain accessible only to legitimate, authorized individuals, thereby bolstering security.

Every transaction, be it digital or physical, leaves a geographical imprint, and when AI dives into this geospatial data, powerful fraud prevention insights emerge [84]. AI algorithms can be trained to recognize and flag transactions emanating from regions historically linked with high levels of fraudulent activities. More intriguingly, by tracking the geographical patterns of card usage, AI can identify improbable scenarios. For instance, if a card registered in New York is used for a purchase and then, within a few hours, is swiped in Paris, AI would flag this due to the impossibility of such rapid travel. This geospatial analysis not only identifies traditional fraud but also sophisticated techniques like card cloning and digital theft.

Deep learning is rooted in the premise that algorithms can learn and make independent decisions by analyzing data. It's a multifaceted branch of machine learning that employs structures called neural networks, which mimic the human brain's functioning, to unearth patterns from vast datasets [85]–[87]. In the context of risk management, understanding patterns and making predictions is of utmost importance. While traditional risk management tools rely on statistical methods and historical data, they often fall short when it comes to capturing non-linear dependencies and sudden market shifts. Deep learning models, however, are adept at handling these complexities. Their capability to process enormous amounts of data and discern intricate patterns means they can forecast potential risks with much higher precision, especially when the past doesn't straightforwardly indicate the future [88].

RNNs and LSTMs, specifically, are designed to recognize sequences and remember patterns over long durations [89]–[91]. In financial sectors, where time-series data is abundant, this is a game-changer. For instance, while predicting loan defaults, LSTMs can evaluate a borrower's entire financial history, including their spending behaviors, past loan records, and more, to gauge the likelihood of a future default. Their 'memory' of past events helps in capturing temporal dependencies that might be overlooked by other models. Similarly, in forecasting stock market movements, these networks can process and learn from countless previous market conditions, corporate financial statements, and broader economic indicators, offering predictions that are both nuanced and robust.

But the real prowess of deep learning in risk management emerges when we consider its ability to fuse multiple types of data. In today's interconnected world, risks in the financial sector may be influenced by a plethora of factors, from geopolitical events to environmental changes. By leveraging deep learning, institutions can integrate diverse data streams [92], such as social media chatter, news articles, and even meteorological data or satellite images. For instance, a sudden spike in negative sentiments on social media platforms might indicate a looming stock market dip or vice versa [93]. By continuously analyzing and learning from such multifaceted data sources, deep learning models offer a more holistic and proactive approach to risk management, enabling businesses and financial institutions to be better prepared and more resilient against future uncertainties [94].

Beyond the physical attributes that make us unique, our interactions with digital devices also paint a distinctive picture. Behavioral biometrics is a cutting-edge domain where AI meticulously observes how a user interacts with their banking applications [95]–[98]. It factors in elements like typing speed, the pressure exerted on the screen, swipe patterns, the angle at which the device is held, and countless other metrics to develop a behavioral profile for the user. Over time, the AI gets finely attuned to the user's typical behavior on the app [99]. Consequently, any deviation from this established behavioral profile—say, a different typing rhythm or unusual swipe trajectory—can be instantly flagged as a potential security concern [100]–[102]. This provides an additional layer of security, one that continually evolves and adapts, ensuring that even if traditional security parameters are breached, anomalies in user behavior can trigger alerts and safeguards [103]–[106].

One of the foundational strengths of Artificial Intelligence, especially in its applications for security, lies in its capacity for self-learning. Traditional fraud detection methods operate on a fixed set of rules which, once established, remain static unless manually updated [107]. AI systems, in contrast, exhibit a dynamic approach. These self-learning models are designed to continuously absorb, process, and learn from new transactional data, refining their understanding of both legitimate and suspicious activities. As fraudsters evolve their techniques, shifting from one tactic to another, these AI systems adapt in tandem, recalibrating their detection mechanisms. The upshot is a perpetually updating defense mechanism that remains a step ahead, ensuring that banks and financial institutions are not caught off guard by novel or evolving fraudulent tactics [2], [3], [108]–[110].

Phishing remains one of the most prevalent cyber threats, where deceptive emails or websites lure unsuspecting users into providing confidential information. AI has emerged as a formidable countermeasure to this threat. By scanning the textual content, metadata, and other attributes of emails, AI algorithms can identify the telltale signs of phishing attempts, even those that closely mimic legitimate communications [7], [8], [111], [112]. Similarly, AI can analyze website structures, content, and domain details to flag potential phishing sites. These systems don't just rely on known phishing patterns but also employ heuristic analysis to detect new phishing techniques. Consequently, users can be alerted in real-time, preventing them from clicking on malicious links or inputting sensitive data, thereby significantly reducing the success rate of phishing attacks [82], [83], [113].

The Internet of Things (IoT) represents the next frontier in digital banking, with devices ranging from smartwatches to home assistants facilitating financial transactions. As the IoT ecosystem proliferates, so does the potential attack surface for fraudsters [114] . AI steps in as a critical security layer in this interconnected landscape. By monitoring device-to-device interactions, transactional patterns, and even the behavioral nuances of how users interact with their IoT devices, AI can ensure that these digital handshakes are genuine. For instance, if a smart refrigerator suddenly initiates a high-value transaction, AI might flag it as an anomaly based on past behaviors [115]. By keeping a vigilant eye on the vast and growing IoT network, AI ensures that as banking becomes more integrated with our daily devices, it remains secure and genuine [116]–[118].

As digital banking ecosystems diversify, they spawn a multitude of transaction channels ranging from online portals and mobile apps to traditional ATMs and point-of-sale terminals. Fraudsters, recognizing the potential vulnerabilities that might arise from this dispersion, often attempt to exploit inconsistencies between these channels. AI, however, provides a robust defense mechanism through cross-channel analysis. Instead of treating each channel as an isolated silo, AI systems integrate and synthesize data from every interaction point [119], piecing together a comprehensive view of a customer's transactional behavior. This panoramic perspective enables the AI to spot anomalies more effectively. For instance, if a customer's mobile app is used to make a large transfer just minutes after an ATM withdrawal in a different city, the AI would recognize the spatial-temporal inconsistency and flag the transaction for review. By weaving together disparate threads of data from multiple channels, AI ensures that fraudsters cannot exploit the gaps between them [120].

In the ever-fluctuating world of finance, being prepared for the unexpected is crucial. AI's capacity for simulations and stress testing has proven indispensable in this regard. These systems can be fed vast amounts of historical financial data, enabling them to simulate a wide range of economic scenarios, from minor market fluctuations to major global recessions. By projecting how these scenarios might impact a bank's portfolio, assets, and liabilities, AI provides invaluable insights into potential vulnerabilities. Beyond mere simulations, AI can also undertake rigorous stress testing, subjecting the bank's financial models to extreme but plausible adverse conditions to assess their resilience. Such proactive assessments help banks fortify their strategies, ensuring they remain robust even in the face of economic adversities [121].

Regulatory compliance is a multifaceted domain that demands precision, timeliness, and adaptability, given the complex and ever-evolving nature of regulations, particularly in sectors like finance, healthcare, and energy. Traditional methods of ensuring compliance, both manual and automated, often grapple with high volumes of data, requiring considerable time and resources, and yet sometimes still missing critical non-compliance issues. Deep learning emerges as a powerful ally in this context, presenting capabilities that are both transformative and efficient. By employing neural networks, deep learning models can learn from vast datasets, assimilating intricate patterns that denote regulatory adherence or violations. Instead of relying on static rules, these models can dynamically evaluate transactions, flagging anomalies or potential breaches with a level of precision that significantly outpaces conventional systems [122]. The promise of deep learning in compliance is further amplified by NLP, a branch that specifically deals with the understanding and generation of human language. Regulations, at their core, are documented in extensive legal and technical texts. Manually keeping up with changes, interpretations, and nuances in these documents is a herculean task. NLP, powered by deep learning, can be utilized to automatically parse, interpret, and categorize information from regulatory documents. It can alert businesses to relevant changes, extract actionable requirements, and even assist in mapping these requirements to specific operational areas. For instance, as a new financial directive is released, NLP models can dissect its contents and provide actionable summaries to relevant departments, ensuring that the business is proactively aligned with the latest compliance demands [123], [124].

Integrating deep learning into the compliance framework offers a dual benefit. First, it enhances the accuracy and speed of monitoring, ensuring that businesses operate within the bounds of regulations, thus mitigating potential legal and reputational risks. Second, it presents a significant reduction in operational costs. Manual reviews, investigations, and the aftermath of regulatory breaches can be expensive [125], [126]. By automating and enhancing the monitoring and interpretation processes, businesses can reduce the manpower and resources dedicated to compliance and also decrease the hefty penalties that come with non-compliance. As regulatory landscapes become more complex, deep learning stands as an essential tool for businesses, ensuring they remain compliant while navigating these intricate terrains efficiently [127].

Navigating the labyrinthine landscape of financial regulations is a complex task, made even more challenging by the frequent updates and amendments to these rules. AI offers a streamlined solution with its automated regulatory compliance capabilities. Instead of manually trawling through transactions and activities to ensure compliance, AI systems can be programmed with the latest regulatory standards, from anti-money laundering directives to data protection mandates. These systems then automatically scrutinize every transaction, ensuring it adheres to the prescribed rules. Should there be any deviations or potential breaches, the AI can flag them for immediate review, ensuring compliance errors are spotted and rectified in real-time. As regulations evolve, the AI models can be updated, ensuring that banks always remain on the right side of the law without incurring excessive manual overheads.

Conclusion

Banking fraud prevention and risk management are rapidly evolving with the advent of advanced technologies. One of the key technological drivers in these domains is Artificial Intelligence (AI). With the exponentially growing volume of data, it becomes impossible for humans to sift through and detect anomalies manually. That's where AI steps in, enabling a shift from reactive to proactive measures in fraud detection and prevention. By harnessing the vast streams of data generated by banks, AI not only offers predictive insights but also facilitates instant action in suspicious scenarios.

Traditional banking systems primarily relied on static, rule-based methods to detect fraud. These methods often lagged, only flagging discrepancies after they occurred and allowing little to no room for real-time intervention. This reactive approach made banks vulnerable to sophisticated fraud strategies. With AI, this landscape is undergoing a sea change. AI’s capacity to analyze copious amounts of transaction data in real-time means that unusual patterns or potential threats can be identified almost instantaneously. Such real-time fraud detection minimizes losses and offers customers a secure banking environment [128].

While AI, in general, offers a heightened ability to recognize patterns, deep learning, a subset of AI, takes this a notch higher. Neural networks, a form of deep learning, mirror the structure of the human brain, enabling the recognition of even the most complex patterns in vast data sets. Training these models on historical fraud data supercharges their predictive capabilities. As these models learn from past instances, they become adept at forecasting potentially fraudulent transactions with remarkable accuracy [129]. This translates to banks being not only vigilant but also predictive in thwarting fraudulent attempts.

AI further refines the 'Know Your Customer' (KYC) process, a critical aspect of banking operations. With Natural Language Processing (NLP), AI can scrutinize textual information from diverse sources, be it customer documents, social media activity, or other digital interactions. Such deep-dive analysis ensures rigorous customer verification, minimizing impersonation risks. Parallelly, graph analytics offers another robust tool in the AI arsenal. Visualizing transactions as a network or graph can spotlight suspicious patterns that might escape conventional screening. For instance, a convoluted web of rapidly moving funds between interconnected accounts could be a telltale sign of money laundering.

Predictive analytics, empowered by AI, is reshaping credit scoring methodologies. Instead of being overly reliant on traditional credit scores, which often provide a myopic view, AI delves into a broader data spectrum. By analyzing diverse parameters like utility payments, online behaviors, and even social media activities, AI can generate a more holistic risk profile of a customer, predicting their likelihood to default on a loan with greater accuracy. Additionally, with the emergence of AI-powered chatbots, customers now have a seamless avenue to report any suspicious activity. These chatbots not only facilitate immediate reporting but also trigger timely investigations, ensuring rapid resolution.

The future of secure banking hinges on the authentication of its users. Biometric verification offers a powerful solution, as it's rooted in the unique physical attributes of individuals. AI takes this a step further by refining and bolstering systems like facial recognition, fingerprint scanning, and voice recognition. Traditional biometric systems could sometimes be fooled with high-quality replicas or recordings. However, when paired with AI, these systems not only become more accurate but also adaptable, recognizing attempts at spoofing and ensuring that only authorized individuals gain access to critical banking services [55], [130]–[132].

Understanding the geographical context of transactions is invaluable in fraud detection. AI-driven geospatial analysis observes the physical locations associated with transactions. This is especially useful when a credit card, for instance, is swiped in two geographically distant locations within a time frame that makes traveling between them impossible [133], [134]. On a more nuanced level, AI dives deep into behavioral biometrics. By analyzing subtle interactions of a user with banking applications - be it typing speed, patterns of swiping, or even the angle at which a device is held - AI crafts a behavioral profile. Any aberration from this established norm can instantly trigger security protocols, protecting the user from potential threats.

As the adage goes, 'change is the only constant'. This holds especially true in the world of cyber threats where fraudsters continually refine their tactics. Self-learning AI systems offer a dynamic solution. By constantly assimilating new data and understanding emerging fraud patterns, these AI mechanisms ensure that detection and prevention tools remain at the cutting edge of security. Furthermore, as banking grows increasingly omni-channel, fraud detection must be holistic. Cross-channel analysis facilitated by AI provides a consolidated view of a customer's activities across various platforms, from online banking to ATM withdrawals, ensuring inconsistencies are promptly flagged.

In the intricate world of banking, risk management isn't solely about fraud prevention. AI-enhanced simulations and stress testing play a pivotal role in preempting economic shocks. By simulating diverse economic scenarios, banks can gauge potential impacts on their portfolios, allowing for informed strategic decisions. Meanwhile, the regulatory landscape in banking is ever-shifting, making compliance a moving target. Automated AI-driven systems can track, interpret, and ensure that all banking activities align with the most current regulatory standards. This not only safeguards institutions against potential legal pitfalls but also streamlines operations. Lastly, as the Internet of Things (IoT) becomes more intertwined with banking - from smart home devices to wearable tech - AI stands as a vigilant sentinel, monitoring these interactions to ensure they remain both secure and authentic.

References

[1] B. Mytnyk, O. Tkachyk, N. Shakhovska, S. Fedushko, and Y. Syerov, “Application of Artificial Intelligence for Fraudulent Banking Operations Recognition,” *Big Data and Cognitive Computing*, vol. 7, no. 2, p. 93, May 2023.

[2] E. Muthu Kumaran, K. Velmurugan, P. Venkumar, D. Amutha Guka, and V. Divya, “Artificial Intelligence-Enabled IoT-Based Smart Blood Banking System,” in *Proceedings of 2nd International Conference on Artificial Intelligence: Advances and Applications*, 2022, pp. 119–130.

[3] S. Singh and L. Agarwal, “Pros and cons of artificial intelligence in banking sector of India,” *BICON-2019*, 2019.

[4] F. Ahmed, “ETHICAL ASPECTS OF ARTIFICIAL INTELLIGENCE IN BANKING,” *Journal of Research in Economics and*, 2022.

[5] S. Jahandari, “Graph-theoretic Identification of Dynamic Networks.” University of Minnesota, 2022.

[6] A. Aljarbouh and B. Caillaud, “On the regularization of chattering executions in real time simulation of hybrid systems,” 2015, p. 49.

[7] A. Suresh and N. J. Rani, “Role of Artificial Intelligence (AI) in the Indian Banking Scenario,” *Journal of Information Technology &*, 2020.

[8] S. Vinoth, “Artificial intelligence and transformation to the digital age in Indian banking industry—A case study,” *Artif. Intell.*, 2022.

[9] A. Aljarbouh *et al.*, “Application of the K-medians Clustering Algorithm for Test Analysis in E-learning,” in *Proceedings of the Computational Methods in Systems and Software*, Springer, 2022, pp. 249–256.

[10] R. Al-Araj, H. Haddad, M. Shehadeh, E. Hasan, and M. Y. Nawaiseh, “The effect of Artificial Intelligence on service quality and customer satisfaction in Jordanian banking sector,” *WSEAS Trans. Bus. Econ.*, vol. 19, pp. 1929–1947, Dec. 2022.

[11] S. Jahandari, A. Kalhor, and B. N. Araabi, “Order determination and transfer function estimation of linear mimo systems: application to environmental modeling,” *Environmental Modeling and Software*, 2016.

[12] K. Thiagarajan, M. Porkodi, S. Gadde, and R. Priyadharshini, “Application and Advancement of Sensor Technology in Bioelectronics Nano Engineering,” 2022, pp. 841–845.

[13] J. B. Awotunde, S. Misra, F. Ayeni, R. Maskeliunas, and R. Damasevicius, “Artificial Intelligence Based System for Bank Loan Fraud Prediction,” in *Hybrid Intelligent Systems*, 2022, pp. 463–472.

[14] J. Sindhu and R. Namratha, “Impact of artificial intelligence in chosen Indian commercial bank-A cost benefit analysis,” *Asian J. Manag.*, vol. 10, no. 4, p. 377, 2019.

[15] M. Thisarani and S. Fernando, “Artificial intelligence for futuristic banking,” *2021 IEEE International Conference*, 2021.

[16] S. Jahandari and A. Srivastava, “Adjusting for Unmeasured Confounding Variables in Dynamic Networks,” *IEEE Control Systems Letters*, vol. 7, pp. 1237–1242, 2023.

[17] T. Carpenter, “Revolutionising the consumer banking experience with artificial intelligence,” *Journal of Digital Banking*, vol. 4, no. 4, pp. 291–300, 2020.

[18] Z. M. E. Kishada, N. A. Wahab, and A. Mustapha, “Customer loyalty assessment in Malaysian islamic banking using artificial intelligence,” *J. Theor. Appl. Inf. Technol.*, 2016.

[19] H. I. Erdal and A. Ekinci, “A Comparison of Various Artificial Intelligence Methods in the Prediction of Bank Failures,” *Comput. Econ.*, vol. 42, no. 2, pp. 199–215, Aug. 2013.

[20] A. J. Albarakati *et al.*, “Microgrid energy management and monitoring systems: A comprehensive review,” *Frontiers in Energy Research*, vol. 10, p. 1097858, 2022.

[21] B. Batiz-Lazo, L. Efthymiou, and K. Davies, “The Spread of Artificial Intelligence and Its Impact on Employment: Evidence from the Banking and Accounting Sectors,” in *Business Advancement through Technology Volume II: The Changing Landscape of Industry and Employment*, A. Thrassou, D. Vrontis, L. Efthymiou, Y. Weber, S. M. R. Shams, and E. Tsoukatos, Eds. Cham: Springer International Publishing, 2022, pp. 135–155.

[22] S. P. S. Ho and M. Y. C. Chow, “The role of artificial intelligence in consumers’ brand preference for retail banks in Hong Kong,” *Journal of Financial Services Marketing*, 2023.

[23] H. Fraisse and M. Laporte, “Return on investment on artificial intelligence: The case of bank capital requirement,” *Journal of Banking & Finance*, 2022.

[24] Z. Bai, R. Yang, and Y. Liang, “Mental task classification using electroencephalogram signal,” *arXiv preprint arXiv:1910.03023*, 2019.

[25] H. Vijayakumar, “Revolutionizing Customer Experience with AI: A Path to Increase Revenue Growth Rate,” 2023, pp. 1–6.

[26] S. Jahandari and D. Materassi, “How Can We Be Robust Against Graph Uncertainties?,” 2023, pp. 1946–1951.

[27] M. S. Ali, I. A. Swiety, and M. H. Mansour, “Evaluating the Role of artificial intelligence in the automation of the banking services industry: Evidence from Jordan,” *Philipp. Soc. Sci. Humanit. Rev.*, 2022.

[28] T. Ravikumar, N. Murugan, and J. Suhashini, “Banking on artificial intelligence to bank the unbanked,” *Annals of the*, 2021.

[29] L. F. Pau, C. Gianotti, L. F. Pau, and C. Gianotti, “Applications of artificial intelligence in banking, financial services and economics,” 1990.

[30] G. Samata, P. Sudhakar, and G. Jyothsna, “In silico Analysis of Spike Protein Glycoprotein A of Omicron variant and identification of variant specific peptide based Vaccine,” *Research Journal of Biotechnology Vol*, vol. 18, p. 7, 2023.

[31] M. Riikkinen, H. Saarijärvi, and P. Sarlin, “Using artificial intelligence to create value in insurance,” *Journal of Bank …*, 2018.

[32] A. Lui and G. W. Lamb, “Artificial intelligence and augmented intelligence collaboration: regaining trust and confidence in the financial sector,” *Information & Communications Technology Law*, 2018.

[33] J. A. Albarakati *et al.*, “Multi-Agent-Based Fault Location and Cyber-Attack Detection in Distribution System,” *Energies*, vol. 16, no. 1, p. 224, 2022.

[34] K. Singh, “Banks banking on ai,” *International Journal of Advanced Research in*, 2020.

[35] G. Qasaimeh, R. Yousef, A. Al-Gasaymeh, and A. Alnaimi, “The Effect of Artificial Intelligence Using Neural Network in Estimating on An Efficient Accounting Information System: Evidence from Jordanian Commercial Banks,” in *2022 International Conference on Business Analytics for Technology and Security (ICBATS)*, 2022, pp. 1–5.

[36] A. Aljarbouh and B. Caillaud, “Robust simulation for hybrid systems: chattering path avoidance,” *arXiv preprint arXiv:1512.07818*, 2015.

[37] S. F. Eletter, S. G. Yaseen, and G. A. Elrefae, “Neuro-based artificial intelligence model for loan decisions,” *Am. J. Econ. Sociol.*, 2010.

[38] A. Golubev, O. Ryabov, and A. Zolotarev, “Digital transformation of the banking system of Russia with the introduction of blockchain and artificial intelligence technologies,” *IOP Conf. Ser.: Mater. Sci. Eng.*, vol. 940, no. 1, p. 012041, Sep. 2020.

[39] T. R. Yu and X. Song, “Big Data and Artificial Intelligence in the Banking Industry,” , *Mathematics, Statistics, and Machine learning*, 2021.

[40] A. Aljarbouh, A. Duracz, Y. Zeng, B. Caillaud, and W. Taha, “Chattering-free simulation for hybrid dynamical systems,” *HAL*, vol. 2016, 2016.

[41] R. Rashmi and R. V. K. Nirmal, “A study on the implementation and the impact of artificial intelligence in banking processes,” *Asian Journal of Management*, 2021.

[42] Y. Liang and W. Liang, “ResWCAE: Biometric Pattern Image Denoising Using Residual Wavelet-Conditioned Autoencoder,” *arXiv preprint arXiv:2307.12255*, 2023.

[43] S. K. Burley, C. Bhikadiya, C. Bi, and S. Bittrich, “… . org): delivery of experimentally-determined PDB structures alongside one million computed structure models of proteins from artificial intelligence/machine learning,” *Nucleic acids*, 2023.

[44] B. D. Bagana, M. Irsad, and I. H. Santoso, “ARTIFICIAL INTELLIGENCE AS A HUMAN SUBSTITUTION? CUSTOMER’S PERCEPTION OF THE CONVERSATIONAL USER INTERFACE IN BANKING INDUSTRY BASED ON UTAUT CONCEPT,” *Review of Management and Entrepreneurship*, vol. 5, no. 1, pp. 33–44, Apr. 2021.

[45] V. Rutskiy *et al.*, “Prospects for the Use of Artificial Intelligence to Combat Fraud in Bank Payments,” in *Proceedings of the Computational Methods in Systems and Software*, Springer, 2022, pp. 959–971.

[46] I. Haq *et al.*, “Machine Vision Approach for Diagnosing Tuberculosis (TB) Based on Computerized Tomography (CT) Scan Images,” *Symmetry* , vol. 14, no. 10, p. 1997, 2022.

[47] S. S. Devi, S. Gadde, K. Harish, C. Manoharan, R. Mehta, and S. Renukadevi, “IoT and image processing Techniques-Based Smart Sericulture Nature System,” *Indian J. Applied & Pure Bio*, vol. 37, no. 3, pp. 678–683, 2022.

[48] O. Raiter, “Segmentation of bank consumers for artificial intelligence marketing,” *International Journal of Contemporary Financial Issues*, 2021.

[49] T. Choithani, A. Chowdhury, S. Patel, and P. Patel, “A comprehensive study of artificial intelligence and cybersecurity on Bitcoin, crypto currency and banking system,” *Annals of Data*, 2022.

[50] A. Aljarbouh and B. Caillaud, “Chattering-free simulation of hybrid dynamical systems with the functional mock-up interface 2.0,” 2016, vol. 124, pp. 95–105.

[51] E. D. Butenko, “Artificial intelligence in banks today: Experience and perspectives,” *Finance and credit*, 2018.

[52] L. F. Pau and C. Gianotti, “Applications of Artificial Intelligence in banking, financial services and economics,” in *Economic and Financial Knowledge-Based Processing*, L. F. Pau and C. Gianotti, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 1990, pp. 22–46.

[53] A. Kumar, A. Srivastava, and P. K. Gupta, “Banking 4.0: The era of artificial intelligence-based fintech,” *Strateg. Change*, vol. 31, no. 6, pp. 591–601, Nov. 2022.

[54] A. Aljarbouh, Y. Zeng, A. Duracz, B. Caillaud, and W. Taha, “Chattering-free simulation for hybrid dynamical systems semantics and prototype implementation,” 2016, pp. 412–422.

[55] M. Thisarani and S. Fernando, “Artificial Intelligence for Futuristic Banking,” in *2021 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC)*, 2021, pp. 1–13.

[56] S. P. S. Ho and M. Y. C. Chow, “The role of artificial intelligence in consumers’ brand preference for retail banks in Hong Kong,” *J. Fin. Serv. Mark.*, Jan. 2023.

[57] S. Jahandari and D. Materassi, “Analysis and compensation of asynchronous stock time series,” 2017, pp. 1085–1090.

[58] R. Vedapradha and H. Ravi, “Innovation in banking: fusion of artificial intelligence and blockchain,” *Asia Pacific Journal of Innovation and Entrepreneurship*, vol. 15, no. 1, pp. 51–61, Jan. 2021.

[59] Y. Zhu *et al.*, “Application of Physics-Informed Neural Network (PINN) in the Experimental Study of Vortex-Induced Vibration with Tunable Stiffness,” in *The 33rd International Ocean and Polar Engineering Conference*, 2023.

[60] S. Subudhi, “Banking on artificial intelligence: Opportunities & challenges for banks in India,” *International Journal of Research in Commerce*, 2019.

[61] N. Cavus, Y. B. Mohammed, and M. N. Yakubu, “An artificial intelligence-based model for prediction of parameters affecting sustainable growth of mobile banking apps,” *Sustain. Sci. Pract. Policy*, 2021.

[62] N. Sharmili *et al.*, “Earthworm Optimization with Improved SqueezeNet Enabled Facial Expression Recognition Model,” *Computer Systems Science & Engineering*, vol. 46, no. 2, 2023.

[63] D. Nelson-Gruel, Y. Chamaillard, and A. Aljarbouh, “Modeling and estimation of the pollutants emissions in the Compression Ignition diesel engine,” 2016, pp. 317–322.

[64] S. Mor and G. Gupta, “Artificial intelligence and technical efficiency: The case of Indian commercial banks,” *Strateg. Change*, vol. 30, no. 3, pp. 235–245, May 2021.

[65] A. S. Samukdjanovna, “Risks and Prospects for the Development of Artificial Intelligence in the Banking Sector,” *J’ Positive School Psychology*, vol. 6, no. 3, pp. 5987–5992, Apr. 2022.

[66] M. Azeroual, Y. Boujoudar, A. Aljarbouh, H. El Moussaoui, and H. El Markhi, “A multi-agent-based for fault location in distribution networks with wind power generator,” *Wind Engineering*, vol. 46, no. 3, pp. 700–711, 2022.

[67] P. Makhija and E. Chacko, “Efficiency and Advancement of Artificial Intelligence in Service Sector with Special Reference to Banking Industry,” in *Fourth Industrial Revolution and Business Dynamics: Issues and Implications*, N. R. Al Mawali, A. M. Al Lawati, and S, Ananda, Eds. Singapore: Springer Singapore, 2021, pp. 21–35.

[68] S. Gadde, E. Karthika, R. Mehta, S. Selvaraju, W. B. Shirsath, and J. Thilagavathi, “Onion growth monitoring system using internet of things and cloud,” *Agricultural and Biological Research*, vol. 38, no. 3, pp. 291–293, 2022.

[69] M. M. Alhaddad, “Artificial Intelligence in Banking Industry: A Review on Fraud Detection, Credit Management, and Document Processing,” *RRST*, vol. 2, no. 3, pp. 25–46, Nov. 2018.

[70] S. Tiwari, S. Bharadwaj, and S. Joshi, “A Study of Impact of Cloud Computing and Artificial Intelligence on Banking Services, Profitability and Operational Benefits,” *TURCOMAT*, vol. 12, no. 6, pp. 1617–1627, Apr. 2021.

[71] A. Aljarbouh, “Accelerated Simulation of Hybrid Systems: Method combining static analysis and run-time execution analysis.(Simulation Accélérée des Systèmes Hybrides: méthode combinant analyse statique et analyse à l’exécution).” University of Rennes 1, France, 2017.

[72] S. Jahandari and A. Srivastava, “Detection of Delays and Feedthroughs in Dynamic Networked Systems,” *IEEE Control Systems Letters*, vol. 7, pp. 1201–1206, 2022.

[73] A. Duracz *et al.*, “Advanced hazard analysis and risk assessment in the ISO 26262 functional safety standard using rigorous simulation,” 2020, pp. 108–126.

[74] C. Vijai and P. Nivetha, “ABC technology-artificial intelligence, blockchain technology, cloud technology for banking sector,” *Advances in Management*, 2020.

[75] S. F. Suhel, V. K. Shukla, and S. Vyas, “Conversation to automation in banking through chatbot using artificial machine intelligence language,” *2020 8th international*, 2020.

[76] W. Liang, Y. Liang, and J. Jia, “MiAMix: Enhancing Image Classification through a Multi-stage Augmented Mixied Sample Data Augmentation Method,” *arXiv preprint arXiv:2308.02804*, 2023.

[77] Y. Boujoudar *et al.*, “Fuzzy logic-based controller of the bidirectional direct current to direct current converter in microgrid,” *Int. J. Elect. Computer Syst. Eng.*, vol. 13, no. 5, pp. 4789–4797, 2023.

[78] A. Aljarbouh, “Accelerated simulation of hybrid systems: method combining static analysis and run-time execution analysis.” Rennes 1, 2017.

[79] K. Thiagarajan, C. K. Dixit, M. Panneerselvam, C. A. Madhuvappan, S. Gadde, and J. N. Shrote, “Analysis on the Growth of Artificial Intelligence for Application Security in Internet of Things,” 2022, pp. 6–12.

[80] I. Pozharkova, A. Aljarbouh, S. H. Azizam, A. P. Mohamed, F. Rabbi, and R. Tsarev, "A simulation modeling method for cooling building structures by fire robots," 2022, pp. 504–511.

[81] S. Jahandari, F. F. Beyglou, A. Kalhor, and M. T. Masouleh, "A robust adaptive linear control for a ball handling mechanism," 2014, pp. 376–381.

[82] L. Shambira, "Exploring the adoption of artificial intelligence in the Zimbabwe banking sector," *European Journal of Social Sciences Studies*, 2020.

[83] M. Sabharwal, "The use of Artificial Intelligence (AI) based technological applications by Indian Banks," *International Journal of Artificial Intelligence and Agent Technology*, vol. 2, no. 1, pp. 1–5, 2014.

[84] E. Lee, F. Rabbi, H. Almashaqbeh, A. Aljarbouh, J. Ascencio, and N. V. Bystrova, "The issue of software reliability in program code cloning," 2023, vol. 2700.

[85] L. D. Wall, "Some financial regulatory implications of artificial intelligence," *J. Econ. Bus.*, 2018.

[86] G. D. B. Swankie and D. Broby, "Examining the impact of artificial intelligence on the evaluation of banking risk," Nov. 2019.

[87] S. Jahandari and D. Materassi, "Optimal selection of observations for identification of multiple modules in dynamic networks," *IEEE Trans. Automat. Contr.*, vol. 67, no. 9, pp. 4703–4716, 2022.

[88] R. Jabeur, Y. Boujoudar, M. Azeroual, A. Aljarbouh, and N. Ouaaline, "Microgrid energy management system for smart home using multi-agent system," *Int. J. Elect. Computer Syst. Eng.*, vol. 12, no. 2, pp. 1153–1160, 2022.

[89] Y. Liang, W. Liang, and J. Jia, "Structural Vibration Signal Denoising Using Stacking Ensemble of Hybrid CNN-RNN," *arXiv e-prints*, p. arXiv-2303, 2023.

[90] M. K. Satheesh and S. Nagaraj, "Applications of artificial intelligence on customer experience and service quality of the banking sector," *International Management*, 2021.

[91] O. Wibisono, H. D. Ari, A. Widjanarti, and A. A. Zulen, "The use of big data analytics and artificial intelligence in central banking," *IFC Bulletins, Bank for*, 2019.

[92] Y. Liang, "Structural Vibration Signal Denoising Using Stacking Ensemble of Hybrid CNN-RNN. Advances in Artificial Intelligence and Machine Learning. 2022; 3 (2): 65." 2006.

[93] M. Sathanapriya *et al.*, "Analysis of Hydroponic System Crop Yield Prediction and Crop IoT-based monitoring system for precision agriculture," 2022, pp. 575–578.

[94] H. Vijayakumar, A. Seetharaman, and K. Maddulety, "Impact of AIServiceOps on Organizational Resilience," 2023, pp. 314–319.

[95] O. Kaya, J. Schildbach, D. B. Ag, and S. Schneider, "Artificial intelligence in banking," *Artif. Intell.*, 2019.

[96] M. Jakšič and M. Marinč, "Relationship banking and information technology: the role of artificial intelligence and FinTech," *Risk Manage.: Int. J.*, vol. 21, no. 1, pp. 1–18, Mar. 2019.

[97] A. Ashta and H. Herrmann, "Artificial intelligence and fintech: An overview of opportunities and risks for banking, investments, and microfinance," *Strategic Change*, 2021.

[98] S. Jahandari and D. Materassi, "Optimal observations for identification of a single transfer function in acyclic networks," 2021, pp. 852–857.

[99] S. Yonbawi *et al.*, “Modified Metaheuristics with Transfer Learning Based Insect Pest Classification for Agricultural Crops,” *Computer Systems Science & Engineering*, vol. 46, no. 3, 2023.

[100] P. K. Donepudi, “Machine learning and artificial intelligence in banking,” *Engineering International*, 2017.

[101] M. Rahman, M. T. Hui, B. T. Azim, and M. Sarker, “Adoption of artificial intelligence in banking services: an empirical analysis,” *International Journal of Emerging Markets*, vol. ahead-of-print, no. ahead-of-print, Jan. 2021.

[102] O. H. Fares, I. Butt, and S. H. M. Lee, “Utilization of artificial intelligence in the banking sector: a systematic literature review,” *Journal of Financial Services Marketing*, Aug. 2022.

[103] S. Jahandari, A. Kalhor, and B. N. Araabi, “Order determination and robust adaptive control of unknown deterministic input-affine systems: An operational controller,” 2016, pp. 3831–3836.

[104] A. Hanif, “Towards Explainable Artificial Intelligence in Banking and Financial Services,” *arXiv [cs.LG]*, 14-Dec-2021.

[105] S. M. Tang and H. N. Tien, “Impact of artificial intelligence on Vietnam commercial bank operations,” *Int. J. Soc. Sci. Econ. Invent.*, vol. 6, no. 07, pp. 296–303, Jul. 2020.

[106] V. Dubey, “FinTech innovations in digital banking,” *International Journal of Engineering Research &*, 2019.

[107] A. Aljarbouh, M. S. Ahmed, M. Vaquera, and B. D. Dirting, “Intellectualization of information processing systems for monitoring complex objects and systems,” *Современные инновации, системы и технологии*, vol. 2, no. 1, pp. 9–17, 2022.

[108] I. E. Ahmed, R. Mehdi, and E. A. Mohamed, “The role of artificial intelligence in developing a banking risk index: an application of Adaptive Neural Network-Based Fuzzy Inference System (ANFIS),” *Artif Intell Rev*, pp. 1–23, Apr. 2023.

[109] E. Mogaji, T. O. Soetan, and T. A. Kieu, “The implications of artificial intelligence on the digital marketing of financial services to vulnerable customers,” *Australasian Marketing Journal*, vol. 29, no. 3, pp. 235–242, Aug. 2021.

[110] A. Aljarbouh, “Non-standard zeno-free simulation semantics for hybrid dynamical systems,” 2019, pp. 16–31.

[111] T. L. Mamela and N. Sukdeo, “Adapting to artificial intelligence through workforce re-skilling within the banking sector in South Africa,” *on Artificial Intelligence …*, 2020.

[112] A. Sarea, M. R. Rabbani, M. S. Alam, and M. Atif, “Artificial intelligence (AI) applications in Islamic finance and banking sector,” in *Artificial Intelligence and Islamic Finance*, London: Routledge, 2021, pp. 108–121.

[113] S. Jahandari and D. Materassi, “Identification of dynamical strictly causal networks,” 2018, pp. 4739–4744.

[114] S. Umamaheswar, L. G. Kathawate, W. B. Shirsath, S. Gadde, and P. Saradha, “Recent turmeric plants agronomy analysis and methodology using Artificial intelligence,” *International Journal of Botany Studies*, vol. 7, no. 2, pp. 233–236, 2022.

[115] H. Vijayakumar, “Business Value Impact of AI-Powered Service Operations (AIServiceOps),” *Available at SSRN 4396170*, 2023.

[116] A. Aljarbouh, M. Fayaz, and M. S. Qureshi, “Non-Standard Analysis for Regularization of Geometric-Zeno Behaviour in Hybrid Systems,” *Systems*, vol. 8, no. 2, p. 15, 2020.

[117] S. F. Suhel, V. K. Shukla, S. Vyas, and V. P. Mishra, “Conversation to Automation in Banking Through Chatbot Using Artificial Machine Intelligence Language,” in *2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, 2020, pp. 611–618.

[118] B. N. Mallah, “Artificial intelligence impact on banks clients and employees in an Asian developing country,” *Journal of Asia Business Studies*, vol. 16, no. 2, pp. 267–278, Jan. 2021.

[119] A. Chavez, D. Koutentakis, Y. Liang, S. Tripathy, and J. Yun, “Identify statistical similarities and differences between the deadliest cancer types through gene expression,” *arXiv preprint arXiv:1903.07847*, 2019.

[120] S. Jahandari and D. Materassi, “Sufficient and necessary graphical conditions for miso identification in networks with observational data,” *IEEE Trans. Automat. Contr.*, vol. 67, no. 11, pp. 5932–5947, 2021.

[121] A. R. A. M. Husain, A. Hamdan, and S. M. Fadhul, “The Impact of Artificial Intelligence on the Banking Industry Performance,” in *Future of Organizations and Work After the 4th Industrial Revolution: The Role of Artificial Intelligence, Big Data, Automation, and Robotics*, A. Hamdan, A. Harraf, P. Arora, B. Alareeni, and R. Khamis Hamdan, Eds. Cham: Springer International Publishing, 2022, pp. 145–156.

[122] A. Padma, S. Gadde, B. S. P. Rao, and G. Ramachandran, “Effective Cleaning System management using JSP and Servlet Technology,” 2021, pp. 1472–1478.

[123] S. Jahandari and D. Materassi, “Topology identification of dynamical networks via compressive sensing,” *IFAC-PapersOnLine*, vol. 51, no. 15, pp. 575–580, 2018.

[124] H. Sadok, F. Sakka, and M. E. H. El Maknouzi, “Artificial intelligence and bank credit analysis: A review,” *Cogent Economics & Finance*, vol. 10, no. 1, p. 2023262, Dec. 2022.

[125] S. Alahmari *et al.*, “Hybrid Multi-Strategy Aquila Optimization with Deep Learning Driven Crop Type Classification on Hyperspectral Images,” *Comput. Syst. Sci. Eng.*, vol. 47, no. 1, pp. 375–391, 2023.

[126] M. Sinha, “Artificial intelligence-banks in India,” *International Journal in Management & Social Science*, 2017.

[127] A. J. Albarakati *et al.*, “Real-time energy management for DC microgrids using artificial intelligence,” *Energies*, vol. 14, no. 17, p. 5307, 2021.

[128] I. Trifonov, A. Aljarbouh, and A. Beketaeva, “Evaluating the effectiveness of turbulence models in the simulation of two-phases combustion,” *International Review on Modelling and Simulations*, vol. 14, no. 4, pp. 291–300, 2021.

[129] X. Wu, Z. Bai, J. Jia, and Y. Liang, “A Multi-Variate Triple-Regression Forecasting Algorithm for Long-Term Customized Allergy Season Prediction,” *arXiv preprint arXiv:2005.04557*, 2020.

[130] A. Aljarbouh, “Selection of the optimal set of versions of N-version software using the ant colony optimization,” 2021, vol. 2094, p. 032026.

[131] G. Qasaimeh and R. Yousef, “The effect of artificial intelligence using neural network in estimating on an efficient accounting information system: Evidence from jordanian commercial banks,” *on Business Analytics …*, 2022.

[132] K. AL-Dosari, N. Fetais, and M. Kucukvar, “Artificial Intelligence and Cyber Defense System for Banking Industry: A Qualitative Study of AI Applications and Challenges,” *Cybern. Syst.*, 2022.

[133] J. Ortiz, A. Marin, and O. Gualdron, “Implementation of a banking system security in embedded systems using artificial intelligence,” *Advances in Natural and Applied Sciences*, vol. 10, no. 17, pp. 95–101, 2016.

[134] N. Van Thuy, “Applications of IOTS, Internet Data, and Artificial Intelligence in Building Better Management Information System (MIS) in Banking Activities in Vietnam,” in *Advances in Computational Intelligence and Communication Technology*, 2022, pp. 195–201.