Revista de Științe Politice. Revue des Sciences Politiques • No. 86 • 2025: 258 – 273

ORIGINAL PAPER

How Artificial Intelligence is Rewriting the Rules of the Game in the Financial Banking Industry. Opportunities, Perspectives, and Challenges for the Future of Banking Activities

Andrei Smarandescu[1)]

Abstract:
This paper explores the profound impact of artificial intelligence (AI) on the financial-banking sector, emphasizing how digitalization and AI are reshaping operational rules and customer interactions. The analysis focuses on the transition from traditional transactions to the extensive use of virtual currencies and the digitization of financial securities, highlighting how emerging technologies, such as open banking and modular architectures, contribute to creating a more integrated and accessible financial landscape. The study underscores AI's ability to optimize financial decision-making processes, from risk management to personalizing customer offerings, and stresses the importance of adapting the regulatory framework to protect consumers and promote responsible innovation. Through this analysis, the paper provides valuable insights into current and future developments in the financial-banking sector, marking a crucial stage in understanding technology's impact on finance.
Keywords: *Digital Transformation, Predictive Algorithms, Financial Intermediation, Open Banking, Financial Sustainability.*
JEL Classification: G21, O32, E58.

[1)] Master's Degree Student, University of Craiova, Faculty of Economics and Business Administration, Finance specialization Craiova, Romania, Email: andrei.smarandescu2001@yahoo.com.

How Artificial Intelligence is Rewriting the Rules of the Game in the Financial Banking Industry. Opportunities, Perspectives, and Challenges for the Future of Banking Activities

1. Introduction

The financial services sector has been profoundly reshaped not only by technological advances and changes in consumer behavior but also by the emergence and integration of artificial intelligence (AI) into its fundamental processes and services. This dual shift towards digitalization and AI has driven a profound transformation in the banking and financial sectors, driving institutions to reconsider traditional business models and innovate in customer interactions. Initially, digitalization facilitated the development of advanced techniques for managing transactions and customer relationships, while AI has deepened this transformation by optimizing financial decision-making, personalizing services, and improving risk management.

Advances in cryptocurrencies and the prospect of introducing central bank digital currencies (CBDCs) have further intensified this shift toward a predominantly digital financial system, where the internet has become an essential catalyst for innovative transactions. This shift towards digitalization and AI is reshaping both financial infrastructure and the fundamental paradigms of trust and security, suggesting that although money is becoming increasingly virtual, it remains anchored in the reality of advanced technological systems and specialized expertise.

Digitalization has also paved the way for significant diversification and expansion of the capital market by reducing entry barriers and increasing operational efficiency. In this context, AI plays a crucial role in creating electronic trading systems that optimize liquidity flows and strengthen financial markets, accelerating the trend of continuous change and innovation.

Thus, the intersection between digitalization and artificial intelligence is redefining not only the structure and functioning of the financial sector but also how financial institutions adapt to the ever-changing needs of customers. This new landscape, marked by dematerialized transactions and electronic signatures, not only amplifies the digitalization of financial banking activities but also opens a vast horizon of possibilities for innovation, efficiency, and unprecedented levels of personalization.

2. Literature review

Digital transformation and artificial intelligence (AI) mark a new era in the banking and financial sector, fundamentally reshaping how financial institutions operate and interact with customers. This section combines a detailed analysis of digitalization's impact, including the emergence of central bank digital currencies (CBDCs), and artificial intelligence, considering associated challenges and opportunities, as well as implications for security, regulation, and product and service innovation.

Digitalization in the financial sector, through the introduction of CBDCs, promises to enhance payment system efficiency and promote financial inclusion. These digital currencies, backed by central banks' credibility, offer a secure and accessible alternative to traditional payment methods, facilitating faster transactions and reducing associated costs (Spulbar & Spulbar, 2022; Auer & Böhme, 2020). The importance of blockchain and Distributed Ledger Technology (DLT) in supporting CBDCs is undeniable, ensuring security, transparency, and efficiency-essential for the credibility and integrity of digital currencies (Spulbar & Mitrache, 2023).

At the same time, AI adoption is transforming financial operations, enabling banks to analyze real-time data, personalize customer services, and optimize risk management. AI applications, from robo-advisory services to fraud detection systems,

illustrate technology's potential to bring significant innovations to the industry, improving customer experience and operational efficiency (Buchanan, 2021).

Despite these advantages, the implementation of digitalization and AI in the banking and financial sector raises numerous challenges. Concerns related to data security, cybersecurity risks, and the impact on the workforce require cautious approaches and appropriate regulations to ensure fairness, transparency, and consumer protection. Additionally, collaboration between financial institutions, regulators, and stakeholders is crucial for navigating the evolving technological landscape and maximizing technological benefits while ensuring global financial system stability (Philippon, 2019).

Emerging technologies like AI and blockchain are reshaping the future of the financial sector, bringing significant improvements in the efficiency, security, and accessibility of financial services. AI's ability to revolutionize risk management and compliance in financial institutions is significant, contributing to enhanced accuracy and efficiency in fraud detection and monitoring of suspicious transactions. Machine learning algorithms allow banks to identify patterns and anomalies in data, offering a superior level of financial security and fraud protection. This advanced analytical capability highlights the necessity of an adaptable regulatory framework that keeps up with technological innovations (Arner, Barberis, & Buckley, 2016).

Concurrently, blockchain is redefining transparency and efficiency in payment systems, offering new perspectives on reducing verification costs and transaction trust. According to Catalini and Gans (2016), blockchain facilitates greater efficiency and reduces payment processing time, paving the way for developing new decentralized financial business models. However, implementing this technology involves challenges related to scalability, energy consumption, and interoperability, requiring innovative solutions and collaboration among industry players.

Thus, the literature highlights a continuously evolving financial landscape where technological innovations play a fundamental role in the evolution of financial services. These technologies not only promise to enhance financial operations' efficiency but also bring complex challenges, emphasizing the importance of adaptation and collaboration in the sector to maximize potential benefits

3. The Impact of digitalization and Artificial Intelligence

In my academic endeavor to map the profound transformation of the financial sector under the auspices of digitalization and advances in artificial intelligence (AI), I have identified a significant inflection point that reconfigures the traditional and operational architecture of the industry. This inflection point, marked by the implementation of emerging technologies, does not merely optimize pre-existing processes but also initiates the emergence of new paradigms of innovation, business models, and financial service spectra adapted to the needs and expectations of the 21st century.

My analysis has focused particularly on the revolutionary impact of artificial intelligence in risk management and data analysis, areas where AI has demonstrated remarkable potential in transforming how financial institutions address challenges and opportunities. A key example of this is the use of machine learning algorithms to enhance fraud detection systems. This technology enables the highly accurate identification of suspicious transactions, significantly surpassing the limitations of traditional methods. Such advanced systems not only enhance the financial security of institutions and their clients but also significantly improve compliance processes, dynamically adjusting to

legislative changes without incurring additional operational costs. The importance of this aspect is accentuated in the context of a continuously evolving global financial landscape, where the ability to respond swiftly and efficiently to new legislative and operational challenges becomes crucial.

On the other hand, digitalization, and particularly the introduction of central bank digital currencies (CBDCs), has generated considerable academic and practical interest. The analysis of pilot initiatives implemented by central banks in various jurisdictions has revealed the significant potential of CBDCs to positively influence the efficiency of payment systems and promote financial inclusion. By reducing transaction-related costs and offering increased accessibility to financial services, CBDCs have the potential to address some of the most pressing challenges of financial exclusion. Their contribution to sustainable development goals is particularly relevant in the current global context, highlighting the role of financial technology in facilitating access to financial services for unbanked populations and supporting inclusive economic growth.

Therefore, the impact of digitalization and artificial intelligence on the financial-banking sector transcends the mere optimization of existing processes, opening new horizons for innovation in banking services, improving access to these services, and strengthening banking security and integrity. The crucial role of these technologies in shaping the future of the financial sector is indisputable, requiring a profound understanding and strategic approach to maximize benefits and minimize associated potential risks.

Based on these observations, I have compiled a conceptual table summarizing the main benefits of AI and digitalization in the financial-banking sector:

Technology	**Impact on the Financial-Banking Sector**	**Examples**	**Specific benefits**
Artificial Intelligence	Optimization of decision-making processes	Algorithms for credit assessment	Faster and more accurate decisions, reduction of human errors
	Improving security	AI-based fraud detection systems	Minimizing fraud-related losses and strengthening customer trust
	Personalization of customer experience	Chatbots for customer service	Enhanced customer satisfaction, increased operational efficiency
Digitalization (CBDCs)	Payment efficiency	Pilot projects for central bank digital currencies	Lower transaction costs, improved access to financial services
	Promoting financial inclusion	Accessible CBDCs for unbanked populations	Expansion of access to financial services, reduction of financial exclusion
	Stimulating financial product innovation	Payment platforms based on CBDCs	Creation of new market opportunities, development of the digital economy

Digitalization (Internet Banking)	Enhanced accessibility and convenience	Mobile banking applications	Remote financial management, 24/7 account access
	Reduction of operational costs	Migration of banking services online	Lower physical infrastructure costs, increased efficiency
	Improved personal financial management	Online budgeting and investment tools	Enhanced financial education, informed financial decisions
Digitalization (Banking Products and Services)	Portfolio diversification	Online investment platforms	Financial products tailored to modern needs, increased flexibility
	Innovation in financial product offerings	Online savings accounts with benefits	Competitive financial services, attraction of new clients
	Increased transparency in financial offerings	Online banking product comparison tools	Accessible product information, better consumer choices
Risk Management Technologies	Improved risk assessment and management	Predictive analytics based on big data	Early risk identification, personalized mitigation strategies
	Effective compliance	Automated regulatory reporting platforms	Lower compliance costs, rapid adaptation to new regulations
	Optimization of due diligence processes	Automated customer verification systems	Faster onboarding processes, reduced fraud risks

Source: processing after Publication CAFR Articol 9718 (2020)

4. Challenges and risks

One of the main concerns regarding the integration of artificial intelligence in the financial sector relates to ethical risks and data privacy. These technologies, while capable of personalizing services and improving efficiency, raise important questions: How do we ensure that AI use respects fundamental client rights and does not conflict with privacy principles? Recent studies highlight the necessity of implementing robust regulatory and ethical frameworks that govern data usage and ensure algorithm transparency (Bostrom & Yudkowsky, 2014).

Another challenge is the potential bias and discrimination in automated decisions made by AI systems, which could perpetuate existing inequalities or introduce new forms of discrimination. This risk requires special attention in the development and training of algorithms to ensure fairness and impartiality in financial services (Mittelstadt et al., 2016).

The extensive digitalization of the financial sector, including the rise of internet banking, the proliferation of digital financial products and services, and the expansion of online platforms, brings significant cybersecurity challenges. A crucial question in this context is: How can financial institutions effectively protect themselves against growing cyber threats while offering secure and accessible digital services? The literature indicates the necessity of continuous investments in advanced security technologies and staff training to address these risks (McKinsey & Company, 2017).

Additionally, the extensive digitalization of the financial sector raises concerns about digital exclusion. As financial services become increasingly digital, how do we ensure that they remain accessible to all clients, including those without access to digital technology or the necessary competencies to use it? This is a crucial challenge for promoting authentic and sustainable financial inclusion (World Bank Group, 2018).

5. Opportunities and Future Perspectives

Exploring opportunities and future perspectives in the context of digitalization and artificial intelligence in the financial sector reveals a landscape full of potential for innovation, growth, and sustainable development. These emerging technologies not only pave the way for significant operational efficiencies and improved customer experience but also offer unique opportunities to address long-standing structural issues within the global financial system.

Artificial intelligence (AI) is emerging as a key catalyst for transformation and innovation in the financial sector. With its ability to process and analyze massive volumes of data in a remarkably short time, AI enables an unprecedented level of personalization of financial services. This evolution raises a fundamental question: To what extent can AI transform interactions between financial institutions and their customers, offering services that address not only explicit needs but also latent consumer demands? The answer lies in the development and implementation of machine learning algorithms that, by analyzing customer behavior and financial history, can recommend products and services precisely tailored to each client's individual needs. This approach not only enhances customer satisfaction and loyalty but also optimizes financial service offerings.

Beyond service personalization, AI plays a crucial role in democratizing access to financial advisory services through robo-advisors. These automated advisors represent a revolution in providing investment and financial planning services, making them accessible to a broader audience, regardless of portfolio size or prior financial knowledge. The impact of robo-advisors on the financial market suggests a significant potential for market expansion and diversification, attracting new customer segments and promoting a culture of prudent and informed investment.

Digitalization represents another driving force in the transformation of the financial sector, fundamentally reshaping how financial services are accessed and offered. Internet banking, mobile banking applications, and online financial trading platforms have revolutionized customer experience, allowing them to access banking and investment services from anywhere, at any time. However, this omnipresence of digital financial services raises important questions regarding security and data privacy: How can financial institutions balance increased accessibility with the protection of customers' personal data in this new digital landscape?

The digitalization of banking products and services expands the portfolio of available offerings, introducing innovative financial solutions such as digital wallets, instant payments, and open banking services. This evolution not only meets the changing demands of modern consumers but also stimulates competition within the financial sector, encouraging institutions to innovate and develop more efficient and accessible financial solutions.

As the world faces challenges related to climate change and sustainability, the financial-banking sector has a unique opportunity to contribute to solutions by focusing on green finance and sustainable investments. The use of digital technologies and AI to

assess climate risks in investment portfolios and to finance projects supporting the transition to a green economy represents a paradigm shift. This direction not only aligns the financial sector with global sustainable development goals but also opens new markets and investment opportunities in clean technologies and renewable energies, redefining finance's role in promoting a sustainable future.

6. Case Study on Customer Digitalization

Over the past decade, the banking sector has undergone a radical transformation, driven by significant technological advancements and changing consumer behavior. This case study aims to explore the dynamics of adopting digital technologies and artificial intelligence within the Romanian financial banking system, with a particular focus on the use of mobile banking services. By conducting a comparative analysis of five major banks in Romania, each with distinct ownership structures and strategic visions, this study seeks to identify the factors contributing to variations in mobile banking adoption rates among these institutions. In an era where digitalization is no longer an option but a necessity, understanding these dynamics becomes essential for shaping future banking strategies and ensuring a smooth transition toward an integrated digital financial landscape. This introduction lays the foundation for an in-depth analysis that aims not only to highlight current trends in banking digitalization but also to anticipate future development directions in the context of a continuously evolving financial sector.

Bank	Ownership	Total Customers	Mobile Banking Users	Mobile Banking Adoption Rate
ING Bank	**Dutch**	**1,6 million**	**1,14 million**	**71,5%**
Banca Transilvania	**Romanian**	**2,99 million**	**1,75 million**	**58,5%**
BCR Esrte Group	**Austrian**	**2,9 million**	**1,75 million**	**60%**
Raiffeisen Bank	**Austrian**	**2,1 million**	**800.000**	**38%**
BRD Group Societe General	**French**	**2,2 million**	**624.000**	**28,3%**

Source: FinZoom.ro. (2022)

From the data presented, it is evident that ING Bank stands out with the highest mobile banking adoption rate, with 71.5% of its customers using this service. This impressive performance aligns with the bank's vision of a "Digital Destiny," indicating a strong commitment to innovation and digitalization. ING Bank's emphasis on innovative digital solutions and a seamless, intuitive user experience is a key factor explaining this penetration rate.

Banca Transilvania and BCR also exhibit solid mobile banking adoption rates, at 58.5% and 60%, respectively. These figures highlight both banks' efforts to improve customer access to digital banking services and promote a digital culture among their clients. Banca Transilvania's vision of providing added value to customers and shareholders, along with BCR's commitment to supporting community development

through financial intermediation, reflects a deep understanding of customer needs and the role of technology in meeting them.

Raiffeisen Bank and BRD, on the other hand, display the lowest adoption rates, with 38% and 28.3%, respectively. Although both banks aim to be the preferred financial ecosystem, the figures indicate challenges in attracting customers to their mobile banking platforms. These lower adoption rates can be attributed to various factors, including the effectiveness of customer awareness and digital education campaigns, as well as the user experience offered by their digital platforms.

The adoption of mobile banking in Romania is influenced by multiple factors, including the strategic vision of banks, investments in technology, and the ability to educate and attract customers to digital services. ING Bank exemplifies the success of a well-directed digitalization strategy, while the lower figures for Raiffeisen Bank and BRD highlight the need for enhanced efforts in this direction. It is essential for banks to continue innovating and investing in technology while maintaining a strong focus on the diverse needs and expectations of their customers to ensure an equitable and inclusive transition to digitalization.

7. Cyber risk assessment in the banking system

Essentially, cybercrime can be classified into two main categories: the first category includes offenses that directly target and impact digital infrastructures, such as malware attacks, viral infections, or denial-of-service (DoS) attacks. The second category encompasses crimes facilitated by the digital environment, although their objectives transcend the technological framework, exemplified by fraud, identity theft, phishing scams, cyber conflicts, or online harassment. This distinction reflects the diversity and complexity of cybercrime, according to statements from the CEO of Cyberlaws.net and a cybersecurity consultant.

1. Malware și ransomeware

Every 14 seconds, someone can fall victim to a cyberattack, as ransomware has already caused damages amounting to $11.5 billion in 2019. If a computer or system utilizing malware or malicious software is compromised, the victim is often required to pay a ransom to regain access. It is estimated that such attacks cost victims billions of dollars annually, as hackers employ sophisticated technologies to hijack an organization's database and seize all critical information for ransom.

2. Phishing attack

Phishing is widely recognized as an accessible and low-effort method to harm a target. It typically involves the distribution of malware through seemingly legitimate emails from reputable sources, granting hackers unauthorized access to victims' systems. With the expansion of services such as Dropbox, Office 365, Salesforce, and others, hackers are continuously enhancing their capabilities with increasingly sophisticated attack strategies.

3. Supply chain & Third-party attacks

A supply chain attack (also known as a third-party attack) occurs when a system gains unauthorized access to other systems through an external source. The rise of digital supply chains has created new opportunities for hackers, making these attacks increasingly prevalent. Key security concerns when working with third-party entities include software patches and updates. Many third-party applications rely on external libraries and sources

for updates. When these external resources are hacked, system updates are redirected to malicious servers, which then spread the infection to their victims.

4. Endpoint attacks

As more companies adopt cloud computing for data storage, the attack surface continues to expand. Hacking vectors have increased due to the culture of device compatibility, as SaaS providers for data services continue to grow.

5. Man-in-the-middle attack

In this type of attack, a malicious actor intercepts communication between two parties, collecting sensitive information and using it to impersonate one of the participants in order to deceive consumers.

6. (DoS) Denial of Service attack

This type of attack is executed against a network user's computer to render it inaccessible to others. The attacker overwhelms the target system with excessive traffic or requests, ultimately disrupting its functionality and causing significant operational damage.

Security scanners, Intrusion Prevention Systems (IPS), Intrusion Detection Systems (IDS), network firewalls, and security applications are some of the advanced technologies used in cybersecurity. Since most hackers exploit port 80 or 443 (SSL) for commercial transactions, many security solutions and technologies are unable to protect against application-level threats. Internal security within organizations is ensured through network firewalls, which remain vulnerable to various forms of cybercriminal attacks. The following recommendations summarize available security options along with their associated limitations.

1. Vulnerability scanners

Web application scanners are automated tools that systematically crawl through a web application and scan its web pages for application vulnerabilities. These scanners generate probe inputs and then analyze responses to identify potential security weaknesses.

2. Intrusion Prevention Systems (IPS)

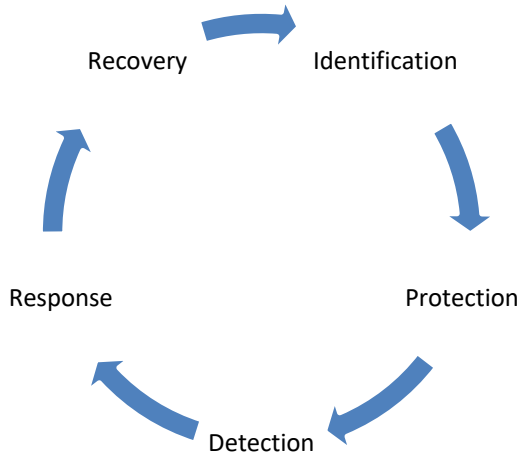
Most IPS solutions operate automatically based on predefined policies set by administrators, designed to detect and prevent unauthorized access to a company's resources or infrastructure.

3. Intrusion Detection Systems (IDS)

An Intrusion Detection System (IDS) is a hardware or software program that monitors hostile activities or policy violations within a network. A Security Information and Event Management (SIEM) system is often used to report or collect data on any harmful activity or breach. Some IDS solutions have the capability to respond to intrusions as soon as they are detected. Intrusion Prevention Systems (IPS) are designed to proactively block such threats.

4. Cybersecurity risk management framework

A common starting point for countries with specific regulatory requirements for cyber risk is the establishment of a documented cybersecurity policy or program within banks. These regulatory criteria are typically structured around key risk management categories, including governance, identification, protection, detection, response, and recovery, as illustrated in the figure below:



Source: Emerging Cyber Security Framework (2019)

• Identification: Within the meticulous identification process, it is imperative to develop a comprehensive profile that encompasses the reference-situation-threat spectrum, the risk exponent, and a detailed assessment of potential losses. This stage requires an in-depth and systematic analysis, grounded in precise data collection and interpretation, to establish an effective framework for preventing and mitigating cyber risks.

• Protection: The paradigm "It is wiser to prevent than to remedy" is of utmost importance in the field of cybersecurity. The optimal strategy involves implementing proactive measures to prevent cyber incidents before they occur. Installing high-quality security software on IT infrastructures is essential, as it serves as a robust barrier against potential attacks.

• Detection: Assessing an application's security capabilities is a fundamental pillar in the early detection of vulnerabilities and security weaknesses. Through regular and meticulous scans, the goal is to identify and promptly remediate any security breaches. Penetration testing, in particular, plays a crucial role in determining the vulnerability level of networks and physical infrastructures, providing a realistic perspective on system resilience.

• Response: Developing an incident management protocol is essential for analyzing and mitigating risks associated with IT systems or approved security policies. This process involves establishing a coordinated and efficient response mechanism that enables institutions to address and resolve security incidents in a structured manner, minimizing their impact on operations.

• Recovery: Developing recovery measures is essential for restoring functionality and business continuity following cyber incidents. This includes creating business connectivity plans at a continental level, disaster recovery plans, and internal data recovery systems. These strategies must be well-integrated to ensure a smooth transition back to normal operations, protecting the organization’s critical resources and maintaining operational continuity under maximum security conditions.

Cyberattacks have also targeted central banking institutions in New Zealand and Pakistan. Incidents involving the European Central Bank have manifested through data integrity breaches (as seen in the United States and Italy) or disruptions to commercial activities (such as in Russia and Azerbaijan). However, in the United States, a significant proportion of these intrusions had a fraudulent nature, resulting in financial losses estimated at $117 million, as presented in Table 1.

Table 1: Cyberattacks on global central banks

Institution	Year of attack	Attack Type	Details
Reserve Bank of New Zealand	**2021**	**Data breach**	**The actors gained unauthorized access to the bank's data using one of its third-party file-sharing services.**
South African Bank	**2020**	**Data breach**	**A person posing as a credit officer sold the personal information of 200,000 customers to third-parties.**
Hungarian Banks	**2020**	**DDoS**	**A large DDoS attack carried out from computer servers in Russia, China, and Vietnam disrupted service.**
CIH Bank	**2020**	**Theft**	**Hacking into customer accounts resulting in unauthorized transactions.**
SberBank of Russia	**2019**	**Data breach**	**60 million customer credit card details leaked.**
Bank Islami in Pakistan	**2018**	**Data breach**	**A cyber attack on the international payment network was detected, causing a system shutdown and losses of Rs 2.6 million.**
Bank of Italy	**2017**	**Fraud**	**Hacking of former CEOs' email accounts**

Bank of Russia	**2016**	**Fraud**	**The bank suffered a loss of $22 million from 21 cyberattacks and $50 million from correspondent banks.**
Central Bank of Azerbaijan	**2015**	**Data breach**	**Theft of thousands of bank customer information**
ECB	**2014**	**Data breach**	**20,000 email addresses and contact information compromised.**
Banco Central del Ecuador	**2013**	**Fraud**	**The city of Riobamba's account at the national bank was robbed of US$13.3 million.**

Source: News & Carnegie Endowment for International Peace (2022)

Cyberattacks are more likely to include fraud and data breaches, but they can also cause significant business disruption. Fraud accounts for 43% of events recorded in the ORX News dataset, followed by data breaches (34%) and outages (23%). While a business disruption is immediately apparent, other forms of cyberattacks may take months or years to be discovered and reported, resulting in a bias in the dataset.

As recently demonstrated by a robbery involving the SWIFT system, cyberattacks can be used for fraudulent purposes (Table 2). Cybercriminals can gain access to personal information, such as customers' online payment details. Cyber-related fraud accounted for 90% of the losses reported in the sample.

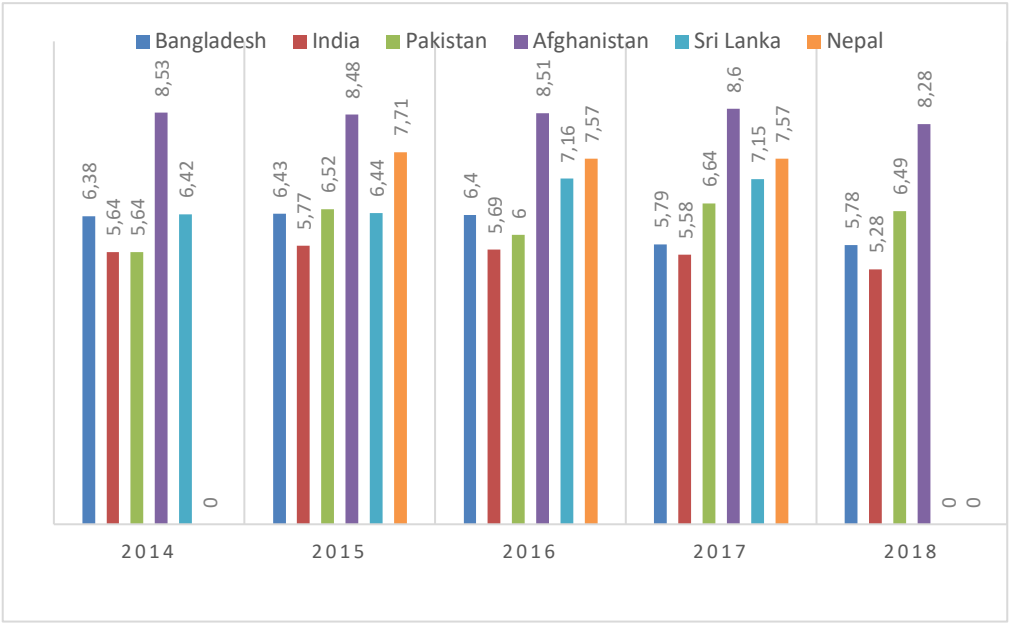
Table 2: Cases of cyber attacks via SWIFT Network

Institution	Date of attack	Initial loss (million dollars)	Current Estimated Loss (million dollars)
Union Bank of India	February, 2015	**12.2**	**9.4**
TP Bank (Vietnam)	May, 2016	**1**	**0**
Bangladesh Centeral Bank	February, 2018	**171**	**0**
Akbank (Turkey)	December, 2016	**4**	**4**
Globex (Russia)	December, 2016	**1**	**0.1**
NIC Ais Bank (Nepal)	October 2017	**4.4**	**0.6**

City Union Bank (India)	January 2018	**2**	**-**
Far Easter International Bank	October 2017	**60**	**0.5**
Banco del Austro(Eucador)	January 2015	**12.1**	**9.4**

Source: ORX News, Financial Times. (2021)

The Basel AML Index reveals that the overall risk score is determined as a weighted average of 14 indicators related to regulations, AML/CFT operations, financial standards, political disclosure, and the rule of law. Data sources used by the Basel Institute include the Financial Action Task Force (FATF), Transparency International, the World Bank, and the World Economic Forum. Rather than analyzing currency volume or illegal exchanges, the index illustrates a country's vulnerability in this way.



Source: Cost of Cybercrime Study in Financial Services Report (2019)

The figure above shows that Bangladesh ranks fifth on the AML list among six South Asian countries, surpassing India over the past five years. The 2018 Basel AML Index was based on a study of 129 countries identified as high-risk for money laundering and terrorist financing. In 2018, Bangladesh was ranked with a score of 5.78 (51st place), while India had the same score of 5.78 but was ranked 68th. Since its inclusion in the Basel AML records, Afghanistan has held the highest risk score. On the other hand, India has

consistently recorded the lowest risk score among the six mentioned countries over the past five years. Compared to 2016, Bangladesh's score steadily declined in both 2017 and 2018. Ultimately, all companies should implement a cyber risk control policy, as projected for 2023 in the table above.

8. Cybersecurity Challenges in the Financial-Banking Sector

Cybersecurity in the financial sector faces increasingly complex challenges, highlighted by the alarming 600% increase in cyberattacks over the past four years, according to Bogdan Patru, Director of Government Engagement at Mastercard, during a specialized forum organized by Financial Intelligence. This alarming situation, with estimated financial damages of $6 trillion in 2022, places the financial sector at the center of cybercriminals' targets, a concerning reality for financial institutions and service users alike.

The digital transformation, accelerated by the pandemic, has fundamentally changed the way we interact and conduct financial transactions. Platforms such as Ghiseul.ro, which has doubled its user base annually, and the expansion of e-commerce reflect this transition towards a virtual space where mobile devices have become essential tools. This shift in consumer behavior enriches the digital ecosystem with vast amounts of data and financial resources, inevitably attracting the attention of malicious actors.

Technological innovation, driven by advancements in artificial intelligence, machine learning, and quantum computing, provides valuable tools for fraud detection and prevention. These technologies can identify fraudulent behaviors before they cause harm through an effective early warning process. However, as security mechanisms become more advanced, cybercriminals also refine their methods, employing techniques such as deepfake manipulation to deceive and exploit victims.

Current legislation struggles to keep up with the rapid evolution of technological innovation. While Romania ranks relatively well compared to other EU member states in terms of regulatory implementation speed and technological adoption, it is clear that no legislative framework can be entirely foolproof in cybersecurity. This underscores the importance of public education and awareness of cybersecurity, a collective responsibility that extends beyond institutional boundaries.

Regarding financial fraud, data from the National Bank of Romania indicates a declining trend in such incidents, with most initially reported fraud cases ultimately being identified as unintentional or mistaken uses of financial instruments. This once again highlights the crucial role of the human factor in the fight against fraud and cyberattacks, emphasizing the need for increased attention to digital security education and awareness.

Awareness efforts and collaboration between the public and private sectors, exemplified through information campaigns and the active exchange of best practices, are essential strategies for strengthening cybersecurity. Initiatives such as those of the Romanian Banking Association, which promotes online security in partnership with state authorities, serve as positive examples of such collaboration.

Thus, in the face of an exponential increase in cyberattacks and a continuously evolving technological landscape, the financial sector must balance innovation with the implementation of robust security measures and the promotion of a cybersecurity culture among its users. This multidimensional approach is essential for successfully navigating current challenges and ensuring a secure financial environment that fosters trust in the technology shaping the future of financial services.

9. Conclusions

The general conclusion regarding the impact of digital technologies and artificial intelligence (AI) within the financial banking system reveals a dynamic and profoundly transformative landscape, offering both significant opportunities for economic growth and essential challenges to the traditional model of human interaction in financial services.

Technological advancements, particularly the proliferation of AI and the expansion of digitization, provide financial institutions with unprecedented tools to optimize processes, enhance operational efficiency, and personalize the services offered to clients. From advanced machine learning algorithms that facilitate real-time fraud detection and prevention, to internet and mobile banking platforms that enable unrestricted access to financial services, technology has fundamentally reshaped the ways in which financial services are designed, offered, and consumed. In this context, it is estimated that the adoption of emerging technologies could generate significant financial growth for the banking and financial sector, contributing to global economic expansion over the next 5-10 years.

However, despite technological progress and its economic potential, it remains essential to acknowledge that society is not yet ready to rely exclusively on digital interactions, especially in such a sensitive and personal field as finance. While digitization facilitates access to financial services for a wide range of clients, it does not equally reach all age groups and demographics. In particular, individuals from older segments or with limited access to technology may often find themselves marginalized by the rapid digital transition. This highlights the importance of maintaining a balance between innovation and human accessibility in providing financial services.

Consequently, maintaining bank branches and face-to-face interactions remains crucial in the next 5-10 years, not only as a means of ensuring financial inclusion for all population segments but also to preserve the human element of interaction, which is often essential in building trust and understanding between clients and financial institutions. It is imperative that, in the journey towards digitalization and automation, the financial sector does not underestimate the value of human relationships and ensures that technological progress goes hand in hand with ethical principles, sustainability, and social equity.

References:

Arner, D. W., Barberis, J., & Buckley, R. P. (2015). The evolution of Fintech: A new post-crisis paradigm. *Geo. J. Int'l L.*, 47, 1271.

Auer, R., & Böhme, R. (2020). The technology of retail central bank digital currency. *BIS Quarterly Review*, March.

Buchanan, B. G. (2019). Artificial intelligence in finance.

Bouveret, A. (2018). Cyber risk for the financial sector: A framework for quantitative assessment. International Monetary Fund.

Bostrom, N., & Yudkowsky, E. (2018). The ethics of artificial intelligence. In Artificial intelligence safety and security (pp. 57-69). Chapman and Hall/CRC.

Catalini, C., & Gans, J. S. (2020). Some simple economics of the blockchain. Communications of the ACM, 63(7), 80-90.

Crisanto, J. C., & Prenio, J. (2017). Regulatory approaches to enhance banks' cyber-security frameworks. Bank for International Settlements, Financial Stability Institute.

Joveda, N., Khan, M. T., Pathak, A., & Chattogram, B. (2019). Cyber laundering: a threat

to banking industries in Bangladesh: in quest of effective legal framework and cyber security of financial information. *International Journal of Economics and Finance*, 11(10), 54-65.

McKinsey & Company. (2017). Strengthening Institutional Cybersecurity: An Overview of Regulatory Guidance for Financial Services.

Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. *Big Data & Society*, 3(2), 2053951716679679.

Philippon, T. (2019). The Finſech Opportunity. The Disruptive Impact of FinTech on Retirement Systems, 190.

Razzaq, A., Hur, A., Ahmad, H. F., & Masood, M. (2013, March). Cyber security: Threats, reasons, challenges, methodologies and state of the art solutions for industrial applications. In 2013 IEEE Eleventh International Symposium on Autonomous Decentralized Systems (ISADS) (pp. 1-6). IEEE.

Spulbăr, A.C., & Spulbăr L.F. (2022). Considerații prinvind monedele digitale emise de băncile centrale. Revistă de cercetare ştiinţifică a studenţilor economişti, Nr. 18/2022

Spulbar, L.F., & Mitrache L.A. (2023). Developments and Perspectives of Central Bank Digital Currencies: A Comprehensive Analysis of Blockchain and Distributed Ledger Technology. The Young Economists Journal, 41, November 2023.

World Bank Group. (2018). Financial Inclusion on the Rise, But Gaps Remain, Global Findex Database Shows

https.//www.revista.cafr.ro/temp/Articol_9718.pdf /

https://www.finzoom.ro/articole/altele/internet-banking/

https://norsit.ro/3-atacuri-cibernetice-care-vor-afecta-companiile-in-anul-2023

Article Info

Received: March 24 2025
Accepted: May 20 2025

How to cite this article:
Smarandescu, A. (2025). How Artificial Intelligence is Rewriting the Rules of the Game in the Financial Banking Industry. Opportunities, Perspectives, and Challenges for the Future of Banking Activities. *Revista de Științe Politice. Revue des Sciences Politiques,* no. 86, pp. 258 – 273.