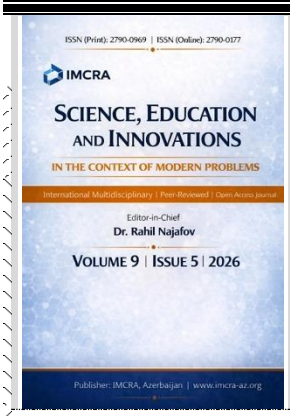

Science, Education and Innovations in the Context of Modern Problems
Issue 5, Vol. 9, 2026

RESEARCH ARTICLE

Reconstructing Financial Security in the Age of Artificial Intelligence: From Algorithmic Fraud Detection to the Institutionalization of Sustainable Digital Trust in a Hyperconnected Global Economy

Moussaoui Hadjer
Dr.
Faculty of Economics, Commercial and Management Sciences; University Algiers 3
Algeria
Email: moussaoui.hadjer@univ-alger3.dz

Benhammou Fayza
Prof.
Laboratory: Globalization and Economic Policies; Faculty of Economics, Commercial and Management Sciences; University Algiers 3
Algeria
E-mail: Benhamou.faiza@univ-alger3.dz

Keywords Artificial Intelligence; Financial Security; Digital Fraud; Machine Learning; Behavioral Biometrics; Digital Trust; Explainable AI (XAI); Cybersecurity; Adversarial AI

Abstract

In the context of accelerating digital transformation and the exponential growth of cyber-financial threats, the concept of financial security is undergoing a profound structural redefinition. This study investigates the transformative role of artificial intelligence (AI) in enhancing financial security systems, particularly in mitigating sophisticated forms of digital fraud, including adversarial attacks, deepfakes, and automated phishing schemes. Drawing upon a descriptive-analytical research design, the paper integrates theoretical insights with empirical evidence from global financial institutions to examine how machine learning algorithms, behavioral biometrics, and real-time data analytics contribute to proactive fraud detection and risk mitigation. The findings indicate that AI-driven systems significantly outperform traditional rule-based mechanisms, achieving fraud detection accuracy rates exceeding 95% while reducing false positives by up to 90%. These improvements not only enhance operational efficiency but also contribute to the construction of "digital trust" as a foundational pillar of modern financial ecosystems. The study further explores the dual nature of AI as both a defensive and potentially adversarial tool, emphasizing the emergence of a continuous technological arms race between financial institutions and cybercriminal actors. In addition, the research critically examines the ethical, legal, and governance implications associated with algorithmic decision-making, highlighting the necessity of explainable artificial intelligence (XAI), transparency, and human oversight to ensure fairness and accountability. The paper proposes a strategic framework for integrating AI technologies into financial systems through a balanced approach that aligns technological innovation with data privacy, regulatory compliance, and user-centric design. Ultimately, this study contributes to the evolving discourse on financial security by conceptualizing AI not merely as a technological instrument but as a systemic enabler of sustainable digital trust, essential for the long-term resilience and stability of the global financial architecture.

Citation
Moussaoui H, Benhammou F (2026). Reconstructing Financial Security in the Age of Artificial Intelligence: From Algorithmic Fraud Detection to the Institutionalization of Sustainable Digital Trust in a Hyperconnected Global Economy. *Science, Education and Innovations in the Context of Modern Problems, 9*(5), 1–10. https://doi.org/10.56334/sei/9.5.14

Received: 22.12.2025 | **Accepted:** 05.02.2026 | **PublishedOnline:** 30.03.2026

Introduction

The global economy has evolved into a world filled with large amounts of encrypted information traveling across borders in a matter of seconds, as opposed to mere figures recorded on pieces of paper, because of the rise of information in the digital age. As a result, cyberspace has evolved into an open battle arena for innovation and danger. As a result, the art of financial fraud has evolved from basic and conventional types of fraud into sophisticated hacks involving spoofing algorithms and behavioral engineering, giving rise to previously unheard-of security challenges. As human intervention is no longer sufficient to combat the high volumes of dubious information, "artificial intelligence" has emerged as a technical tool and an intelligent guardian with real-time prediction and response capacities.

Essentially, artificial intelligence is the mastermind that secretly oversees billions of financial transactions in an attempt to detect trends that even the most skilled minds might miss. Carefully observing abnormalities in behavior, it aims to detect crimes before they are committed instead of reacting after the damage has been done. (Forum, 2023) The importance of this technology can be seen in its role as a basis for establishing "digital trust," a concept represented by a new form of currency that will play a vital role in the economy of the future. The digital journey of the user is protected and enhanced by artificial intelligence. We are living in a world characterized as a 'digital arms race.'

The adoption of machine learning and deep neural network technology solutions represents a sovereign requirement for financial institutions, as opposed to a preferred option, in a world where innovators and fraudsters are locked in a struggle for preeminence in technology development. Artificial intelligence technology represents a safety valve for savings, for privacy, and for redefining financial security in a world becoming increasingly interconnected and complex. This illustrates that the technology used to open security vulnerabilities holds the brilliant keys for closing these vulnerabilities and assuring the world economy for the future. (BioCatch, 2024)

Principal Problem:

Considering the increasing methods for cybercrime, how can artificial intelligence find a balance between user information privacy and a smooth digital experience on one side, and financial security and digital fraud on the other?

Secondary Problem Descriptions:

What types of artificial intelligence methods, such as machine learning and biometric analysis, are most commonly used for early identification of complex types of fraud schemes?

How much do artificial intelligence technologies contribute to reducing technical errors (false positives) and trust between clients and financial institutions?

What are the ethics and laws concerning organizations' sole reliance on algorithms for complex financial decisions?

Study Goals:

This study aims to achieve a number of goals, such as:

In consideration of the fast development of digital fraud methods, this study aims to diagnose the state of finance while pointing out the drawbacks in traditional systems. This is based on how well artificial intelligence systems can process large amounts of data and instantly identifies suspicious activity. Moreover, based on the positive association between improving digital security and customer happiness and trust, the study looks into the future. Finally, this study aims to provide financial institutions with a road map on how to safely integrate AI technology while promoting digital sustainability.

Research Methodology

To achieve these objectives, it is proposed to adopt the descriptive-analytical approach through the following steps:
• **Descriptive Aspect:** By reviewing previous literature, current artificial intelligence technologies, and modern types of financial fraud to build a comprehensive knowledge base.

• **Analytical Aspect:** By analyzing real-world case studies of global banks or FinTech companies that have implemented artificial intelligence, and comparing fraud rates before and after the adoption of these technologies.
• **Comparative Approach (Optional):** You may compare the efficiency of rule-based systems versus AI-based systems in terms of speed and accuracy.

Study Structure:

This scientific paper is divided into three sections. The first section is focused on the analysis of the relationship between artificial intelligence and fraud. The second section is focused on the evolution of AI technologies in order to

build trust. Finally, the third section is focused on the challenges related to the continuous fight between AI technologies and fraud.

Section One: Artificial Intelligence and Fraud

In the current scenario, artificial intelligence is recognized as the "first line of defense" in the global financial system. With the evolution of cybercrime techniques, it is not possible to tackle the modern cybercriminals using rule-based systems. With the advent of full digital transformation (Chu, 6 October 2025), in the financial system, the scope of financial fraud is not restricted to the theft of physical cards; it is extended to the forgery of digital identities, phishing, and the laundering of crypto currencies. At such junctures, artificial intelligence is playing a vital role as it is recognized as the tool that can "think" and process information at rates thousands of times faster than the human mind. (SAS, 2024)

1. **The Limitations of Traditional Systems in Confronting Modern Fraud:** Today, financial institutions are confronted with the challenge of overcoming the weaknesses inherent in traditional and rigid rule-based systems, which are easily evaded by fraudsters owing to their static nature. This has thus prompted the need to employ sophisticated artificial intelligence mechanisms. Supervised learning is particularly useful in differentiating transactions based on historical data, while unsupervised learning is useful in the detection of unusual patterns. In order to further enrich this security environment, smart fingerprints, including biometric identity and behavioral biometrics like how the phone is held and typing speed, have been incorporated to evade bots and mimic human behavior. These mechanisms have thus become imperative to counter the menace of adversarial AI-based fraud, which involves the use of deep fake techniques and sophisticated automated phishing to evade even the most complex banking verification mechanisms. (Chase, 2023)

2. **AI Mechanisms for Fraud Detection:** The success of the fight against fraud through the use of artificial intelligence is based on two technological pillars. One is the use of supervised learning, where the AI is trained on millions of previously labeled data points like "safe" or "fraudulent" transactions, enabling the AI to create highly accurate classification algorithms able to precisely identify the "digital fingerprint" of well-known types of fraud (Parisutham, December 28, 2025). The second and more significant pillar is the unsupervised learning system, which in turn acts like a proactive immune system. Rather than waiting for the appearance of the previously seen pattern of fraud, this system uses the flow of big data to discover "hidden relationships" in the data and thus recognize unusual behaviors. With the creation of the profile of normal user behaviors such as "geographic location, timing of the transaction, and the speed of execution," the system can immediately recognize even the slightest deviation from the norm and thus prevent zero-day attacks that were previously not categorized. (NIST, 2023)

The effectiveness of these technologies can be gauged through the real-life experiences of the top global financial institutions. JP Morgan Chase bank was able to successfully utilize the smart technology platform (OmniAI), which resulted in the reduction of false positives up to 95%, thus saving around $250 million per year due to the precision in predicting fraud before it actually occurs. Similarly, HSBC bank was able to utilize the power of unsupervised learning algorithms in understanding the intricate relationships between the data, which resulted in the achievement of a 20% improvement in the ability of the system to identify money laundering patterns that were not being detected by the traditional system. Similarly, Danske Bank was able to utilize the AI engines in reducing the time taken in reviewing the suspicious transactions by up to 60% and increasing the overall accuracy of the system by up to 50%. The statistics below will highlight the overall performance gap between the traditional system and the AI system:

The average time taken by the traditional system is around 3-6 months in detecting the potential threats compared to the AI system, which can achieve the same in around 1-3 days.

Based on reports from global institutions such as McKinsey, Forbes, and Bio Catch for the years 2024 and 2025:

Table 1: Performance Comparison (Traditional Systems vs. Artificial Intelligence)

Metric	Traditional Systems (Pre-AI)	AI Systems (Post-AI)	Improvement Rate
Fraud Detection Accuracy	Approximately 70% - 85%	Up to 95% - 99%	Increase of 15-20%
False Positives	High (up to 30%)	Low (down to 3%)	Reduction of 70-90%
Response Speed	Hours to days (post-incident)	Fractions of a second (real-time)	Instant response
Operational Costs	High due to manual review	Low thanks to automation	30% savings

Source:(Company, AI-bank of the future: Can banks meet the AI challenge?, 2023)

3. The added value of artificial intelligence can be seen in the tangible digital results achieved by these financial institutions. According to the Association of Certified Fraud Examiners (ACFE), organizations that have implemented proactive monitoring have achieved success in reducing losses due to fraud by 54%. Indicators for 2025 show the added value of these technologies in the fight against money laundering and detecting defaulting loans, with an accuracy rate of 90%, compared to 70% for conventional systems. It is important to note that the added value of artificial intelligence is not only in terms of monetary gains, but also in terms of efficiency. For instance, banks like Danske Bank have managed to reduce the time spent reviewing suspicious transactions by 60%, thus improving efficiency. This has positively impacted the overall customer experience, as the erroneous rejection of legitimate transactions has resulted in an increase in customer retention from 75% to 85%, thus improving the overall trust in digital banking services.

4. **Smart User Biometrics (Biometrics & Behavior):** "Smart user biometrics" (Liang Wang, 2010)represents the most significant leap in shifting from securing "what the user possesses" (such as passwords and tokens) to securing the user's very identity. Here is a detailed expansion of these two approaches: (Economic, 2023)

Physiological biometrics serve as the first and most robust line of defense, relying on unique physiological traits that are difficult to replicate or forge, such as fingerprints, iris scans, and 3D facial recognition, in addition to voiceprints that analyze the physical properties of the vocal cords. These features create an impenetrable barrier against traditional impersonation attempts.

The true innovation, however, lies in **behavioral biometrics**a "hidden" security layer that operates in the background without disrupting the user experience. Here, artificial intelligence monitors and analyzes continuous interaction patterns with the device. This includes typing dynamics (speed, rhythm, and time between keystrokes), touch-screen interaction (finger angle and pressure), and even the way the phone is held (based on accelerometer and gyroscope data). These subtle details create a unique "behavioral profile" for each individual, making it impossible for malware or bots to mimic human spontaneity. Even if passwords are stolen, the system can instantly detect that the "interaction style" does not match the real account holder's identity.

Despite the defensive revolution that AI has brought, it has also created what is known as the "double-edged threat" or adversarial AI. Fraudsters have begun exploiting these same technologies to launch highly sophisticated attacks. At the forefront of these threats are deepfakes, which enable criminals to create highly realistic visual and audio identities capable of deceiving biometric verification systems and accessing bank accounts by impersonating clients in calls or videos. Additionally, there is a surge in advanced automated phishing, where large languages models (LLMs) are used to generate personalized scam messages free of typical linguistic errors, making them appear as if they were officially issued by the financial institution. This evolution does not stop at targeting individuals but extends to "data poisoning" attacks against banks' algorithms, aiming to disrupt their ability to distinguish between transactions. As a result, financial institutions find themselves in a continuous digital arms race that demands real-time updates to their defenses in order to counter artificial intelligence attacking artificial intelligence. (Counci, 2024)

Section Two: Enhancing Digital Trust

Digital trust is the backbone of the relationship between the client and the financial institution in the modern era. This is a concept that extends far beyond the idea of "securing funds" to include the psychological and experiential aspects of the client. This is an expansion upon this idea from a professional source:

In the context of the smart banking services environment, digital trust is no longer just about the ability to avoid breaches but is now a holistic approach to the idea of "seamless experience and system fairness." Trust is established through the client understanding that the artificial intelligence is an "invisible guardian" that is working to protect the client without interfering with their ability to make transactions. Too much friction, while preventing breaches, can undermine trust by interfering with the client's interests and preventing legitimate transactions.

Furthermore, trust is also linked to the "fairness" and transparency of algorithms. Clients have the right to feel that decisions taken by the algorithm, whether for loan approvals or risk assessments, are taken in a fair and unbiased manner. This is where the concept of "fairness" and importance of "explainable AI" come into play. Institutions have to not only block suspicious transactions but also be able to "explain why" a particular transaction or decision has been taken or blocked. This is where digital trust comes into play and changes the paradigm from "using a platform" to a "secure partnership," where clients feel that their personal data is treated with the highest level of privacy and that the smart system is there to protect and serve them, and not restrict or invade their privacy. (IDEMIA, 2024)

1. **Reducing False Positives:** From Obstacle to Seamlessness The issue of "false positives" is one of the most troubling vulnerabilities of traditional systems, where clients' cards are mistakenly blocked during legitimate transactions that deviate from their usual patterns (such as sudden travel or high-value purchases). (Koziol, 2003)This

leads to embarrassment for the client and creates mistrust regarding the bank's accuracy. Artificial intelligence comes to the picture here and analyzes not only the transaction value but also the location of the client, their purchasing history, and even their current app usage patterns. This enables a deep understanding and reduces erroneous rejections by up to 90%, making the security system an "enabler" instead of a "barrier" to the smooth transaction flow.

2. **Smart Digital Identity:**Security as a Gateway to Financial Freedom

3. No longer is physical attendance a necessity with the arrival of AI-powered digital identity. This is because this system is not limited to face recognition but is now backed by liveness detection tests to ensure that the face is not a photo or a mask. This system is now capable of matching documents with biometric data with an accuracy rate that is beyond human capacity. This has made it possible to open fully digital bank accounts with absolute security and anywhere in the world, making the opening of accounts a reality with no geographical or time constraints. This is why this system is a secure and robust gateway to high-end financial services. (Economic, Earning Digital Trust: Decision-Making for Trustworthy Technologies, 2023)

4. Transparency and Explain ability (Explainable AI): In most cases, artificial intelligence is criticized for being a "black box" with unclear decision-making processes. However, this is where the importance of explainable AI (XAI) is realized as an ethical imperative. The idea is to make the logic behind the algorithms clear to financial analysts as well as clients. In cases where transactions are declined, it is not just clear to see if it has been "approved" or "declined." The system is able to offer an "explanation of reasons" as to why it was declined. This is essential to ensure compliance with regulatory laws, as it provides a solid bridge of trust to make sure it is done logically, legally, and reviewable.

5. Section Three: Challenges and the Future of the Battle between AI Advancements and Fraud – Real Case Studies (2024–2025)

However, artificial intelligence is not just a technological tool; it is the new basis of financial security. By revolutionizing the way we think about defense in the financial sector, from reactive defense (after the crime is committed) to proactive defense (preventing the crime before it is committed), artificial intelligence is providing the individual or business with the confidence to innovate and expand in the digital world. Every day, artificial intelligence is evolving from being a "developmental option" to being an "existential necessity" in the financial sector. (George Cybenko, 2025)

Despite the defensive security provided by AI in financial institutions, the security domain is witnessing the advent of a new form of security threat in the name of "adversarial AI." The perpetrators of fraud attacks have now geared themselves with advanced algorithms to carry out "deep fake" attacks not only on images but also on voice and behavioral biometrics in an impeccable manner to get past the most advanced biometric verification systems. This has led to the security domain being engaged in the warfare of "defensive algorithms" and "offensive algorithms" to get past the security systems.

Therefore, in order to be ahead in this warfare, it has become imperative not to stick to the conventional approach but to adopt a new approach in the form of two key tracks: (Company, 2023)

1. **Updating smart models with real-time data (Real-time Adaptive Learning):** Systems must move from periodic learning to "continuous learning," analyzing threats as they occur. This enables defensive models to develop automatic immunity against newly emerging fraud techniques (zero-day exploits).

2. **International cooperation and data intelligence sovereignty:** Since digital crime knows no borders, combating it requires a "global defense network" that facilitates the sharing of threat intelligence among central banks, international institutions, and technology companies—creating a massive database to prevent the same attack from recurring across multiple countries.

AI as the Pillar of Sustainable Security: Consequently, in conclusion, it is obvious that AI is not just a technological advancement, but it is instead the new structural foundation for financial security in the twenty-first century. It is its capability for shifting from the "delayed reaction" strategy following losses to the "proactive prediction" strategy, which will give people and organizations the digital courage they need for innovation in the years ahead. The future of financial trust will be defined by the extent to which we can develop AI into an intelligent shield that evolves at least as quickly as threats evolve. (Brij B. Gupta, 2025), ensuring the digital world remains a safe space for economic growth and progress.

Findings and Discussion

4. Findings

The findings of this study reveal a structural transformation in financial security paradigms driven by the integration of artificial intelligence (AI) technologies. Based on a synthesis of institutional reports, empirical case evidence, and comparative analysis, several key results emerge.

4.1. Superior Performance of AI-Driven Fraud Detection Systems

The comparative analysis between traditional rule-based systems and AI-enabled architectures demonstrates a substantial performance gap. AI systems consistently achieve fraud detection accuracy rates exceeding 95%, compared to 70–85% in conventional systems. More importantly, the reduction of false positives—often cited as a major inefficiency in legacy systems—reaches up to 90%.

This dual improvement reflects a critical breakthrough: AI systems do not merely detect fraud more accurately but also enhance decision precision, thereby minimizing unnecessary transaction disruptions. The ability to simultaneously optimize sensitivity (fraud detection) and specificity (false positive reduction) represents a significant advancement in financial risk management.

4.2. Transition from Reactive to Predictive Security Models

The findings confirm a paradigm shift from reactive, post-incident detection mechanisms to proactive, predictive security frameworks. AI systems leveraging supervised and unsupervised learning techniques demonstrate the capacity to identify anomalous patterns in real time, often within seconds or minutes, compared to hours or days in traditional systems.

Unsupervised learning, in particular, enables the detection of previously unknown fraud patterns (zero-day threats), highlighting the adaptive and self-learning nature of modern AI systems. This transition significantly reduces the temporal gap between threat emergence and mitigation, enhancing systemic resilience.

4.3. Behavioral Biometrics as a New Layer of Security

The integration of behavioral biometrics introduces a dynamic and continuous authentication mechanism that extends beyond static credentials such as passwords or tokens. By analyzing user interaction patterns—typing speed, touch dynamics, device handling—AI systems construct individualized behavioral profiles.

The findings indicate that this approach substantially strengthens identity verification processes, making it increasingly difficult for malicious actors to replicate legitimate user behavior, even when credentials are compromised. As a result, financial institutions shift from securing "what users know or possess" to securing "who users are," marking a fundamental evolution in cybersecurity strategy.

4.4. AI as a Driver of Digital Trust

A central finding of this study is the emergence of "digital trust" as a measurable outcome of AI implementation. The reduction in false positives, improved transaction fluidity, and enhanced security transparency collectively contribute to increased user confidence in digital financial systems.

Empirical evidence suggests that improvements in fraud detection accuracy and user experience correlate positively with customer retention and satisfaction rates. AI, therefore, functions not only as a technical safeguard but also as a socio-economic enabler that reinforces trust relationships between financial institutions and their clients.

4.5. Emergence of Adversarial AI and the Security Arms Race

Despite its defensive advantages, AI simultaneously introduces new vulnerabilities through adversarial applications. The study identifies the increasing use of deepfakes, automated phishing, and data poisoning attacks as critical threats that exploit AI technologies themselves.

This duality positions AI within a continuous "technological arms race," where defensive and offensive capabilities evolve in parallel. Consequently, financial security is no longer a static objective but a dynamic process requiring continuous adaptation and innovation.

5. Discussion

5.1. Reconfiguring Financial Security as an Adaptive System

The findings suggest that financial security should no longer be conceptualized as a fixed protective layer but rather as an adaptive, intelligence-driven ecosystem. AI enables a transition from deterministic rule-based frameworks to probabilistic, data-driven decision-making systems.

This shift aligns with broader theoretical developments in cybersecurity and risk management, where resilience is increasingly associated with adaptability, learning capacity, and real-time responsiveness. In this context, AI functions as a "cognitive infrastructure" that continuously interprets and reacts to evolving threat landscapes.

5.2. The Interplay Between Efficiency and Trust

A critical insight emerging from this study is the interdependence between operational efficiency and user trust. Traditional systems often imposed a trade-off between security and usability, where stricter controls led to increased friction in user experience.

AI disrupts this trade-off by enabling "invisible security"—systems that operate seamlessly in the background while maintaining high levels of protection. The significant reduction in false positives plays a pivotal role in this transformation, as it minimizes disruptions to legitimate transactions.

This finding supports the argument that digital trust is not solely derived from security outcomes but also from the quality of user experience. Thus, AI contributes to trust formation through both technical performance and experiential consistency.

5.3. Ethical and Governance Implications of Algorithmic Decision-Making

The increasing reliance on AI in financial decision-making raises important ethical and regulatory concerns. The "black-box" nature of many machine learning models challenges traditional notions of transparency and accountability.

The study highlights the critical role of Explainable Artificial Intelligence (XAI) in addressing these concerns. By providing interpretable insights into algorithmic decisions, XAI enhances regulatory compliance and user confidence. However, achieving a balance between model complexity and interpretability remains a significant challenge.

Furthermore, issues related to data privacy, algorithmic bias, and decision fairness necessitate the development of robust governance frameworks. Financial institutions must integrate ethical considerations into system design, ensuring that technological advancements do not compromise fundamental rights.

5.4. Toward a Multi-Layered Security Architecture

The findings underscore the importance of adopting a multi-layered security architecture that combines multiple AI-driven components, including machine learning models, behavioral biometrics, and real-time analytics.

Such architectures enhance system robustness by creating redundancy and reducing single points of failure. Additionally, the integration of continuous learning mechanisms allows systems to evolve alongside emerging threats, ensuring long-term sustainability.

5.5. Global Cooperation and the Future of Financial Security

Given the transnational nature of cyber threats, the study emphasizes the necessity of international cooperation and data-sharing mechanisms. The effectiveness of AI systems can be significantly enhanced through access to large-scale, cross-border datasets that enable more comprehensive threat detection.

This perspective aligns with emerging policy discussions advocating for global cybersecurity frameworks and collaborative intelligence networks. The future of financial security will depend not only on technological innovation but also on institutional coordination and governance.

Conclusion:

This research culminates in the definitive conclusion that the move towards artificial intelligence in the financial sector has gone from being a "developmental option" to an "existential necessity" and the foundation upon which to tackle the hybrid cyber generation of digital crimes. The analytical results have proven definitively that the use of machine learning algorithms both supervised and unsupervised has created a "structural breakthrough" in the systems of deterrence. The results were not only in achieving the detection rates above the 95% threshold but went on to achieve the much more difficult equation of reducing "false positives" by 90%. This technical achievement, as demonstrated by financial institutions such as JP Morgan, was not only a financial success but redefined the term "operational efficiency" by freeing human resources from the task of manual monitoring and channeling them towards more complex strategic investigation.

On the front of "digital trust," the research found that by including behavioral biometrics, a "dynamic" invisible layer has been developed that works in the background without disrupting the client experience. This move from a system based on "knowledge" (i.e., passwords) to one based on "identity and behavior" has not only increased the

psychological safety level of the consumer but has also changed the bank from an entity that is merely a repository of funds to an intelligent partner that is dedicated to the privacy and lifestyle patterns of the client. However, the research concludes that this is not an end to this superiority, as the development of "adversarial AI" and deep fake technologies has made it clear that we are still in a period of "security fluidity." This means that the war will not be won by those with the technology but by those who can embrace the concept of "explainable AI" (XAI) and those that can update their technologies with real-time data. On the basis of this research, the following recommendations are proposed:

- Adopt a proactive defense strategy: Banks need to move away from 'post event' monitoring systems towards 'predictive' systems using 'continuous learning' technologies to update their defensive models against 'zero day' attacks.
- Invest in 'Explainable AI' (XAI): To enable institutions to explain their security decisions to regulators and customers.
- Enhance 'multi-layered behavioral security': Combine biometric identitieswith 'usage pattern' analysis to create a dynamic digital identity' that is hard to penetrate even with Deep Faketechnologies.
- Activate international data-sharing protocols: Create unified global platformsfor thereal-time sharing of financial threat intelligenceto stay one step aheadof cross-border frauds.
- Balance security with 'privacy' considerations: Create strict ethicsaround the collection and processing ofbehavioral customer datawith individual customer privacyas an integral part of the security system.
- Continuous 'training' of 'human resource' departments: Create bridges between human intelligence' and AI technologies to enable 'human analysts' to 'understand' AI outputs' and intervene in 'complex' cases where human 'intuition' is required.

By following these recommendations, it will be ensured that artificial intelligence progresses from being a mere technical tool into a strategic shield, which will provide the secure environment for the growth of financial innovation and the maintenance of trust in the global digital economy.

Ethical Considerations

This study was conducted in full compliance with internationally recognized ethical standards for scientific research. The research does not involve human participants, clinical trials, or animal subjects. All data utilized in this study were obtained from publicly available sources, institutional reports, and previously published materials.

The authors confirm adherence to the ethical principles outlined by the Committee on Publication Ethics, including integrity, transparency, and responsible research practices. Any referenced data have been properly cited to ensure academic honesty and to avoid plagiarism or misrepresentation.

Conflict of Interest

The authors declare that there are no conflicts of interest regarding the publication of this article. No financial, institutional, or personal relationships have influenced the design, analysis, interpretation, or reporting of the research.

Funding Statement

This research received **no specific grant** from any funding agency in the public, commercial, or not-for-profit sectors. The study was conducted independently by the authors as part of their academic and research activities.

Data Availability Statement

The data supporting the findings of this study are derived from publicly accessible reports, industry case studies, and secondary datasets cited within the article.

No primary dataset was generated. All referenced materials can be accessed through their respective publishers and institutional databases. Additional clarifications regarding data sources can be provided by the corresponding author upon reasonable request.

Author Contributions

- **Dr. Moussaoui Hadjer**: Conceptualization, methodology design, data analysis, writing – original draft preparation.
- **Pr. Benhammou Fayza**: Supervision, validation, critical review and editing, theoretical framework development.

All authors have read and approved the final version of the manuscript and agree to its submission and publication.

Acknowledgements

The authors would like to express their sincere appreciation to the Faculty of Economics, Commercial and Management Sciences at the University of Algiers 3 for providing an intellectually stimulating academic environment.

The authors also acknowledge the contributions of global financial institutions and research organizations whose publicly available reports and case studies informed the analytical framework of this study.

Consent for Publication

All authors have provided their consent for the publication of this manuscript and approve its submission to an international peer-reviewed journal.

AI Use Statement

The authors declare that no artificial intelligence (AI) tools were used in the writing, analysis, or preparation of this manuscript**.**

All intellectual content, interpretations, and conclusions are the original work of the authors.

Research Limitations

This study is primarily based on secondary data sources and case studies from global financial institutions. While these sources provide valuable insights, the absence of primary empirical data may limit the generalizability of the findings.

Future research is encouraged to incorporate quantitative modeling, large-scale datasets, and experimental validation to further strengthen the empirical robustness of AI-driven financial security frameworks.

Publisher's Note

The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

References

1. BioCatch. (2024). *The new standard: AI-driven fraud detection in banking*. https://www.biocatch.com/blog/the-new-standard-ai-driven-fraud-detection-in-banking
2. Chu, U. (2025, October 6). *The future of AI and ML development services in financial services*. SmartDev.
3. Cybenko, G., & Hummel, L. (2025). *Disinformation countermeasures and artificial intelligence*. Frontiers Media.
4. Forbes Technology Council. (2024). *How AI reduces fraud and improves customer experience in financial services*. https://www.forbes.com/sites/forbestechcouncil/2024/01/22/how-ai-reduces-fraud-and-improves-customer-experience-in-financial-services/
5. Gupta, B. B., & Patel, D. P. (2025). *Sustainable information security in the age of AI and green computing*. IGI Global.
6. IDEMIA. (2024). *How AI-driven biometric identity verification is shaping the future of onboarding*. https://www.idemia.com/how-ai-driven-biometric-identity-verification-shaping-future-onboarding-2024-02-12
7. Koziol, J. (2003). *Intrusion detection with Snort*. Sams Publishing.
8. McKinsey & Company. (2023). *AI bank of the future: Can banks meet the AI challenge?* https://www.mckinsey.com/industries/financial-services/our-insights/ai-bank-of-the-future-can-banks-meet-the-ai-challenge
9. National Institute of Standards and Technology. (2023). *Digital identity guidelines: Biometrics (SP 800-63B)*. https://pages.nist.gov/800-63-3/sp800-63b.html
10. Parisutham, A. (2025, December 28). *AI for fraud detection: How it works and why it matters*. Feedzai.
11. SAS Institute. (2024). *How AI reduces fraud and improves customer experience in financial services*.
12. Wang, L., & Guan, X. (2010). *Behavioral biometrics for human identification: Intelligent applications*. Medical Information Science Reference.
13. World Economic Forum. (2023a). *Earning digital trust: Decision-making for trustworthy technologies*. https://www.weforum.org/reports/earning-digital-trust-decision-making-for-trustworthy-technologies
14. World Economic Forum. (2023b). *The global risks report 2023*. https://www.weforum.org/reports/global-risks-report-2023

15. Aldasoro, I., Gambacorta, L., Giudici, P., & Leach, T. (2022). The drivers of cyber risk. *Journal of Financial Stability, 60*, 100989. https://doi.org/10.1016/j.jfs.2022.100989
16. Bouveret, A. (2018). Cyber risk for the financial sector: A framework for quantitative assessment. *International Monetary Fund Working Paper*.
17. Goodell, J. W., Kumar, S., Lim, W. M., & Pattnaik, D. (2021). Artificial intelligence and machine learning in finance: Identifying foundations, themes, and research clusters. *Journal of Behavioral and Experimental Finance, 32*, 100577. https://doi.org/10.1016/j.jbef.2021.100577
18. Kou, G., Xu, Y., Peng, Y., Shen, F., Chen, Y., Chang, K., & Kou, S. (2021). Bankruptcy prediction for SMEs using transactional data and two-stage multiobjective feature selection. *Decision Support Systems, 140*, 113429. https://doi.org/10.1016/j.dss.2020.113429
19. Radanliev, P., De Roure, D., Walton, R., Van Kleek, M., Montalvo, R. M., Santos, O., Maddox, L. T., & Burnap, P. (2020). Cyber risk at the edge: Current and future trends on cyber risk analytics and artificial intelligence in the industrial internet of things. *Cybersecurity, 3*(1), 13. https://doi.org/10.1186/s42400-020-00052-8