Journal of Information Systems Engineering and Management
2025, 10(60s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Artificial Intelligence and Financial Modernization: Navigating the Security-Innovation Paradox in Contemporary Banking Systems

Manisha Sengupta
Independent Researcher, USA

ARTICLE INFO

Received: 13 Oct 2025
Revised: 16 Oct 2025
Accepted: 23 Oct 2025

ABSTRACT

The introduction of artificial intelligence into the world of finance is a big change. It alters how banks work, how transactions are handled, and how customers are engaged. This article looks at the tricky situation between tech improvements and the need for security in today's finance. There's a strange situation where getting better tech also means facing new dangers. The progress from legacy and rule-based systems to advanced machine learning architectures has made financial institutions achieve unprecedented enhancements in fraud prevention, risk evaluation, and business processes. The advancements also introduce new attack surfaces, such as adversarial manipulation, data poisoning, and model extraction attacks that traditional security paradigms are ill-equipped to deal with. By conducting extensive evaluation of present-day deployment trends, future threats, and defensive standpoints, this article illustrates that effective AI integration also necessitates an essential reconceptualization of security paradigms. The discourse includes multi-layered defense systems with differential privacy, federated learning approach, and explainable AI methods while ensuring strategic human control. Financial institutions face upcoming challenges, particularly for cybersecurity and data privacy, due to quantum computing-led disruptions and a shifting regulatory landscape, which they should handle preemptively. This means balancing security with new ideas by constantly testing concepts, creating strong management systems, and thinking about how these changes affect society, like market dominance and protecting the environment.

Keywords: Artificial Intelligence, Financial Security, Adversarial Machine Learning, Quantum-Safe Cryptography, Explainable AI

1. Introduction

The use of AI in finance shows a major technology shift in today's banking world. As banks are globally adopting digital solutions, artificial intelligence is now central to their operations, moving beyond initial trial phases. This change could lead to big steps forward in how transactions are processed, how fraud is found, and how customers are helped. Nonetheless, the quick adoption of AI brings unprecedented security risks to standard risk handling methods.

Modern financial systems are under increasing pressure to upstage antiquated technology while ensuring strong security measures critical to safeguarding sensitive financial information. The use of adversarial machine learning methods in high-frequency trading scenarios has been shown to possess incredible ability to detect fraudulent patterns in millisecond time frames, but is still susceptible to

Journal of Information Systems Engineering and Management
2025, 10(60s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

more advanced manipulation attempts [1]. Studies into adversarial robustness within financial fraud detection systems indicate that gradient-based attacks can effectively bypass detection systems when volumes of transactions are above certain levels, especially in scenarios involving thousands of transactions per second. The use of defensive distillation and ensemble approaches has proven effective in countering such exposures, although computational cost is greatly heightened in handling high-frequency financial data streams [1].

Fintech industries that apply machine learning algorithms for fraud detection have experienced significant accuracy rate improvements over conventional rule-based systems. Despite such advancements, adversarial attacks on AI models have proven alarming success rates in evading detection mechanisms via ingeniously crafted input perturbations. The application of deep learning networks in credit risk scoring has lowered processing times by a very significant margin, while at the same time opening up vulnerabilities to model inversion attacks that can reveal training data under certain circumstances. These compound properties of increased performance and heightened vulnerability form a nuanced security environment that calls for out-of-the-box risk management strategies.

Recent deployments of AI-based cybersecurity solutions in online banking settings have both established the potential and the limits of machine-driven threat detection [2]. Natural language processing platforms are used for automating the customer service process, handling millions of requests on a monthly basis with a high rate of resolution without any human intervention. Still, these platforms continue to remain vulnerable to prompt injection attacks. Research has indicated that sampled models could be tricked to avoid security measures through specific input string combinations. The blending of behavior analytics and anomaly detection routines has improved threat recognition capabilities, especially in detecting unusual transaction patterns and takeover attempts [2]. Computational demands of keeping a secure AI infrastructure have become remarkably high, with encryption overhead and monitoring systems devoting lots of processing power on a daily basis in large deployments.

The article discusses the holistic interaction between AI-led modernization and security necessities in financial systems. Through rigorous analysis of current deployment patterns, emerging threat vectors, and defensive strategies, successful AI integration requires a fundamental reconceptualization of security frameworks that balances technological advancement with risk mitigation. The discussion encompasses technical vulnerabilities unique to AI systems, including adversarial attacks and data poisoning incidents, while proposing a multi-layered defense strategy incorporating explainable AI mechanisms, continuous validation protocols, and strategic human oversight.

Metric Category	Value/Description
Gradient-based attack success rate	Effective bypass when transactions exceed threshold levels
Processing capability	Thousands of transactions per second
Defensive distillation effectiveness	Proven mitigation with increased computational overhead
Customer service automation	Millions of queries monthly
Resolution rate without human intervention	High resolution rates achieved
Prompt injection vulnerability	Models manipulated through specific input sequences

Table 1: Security Vulnerabilities and Detection Capabilities in AI-Enabled Financial Infrastructure [1, 2]

Journal of Information Systems Engineering and Management
2025, 10(60s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

2. Theoretical Framework and Literature Review

2.1 AI Evolution in Financial Services

Theoretical foundations for AI integration in finance are derived from several fields, such as computational finance, cybersecurity theory, and studies in human-computer interaction. Conventional financial modeling based on statistical inference and rule-based systems has increasingly been replaced by machine learning algorithms that can detect intricate, non-linear patterns in huge amounts of data. Deep neural network architectures have also proved to be very effective tools for processing financial time series data, and recent applications show improved performance in capturing temporal relationships and market movements [3]. The use of Recurrent Neural Network-like long short-term memory (LSTM) networks and gated recurrent units (GRUs) in stock price forecasting and volatility prediction has brought about remarkable advancements over traditional autoregressive models, especially when applied to high-frequency trading data with non-stationary patterns and abrupt regime changes [3]. This change represents a qualitative shift from deterministic to probabilistic decision-making models, bringing with it both opportunities and weaknesses not previously examined in financial system design.

Transformer models processing financial time series data have transformed the pattern recognition abilities of market analysis tools. Current deployment of attention mechanisms in neural network designs allows for processing long temporal sequences with efficiency, solving the problems inherent in the traditional recurrent models. Graph neural networks graphing transaction networks identify subtle patterns of relationships inaccessible to efficient finding with conventional database queries. A combination of convolutional neural networks and temporal convolution layers has supported reliable feature extraction from multivariate financial data to enable better risk estimation and portfolio optimization methods.

2.2 Security Paradigms in AI-Enabled Systems

Recent security literature highlights three major categories of vulnerabilities that are relevant to AI deployments: model manipulation via adversarial inputs, corruption of training data through poisoning attacks, and model parameter-based inference attacks. Examination of adversarial attack detection mechanisms shows that explainable AI methods coupled with generative models yield robust countermeasures against pervasive fraud exploits in real-time monitoring systems [4]. The use of SHAP (Shapley Additive exPlanations) values and LIME (Local Interpretable Model-agnostic Explanations) methods allows security analysts to comprehend model decision paths, enabling quick detection of anomalous behaviors representative of adversarial manipulation [4]. In contrast to traditional cybersecurity attacks that can target system infrastructure or data stores, AI-specific attacks target learning mechanisms themselves, presenting attack surfaces that are not easily addressed by traditional security solutions.

Data poisoning can be a particularly troubling threat to AI-enabled financial applications. It involves bad actors inserting flawed data into training sets, subtly altering how the model functions in ways that typical validations might miss. Model extraction attacks also pose a grave risk to intellectual property. Competitors could essentially reverse-engineer algorithms by carefully studying public APIs, nullifying any competitive edge. Gradient-based reconstruction attacks compromise privacy in federated learning settings by potentially revealing sensitive customer data contained within model parameters. Theoretical foundations for interpreting these vulnerabilities are rooted in the field of adversarial machine learning research, showing that imperceptible perturbations induce catastrophically failed models at a disturbing rate.

2.3 Human-AI Collaboration Models

Integrating artificial intelligence into finance requires a rethinking of how people and machines work together. Traditional theoretical frameworks suggest interaction spectrums in which routine processing is left to AI systems while passing on complex or risk-heavy decisions to human analysts. Research suggests that human-in-the-loop architectures dramatically lower error rates than fully

Journal of Information Systems Engineering and Management
2025, 10(60s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

automated systems, yet provide acceptable processing velocities for high-volume transaction domains. Human-on-the-loop architectures show operational effectiveness with low intervention rates in regular operations, ramping up to higher human intervention in the occurrence of detected anomalies. Hybrid models that merge automated processing with judicious human monitoring realize the best performance metrics in terms of accuracy, response time, and reduction in false positives.

Architecture Component	Performance Characteristic
LSTM and GRU networks	Superior to autoregressive models for high-frequency data
Temporal pattern detection	Handles non-stationary patterns and regime shifts
Transformer models	Processes long temporal sequences efficiently
SHAP and LIME methods	Enables understanding of model decision paths
Anomaly detection capability	Quick identification of adversarial manipulation
Attack surface vulnerability	Learning mechanisms create new security challenges

Table 2: Performance characteristics of advanced neural networks in financial contexts [3, 4]

3. Methodology and Implementation Analysis

3.1 Current Deployment Architectures

AI systems created with machine learning tools like TensorFlow and PyTorch are used by financial institutions and generally hosted on cloud platforms like AWS SageMaker, Azure AI, and Google Vertex AI. These systems usually follow a pattern where data intake processes handle transaction flows, feature engineering converts raw data into model inputs, and inference engines create predictions. Studies that analyzed the patterns of AI deployment in financial service firms find that the adoption of artificial intelligence has a major effect on operational effectiveness and decision-making, with firms achieving significant gains in measures of service delivery and customer satisfaction upon AI integration [5]. Standardization of deployment architectures, for the benefit of speedy deployment, renders consistent attack points that are systematically exploited by malicious agents on many financial platforms. TensorFlow deployments based on distributed training across multiple GPU nodes illustrate increased processing power on large-scale financial data, where model convergence is accomplished much more rapidly compared to conventional CPU-based infrastructure. PyTorch deployments show more flexibility in building dynamic computational graphs, aiding adaptive model designs that can change based on current market situations. Cloud-native platforms use auto-scaling to allocate computing power based on transaction amounts, which lowers expenses and keeps response times steady. Employing Kubernetes for managing various model replicas within containers provides a means for A/B testing. This approach helps in assessing model performance across diverse market conditions while maintaining infrastructure stability.

3.2 Security Assessment Framework

Multi-dimensional security assessment frameworks analyze technical vulnerabilities, operating risks, and systemic threats in deployed systems. Technical vulnerabilities are realized through multi-vector attacks, with the generative AI systems bringing forth especially sophisticated security issues in financial systems [6]. The advent of advanced adversarial methods aimed at generative models creates risks unprecedented in their nature, as such models can be used to generate fake financial documents, artificial identities, and deceptive market analysis that looks real to conventional verification mechanisms [6]. Operational risks cover configuration mistakes impacting large segments of deployments, poor access controls allowing illegitimate API exploitation, and ineffective monitoring capabilities that are unable to identify odd behavior related to the incidence of continuous attacks.

Security evaluations indicate that gradient-based attacks pull model parameters with alarming fidelity by probing systematically, and black-box attacks attain huge success rates with access to the model not necessary. The growth of generative AI models in the financial ecosystem creates new attack

Journal of Information Systems Engineering and Management
2025, 10(60s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

surfaces such as prompt injection vulnerabilities, data leakage via model memorization, and the possibility of creating adversarial content that evades classic security controls. Systemic threats are cascading failures in which single-point vulnerabilities spread throughout coupled systems quickly, impacting downstream processes that process key financial transactions. Simultaneous attacks on multiple institutions at once exhibit compounded success rates over individual attempts with similar goals, utilizing common architectural patterns present in standardized layouts throughout the financial industry.

3.3 Performance Metrics and Trade-offs

Implementation analysis showcases blatant trade-offs between performance in models and security resilience within production settings. AI systems exhibit significant increases in fraud detection rates, handling much larger volumes of transactions than legacy systems, but these improvements tend to be at the expense of heightened susceptibility to highly sophisticated attacks. Banks that have adopted AI solutions report improved operational performance metrics, although security-hardened models that include privacy-preserving technologies suffer from quantifiable accuracy loss [5]. Adversarial training enhances model resilience to known attack patterns but significantly increases training time and consumes orders of magnitude more resources. Performance fluctuations underscore the indispensable necessity of ongoing model verification, with drift detection programs flagging degradation in performance and initiating automated retraining procedures that work with large volumes of historical transaction data to preserve model accuracy.

4. Risk Mitigation Strategies and Best Practices

4.1 Layered Defense Architecture

To ensure strong security in AI-based financial systems, defense mechanisms should be layered to counter threats at different levels. The base layer should include secure data pipelines with encryption, checks for integrity, and controls for access. These things protect sensitive financial data as it is being processed. Studies of multi-layered cybersecurity architectures illustrate how using end-to-end security architectures that weigh data confidentiality against financial ingenuity helps institutions harness AI-enabled analytics while remaining strong against potential threats [7]. Homomorphic encryption methods, integrated into frameworks, facilitate computation on encrypted data without revealing basic information, although computational overhead remains a key concern in high-frequency trading contexts [7]. The model layer adopts methods like differential privacy, federated learning, and adversarial training to maintain robustness against attacks while keeping data private.

Federated learning structures spread the training to edge nodes, handling local datasets without centralized exposure of sensitive data, thus keeping data breaches and compliance issues lower. Adversarial training with synthetic attack samples makes models more resilient against gradient-based attacks and other types of advanced attack channels. The application layer includes explainable AI mechanisms that allow security teams to comprehend and confirm model decisions, especially in high-risk situations such as large financial transactions or unusual patterns of activity. To safeguard financial systems managed by AI, employ defense-in-depth approaches. These strategies involve diverse, overlapping security measures to minimize the risk of a single point of failure being exploited.

4.2 Continuous Validation and Monitoring

Static security controls fall short in dynamic AI settings in which models learn and evolve increasingly from changing transaction patterns and market forces. Dynamic risk management capabilities are improved with real-time financial surveillance systems that incorporate continuous monitoring mechanisms that identify anomalies and prospective security violations as they transpire [8]. Implementation of advanced monitoring infrastructures allows financial institutions to have visibility throughout complex AI deployments, monitoring model performance metrics as well as security

Journal of Information Systems Engineering and Management
2025, 10(60s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

indicators indicative of potential compromise or degradation [8]. Continuous validation procedures are required to include both model performance metrics and security indicators, and in doing so, create robust monitoring ecosystems that defend against multiple threat vectors.

Drift detection algorithms detect when models stray from anticipated behavior patterns, indicating possible poisoning attacks or natural distribution drifts that need model retraining. Anomaly detection systems alert abnormal input patterns possibly suggesting adversarial attempts at model output manipulation, invoking automated defensive actions that quarantine suspicious transactions for human inspection. Periodic adversarial testing evaluates model resistance against established attack vectors, offering quantitative metrics of security posture that guide risk management decisions. Real-time monitoring dashboards display key security indicators in real time, allowing response teams to quickly investigate alerts and still maintain operational efficiency. Coupling automated response capabilities with human supervision also guarantees swift reaction to developing threats without flooding security personnel with false positives.

4.3 Human Oversight and Governance

Even as AI becomes more independent, human oversight remains key for secure and ethical financial systems. Governance should define clear boundaries for AI decisions, specifying the points where human review is required. Escalation procedures channel high-risk situations to specialized teams that possess domain-specific expertise required to analyze complex financial choices outside routine operating parameters. Audit trails recording complete model decision histories permit post-incident examination and regulatory compliance, establishing accountability functions critical to the preservation of stakeholder trust. The problem is developing oversight mechanisms that allow effective human control without introducing bottlenecks that eliminate efficiency gains inherent in AI automation. Hybrid decision models designate mundane transactions to automated systems and leave high-stakes or complex decisions to human analysts, getting the best of both speed and accuracy. Compliance dashboards monitor a multiplicity of regulatory obligations across various jurisdictions, producing automated reports that prove compliance with changing legal frameworks governing the use of AI in financial services.

Defense Layer	Implementation Feature
Base layer security	Encryption, integrity checks, and access controls
Homomorphic encryption	Computation without revealing information
Federated learning	Local processing without centralized exposure
Drift detection	Identifies behavior pattern deviations
Real-time monitoring	Continuous oversight of complex deployments
Human-AI hybrid decisions	Automated routine, human complex decisions

Table 3: Multi-Layered Defense Architecture and Monitoring Capabilities [7, 8]

5. Future Directions and Emerging Challenges

5.1 Technological Evolution and Threat Landscape

AI is changing finance through advances in both security and innovation. Quantum computing has the possibility to greatly change current security methods in this field. The transition to quantum-safe cryptography represents a critical imperative for financial institutions, as quantum computers threaten to render current encryption methods obsolete within the next decade [9]. The EU Digital Operational Resilience Act framework emphasizes the necessity of adopting precautionary approaches to quantum threats, recognizing that financial sector cybersecurity must evolve proactively rather than reactively to maintain system integrity [9]. Post-quantum cryptographic algorithms, as they provide security against quantum attacks, bring unprecedented computational overhead that financial infrastructures need to support without sacrificing transaction processing performance or efficiency.

Journal of Information Systems Engineering and Management
2025, 10(60s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Next-generation large language models and multimodal AI frameworks bring new attack surfaces that existing security paradigms are incapable of effectively addressing, and this poses vulnerabilities that cut across text, numbers, and visual data processing landscapes. Emergent transformer architecture for next-generation transformers that are handling enormous amounts of financial data shows emergent behavior that cannot be predicted using traditional testing paradigms, which could result in catastrophic failure under certain market conditions. Neuromorphic computing systems, although promising extraordinary energy efficiency benefits, introduce timing-based vulnerabilities that are exploitable through side-channel attacks that conventional security controls cannot pick up on. Sophisticated persistent threats employing AI-generated polymorphic malware continue to evolve and refine attack approaches according to countermeasures and evade detection with sophisticated evasion tactics that defy traditional detection measures.

5.2 Regulatory and Compliance Issues

Regulatory environments are unable to keep up with AI developments, and compliance uncertainties arise that make implementation strategies difficult across financial institutions. Regulatory environments for AI deployment in the financial sector are under unparalleled pressure to strike a balance between stimulating innovation and preventing risk, especially as algorithmic decision-making becomes more autonomous and inscrutable [10]. AI complexity creates the need for new forms of regulation that transcend rule-based compliance and move toward principle-based environments that can accommodate evolutionary change in technology [10]. Future legislation will probably require explainability standards that make AI choices interpretable to regulators and consumers alike, algorithmic auditing processes that confirm model fairness and accuracy, and liability regimes that clearly define responsibility for AI-based choices leading to financial losses.

Regulatory compliance monitoring systems will need to adapt to monitor increasingly sophisticated regulatory standards across multiple countries with varying models of AI governance and data protection. Model governance platforms recording architectural updates, hyperparameter tuning, and retraining activities produce large audit trails required to prove regulatory compliance, but storage and processing demands place substantial operational costs. Restrictions on cross-border data transfers that only allow AI processing on domestic infrastructure place performance bottlenecks and add latency to cross-border transactions, contravening the globalized character of today's financial markets. To maintain accuracy in identifying potential violations, automated compliance verification systems that scan model code and behavior patterns must adapt to rapidly changing regulatory standards.

5.3 Socioeconomic Implications

The widespread use of AI in finance has important social and economic consequences that extend past pure tech issues to fundamental questions about how markets are organized and who can participate. Market concentration patterns intensify with the computational demands of sophisticated AI deployment, erecting barriers to entry for smaller institutions in order to engage in technological progress, possibly lowering market diversity and competition. Concerns related to environmental sustainability are raised due to the high energy needs of training and running big AI models, and careful attention to carbon emission footprints and strategies involving renewable energy integration is needed. Displacement of classic financial functions by automation poses questions regarding the transformation of the workforce and reskilling initiatives that equip workers for AI-enpowered workspaces.

Challenge Category	Implication/Requirement
Quantum computing threat	Current encryption will be obsolete within the next decade
EU Digital Operational Resilience Act	Proactive cybersecurity evolution is required
Post-quantum algorithms	Substantial computational overhead introduced
Explainability mandates	AI choices are interpretable to regulators and consumers

Journal of Information Systems Engineering and Management
2025, 10(60s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Algorithmic auditing	Confirm model fairness and accuracy
Cross-border restrictions	Performance bottlenecks for international transactions

Table 4: Next-generation challenges in financial AI security [9, 10]

Conclusion

The evolution of financial systems with artificial intelligence integration is a turning point in the development of banking history, where technological innovation and security concerns have to be harmoniously balanced to achieve sustainable growth. The evidence discussed in this article shows that although AI technologies provide unparalleled functionality in transaction processing, fraud detection, and customer service automation, these advantages are accompanied by equally meaningful security threats requiring imaginative defense mechanisms. Banks are confronted with the daunting challenge of introducing advanced machine learning architectures while safeguarding against adversarial attacks, poisoning attempts, and new quantum computing-based threats that may make traditional encryption obsolete. The future demands embracing multi-layered security frameworks that integrate technical protection mechanisms with human monitoring, so as to ensure automated systems run within tolerable risk limits while maintaining operational effectiveness. Regulatory frameworks need to adapt to cope with the peculiar challenges raised by autonomous decision systems, setting out transparent accountability frameworks and explainability standards that maintain consumer confidence. Socioeconomic consequences of general adoption of AI, such as market concentration and environmental sustainability issues, require careful consideration of how technological advances can be made equitably. Finally, effective incorporation of artificial intelligence into financial systems rests not so much on technical complexity but on the capacity to develop systems that support, and do not undermine, the basic trust all financial interactions require.

References

[1] Mohammad Kowshik Alam et al., "Adversarial Machine Learning for Robust Fraud Detection in High-Frequency Financial Transactions", ResearchGate, 3rd August 2025. [Online]. Available: https://www.researchgate.net/publication/394256810_Adversarial_Machine_Learning_for_Robust_Fraud_Detection_in_High-Frequency_Financial_Transactions
[2] Sanhita Dasgupta et al., "AI-Powered Cybersecurity: Identifying Threats in Digital Banking", ResearchGate, 2023. [Online]. Available: https://www.researchgate.net/publication/372603188_AI-Powered_Cybersecurity_Identifying_Threats_in_Digital_Banking
[3] Zheng Fang and Toby Cai, "Deep neural network modeling for financial time series analysis", ScienceDirect, 28th August 2025. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2214579625000486
[4] Ugoaghalam Uche James et al., "Adversarial Attack Detection Using Explainable AI and Generative Models in Real-Time Financial Fraud Monitoring Systems", IJSRMT, 2024. [Online]. Available: https://ijsrmt.com/index.php/ijsrmt/article/view/644/181
[5] Freda Moraa Omambia, "Artificial Intelligence (AI) And Financial Performance of the Financial Service Industry in Kenya", ResearchGate, July 2025. [Online]. Available: https://www.researchgate.net/publication/394692238_Artificial_Intelligence_AI_And_Financial_Performance_of_the_Financial_Service_Industry_in_Kenya
[6] Nikhil Gupta, "Security Risks of Generative AI in Financial Systems: A comprehensive review", ResearchGate, March 2025. [Online]. Available: https://www.researchgate.net/publication/390109409_Security_Risks_of_Generative_AI_in_Financial_Systems_A_comprehensive_review

[7] Adam Rajuroy et al., "Balancing Data Privacy and Financial Innovation: A Multi-Layered Cybersecurity Framework for AI-Driven Analytics in Banking and Fintech", ResearchGate, February 2025. [Online]. Available: https://www.researchgate.net/publication/388870090_Balancing_Data_Privacy_and_Financial_Innovation_A_Multi-Layered_Cybersecurity_Framework_for_AI-_Driven_Analytics_in_Banking_and_Fintech
[8] Bibitayo Ebunlomo Abikoye et al., "Real-Time Financial Monitoring Systems: Enhancing Risk Management Through Continuous Oversight", ResearchGate, 2024. [Online]. Available: https://www.researchgate.net/publication/383056885_Real-Time_Financial_Monitoring_Systems_Enhancing_Risk_Management_Through_Continuous_Oversight
[9] Laima Jančiūtė, "Cybersecurity in the financial sector and the quantum-safe cryptography transition: in search of a precautionary approach in the EU Digital Operational Resilience Act framework", Springer Nature, March 2025. [Online]. Available: https://link.springer.com/article/10.1365/s43439-025-00135-7
[10] Mirishli Shahmar Sakit, "Regulating AI in Financial Services: Legal Frameworks and Compliance Challenges", arXiv, 2024. [Online]. Available: https://arxiv.org/pdf/2503.14541