ORIGINAL ARTICLE

INTERNATIONAL JOURNAL OF ARTIFICIAL INTELLIGENCE

ISSN: 2692-5206, Impact Factor: 12,23
American Academic publishers, volume 05, issue 06,2025

Journal: https://www.academicpublishers.org/journals/index.php/ijai

AN OVERVIEW OF FINANCIAL RISK TYPES AND THE SIGNIFICANT ROLE OF ARTIFICIAL INTELLIGENCE TECHNOLOGIES IN THEIR MITIGATION

Zaynalov Jahongir Rasulovich

Professor, Samarkand Institute of Economics and Service

Latipova Shakhnoza Mahmudovna

Associate Professor of the Department of "Finance" of the

Samarkand Institute of Economics and Service

Kholmurodova Sevara Askarovna

Student of the Samarkand Institute of Economics and Service,

missfinancier7.5@gmail.com

Annotation: This article analyzes the integration of artificial intelligence and cybersecurity technologies against the backdrop of emerging digital threats in modern financial systems. The article scientifically highlights the development of mechanisms for detecting, assessing and preventing financial fraud, cyberattacks and other risks using artificial intelligence. It also provides theoretical justification and practical examples of how these technologies can jointly strengthen the security of the financial sector.

Key words:artificial intelligence, financial security, cyberattack, financial technologies (FinTech), machine learning, anomaly detection, threat response system, risk monitoring

Risk management has become a fundamental component of sustainable business operations in the rapidly changing financial landscape of today.Market volatility, credit defaults, operational disruptions, and cybersecurity threats are among the numerous risks to which financial institutions and enterprises are becoming more susceptible.Decision-makers who are striving to protect assets, maintain regulatory compliance, and guarantee long-term profitability face substantial obstacles due to the complexity and unpredictability of these risks.Decision-makers who are striving to protect assets, maintain regulatory compliance, and guarantee long-term profitability face substantial obstacles due to the complexity and unpredictability of these risks.With the advent of digital transformation, (AI) has emerged as a powerful tool in the financial sector, offering advanced capabilities for identifying, analyzing, and mitigating various forms of financial risk. AI such as machine learning, natural language processing, and predictive analytics—enable institutions to process massive volumes of data in real time, uncover hidden patterns, and make more informed and proactive decisions.

Cybersecurity is extremely important in the field of financial technology. The use of artificial intelligence (AI) algorithms to detect, analyze, and respond to threats in real time greatly improves the effectiveness of financial protection systems. AI systems that work in tandem with cybersecurity tools protect financial institutions not only from existing threats, but also from emerging risks. This integration is critical to ensuring financial stability, increasing customer trust, and strengthening economic security. In the financial industry, cybersecurity is of great importance, as each individual using financial services faces the risk of having their financial data compromised. Every transaction involves a certain level of risk, particularly in terms of access to personal and corporate data. The main types of threats include:

Phishing – A form of internet-based financial fraud that aims to obtain a user's identification data (such as login credentials and passwords for bank accounts or cards) through deceptive online platforms.

Smishing – A type of phishing that uses SMS messages to trick users. Fraudsters send messages containing links to fake websites, prompting victims to enter sensitive financial information or payment credentials.

Vishing – A voice phishing method where fraudsters call the victim, impersonating a bank employee or another trustworthy figure, to manipulate them into revealing confidential information or authorizing financial transactions.

Pretexting – A method of social engineering where the fraudster fabricates a scenario to impersonate someone else, often using previously obtained personal details such as date of birth, passport number, or taxpayer ID to gain the victim’s trust and extract sensitive financial data. This type of fraud is commonly carried out through phone calls or emails.

Malware – Refers to malicious software designed to steal confidential data or money from individuals and financial institutions. This includes banking details, personal information, and other data that can be exploited for fraud. Malware is often spread through phishing, fake emails, or seemingly legitimate websites that trick users into installing harmful software.

Preventing financial fraud requires a proactive and multi-layered approach. Here are some of the most effective and practical strategies that organizations and institutions can adopt:

Preventive Measures: Regular security audits, ongoing employee training, up-to-date protective protocols, and consistently updated systems are fundamental in reducing vulnerabilities. Staying one step ahead through prevention is often the best defense.

Technological Solutions: Tools like multi-factor authentication, strong encryption techniques, blockchain applications, and biometric verification systems offer robust layers of protection. These technologies help secure both user identity and transaction integrity.

Real-Time Monitoring: Advanced AI systems can scan and analyze transactions in as little as 50 milliseconds. This allows for the immediate detection of suspicious activity and enables systems to automatically block potentially fraudulent actions before damage is done.

Machine Learning Algorithms: By learning from past financial transactions, machine learning tools can identify irregular patterns and assess risk in real time. This makes it possible to predict and prevent fraudulent behavior more accurately and efficiently.

Key Recommendations for Strengthening Financial Cybersecurity with AI

Introducing a Specialized AI Certification System for the Financial Sector:

To enhance the security and reliability of AI systems used in banks and financial institutions, it is important to implement a certification and licensing framework. Such a system would ensure that AI technologies meet established safety and ethical standards before being deployed.

Adapting International Best Practices to Local Conditions:

Countries like the United States, Japan, and members of the European Union have already developed robust models for integrating AI into financial security. Drawing from these experiences and adapting them to local regulatory and operational environments can help create more effective and context-appropriate solutions.

Implementing Real-Time AI-Based Monitoring Systems:

The integration of AI and cybersecurity technologies into financial operations is vital—not just for preventing fraud, but for ensuring the long-term stability of the digital economy. Real-time AI systems play a key role in detecting threats instantly, allowing institutions to respond before any serious damage occurs. When these technologies are used in harmony, they provide a much stronger line of defense against today's complex cyber threats.

Deploying Early Fraud Detection Mechanisms:
Artificial intelligence, particularly machine learning algorithms, can analyze financial transactions in real time and flag unusual or suspicious behavior. For institutions that offer a wide range of financial services, integrating AI with cybersecurity tools is essential for managing risks more effectively and building customer trust. This comprehensive, technology-driven approach is critical for maintaining the resilience and sustainability of the financial sector.

References:

1. Decree No. PQ-358 on the approval of the strategy for the development of artificial intelligence technologies until 2030, dated October 14, 2024.
2. Shakarian, P. (2021). Artificial Intelligence Tools for Cyber Attribution. SpringerBriefs in Computer Science.
3. Healey, J. (2013). A Fierce Domain: Conflict in Cyberspace, 1986 to 2012. Cyber Conflict Studies Association.
4. Danielsson, J., & Uthemann, A. (2023). Artificial Intelligence and Systemic Risk. Journal of Banking and Finance.
5. Tojimatov, D., & Mirzaev, J. (2023). Use of Artificial Intelligence Opportunities for Early Detection of Threats to Information Systems. Central Asian Journal of Theoretical and Applied Science, (18), 1146.

6. Bekmirzayev, O., & Muminov, B. (2024). The Role and Application of Artificial Intelligence in Identifying Threats to Information Systems. DTAI Journal. Retrieved from https://dtai.tsue.uz/index.php/DTAI2024/article/view/o0303
7. O‘rinov, N. T., & Yunusov, O. F. (2023). Artificial Intelligence and its Application in Information Security Management. Central Asian Journal of Theoretical and Applied Science, (12), 451. Retrieved from https://cajotas.centralasianstudies.org/index.php/CAJOTAS/article/view/451