UDC 336.7:004.8

FINANCIAL TECHNOLOGY ANTI-FRAUD SYSTEMS: NEW TRENDS

Yang Minhao, master's degree student,
Boyarshinova O. A., PhD in Physics and Mathematics, associate professor
Belarusian National Technical University
Minsk, Belarus

Abstract. As emerging technologies like artificial intelligence and blockchain become increasingly integrated into finance, financial fraud methods have grown more complex and hidden. This paper focuses on the latest development trends of anti-fraud systems in fintech, analyzing how these systems are advancing through technological innovation, application expansion, and regulatory optimization. Our research shows that three core directions – intelligent upgrading, ecological integration, and compliant operation – are driving innovation in anti-fraud systems, significantly boosting the accuracy and real-time performance of fraud detection.

Keywords: financial technology, anti-fraud system, artificial intelligence, blockchain, regulatory technology.

Financial technology (fintech) has reshaped how the global financial industry operates, with digital payments, cross-border finance, and other areas seeing exponential growth in transaction volumes. Yet this rapid development has also created new challenges for fraud prevention. Fraudulent activities – from credit card information leaks and fake identity loans to blockchain-based financial scams – are constantly evolving, taking on more diverse, tech-driven, and hidden forms. Data from the People's Bank of China shows that in 2023, fraud-related losses in China's financial sector exceeded 3 billion yuan, while the number of new fraud types rose by 27 % year-on-year [1]. What's more, the rise of mobile finance has made fraud more "fragmented": fraudsters now target individual users through phishing links, fake apps, and social engineering, making it harder for traditional batch-monitoring systems to track.

Anti-fraud systems are a cornerstone of financial security, and their innovation is critical to protecting the assets of financial institutions and customers alike. Studying the latest trends in fintech anti-fraud systems

helps identify key directions for technological advancement, provides financial institutions with a theoretical framework to optimize their anti-fraud strategies, and supports the healthy, sustainable growth of the fintech industry. Additionally, these insights can assist regulators in refining anti-fraud oversight frameworks – especially as cross-border fraud becomes more prevalent, requiring coordinated global responses.

Current State and Challenges of Fintech Anti-Fraud Systems.

Financial anti-fraud systems have evolved through three key phases: rule-based engines, data analysis, and artificial intelligence (AI). In the rule-based era, systems relied on manual thresholds (e. g., "block transactions over 50.000 yuan from unregistered devices"), which were rigid and prone to missing new fraud patterns. The data analysis phase introduced basic statistical models, but these struggled with large, unstructured datasets. Today, most financial institutions have built intelligent anti-fraud systems that integrate data mining, machine learning, and biometrics. These systems have drastically improved fraud detection accuracy – for example, the fraud rate in high-priority areas like third-party payments has dropped to just 0.003 % [1].

Fraud methods grow more complex: Fraudsters use advanced tools like deepfakes and proxy servers to evade detection, making traditional anti-fraud rules ineffective against new scenarios. For instance, "deepfake voice fraud" can mimic a user's voice to bypass phone verification, while proxy networks hide the true location of fraudulent transactions.

Data silo issues: Without effective data-sharing mechanisms between financial institutions, tracking cross-institutional or cross-industry fraud becomes difficult. A fraudster rejected by one bank may simply apply for a loan at another, as there's no unified database of suspicious individuals.

Balancing security and user experience: overly strict anti-fraud measures can frustrate users – for example, repeatedly blocking legitimate transactions for frequent travelers – while lax monitoring increases fraud risks.

Regulatory compliance pressure: with the expansion of data privacy laws like GDPR and CCPA, anti-fraud systems must now meet both security and compliance requirements. Collecting user behavior data for fraud detection, for instance, requires explicit consent, limiting the availability of training data [2].

New Development Trends of Fintech Anti-Fraud Systems.

1. Technological Innovation: Toward Intelligence and Diversification.

1.1. Deep Integration of Artificial Intelligence.

Machine learning algorithms now form the core of anti-fraud systems, boasting a fraud identification accuracy rate of 92 % [4]. Supervised learning

models – such as random forests and gradient boosting – excel at detecting known fraud types, while unsupervised learning tools like autoencoders can spot previously unknown fraud patterns. For example, in online credit approval scenarios, gradient boosting decision trees (GBDT) can analyze 50+ user feature dimensions – including income stability, credit history, and transaction frequency – to identify fake loan applications, with a misjudgment rate of less than 1.2 %. For time-series transaction data (such as continuous small-amount transfers within 1 hour), RNNs excel at capturing abnormal temporal patterns, which is particularly effective in preventing "cash-out fraud" commonly seen in e-commerce platforms. Deep learning technologies, including convolutional neural networks (CNNs) and recurrent neural networks (RNNs), extract high-level features from transaction and user behavior data, cutting fraud recognition time by 50 % compared to traditional models. One third-party payment provider, for instance, cut its annual fraud-related losses by over 500 million yuan after deploying an AI-powered anti-fraud system [1].

Reinforcement learning is also gaining traction for optimizing anti-fraud strategies. By creating an interactive model between an "intelligent agent" and the fraud environment, systems can dynamically adjust monitoring thresholds and identification rules as fraud methods evolve – greatly enhancing adaptability.

1.2. Blockchain's Expanding Role in Anti-Fraud.

Blockchain's decentralized and tamper-proof nature offers a new approach to anti-fraud efforts. In cross-border payments and trade finance, blockchain enables end-to-end transaction traceability, reducing processing time for individual transactions from 7 business days to just 24 hours [3]. For bill fraud, blockchain-based deposit technology resolves disputes over bill circulation, lowering litigation costs by 52 %. One supply chain finance platform, for example, used blockchain to authenticate trade data, successfully preventing 386 cases of counterfeit bill fraud [3].

1.3. Multi-Modal Biometrics.

Biometric technology has evolved beyond single-modal recognition (e. g., fingerprint scanning) to multi-modal fusion – combining fingerprints, facial recognition, voiceprints, and iris scans. This integration has pushed fraud detection accuracy to 99.2 %. A mobile payment platform, for instance, saw an 83 % year-on-year drop in account theft cases after adopting multi-modal biometric verification [1]. Beyond security, this technology improves user experience by eliminating the need for frequent password entry.

1.4. Emerging Frontier Technologies.

Federated learning addresses data silo issues by training models without sharing raw data – enabling "data availability without exposure". A research institution's federated credit anti-fraud model, for example, increased fraud detection coverage by 30 % while complying with data privacy rules [4]. Quantum computing, meanwhile, is poised to overcome traditional algorithm limitations; experts predict its application in risk pricing and fraud pattern mining could boost computational efficiency by 300 %, drastically improving real-time processing of massive transactions [2].

2. Application Expansion: Ecological Integration and Full-Scenario Coverage.

2.1. Building Embedded Anti-Fraud Ecosystems.

Fintech companies are creating embedded financial service ecosystems via API open platforms, integrating anti-fraud functions into ecommerce, logistics, healthcare, and other sectors. One leading payment institution, for example, partners with over 800 industry players – its ecosystem now handles 67 % of total transactions, enabling real-time fraud risk monitoring across the entire transaction chain [1]. Open-source communities are also driving standardization: the Hyperledger Fabric alliance chain framework now includes over 200 institutions, with transaction throughput exceeding 100 000 transactions per second – laying the groundwork for cross-institutional anti-fraud system connectivity [3].

2.2. Extending to Inclusive Finance.

Anti-fraud systems are increasingly serving small and micro-enterprises (SMEs) and individual users in inclusive finance. By integrating alternative data – such as industrial and commercial records, judicial information, and social media activity – lenders have kept SME loan nonperforming rates at 1.5 %, 0.7 percentage points lower than traditional models [4]. Take a tech-based SME in southern China as an example: before adopting the new anti-fraud system, the company's loan application was repeatedly rejected due to insufficient credit history. After the system integrated its intellectual property (IP) pledge data and supply chain transaction records into the risk assessment model, the company successfully obtained a 500 000-yuan credit line, with the approval process compressed from 15 days to 48 hours. This not only solved the enterprise's financing dilemma but also kept the lender's non-performing rate for such loans below 1.0 %. An agricultural supply chain platform, for instance, used anti-fraud technology to reduce farmer loan approval times from 30 days to 3 days, all while maintaining low fraud rates [2].

2.3. Covering Cross-Border Financial Scenarios.

As financial globalization accelerates, cross-border fraud has risen sharply. Anti-fraud systems now strengthen monitoring by integrating cross-border payment data, foreign exchange regulatory information, and international blacklists. The cross-border payment system co-developed by the People's Bank of China and other central banks saw 120 % annual transaction growth, and its built-in anti-fraud system has effectively blocked cross-border fund transfer fraud [1].

3. Regulatory Optimization: Compliant Operation and Collaborative Governance.

3.1. Widespread Adoption of Regulatory Sandboxes.

Regulatory sandboxes provide a safe testing environment for innovative anti-fraud technologies and products. The EU's Crypto-Asset Markets Regulation (MiCA), for example, has supported over 140 anti-fraud innovations through sandbox testing [5]. Chinese financial regulators have also launched multiple sandbox pilots, cutting time-to-market for innovative anti-fraud products by 40 % [1].

3.2. Strengthened Data Privacy Protection.

Financial institutions are building dynamic data governance systems to balance anti-fraud needs with privacy protection. A multinational bank invested $ 270 million in a privacy computing platform, using technologies like homomorphic encryption and differential privacy to enable compliant anti-fraud analysis of sensitive data [2]. An internet finance platform, meanwhile, reduced user privacy breaches by 91 % year-on-year after implementing a hierarchical digital identity authorization system [1].

3.3. Improved Cross-Departmental Collaborative Oversight.

A financial regulatory data-sharing platform now integrates data from 17 regulators, enabling real-time monitoring of anti-fraud risk indicators. One provincial financial supervision bureau used a blockchainbased regulatory reporting system to conduct penetrating oversight of 1 200 small and medium-sized financial institutions, boosting off-site supervision efficiency by 58 % [3]. Collaboration between financial institutions, public security agencies, and telecommunications providers has also strengthened – creating a unified front against cross-industry and cross-regional financial fraud.

Through this research, we identify three key new trends in fintech anti-fraud systems:

Technological innovation: AI and blockchain are deeply integrated, with frontier technologies like federated learning and quantum computing

emerging as game-changers. These technologies address core pain points such as data silos and low real-time performance.

Application expansion: Embedded ecosystems and full-scenario coverage have become mainstream, extending services to inclusive finance and cross-border markets – ensuring that anti-fraud protection is not limited to large institutions but reaches SMEs and individual users.

Regulatory optimization: Regulatory sandboxes, privacy computing, and collaborative oversight are driving compliant system development, balancing innovation with risk control.

Together, these trends enhance the accuracy, real-time performance, and compliance of anti-fraud systems – addressing core industry challenges.

Future Outlook:

Technological innovation: Brain-computer interface (BCI) technology may reshape financial interactions by using neural signals to dynamically assess user risk preferences, further boosting anti-fraud system intelligence [2]. For example, BCI could detect subtle changes in user brain activity when entering sensitive information under duress, flagging potential fraud.

Ecological construction: The integration of metaverse and Web3.0 will spawn decentralized autonomous organization (DAO) financial ecosystems. Anti-fraud systems must adapt to new risks related to virtual assets and cross-border transactions in these environments – such as fraud involving NFTs or decentralized lending platforms [4].

Regulatory coordination: Cross-border anti-fraud regulatory cooperation networks will expand, with countries sharing information and technical standards to combat transnational financial fraud. This could include unified global blacklists of fraudsters or cross-jurisdictional sandbox testing [5].

Talent development: Demand for interdisciplinary talent – combining finance, technology, and law – will grow. Industry-academia-research collaboration models need to be refined to train professionals supporting anti-fraud system advancement. For example, universities could partner with fintech firms to develop hands-on courses in AI fraud detection or blockchain security [1].

Table of contents

1. Financial Technology Pilot Zone Anti-Fraud System Effect Evaluation Report // People's Bank of China. – 2023. – URL: www.pbc.gov.cn (date of access: 20.10.2025).

2. Technology Trend Report: Financial Anti-Fraud System Innovation // Gartner Inc. – 2022. – URL: www.gartner.com (date of access: 20.10.2025).

3. Research on the Application of Blockchain Technology in Financial Anti-Fraud / China Banking Association // China Banking Journal. – 2023. – № 5. – P. 45–53.

4. Global FinTech Report 2023 // McKinsey & Company. – 2023. – URL: www.mckinsey.com (date of access: 20.10.2025).

5. FinTech White Paper: Anti-Fraud Technology and Practice // World Bank Group. – 2022. – URL: www.worldbank.org (date of access: 20.10.2025).

UDC 331.108.45

GAMIFICATION AS A FACTOR IN IMPROVING THE EFFICIENCY OF THE ORGANIZATION'S HUMAN RESOURCES

Li Kunjian, master's degree student,
Boyarshinova O. A., PhD in Physics and Mathematics, associate professor
Belarusian National Technical University
Minsk, Belarus

Abstract. This article examines the potential of gamifying tools as a motivational component for staff performance. Experience with gamification is analyzed to identify the advantages and disadvantages of using gamification as a motivational tool.

Keywords: Gamification, the emotional commitment of employees, company success, psychological factors.

The successful functioning of any organization depends on a multitude of external and internal factors that, to varying degrees, influence its key processes. Instability in the economic, social, political, and industrial environments, rapid scientific and technological progress, and ever-increasing competition compel managers to adapt their management style to the changing context of management activities, develop new ways to motivate staff, and improve existing ones [1].