eISSN: 2229-3213 pISSN: 2229-3205
The Journal of Applied Science and Social Science
Volume 16,Issue 04 April, 2026

EFFECTIVENESS OF AI-BASED FINTECH SYSTEMS IN DETECTING AND PREVENTING FINANCIAL FRAUD

Maxmudov Anvarjon Maxmudovich

Fergana State Technical University,

Senior Lecturer, PhD*

Tursunboyev Og'abek Otabek o'g'li

Fergana State Technical University,

2nd-year student

Tursunboyev Asadbek Otabek o'g'li

Student at Fergana District Secondary School No. 8

Abstract. The article analyzes modern forms of fraud, their methods, and prevention strategies in the context of digital banking development. Additionally, the significance of artificial intelligence and biometric technologies is highlighted.

Keywords: fraud, artificial intelligence, biometric authentication, phishing, security.

Digital economies are rapidly developing worldwide. Particularly over the past five years, digital banking services, mobile payments, and the FinTech ecosystem have been widely implemented in Uzbekistan as well. According to Central Bank data, by the end of 2024, the number of active bank cards in the country exceeded 30 million, while mobile banking application users reached 15 million. While such digital transformation has created conveniences for the population, it has also significantly increased the risk of financial fraud.

Financial fraud is a set of actions aimed at illegally seizing the financial resources of an individual or organization. In recent years, such fraud types have spread not only in traditional banking systems but also through internet and mobile applications. Particularly, social engineering, phishing (fake links), smishing (SMS fraud), vishing (voice call fraud), and fake mobile applications have become the most common methods.

The state in Uzbekistan is paying serious attention to this problem. A number of laws and regulations have been implemented to protect the banking system. These include the Law "On Payments and Payment Systems," the draft Law "On Cybersecurity," as well as systems for protecting clients' personal data, monitoring banking operations, and detecting suspicious transactions. However, these measures are not sufficiently adaptable to the rapidly changing dynamics of fraud methods.

Banks are also strengthening their security measures. Many banking applications employ methods such as two-factor authentication (SMS codes, TOTP) and biometric verification (fingerprint, facial recognition, voice analysis). These methods play an important role in protecting client accounts. Nevertheless, cybercriminals are increasingly using more sophisticated methods. For example, attacks such as "SIM swapping" (transferring a user's phone number to another SIM card to receive SMS codes) or "man-in-the-middle" (intercepting traffic between the user and the bank) are on the rise.

Improving the population's financial literacy is also considered an important direction.

Because in many cases, people fall for fraudsters' simple tricks. For this reason, banks and government organizations regularly conduct awareness campaigns and educational activities. However, the scope and regularity of these efforts are still insufficient. Specifically, elderly people living in rural areas and citizens who cannot fully utilize digital technologies remain the most vulnerable groups.

Looking at international experience, AI-based security systems are being successfully implemented in countries such as Singapore, Estonia, and South Korea. For example, Singapore has implemented the "National Authentication Framework," which analyzes transactions in real-time based on biometric data and AI. In Estonia, every citizen has their digital identifier, and all government and banking services are protected through this system. Uzbekistan is still in the initial stages of implementing such systems.

Furthermore, international financial organizations, including the International Monetary Fund (IMF) and the World Bank, recommend using artificial intelligence and machine learning technologies in the fight against financial fraud. These technologies are much more adaptable and accurate compared to traditional rule-based systems. Nevertheless, the current system in Uzbekistan has several problems. The biggest problem is that fraudsters' methods are rapidly evolving, and existing security systems cannot adapt to these changes. For example, fraudsters call people posing as bank employees or law enforcement officers (vishing). They intimidate or persuade people to provide card details, CVV codes, or SMS codes. Unfortunately, many people believe them and disclose their information. In some cases, fraudsters even call in the name of the "bank security service" and demand that money be transferred to another account to "protect" the client's account.

Another widespread method is fake mobile applications. Fraudsters create programs that closely resemble popular banking apps and distribute them through social networks, Telegram, or SMS. When a user downloads it and enters their login and password, all information goes to the fraudsters. Some applications even steal contacts, SMS messages, and other private data from the device.

Additionally, phishing (fake links) remains a major problem. People receive links via SMS or Telegram. The link appears to resemble the official bank website, but in reality, it leads to a site belonging to fraudsters. As soon as the user enters their information, it immediately falls into the hands of fraudsters. In some cases, malicious programs (malware) are also downloaded through these links.

There are technical problems as well. Many security systems operate using old methods, meaning they rely on simple rules: they look at parameters such as transaction limits, geolocation, and time intervals. But this is not sufficient against modern fraud methods. Fraudsters employ methods such as hiding their real-time location, changing IP addresses, and even using artificial intelligence to deceive authentication systems.

Another problem is the insufficient integration of data. Information exchange between banks, fintech companies, and government organizations is weak. This hinders the rapid detection and prevention of fraud. For example, a person who committed fraud at one bank can easily open an account at another bank and commit new crimes. The absence of a unified centralized "blacklist" or fraud monitoring system further exacerbates this problem.

First, it is necessary to widely implement artificial intelligence (AI) and machine learning technologies. AI systems can analyze large volumes of transaction data in real-time and detect unusual activities. It is based not only on predefined rules but also on the model of the user's

usual behavior. For example, if a user typically transfers small amounts only during the day and from a certain geolocation, but suddenly attempts to transfer a large amount at night to another country, the AI system flags this as suspicious and blocks the transaction or requests additional verification.

Second, it is necessary to further expand biometric protection. Methods such as facial recognition, fingerprint scanning, voice analysis, and even heart rhythm detection are much more secure than simple passwords. These methods help accurately identify the user and sharply reduce fraudsters' ability to bypass authentication. Biometric data should be stored locally on the device and never sent to external servers.

Third, it is necessary to develop systems that automatically detect phishing and fake messages. Special AI models can scan messages in SMS, email, and social networks to identify suspicious links, unusual language, and fake sender information. If the system finds such a message, it automatically blocks it or issues a warning to the user.

Fourth, improving the population's financial literacy is very important. If people know fraudsters' methods, they will not be deceived. For this reason, financial literacy and cybersecurity subjects should be introduced in schools, colleges, and universities, and regular awareness campaigns should be conducted through television and social networks. Especially, organizing special training sessions for elderly people and rural residents would be purposeful.

Fifth, it is necessary to strengthen cooperation between organizations. Real-time information exchange should be established between banks, government agencies (for example, the Central Bank, Ministry of Internal Affairs, Cybersecurity Center), and fintech companies. Through a unified centralized fraud monitoring system, any suspicious transaction or person can be simultaneously notified to all organizations.

Sixth, it is necessary to further improve the legislative framework and strengthen liability for financial fraud. The certainty and severity of punishment serve to reduce fraud cases. Additionally, compliance with security standards should be mandatory for banks and fintech companies, and regular inspections should be conducted in this regard.Financial fraud is increasing alongside the development of the digital economy. To effectively combat it, it is important to widely use modern technologies, especially artificial intelligence and biometric systems. At the same time, it is necessary to improve financial literacy and cybersecurity knowledge so that people can protect themselves. Only when technology and conscious users act together can this problem be significantly reduced. In the future, Uzbekistan can fully comply with international standards in the field of digital financial services security and even join the ranks of leading countries. For this, all stakeholders—the state, banks, IT companies, and citizens—must work together.

REFERENCES AND SOURCES

1. Law of the Republic of Uzbekistan "On Payments and Payment Systems." – Tashkent, 2019.

2. Central Bank of the Republic of Uzbekistan. "Annual Report on the Development of Digital Banking Services in Uzbekistan," 2024.

3. Ministry of Information Technologies and Communications Development of the Republic of Uzbekistan. "Cybersecurity Concept," 2023.

4. Strategy of the President of the Republic of Uzbekistan "Digital Uzbekistan – 2030."

5. Official Website of the Central Bank of the Republic of Uzbekistan – www.cbu.uz State Statistics Committee. "Digital Economy Indicators," 2024.

6. European Banking Authority (EBA). "Guidelines on Fraud Reporting and Management under the Payment Services Directive 2 (PSD2)," 2023.

7. Financial Action Task Force (FATF). "Guidance on Digital Identity and Financial Crime Prevention," 2023.

8. Russell S., Norvig P. "Artificial Intelligence: A Modern Approach." – Pearson, 2021.

9. Goodfellow I., Bengio Y., Courville A. "Deep Learning." – MIT Press, 2016.

10. IBM Corporation. "AI in Financial Fraud Detection Report," 2023.