TASHKENT STATE UNIVERSITY OF ECONOMICS

International journal of topics

INNOVATION SCIENCE AND TECHNOLOGY

Scopus || Electronic journal specializing in Scopus

ISSUE 10

Acceptance of papers **October, 2025**

Acceptance of papers

Published monthly

Topics

economics, technology, social sciences

ISSN 3060-5229

THE SCIENTIFIC-POPULAR ELECTRONIC JOURNAL **"INNOVATION SCIENCE AND TECHNOLOGY"** HAS BEEN REGISTERED UNDER THE NUMBER **C-5669633** BY THE AGENCY FOR INFORMATION AND MASS COMMUNICATIONS (AOKA) OF THE REPUBLIC OF UZBEKISTAN, EFFECTIVE FROM OCTOBER 9, 2024.

CONTACTS

Phone: **+998 50 737 87 88**

Website: https://ist-journal.uz

Email: innovationist2025@gmail.com

The scientific electronic journal “Innovation Science and Technology” has been included in the list of scientific publications recommended for the publication of main scientific results of dissertations for the award of PhD and DSc degrees in economics and technical sciences, in accordance with the Resolution No. 370 of the Presidium of the Higher Attestation Commission of the Republic of Uzbekistan, dated May 8, 2025.

Electronic publication, Issue 10. 320 pages.
Approved for publication on October, 2025.

Editorial board:

CONTENTS

CONTENTS

CONTENTS

ENHANCING CYBERSECURITY OF PLASTIC CARD TRANSACTIONS IN THE “MY CARD” MOBILE APPLICATION

Kurbonbekova Mohichehra Turobjonovna
Associate Professor of the Department of Banking, Doctor of Economics (DSc)
Email: mohichehra89@list.ru
ORCID: 0000-0002-0779-2632

Mashrapova Sabina Turobjonovna
Director of Experimental State Preschool Educational Organization No. 324
Email: sabina.turobjonovna@gmail.com

Abstract: The purpose of this study is to develop an intelligent real-time anomaly detection model within the “My Card” mobile application to enhance the cybersecurity of plastic card transactions. The research utilizes a mixed-method approach, incorporating quantitative analysis of transaction data, surveys of 520 users, and machine learning algorithms for detecting anomalous transactions. Fraud patterns were evaluated through statistical analysis, correlation analysis, and supervised classification algorithms. The findings demonstrate that real-time detection of anomalous transactions significantly reduces the risk of financial fraud. Digital behavioral indicators, such as transaction frequency, location deviation, and device fingerprinting, exhibit strong predictive power in fraud identification. The proposed model can be practically implemented in mobile banking systems, increasing customer trust, reducing operational risks, and reinforcing the security of the national payment system. This study represents one of the first empirical, data-driven fraud detection frameworks adapted to Uzbekistan’s digital payment ecosystem.

Key words: fraud detection, real-time analytics, digital banking, cybersecurity, anomaly detection, My Card, financial technology.

Annotatsiya: Ushbu tadqiqotning maqsadi “My Card” mobil ilovasida plastik kartalardagi operatsiyalarda kiberxavfsizlikni oshirish maqsadida real vaqt rejimida anomal tranzaksiyalarni aniqlashga qaratilgan aqlli modelni ishlab chiqishdir. Tadqiqot aralash metodologiyaga asoslangan bo‘lib, unda tranzaksiya ma’lumotlarining kvantitativ tahlili, 520 nafar foydalanuvchi so‘rovnomalari va mashinani o‘rganish algoritmlari orqali anomal tranzaksiyalarni aniqlash usullari qo‘llanildi. Statistika, korrelyatsiya tahlili va nazoratli klassifikatsiya algoritmlari yordamida firibgarlik naqshlari baholandi. Tadqiqot natijalari shuni ko‘rsatadiki, real vaqt rejimida anomal tranzaksiyalarni aniqlash moliyaviy firibgarlik xavfini sezilarli darajada kamaytiradi. Tranzaksiya chastotasi, geografik o‘zgarish va qurilma barmoq izlari kabi raqamli xulq-atvor ko‘rsatkichlari firibgarlikni aniqlashda yuqori bashorat kuchiga ega. Taklif qilingan model mobil banking tizimlariga amaliy tatbiq qilinishi mumkin, bu esa mijozlar ishonchini oshiradi, operatsion xavflarni kamaytiradi va milliy to‘lov tizimining xavfsizligini mustahkamlaydi. Ushbu tadqiqot O‘zbekistonning raqamli to‘lov ekotizimiga moslashtirilgan birinchi empirik, ma’lumotga asoslangan firibgarlikni aniqlash ramkalaridan biridir.

Kalit so‘zlar: firibgarlikni aniqlash, real time tahlil, raqamli bank xizmatlari, kiberxavfsizlik, anomaliyalarni aniqlash, My Card, moliya texnologiyalari.

Аннотация: Цель данного исследования – разработка интеллектуальной модели для выявления аномальных транзакций в реальном времени в мобильном приложении “My Card” с целью повышения кибербезопасности операtsий с пластиковыми картами. Исследование основано на смешанной методологии, включающей количественный анализ данных о транзакциях, опрос 520 пользователей и методы машинного обучения для обнаружения аномальных транзакций. С помощью статистического анализа, корреляционного анализа и алгоритмов контролируемой классификатsии оценивались шаблоны мошенничества. Результаты показывают, что обнаружение аномальных транзакций в реальном времени значительно снижает риски финансового мошенничества. Цифровые поведенческие показатели, такие как частота транзакций, отклонение геолокатsии и отпечатки устройств, обладают высокой предсказательной силой при выявлении мошенничества. Предложенная модель может быть практически внедрена в системы мобильного банкинга, что повышает доверие клиентов, снижает операtsионные риски и укрепляет безопасность натsиональной платежной системы. Данное исследование является одной из первых эмпирических, основанных на данных, рамок выявления мошенничества, адаптированных к цифровой экосистеме платежей Узбекистана.

Ключевые слова: выявление мошенничества, анализ в реальном времени, цифровой банкинг, кибербезопасность, выявление аномалий, My Card, финансовые технологии.

INTRODUCTION

Over the past decades, the rapid development of digital payment systems has fundamentally transformed global financial operations. In the context of Uzbekistan, the widespread use of plastic cards and mobile banking applications, particularly “My Card,” has significantly expanded access to financial services, including in remote areas, by facilitating convenient financial transactions.

However, alongside these technological advancements, cybersecurity threats have also increased. Transactions conducted via plastic cards and mobile applications are increasingly exposed to risks such as fraud, phishing attacks, identity theft, and unauthorized transactions. According to reports from the national banking system, cases of financial fraud related to plastic cards have been rising annually, mainly due to the insufficient development of real-time monitoring mechanisms [3,10,11].

Current security systems primarily rely on post-transaction verification, which cannot prevent immediate financial losses. Therefore, the development of adaptive, real-time intelligent fraud detection models for mobile applications has become a pressing issue.

Existing fraud prevention systems in mobile banking applications lack intelligent mechanisms capable of detecting anomalous behavior during transactions in real time.

Research hypothesis: If an intelligent real-time anomaly detection model based on transaction data and user behavior is implemented, the effectiveness of fraud prevention in mobile payment systems will significantly increase.

To scientifically validate this hypothesis, the following research objectives were defined:

- to analyze fraud patterns in plastic card transactions;
- to develop a real-time anomaly detection model;
- to empirically evaluate the effectiveness of the developed model within the ecosystem of the “My Card” mobile application.

REVIEW OF LITERATURE ON THE SUBJECT

In recent years, the rapid development of the digital economy, particularly the widespread adoption of mobile payments and digital banking services, has made financial transaction security a priority area of scientific research. In particular, the real-time detection of fraud and anomalous transactions is considered one of the most pressing scientific and practical challenges in the field of financial technologies (FinTech).

In their studies, Y. Zhang and X. Zhou thoroughly analyze the problem of real-time fraud detection in mobile payment systems and demonstrate that deep learning models, including CNN and LSTM algorithms, ensure high accuracy and speed. According to their conclusions, neural networks capable of identifying time-dependent transaction patterns are significantly more effective than traditional rule-based systems [1]. This approach provides an important methodological foundation for real-time risk detection in mobile applications such as My Card.

In a comprehensive review conducted by H. Liu, J. Wang, and T. Chen, anomaly detection methods in digital transactions are systematically classified. The authors analyze the advantages and limitations of supervised, unsupervised, and hybrid models, concluding that unsupervised and adaptive models are particularly advantageous in real-time environments [2]. This work establishes a theoretical and conceptual foundation for fraud detection and outlines key directions for further empirical research.

P. Sharma and R. Kumar propose hybrid machine learning models for fraud detection in financial services, showing that integrating multiple algorithms can reduce the number of false positives [4]. This approach is particularly important in minimizing user inconvenience caused by erroneous system alerts in real-world applications.

In their research, L. Wang and Y. Li demonstrate that LSTM-based models enable the detection of anomalous transactions in mobile banking systems by accounting for sequential time dependencies [5]. Their findings confirm the effectiveness of deep recurrent neural networks in systems requiring real-time decision-making.

The studies by M. Abdi and R. Hasan, as well as S. Khan and M. Ali, provide a comparative analysis of classical statistical methods and artificial intelligence-based approaches in fraud detection [17]. These studies indicate that machine learning and AI-based models represent the most promising direction for real-time fraud detection in banking systems.

Z. Li and P. Xu develop adaptive anomaly detection models for mobile payment systems and emphasize the importance of self-updating system capabilities in response to constantly evolving fraud schemes [19]. This approach is particularly relevant for developing countries, including Uzbekistan.

R. Patel and A. Singh highlight the strategic importance of AI-driven fraud detection models in digital banking services, demonstrating that such systems not only reduce financial losses but also enhance user trust and strengthen financial stability [20].

Research conducted by international organizations further confirms the institutional importance of this issue. Reports by the OECD and the World Bank identify security concerns as one of the main barriers in the digitalization of small businesses and financial ecosystems [9,10]. These documents emphasize that real-time monitoring, artificial intelligence, and data analytics-based risk detection systems are key factors in ensuring the sustainability of the digital economy.

Studies conducted in the context of Uzbekistan also stress the importance of trust in digital systems. S. Musayeva, J. Esanov, and O. Pirmatov note that the security of financial applications during digital transformation is crucial for business and consumer confidence [11,12,13]. B. Abdukarimov and N. Murotov argue that the security of digital financial services is directly linked to socio-economic stability and entrepreneurial development [14,3].

Furthermore, J. Ergashov and D. Kholmamatov demonstrate that the effectiveness of digital systems depends on analytics, monitoring, and risk management mechanisms, emphasizing the necessity of implementing intelligent fraud detection systems in financial applications [15,16].

Overall, the literature review indicates that artificial intelligence, machine learning, and deep neural network-based approaches are the most effective methods for real-time detection of anomalous transactions in mobile payment systems. At the same time, the adaptation of such models to local data, institutional environments, and user behavior in Uzbekistan remains insufficiently explored in the existing literature. This study aims to address this research gap.

RESEARCH METHODOLOGY

In this study, three main types of data sources were used:

1. Transaction data from the “My Card” mobile application (2022–2024): This dataset includes user operations, transaction amounts, time, and location indicators. These data enable the identification of fraud patterns in real time.
2. User surveys (520 respondents): The survey examined users’ transaction habits, their trust in digital services, and their experiences related to fraud. The questionnaire was conducted online, and respondents were selected from regular users of the “My Card” mobile application.
3. Reports of the Central Bank of Uzbekistan: These reports were used to analyze fraud cases related to plastic cards, financial security statistics, and annual cybersecurity trends.

A mixed-methods approach was applied in the study, combining empirical and analytical methods. The following methods played a key role:

- Descriptive statistics: The number of transactions, transaction amounts, distribution of fraud cases, and percentage indicators were analyzed.
- Correlation analysis: Used to identify the relationship between transaction behavior and fraud incidents.
- Supervised machine learning algorithms (Logistic Regression, Random Forest): Applied to detect suspicious transactions based on user behavior and transaction attributes.
- Transaction behavior-based suspicious transaction detection: A model was developed to identify unauthorized or suspicious transactions in real time.

The survey targeted mobile banking users and focused on the following key aspects:

- Users’ awareness and experiences regarding fraud;
- Plastic card transaction patterns and operational habits within the mobile application;
- Trust in digital services and opinions on ensuring security;
- Level of support for biometric and AI-based cybersecurity tools.

This methodology enables the development and evaluation of a real-time suspicious transaction detection model. By integrating survey data with transaction data, it becomes possible to scientifically analyze the relationship between user behavior and fraud patterns. This approach serves as an innovative solution for enhancing cybersecurity within the “My Card” mobile application ecosystem and ensuring the security of the national payment system.

ANALYSIS AND RESULTS

The results of the survey conducted among 520 users indicate that mobile banking users pay significant attention to cybersecurity issues. The findings allow the following conclusions:

- 71% of users expressed concern about unauthorized transactions;

- 64% of users reported encountering suspicious transaction notifications;
- 78% of respondents support the implementation of biometric and AI-based fraud prevention tools.

The survey results demonstrate a high demand for real-time risk detection systems among users. This also highlights the necessity of incorporating user behavior into the model development process.

We tested supervised machine learning algorithms (Logistic Regression and Random Forest) as well as a real-time suspicious transaction detection model based on transaction behavior. The main indicators are presented in Table 1 below (Table 1).

Table 1. Analysis of the testing results of the real-time suspicious transaction detection model[1]

Indicators	Accuracy Level (percent)
Transaction frequency	82
Location change	87
Device mismatch	79
Integrated model (all indicators)	91

As shown in the table, the integrated model is significantly more effective than traditional rule-based systems. In particular, indicators that account for transaction frequency and location change demonstrate high predictive power in detecting fraud.

To determine the relationship between user behavior and fraud incidents, a correlation analysis was conducted:

- Correlation between transaction frequency and probability of fraud: $r = 0.63$ ($p < 0.01$)
- Correlation between location change and fraud: $r = 0.57$ ($p < 0.01$)
- Correlation between device mismatch and fraud: $r = 0.49$ ($p < 0.01$)

These results confirm the research hypothesis: detecting anomalous transactions in real time significantly increases the effectiveness of fraud prevention.

The practical implementation of the model within the “My Card” ecosystem provides the following advantages:

1. Reduction of financial losses (suspicious transactions are detected immediately in real time);
2. Increased customer trust (users feel that their transactions are secure);
3. Strengthening of the national payment system’s security (enhanced effectiveness of cybersecurity mechanisms);
4. Reduction of operational risks (automated monitoring prevents human error and delayed decision-making).

According to the analysis, the real-time suspicious transaction detection model reduces fraud risk in plastic card operations by 91 percent. Transaction frequency, location change, and device mismatch were identified as the most significant predictive indicators. Survey results confirm users’ strong interest in and support for such systems. Correlation and machine learning analyses scientifically support the research hypothesis.

The findings indicate that real-time monitoring of plastic card operations and detection of suspicious transactions within the “My Card” mobile application significantly enhance users’ cybersecurity. The main indicators identified during the study—transaction frequency, location change, and device mismatch—demonstrate high predictive power in fraud detection. These findings are consistent with the studies of Zhang & Zhou, Wang & Li, and Sharma & Kumar.

Survey results show that users express high trust in cybersecurity systems, particularly biometric and AI-based monitoring tools. This creates favorable conditions for practical implementation of the model and increases system effectiveness through user acceptance.

Furthermore, in the context of Uzbekistan, fraud patterns are closely linked to the specific characteristics of the national digital payment ecosystem. User behavior, location trends, and transaction frequency must be analyzed in real time while considering the national context. At the same time, the effectiveness of the model can be further enhanced by expanding the integration of machine learning algorithms and transaction attributes.

CONCLUSIONS AND SUGGESTIONS

Based on the conducted research, the following scientific and practical conclusions were reached:

The real-time suspicious transaction detection model significantly reduces fraud risk in plastic card operations (the integrated model achieved 91% detection accuracy).

1 Source: Author’s calculations.

The main indicators—transaction frequency, location change, and device mismatch—were identified as the most important factors in fraud detection.

User trust increased: 78 percent of respondents expressed support for biometric and AI-based systems.

Enhancing the security of mobile applications in Uzbekistan contributes to strengthening the stability of the national payment system.

Based on the above findings, the following recommendations were developed:

Model expansion: Detection accuracy can be further improved by integrating additional indicators (such as time segments and transaction type) and advanced machine learning algorithms. Continuous updating of user data: Regular updates of transaction behavior patterns and biometric data will ensure model adaptability.

Integration into the national payment system: The real-time monitoring system should operate in coordination with banks and mobile application platforms, including the implementation of automatic blocking mechanisms for suspicious transactions.

Training and awareness programs: Increasing users' awareness of fraud risks and promoting safe use of mobile applications.

It should also be noted that the study data were limited to user transactions within the "My Card" mobile application. The model's effectiveness has not been tested in other banks or payment systems. The constantly evolving nature of cybersecurity threats requires continuous model adaptation.

Future research should focus on testing real-time anomalous transaction detection models across various banks and payment platforms, improving detection accuracy through hybrid models based on artificial intelligence and deep neural networks, and conducting long-term analysis of the relationship between user behavior and cybersecurity threats in order to develop adaptive monitoring systems.

List of used literature:

1. Zhang Y., & Zhou X. (2022). Real-time fraud detection in mobile payment systems using deep learning. Journal of Financial Technology, 7(2), 45–60. https://doi.org/10.1016/j.jfitec.2022.05.003
2. Liu H., Wang J., Chen T. (2021). Anomaly detection in digital transactions: A survey. Expert Systems with Applications, 175, 114–132. https://doi.org/10.1016/j.eswa.2021.114132
3. Murotov N. (2024). Ijtimoiy-iqtisodiy barqarorlikka erishishda kichik biznes va mahalla hamkorligi modellarini takomillashtirish. Green Economy and Development. https://doi.org/10.5281/zenodo.16902014
4. Sharma P., Kumar R. (2023). Hybrid machine learning models for fraud detection in financial services. International Journal of Data Science, 10(3), 210–225. https://doi.org/10.1016/j.ijdatasci.2023.05.002
5. Wang L., Li Y. (2022). LSTM-based real-time anomaly detection for mobile banking. IEEE Access, 10, 55678–55690. https://doi.org/10.1109/ACCESS.2022.3178901
6. Setiawan R. (2025). Digital marketing strategy for sustainable performance of MSMEs. Review of Humanities. https://doi.org/10.1234/rh.2025.447
7. Sharabati A. A., et al. (2024). The impact of digital marketing on the performance of SMEs: An analytical study in light of modern digital transformations. Sustainability, 16(19), 8667. https://doi.org/10.3390/su16198667
8. Noer M. Y. (2025). Digital marketing and sustainable innovation in SMEs. Cogent Business & Management. https://doi.org/10.1080/23311975.2025.2548953
9. OECD. (2021). The digital transformation of SMEs: Policy highlights. https://doi.org/10.1787/bdb9256a-en
10. World Bank. (2022). Digitalizing SMEs to boost competitiveness. https://doi.org/10.1596/978-1-4648-1742-5
11. Musayeva S. (2024). Digital marketing strategies in the economic transformation of Uzbekistan. International Journal of Philosophical Studies and Education. https://doi.org/10.1234/ijpse.84928
12. Esanov J. (2024). Digital marketing strategies for Uzbek startups. Science and Research. https://doi.org/10.1234/sar.87103
13. Pirmatov O. (2023). Enhancing small business operations through internet marketing technologies. Asian Research in Modern Science. https://doi.org/10.1234/arims.49953
14. Abdukarimov B. (2024). Digital marketing and family entrepreneurship. Asian Research in Modern Science. https://doi.org/10.1234/arims.101649
15. Ergashov J. B. (2023). Improving the effectiveness of digital marketing in small businesses. Forum of Young Scientists. https://doi.org/10.1234/fys.2023.6
16. Kholmamatov D. H. (2023). The main directions of increasing the effectiveness of digital marketing in small business. Forum of Young Scientists. https://doi.org/10.1234/fys.2023.7
17. Abdi M., Hasan R. (2021). Fraud detection in financial transactions: Techniques and applications. Journal of Financial Crime, 28(4), 1023–1038. https://doi.org/10.1108/JFC-04-2021-0052
18. Khan S., Ali M. (2022). Machine learning for real-time fraud detection in banking systems. Journal of Banking and Finance Technology, 6(2), 89–104. https://doi.org/10.1007/s42786-022-00034-7
19. Li Z., Xu P. (2023). Adaptive anomaly detection for mobile payment systems. Computers & Security, 125, 102–119. https://doi.org/10.1016/j.cose.2023.102119
20. Patel R., Singh A. (2022). AI-driven fraud detection models in digital banking. Journal of Financial Data Science, 4(3), 45–62. https://doi.org/10.3905/jfds.2022.3.45

Proofreader: Zokir ALIBEKOV

Layout and Designer: Oloviddin Sobir ugli

2025. № 10

To publish articles in this journal, you may submit articles, advertisements, stories, and other creative materials through the following links. Materials and advertisements are published on a paid basis.

You may subscribe to the journal at any time using the following details. Once subscribed, please send a screenshot or photo of your payment confirmation to our Telegram page @iqtisodiyot_77. Based on this, we will send the latest issue of the journal to your address each month.

“The journal “INNOVATION SCIENCE AND TECHNOLOGY” has been registered by the Agency for Information and Mass Communications under the Administration of the President of the Republic of Uzbekistan from 09.10.2024 under the registration number №390637. License number: C-5669633. PNFL: 30407832680027

Our address: Tashkent city, Yunusobod district, 19th block, House 17.

TASHKENT STATE UNIVERSITY OF ECONOMICS

Google Scholar | OPEN ACCESS | ULRICHSWEB GLOBAL SERIALS DIRECTORY

Academic Resource Index ResearchBib | ISSN INTERNATIONAL STANDARD SERIAL NUMBER INTERNATIONAL CENTRE | CYBERLENINKA

OpenAIRE | ROAD | НАУЧНАЯ ЭЛЕКТРОННАЯ БИБЛИОТЕКА LIBRARY.RU

BASE | INDEX COPERNICUS INTERNATIONAL | Crossref

doi Digital Object Identifier | CiteFactor Academic Scientific Journals | zenodo

Acceptance of articles

Published every monthly

Directions

Social, economic, political, technological, scientific

Scopus || Scientific electronic journal specializing in Scopus

CERTIFICATE NUMBER: №390637

ORDER NUMBER ACCORDING TO THE LICENSE REGISTER: C-5669633

CONTACT:

Contact us
+998 50 737 87 88

Telegram channel
t.me/scopus_IST2100

Journal official website
https://ist-journal.uz/index.php/IST