TASHKENT STATE UNIVERSITY OF ECONOMICS

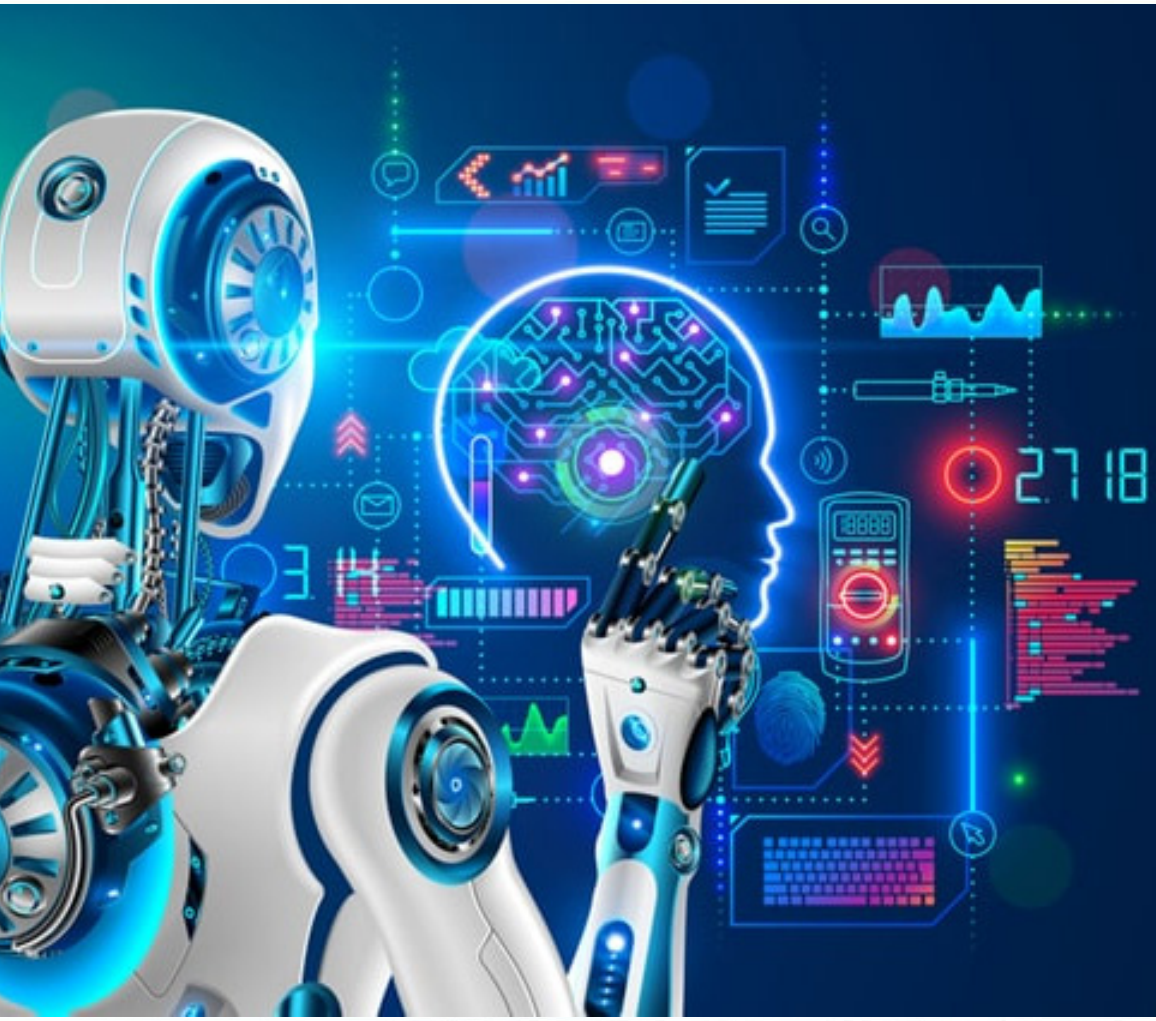
International journal of topics

INNOVATION SCIENCE AND TECHNOLOGY

Scopus || Electronic journal specializing in Scopus

ISSUE 12

Acceptance of papers **December, 2025**



Acceptance of papers

Published monthly

Topics

economics, technology, social sciences

ISSN 3060-5229

Visit the website t.me/scopus_IST2100

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 12. 288 pages.
Approved for publication on December, 2025.

Editorial board:

CONTENTS

CONTENTS

CONTENTS

DEVELOPMENT OF AN ARTIFICIAL INTELLIGENCE–BASED CYBERSECURITY SYSTEM FOR THE AUTOMATIC DETECTION OF FAKE FINANCIAL RECEIPTS, PHISHING URLS, AND MALICIOUS APK FILES

Shermatov Axlidin Sharobiddin o‘g‘li
Andijan State University
Faculty of Physics, Mathematics, and IT Engineering
Second-year master’s student in the educational program
70610101 – Computer Systems and Their Software
Email: akhlidinshermatov00@gmail.com

Abstract: It is through phishing attacks, fake payment documents and malicious mobile applications that a large part of financial fraud around the world is happening. As a result of such attacks, users ' bank card information, personal information and financial resources are being stolen. Especially young people and users who are actively using the internet are more susceptible to this type of attack. Therefore, the issue of ensuring financial information security is one of the most important tasks of today.

Key words: cyberattack, social environment, psychological factors, financial information, fake payment, mobile application.

Annotatsiya: Dunyo bo‘yicha moliyaviy firibgarliklarning katta qismi aynan phishing hujumlari, soxta to‘lov hujjatlari va zararli mobil ilovalar orqali sodir etilmoqda. Bunday hujumlar natijasida foydalanuvchilarning bank kartalari ma’lumotlari, shaxsiy axborotlari va moliyaviy mablag‘lari o‘g‘irlanmoqda. Ayniqsa, yoshlar va internetdan faol foydalanayotgan foydalanuvchilar ushbu turdagi hujumlarga ko‘proq duch kelmoqda. Shu sababli moliyaviy axborot xavfsizligini ta’minlash masalasi bugungi kunning eng muhim vazifalaridan biri hisoblanadi.

Kalit so‘zlar: kiberhujum, ijtimoiy muhit, psixologik omillar, moliyaviy axborot, soxta to‘lov, mobil ilova.

Аннотация: подавляющее большинство финансовых махинаций во всем мире совершается именно с помощью фишинговых атак, поддельных платежных документов и вредоносных мобильных приложений. Такие атаки приводят к краже данных банковских карт, личной информации и финансов пользователей. Особенно молодые люди и пользователи, активно пользующиеся интернетом, более подвержены этому типу атак. Поэтому вопрос обеспечения финансовой информационной безопасности является одной из важнейших задач сегодняшнего дня.

Ключевые слова: киберзапугивание, социальная среда, психологические факторы, финансовая информация, поддельные платежи, мобильное приложение.

INTRODUCTION

Today, the rapid development of information and communication technologies is deeply penetrating all spheres of social life, particularly the systems of finance, banking, electronic payments, and digital services. The widespread adoption of the internet, mobile applications, and electronic payment systems, while making everyday life more convenient, has also led to the emergence of new types of risks and threats. In particular, cybercrimes carried out through fake financial receipts, phishing URLs, and malicious APK files have become one of the most pressing problems of our time. According to statistical data, a significant share of financial fraud worldwide is committed precisely through phishing attacks, counterfeit payment documents, and malicious mobile applications. As a result of such attacks, users’ bank card details, personal information, and financial assets are stolen. Young people and active internet users are especially vulnerable to these types of threats. Therefore, ensuring the security of financial information has become one of the most important tasks today.

In his speech at the 72nd session of the United Nations General Assembly in September 2017, the President of the Republic of Uzbekistan, Shavkat Mirziyoyev, placed special emphasis on the importance of youth, education, and modern technologies, stating: “The development of any state and the well-being of its people primarily depend on young people growing up educated, proficient in modern technologies, and patriotic.” These remarks clearly demonstrate the growing attention currently being paid to the development of information technologies, particularly in the fields of cybersecurity and artificial intelligence. In addition, in a series of meetings and speeches held during 2020–2023, President Shavkat Mirziyoyev identified the development of the digital economy, information security, and the strengthening of cybersecurity as priority directions of state policy. As emphasized by the Head of State, “Along with the development of digital technologies, it is necessary to ensure information security and to introduce effective mechanisms to prevent cyber threats.” In implementing these tasks, the use of artificial intelligence and machine learning technologies is of particular importance.

REVIEW OF LITERATURE ON THE SUBJECT

A cybersecurity system designed to automatically detect fake financial receipts, phishing URLs, and malicious APK files based on artificial intelligence provides effective protection against modern threats [2]. In the field of cybersecurity, artificial intelligence (AI) plays a crucial role in the rapid detection of malware, phishing attacks, and counterfeit documents. Fake financial receipts, fraudulent URLs, and malicious APK files lead to significant financial losses for users [1][2].

This system analyzes behavioral patterns using machine learning algorithms and predicts threats in advance. Phishing URLs are intended to deceive users and steal personal information and are often distributed through unofficial websites. Malicious APK files cause harm on Android devices in the form of trojans and ransomware [1][3].

Fake financial receipts are often generated using AI-based image generation techniques, allowing them to appear authentic and bypass traditional verification methods. Machine learning algorithms, such as deep learning, identify malicious files through detailed analysis. For phishing detection, website content and URL structures are thoroughly analyzed [2].

In detecting fake receipts, computer vision technologies (CNNs) are used to verify the authenticity of text, shapes, and signatures. The system consists of a data ingestion module, an AI analytical core, and a response module. Incoming files and URLs are scanned in real time, and suspicious items are blocked immediately [2].

During the training process, both supervised and unsupervised algorithms are applied. For malicious APKs, behavioral analysis is combined with static scanning. For phishing URLs, natural language processing (NLP) is used to identify fraudulent text patterns [2]. For fake receipts, pixel-level image analysis and blockchain-based verification are integrated to reduce false positives.

RESEARCH METHODOLOGY

Artificial Intelligence Algorithms, Machine Learning Methods, Software Tools, and Databases Used for Detecting Fake Financial Receipts, Phishing URLs, and Malicious APK Files

ANALYSIS AND RESULTS

In the context of globalization and digitalization, cybersecurity issues have become one of the most significant challenges, carrying not only technical but also economic and social importance. Along with the widespread adoption of digital financial services, electronic payment systems, mobile banking applications, and online commerce platforms, the scale and complexity of cybercrime have increased substantially. Practical experience shows that traditional cybersecurity tools are often unable to provide sufficient effectiveness in detecting and preventing many modern attacks. This situation necessitates a fundamental improvement of cybersecurity systems and the introduction of new approaches based on advanced technologies.

In particular, fake financial receipts are visually very similar to genuine documents, making them difficult to identify not only for ordinary users but, in some cases, even for experienced specialists. Since such documents are created using high-quality graphic tools, conventional visual inspection methods fail to deliver reliable results. At the same time, phishing URLs are designed on behalf of trusted banks or financial institutions and aim to exploit user trust to obtain login credentials, bank card details, and other sensitive information. Malicious APK files, in turn, are capable of stealing personal data without user consent, controlling financial transactions, or damaging system resources on mobile devices.

The common characteristic of these threats is that they continuously evolve and are able to bypass traditional signature-based protection mechanisms. However, it would be incorrect to view this situation solely as a limitation. On the contrary, it demonstrates the broad opportunities for applying artificial intelligence

technologies in the field of cybersecurity. AI-based approaches are particularly well suited to detecting complex, hidden, and rapidly changing cyber threats with a high level of effectiveness.

From this perspective, the development of AI-based automatic detection systems represents a highly relevant scientific and practical task. Such systems are capable of processing large volumes of data in real time, identifying anomalous behavior, and adapting to new types of attacks. For example, in image analysis, the use of OCR technologies enables in-depth examination of text, numbers, and visual elements in financial receipts. The application of natural language processing (NLP) methods in semantic analysis of texts and URLs significantly increases the accuracy of phishing link detection. With regard to malicious APK files, assessing their potential risk level is achieved through the analysis of both static and dynamic behavioral characteristics.

A key advantage of this approach is that it is not limited to detecting only known attacks but is also capable of identifying new and previously unseen cyber threats. For this reason, artificial intelligence–based cybersecurity systems serve as effective, adaptive, and resilient tools for preventing financial fraud.

This article comprehensively examines the development of a cybersecurity system designed to automatically detect fake financial receipts, phishing URLs, and malicious APK files using artificial intelligence. Particular attention is paid to the selection of modern machine learning algorithms, the evaluation of their effectiveness, and their testing on real-world data. The main objective of the study is to create a reliable and efficient mechanism for detecting cyber threats through the use of artificial intelligence technologies and to expand its practical applicability.

Within the scope of this project, the defined tasks are structured through a consistent and systematic approach. Specifically, the sources and characteristics of threats are identified through an in-depth analysis of financial cyber risks and their main types. Studying the attack mechanisms implemented via fake receipts, phishing URLs, and malicious APK files enables the proper design of the system architecture. In the process of selecting and justifying artificial intelligence and machine learning algorithms, criteria such as accuracy, speed, and adaptability are taken into account.

In addition, the formation of datasets and the design of the database represent critical stages in ensuring the stable operation of the system. By developing the software of the automatic detection system and implementing it in the form of a web platform or bot, a user-friendly and widely accessible solution is created. At the final stage, the developed system is tested, the obtained results are analyzed, and practical recommendations are formulated to further enhance system performance.

CONCLUSIONS AND SUGGESTIONS

Within the framework of the developed application, the cybersecurity system can be applied to protect users through banks and financial institutions, IT companies, electronic payment services, as well as Telegram and web platforms. The system enables rapid, reliable, and automatic detection of fake financial receipts, phishing URLs, and malicious APK files, provides a user-friendly interface, improves detection accuracy, and helps prevent financial fraud. By strengthening cybersecurity, the system contributes to reducing financial fraud incidents. In the future, the integration of quantum computing and federated learning may be considered [2]. Continuous updates and increased user awareness will further enhance the system's effectiveness.

List of used literature:

1. Ian Goodfellow, Yoshua Bengio, Aaron Courville. Deep Learning. – Cambridge: MIT Press, 2016. – 775 p.
2. Christopher M. Bishop. Pattern Recognition and Machine Learning. – New York: Springer, 2006. – 738 p.
3. Ting-Fang Yen, Michael K. Reiter. Traffic Aggregation for Malware Detection. // IEEE Transactions on Dependable and Secure Computing. – 2010. – Vol. 7. – No. 2. – P. 131–145.
4. Maikantis P., Medvedev A., Jansen J. Phishing URL Detection Using Machine Learning Techniques. // International Journal of Cyber Security and Digital Forensics. – 2018. – Vol. 7. – No. 2. – P. 109–121.
5. Shafiq M.Z., Tabish S.M., Mirza F., Farooq M. Android Malware Detection Using Static Analysis and Machine Learning. // International Conference on Emerging Technologies. – IEEE, 2019. – P. 1–6.
6. Andrei G. Chuvakin, Kevin Schmidt, Chris Phillips. Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management. – Waltham: Syngress, 2013. – 384 p.
7. Enrico De Cristofaro, Giovanni Vigna. Automated Detection of Phishing Attacks Using Natural Language Processing. // ACM Conference on Computer and Communications Security. – 2017. – P. 241–252.
8. Arp D., Spreitzenbarth M., Hubner M., Gascon H., Rieck K. Drebin: Effective and Explainable Detection of Android Malware in Your Pocket. // NDSS Symposium. – 2014. – P. 1–15.
9. Nidal K. Kheir, Nael Salman. OCR-Based Fraud Detection in Financial Documents Using Deep Learning. // Journal of Information Security and Applications. – 2020. – Vol. 55. – Article 102627.
10. Stuart Russell, Peter Norvig. Artificial Intelligence: A Modern Approach. – 4th ed. – London: Pearson, 2021. – 1136 p.

Proofreader: Zokir ALIBEKOV

Layout and Designer: Oloviddin Sobir ugli

2025. № 12

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