AMERICAN JOURNAL OF EDUCATION AND LEARNING
ISSN: 2996-5128 (online) | ResearchBib (IF) = 10.91 IMPACT FACTOR
Volume-3| Issue-9| 2025 Published: |30-10-2025|

AI-POWERED PHISHING DETECTION IN UZBEKISTAN: IMPLEMENTATION STRATEGIES AND CHALLENGES

https://doi.org/10.5281/zenodo.17439674

Kattabek Norbaev
Presidential School in Samarkand, Uzbekistan
Email: norboyevkattabek@gmail.com

Abstract

Phishing and related cyber threats are rising worldwide and have become a significant issue in Uzbekistan. The country's digital adoption is high (89% internet penetration as of 2024), and recent reports highlight surging cyberattacks and fraud (e.g., over 12 million attack attempts in 2024, with fraud complaints up 34%). AI-powered detection systems—using techniques like natural language processing (NLP), machine learning (ML), and fine-tuned language models—offer promising accuracy; for example, a recent fine-tuned language model achieved 97.5% accuracy on a phishing dataset, and classical ML methods have yielded comparable results. This study examines the potential implementation of such AI solutions in Uzbekistan's context. We review state-of-the-art anti-phishing algorithms and analyze local factors (language, internet usage, regulatory environment). Our analysis finds that while technically feasible—supported by Uzbekistan's national AI strategy and digital initiatives—effective deployment faces challenges: Uzbek is a low-resource language with limited corpora, and infrastructure or data limitations may impede training and deployment. We propose a framework combining multilingual NLP, continual learning, and integration with cybersecurity policies. The findings suggest AI-driven phishing defenses could substantially reduce risk, but success depends on building local datasets, computational capacity, and expertise. Future work should focus on creating Uzbek phishing corpora and pilot deployments to validate these approaches.

Keywords

artificial intelligence, phishing detection, cybersecurity, machine learning, natural language processing, Uzbekistan, Central Asia, deep learning, cyber threats

1. Introduction

Phishing is a pervasive and growing cyber threat worldwide, wherein attackers deceive users into revealing sensitive information. According to the Anti-Phishing Working Group (APWG), phishing incidents increased by over 25% in

2022, as attackers employ AI-generated emails and sophisticated social-engineering tactics. Traditional defenses (signatures, blocklists) have struggled to keep pace, leading researchers to develop AI-driven detection methods. Modern approaches using ML, deep learning (DL), and NLP automatically extract features from email content and URLs, achieving extremely high accuracy on benchmark datasets. For example, long short-term memory (LSTM) models have reached >99% accuracy on phishing email datasets, and character-level convolutional networks have achieved ~98.7% accuracy in URL-based detection. Hybrid architectures combining CNN and LSTM also show strong results by capturing both local and sequential patterns. These advances suggest that AI-powered phishing detectors can significantly outperform older methods in theory.

In Uzbekistan, the digital landscape has expanded rapidly, making the population an attractive target for phishing. By 2024, about 89% of Uzbeks were online, driven by e-government and mobile payment initiatives. Correspondingly, cybercrime in Uzbekistan has surged: official data report over 12 million attempted cyberattacks in 2024 (up from 11 million in 2023), and fraud complaints increased by 34%. Over the past five years, Uzbek law enforcement notes a 68-fold increase in cybercrime cases, with nearly half of all criminal cases in 2024 involving digital offenses. In particular, financial fraud now accounts for a large share (≈35%) of incidents. The Central Bank and regulators have responded by mandating banks to monitor and report phishing websites, fake banking apps, scam emails/SMS, and other online fraud. New laws require implementation of advanced anti-fraud systems and Digital Risk Protection platforms to detect phishing and brand abuse in real time. This regulatory backdrop creates both an imperative and opportunity for deploying AI defenses.

1.1 The Ajina Banking Trojan Campaign

Figure 1. Timeline of daily infections from the "Ajina" banking trojan campaign (November 2023–August 2024). This chart, based on Group-IB's analysis, shows a steady rise in infections among Central Asian users. Such persistent trends underscore how quickly new phishing and malware scams can spread in the region. Notably, Uzbek attackers and malware often localize their lures: Group-IB reports describe fraudulent messages in Uzbek offering fake bonuses, disseminated via Telegram with malicious APK links. At the same time, classic scams like the "Hello, Mom" phone fraud have targeted Uzbek residents (especially Russian speakers). These examples illustrate that effective detection in Uzbekistan must handle multiple channels (email, messaging, SMS) and languages (Uzbek, Russian) attuned to regional contexts.

1.2 Research Objectives

This paper explores how AI-powered phishing detection systems could be effectively implemented in Uzbekistan. We bridge global AI detection research with Uzbekistan's specific cybersecurity landscape. Key questions include: What AI techniques (e.g., ML classifiers, deep learning, LLMs) are most suitable for phishing detection? How can these be adapted to Uzbek/Russian languages and local data? What infrastructural and policy factors will influence deployment? We address these by (1) reviewing technical approaches (NLP, anomaly detection, model fine-tuning) used in anti-phishing systems, (2) analyzing Uzbekistan's cyber data and legal framework, and (3) synthesizing a feasibility assessment. In the following sections, we outline our methodology, present the findings of this analysis, discuss the technical and contextual challenges, and conclude with recommendations for implementing AI detection in the Uzbek cybersecurity environment.

2. Methods

Our study combines a systematic literature review with analysis of local cybersecurity sources. We first surveyed recent research on AI-based phishing detection, including academic papers and industry reports. We focused on techniques such as natural language processing of email content, ML classification of URLs, and fine-tuning of language models for phishing email analysis. Key works included Naveen et al. (2025) on integrated email/URL detection, Blake (2025) on a fine-tuned LLaMA-based phishing detector, and Thapa et al. (2025) on comparative ML vs. LLM methods.

Second, we collected data on Uzbekistan's digital environment from news articles, government reports, and cybersecurity forecasts. Relevant information included statistics on attack volume, typical phishing vectors (e.g., messaging apps, local scams), and new regulations mandating fraud monitoring.

Third, we mapped the technical requirements of AI phishing systems to Uzbekistan's context. This involved considering language models (Uzbek/Russian), available computing infrastructure, and institutional factors (e.g., IT sector capacity, regulatory compliance). Based on these inputs, we developed a conceptual framework for an AI-driven phishing filter tailored to Uzbekistan and identified technical capabilities and potential obstacles. Our results synthesize these findings rather than report novel experimental data.

2.1 Methodological Steps

1. Literature review: Gather and analyze AI/ML/NLP techniques for phishing detection, including model architectures (CNN, RNN, Transformers) and training strategies.

2. Local data analysis: Compile Uzbekistan-specific cyber threat information, including incident statistics, case studies (malware campaigns, local scams), and regulatory guidelines.

3. Requirements identification: Determine system requirements by aligning detection methods with local constraints (e.g., language, data, infrastructure).

4. Design conceptual system: Propose a high-level architecture for an AI-powered phishing detection platform in Uzbekistan, highlighting integration points (email servers, mobile platforms) and operational workflow.

3. Results

Our analysis yields several insights about the potential effectiveness and design of AI-based phishing detection in Uzbekistan:

3.1 High Detection Accuracy in Research

AI models have demonstrated very high accuracy on phishing datasets. Studies report >95% accuracy (and near 100% recall) using ML and DL classifiers. For example, the "PhishSense-1B" model (a fine-tuned LLM) achieved 97.5% accuracy on a custom phishing dataset. Classical models like XGBoost have also reached ~99.9% accuracy on benchmark sets. These results suggest that, under ideal conditions, AI systems can effectively distinguish phishing from legitimate messages. Moreover, hybrid approaches that combine email body (textual) analysis with URL/link analysis have been shown to improve performance, indicating that a multi-modal system would be most robust.

3.2 Multilingual and Multimodal Inputs

In practice, an Uzbek system must handle multi-language and multi-channel data. Existing detection research often focuses on English email corpora, but Uzbekistan's phishing content will include Uzbek and Russian text. Preliminary NLP work in Uzbek shows that transformer models can achieve ~85% F1-score on news classification, implying they may be trainable for phishing content if data is available. Additionally, phishing attacks in Uzbekistan frequently exploit non-email channels (e.g., social media messages, SMS, malicious apps). Therefore, a practical system should integrate with email servers, web gateways, and even messaging platforms (via APIs) to capture all relevant indicators.

3.3 Infrastructure and Sector Readiness

Uzbekistan's developing IT ecosystem can support AI deployment. The country hosts over 2,000 IT firms (IT Park initiative) and is investing in data center capacity. Government support for AI (Uzbekistan's 2030 AI strategy) provides a favorable environment. However, many small businesses have limited cybersecurity budgets and expertise, suggesting reliance on cloud/Security-as-a-

Service rather than in-house systems. In the financial sector, strong regulatory pressure (mandatory fraud detection, reporting to the Central Bank) creates a use-case for integrating AI filters into banking infrastructure.

3.4 Regulatory Alignment

New laws explicitly require real-time phishing/fraud monitoring and reporting in finance and state institutions. This means that banks and payment processors have both legal obligation and incentive to deploy advanced detection. AI tools could be incorporated into banks' transaction monitoring systems or fraud centers. The existing practice of "name-and-shame" for breaches further motivates robust defenses. In summary, the alignment of technical capability (AI methods) with policy push (cybersecurity mandates) suggests feasibility for implementation, provided technical challenges are addressed.

4. Discussion

Implementing AI phishing detection in Uzbekistan poses several interrelated technical and contextual challenges:

4.1 Data and Language Resources

Uzbek is a low-resource language for NLP. There are few public corpora of Uzbek text, let alone labeled phishing examples. Building effective models will require collecting and annotating local phishing emails and websites. Russian is better supported, but culturally contextual content (e.g., idioms, official templates) still requires localization. Models like multilingual BERT (mBERT) or a monolingual Uzbek BERT (e.g., BERTbek) exist, but both will need domain-specific fine-tuning. Without sufficient Uzbek-language training data, the AI detectors may have lower accuracy or higher false positives.

4.2 Technical Resources and Scalability

State-of-the-art deep learning and LLM-based detectors are often resource-intensive. For instance, the best small-model variant (DeepSeek R1 Qwen 14B) used ~15GB VRAM and hours of processing. Uzbekistan's data centers are expanding (e.g., new 250 MW facility), but many organizations (especially SMEs) cannot afford such hardware. Cloud-based deployment (leveraging regional cloud services or hybrid cloud) could alleviate this, but raises data residency and latency issues. Moreover, internet bandwidth in some areas may limit real-time processing of incoming messages. Thus, a practical system might need to balance model complexity: for example, using smaller quantized models or distillation techniques, combined with periodic batch analysis.

4.3 Integration with Local Ecosystem

Phishing detection cannot operate in isolation. Integration points include email servers, web proxies, payment gateways, and mobile OS (for app

downloads). Uzbekistan's high smartphone adoption means many phishing links arrive via mobile apps or SMS. Any solution must integrate with mobile messaging (e.g., scanning links in Telegram chats) or email clients popular locally. This raises challenges of platform compatibility and user privacy. On the policy side, data-protection laws and upcoming regulations (e.g., data localization requirements) may constrain centralized data collection, forcing on-premises or hybrid architectures. Collaboration with local telecoms and ISPs might be necessary to block known phishing domains at the network level.

4.4 User Behavior and Awareness

Technology alone is not sufficient. Uzbekistan reports emphasize that human factors (social engineering, urgency, and trust) are exploited by phishers. Users may be less familiar with spotting scams, especially in Uzbek language which has only recently become the primary script. AI systems should therefore provide user-friendly explanations or warnings when blocking a message (some LLM-based systems can output natural-language rationales). Ongoing training and awareness campaigns will be needed alongside AI tools to reinforce safe behavior.

4.5 Adversarial and Evasion Tactics

As AI detectors improve, attackers may adapt. For example, prompts or generative AI could be used by phishers to craft emails that bypass static filters. The literature notes that detectors degrade in performance when faced with AI-rephrased phishing content. This implies the need for continual learning and possibly adversarial training of models. Given the rapid evolution of phishing tactics (including AI-generated deepfakes and multilingual campaigns), any deployed system must be regularly updated and possibly supported by threat intelligence feeds.

4.6 Economic and Ethical Factors

Only 30% of Uzbek SMEs currently use modern cybersecurity, often due to cost. Widespread AI deployment may require government subsidies or inclusion in IT Park programs. Ethically, AI systems must avoid bias—for instance, misclassifying legitimate Uzbek-script emails due to tokenization issues. Privacy is another concern: email scanning requires handling personal data, so strong data protection and possibly anonymization must be built in to comply with national laws.

4.7 Opportunities through Government Support

Uzbekistan's leadership is actively pursuing AI and digital goals. The first national AI strategy (approved 2024) emphasizes human-centered AI development and regulatory readiness. Large-scale projects (e.g., UN-hosted forums, big data center investments) indicate the country is building capacity. These factors could be

leveraged to fund pilot deployments in critical sectors (banking, telecom) and partnerships between government, universities, and IT companies. For example, Uzbekistan's Cybersecurity Center could collaborate with research labs to curate phishing datasets, and universities could run detection models as part of cybersecurity curricula.

5. Conclusion

AI-driven phishing detection systems can be effectively implemented in Uzbekistan, but only by carefully adapting to local conditions. The country's high connectivity and supportive AI policy framework create an opportunity for advanced cyber defenses. However, significant challenges must be addressed: the Uzbek language's low-resource status and mixed-language context, scarcity of labeled phishing data, and limited technical expertise in many organizations.

Successful implementation will require a phased approach. Initially, focused efforts should build annotated Uzbek phishing corpora and fine-tune multilingual models. Pilot deployments in larger banks or government agencies (which have regulatory mandates and resources) can validate performance and workflows. Concurrently, less-resourced businesses may adopt cloud-based or managed AI security services. Continuous collaboration between the government, industry, and academia is essential to keep models updated as attacks evolve.

Our analysis indicates that with these measures, AI-based filters could dramatically reduce phishing success rates. Key to this will be integrating machine learning outputs with user education and incident response processes. For future work, researchers should develop specialized NLP tools for Turkic languages and create benchmarks for Uzbek phishing detection. Field trials could measure real-world efficacy and refine detection thresholds. In summary, AI-powered anti-phishing holds great promise for Uzbekistan's cybersecurity, but its benefits will only be realized through targeted localization efforts, capacity-building, and alignment with national strategies.

REFERENCES:

Abdullayev, B. (2024). Enhancing cybersecurity in Uzbekistan: Leveraging artificial intelligence solutions. International Journal of Innovative Science and Research Technology, 9(10), 1–8.

Blake, S. E. (2025). PhishSense-1B: A technical perspective on an AI-powered phishing detection model. arXiv preprint arXiv:2503.10944.

Dentons. (2025, May 14). Uzbekistan tightens cybersecurity obligations: What businesses need to know.

https://www.dentons.com/en/insights/articles/2025/may/14/uzbekistan-tightens-cybersecurity-obligations

Grau, G. (2024, December 6). Harnessing AI for development: Uzbekistan's progress towards becoming a regional IT hub. Oxford Insights. https://oxfordinsights.com/insights/harnessing-ai-for-development-uzbekistans-progress-towards-becoming-a-regional-it-hub/

Group-IB. (2024, September 12). Ajina attacks Central Asia: Story of an Uzbek Android pandemic [Blog post]. https://www.group-ib.com/blog/ajina-malware/

Kun.uz. (2025, February 3). Over 12 million cyberattacks recorded in Uzbekistan in 2024. https://kun.uz/en/news/2025/02/03/over-12-million-cyberattacks-recorded-in-uzbekistan-in-2024

Kuriyozov, E., Salaev, U., Matlatipov, S., & Matlatipov, G. (2023). Text classification dataset and analysis for Uzbek language. arXiv preprint arXiv:2302.14494.

Naveen, P. K., Pranessh, A. C. N., & Sasikala, L. (2025). AI-driven phishing detection using NLP and URL analysis. SSRN Electronic Journal. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5560918

Thapa, J., Chahal, G., Voinea Gabreanu, Ș., & Otoum, Y. (2025). Phishing detection in the gen-AI era: Quantized LLMs vs. classical models. arXiv preprint arXiv:2507.07406.

UZCERT. (2024). Forecast of major cyber threats in Uzbekistan for 2025. Uzbekistan Computer Emergency Response Team. https://uzcert.uz/en/forecast-of-major-cyber-threats-in-uzbekistan-for-2025/

UzDaily. (2025, October 14). Security of growth: Why 2025 became a point of no return for cybersecurity in Uzbekistan. https://www.uzdaily.uz/en/security-of-growth-why-2025-became-a-point-of-no-return-for-cybersecurity-in-uzbekistan/

Uzbekistan Ministry of Digital Technologies. (2025). Uzbekistan: Cybersecurity obligations for companies [In Uzbek]. (Presidential Decree No. PQ-153).

Author Information:

Kattabek Norbaev is a student at the Presidential School in Samarkand, Uzbekistan, with research interests in artificial intelligence, cybersecurity, and their applications in Central Asian contexts.