Volume 4, Issue 3 March 2026 **ISSN (E):** 2938-3757

CYBERSECURITY IN UZBEKISTAN'S BANKING SYSTEM: RISKS AND MITIGATION

A. B. Mirzayeva 1, 2,
N. B. Nasrullayev 1,
I. I. Qobilov 3
1) Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti
2) Eurasian Multidisciplinary University
3) Student, Eurasian Multidisciplinary University

Abstract
Uzbekistan's banking sector is becoming increasingly digital, and this transformation is reshaping its cybersecurity risk profile. As mobile banking, online payments, and interconnected financial services continue to grow, vulnerabilities are no longer confined to technical infrastructure alone. They increasingly arise from the interaction between human behavior, weak authentication, insecure integrations, fragmented monitoring, and limited incident-response maturity. This article explores the main cybersecurity vulnerabilities affecting Uzbekistan's banking system and outlines practical directions for improving resilience. The analysis shows that phishing, social engineering, access-control weaknesses, mobile banking and API security gaps, and underdeveloped anti-fraud and governance mechanisms remain among the most serious concerns. The article argues that these risks should be addressed through a layered security model that combines stronger identity protection, secure development practices, integrated monitoring, AI-assisted fraud detection, and sustained awareness-building. In doing so, it provides a more grounded view of how cybersecurity resilience can be strengthened in the national banking sector.

Keywords: Banking system, cybersecurity, mobile banking, API security, anti-fraud, zero trust, cyber resilience, phishing, compliance.

Introduction

Uzbekistan's banking sector has changed rapidly in recent years. Mobile banking, online payments, remote services, and digital financial platforms have become a routine part of how banks interact with customers and deliver services [1], [3]. This shift has made banking faster and more accessible, but it has also created a more exposed and more complicated cybersecurity environment. Risk is no longer confined to internal infrastructure alone. It now extends across customer-facing applications, employee accounts, mobile devices, API connections, transaction processes, and third-party integrations that support the delivery of digital services [2], [11].

Because of this, cybersecurity in banking cannot be understood only as a matter of protecting servers, databases, or networks. In practice, many incidents emerge when several weaknesses begin to overlap. A phishing email may lead to stolen credentials, weak authentication may allow unauthorized access, insecure API connections may widen the scope of compromise, and

Web of Technology: Multidimensional Research Journal
webofjournals.com/index.php/4

fragmented monitoring may delay detection until the damage has already spread [7], [8], [11]. In highly digital banking environments, vulnerabilities rarely remain isolated. They tend to interact across human, technical, and organizational layers, which makes the overall risk environment more difficult to manage.

This issue is especially important for Uzbekistan, where the banking sector continues to expand its digital reach and where customer expectations around speed, convenience, and always-available service are growing [1], [3], [5]. As more banking activity moves into mobile and online channels, the pressure on institutions is no longer just to innovate, but to do so without weakening security. That is not always easy. A bank may appear secure in formal terms and still remain vulnerable in practice if its controls are poorly connected, if monitoring is inconsistent, or if staff and customers are not prepared for realistic attack scenarios [4], [5]. In other words, the real challenge is not only whether security mechanisms exist, but whether they work together in a way that reflects actual operational risk.

Recent research also shows that banking cybersecurity is no longer discussed only in narrow technical terms. It is increasingly approached as a broader issue shaped by trust, user behavior, fraud patterns, governance, privacy, and the security of interconnected digital services [6], [7]. This shift is visible across several lines of research. One group of studies focuses on trust and digital adoption, showing that users are more willing to rely on fintech and digital banking services when they see the environment as secure and reliable [6]. That perspective is useful, but it also has limits. Trust may encourage adoption, yet trust by itself does not reduce exposure if weak controls remain embedded in the system. Another important strand of the literature examines fraud and financial crime in digital payment environments. These studies suggest that fraud patterns are becoming faster, more adaptive, and harder to detect through static or purely rule-based controls [7]. As transaction speed increases, delayed response becomes more costly, which is why recent research places greater emphasis on real-time monitoring, behavioral analytics, and more intelligent transaction scoring. This point matters for banking systems that are expanding digital payment services while still trying to build more mature anti-fraud capacity.

The human factor remains one of the most consistent themes in the literature. Research on employee cybersecurity awareness repeatedly shows that the security posture of an institution depends heavily on whether staff can recognize phishing attempts, suspicious requests, and manipulation tactics that exploit routine behavior or urgency [8]. In banking, this issue is particularly serious because employees work directly with customer data, payment instructions, approvals, and privileged access. A technically strong environment can still be compromised if the people operating within it are not prepared for deception-based attacks. That is why awareness is increasingly treated not as a secondary training matter, but as a structural part of security itself.

Mobile banking has also become one of the most discussed areas in recent research. Existing studies suggest that users often associate convenience with safety, even though the actual strength of protection behind mobile banking services may vary considerably [9], [10]. Questions of authentication, privacy, session security, and user-facing protection remain central here. At the same time, stronger measures such as biometrics, device-aware controls, and

Web of Technology: Multidimensional Research Journal
webofjournals.com/index.php/4

enhanced warning systems are not always adopted consistently across platforms or user groups [10]. This makes mobile banking one of the most visible and sensitive parts of the broader cybersecurity landscape in financial services.

A closely related area of research concerns API and open banking security. As banks become more connected to external platforms and digital service ecosystems, API security has moved from being a narrow technical issue to a central question of governance and service integrity. Studies in this area point to weaknesses in authorization logic, token management, consent handling, and access control over sensitive financial data [11]. These weaknesses are significant because they do not only expose information; they may also create paths for abuse inside transaction processes and customer-account operations.

More recently, attention has also shifted toward AI-based fraud detection and cybersecurity analytics. These studies suggest that machine-learning approaches can improve the detection of suspicious activity, particularly in high-volume digital environments where static controls no longer provide enough visibility [12], [13]. At the same time, the literature is far from uncritical. Concerns about false positives, explainability, privacy, and accountability remain especially important in regulated sectors such as banking. For that reason, AI is increasingly viewed not as a standalone answer, but as one layer within a broader security architecture that still depends on governance, oversight, and operational discipline.

Taken together, this body of research makes one thing clear: cybersecurity risk in banking is no longer defined by individual technical flaws alone. It is shaped by how human behavior, digital service architecture, fraud dynamics, access control, and institutional governance come together in practice. Yet despite the growing richness of international research, studies that examine Uzbekistan's banking system from this integrated perspective remain relatively limited [2], [6]–[13]. Much of the available literature treats trust, fraud, mobile security, or API risk as separate concerns, while actual vulnerabilities in banking tend to emerge at the intersection of these areas.

Against this background, the present article examines the major cybersecurity vulnerabilities affecting Uzbekistan's banking system and identifies practical directions for improving cyber resilience in the sector. Particular attention is given to phishing and social engineering, authentication and access-control weaknesses, mobile banking and API security gaps, fragmented monitoring and anti-fraud mechanisms, and the broader issue of governance and incident-response maturity. Bringing these issues together in one analytical frame makes it easier to see not only where the main weaknesses lie, but also why they become more dangerous when they begin to reinforce one another.

Materials and Methods

The study adopts a qualitative analytical approach to identify the main cybersecurity vulnerabilities relevant to Uzbekistan's banking system and to interpret them within their local institutional context. It focuses on the cybersecurity weaknesses most frequently observed in modern banking environments and examines their relevance to the operational and regulatory setting of Uzbekistan's banking sector. The analysis relied on two main groups of sources. The first included recent academic publications on banking cybersecurity, digital payment fraud,

Web of Technology: Multidimensional Research Journal
webofjournals.com/index.php/4

mobile banking security, open banking and API risks, employee cybersecurity awareness, and AI-assisted fraud detection. These sources helped identify the risk patterns, solution directions, and unresolved issues most frequently discussed in the broader literature. The second group included regulatory and institutional materials related to Uzbekistan's banking and payment environment, particularly documents addressing sectoral cybersecurity oversight and minimum security requirements for financial institutions and payment systems. This combination made it possible to interpret the problem in light of Uzbekistan's own regulatory and institutional setting rather than through global research trends alone.

The study did not attempt to build a statistical model or conduct an empirical incident-based evaluation, since openly available bank-specific cybersecurity incident data for Uzbekistan remain limited. Instead, the methodology relied on comparative thematic analysis. At the first stage, the reviewed sources were examined to identify recurring categories of cybersecurity risk. At the second stage, these risks were grouped into broader analytical themes, including human-factor vulnerability, authentication and access-control weakness, mobile banking and API exposure, fragmented monitoring and anti-fraud capacity, and governance together with incident-response maturity. At the third stage, these themes were interpreted in relation to the regulatory and operational setting of Uzbekistan's banking system.

This approach made it possible to move beyond a simple descriptive review of literature. Rather than listing risks in isolation, the analysis focused on how different vulnerabilities interact and how they may reinforce one another in practice. This is particularly important in banking, where cyber incidents rarely emerge from a single failure alone. More often, they develop through the combined effect of weak identity protection, human error, insecure integration, delayed detection, and insufficient organizational readiness.

The main strength of this approach is that it connects academic findings with local regulatory realities in a single analytical framework. It brings together academic findings and local regulatory realities within a single analytical framework, making it possible to identify not only what kinds of vulnerabilities are discussed in the literature, but also why they matter in the specific context of Uzbekistan's banking sector. At the same time, the study has clear limitations. Because the analysis is based on open literature and public regulatory documents, it does not capture confidential incident records, internal bank audit results, or institution-specific security metrics. Even so, the selected materials provide a sufficiently strong basis for identifying the dominant cybersecurity risk directions relevant to the sector.

Results

The analysis shows that one of the most significant cybersecurity weaknesses in the banking sector is the human factor. In practice, phishing, spear-phishing, social engineering, and deception-based attacks often succeed not because banking systems lack all technical protection, but because attackers are able to exploit trust, routine behavior, and limited situational awareness. This makes employee behavior and customer awareness central to cybersecurity resilience rather than secondary concerns. In the context of Uzbekistan, this issue is especially important as digital banking services continue to expand and users increasingly rely on remote channels for routine financial activity [1].

Web of Technology: Multidimensional Research Journal
webofjournals.com/index.php/4

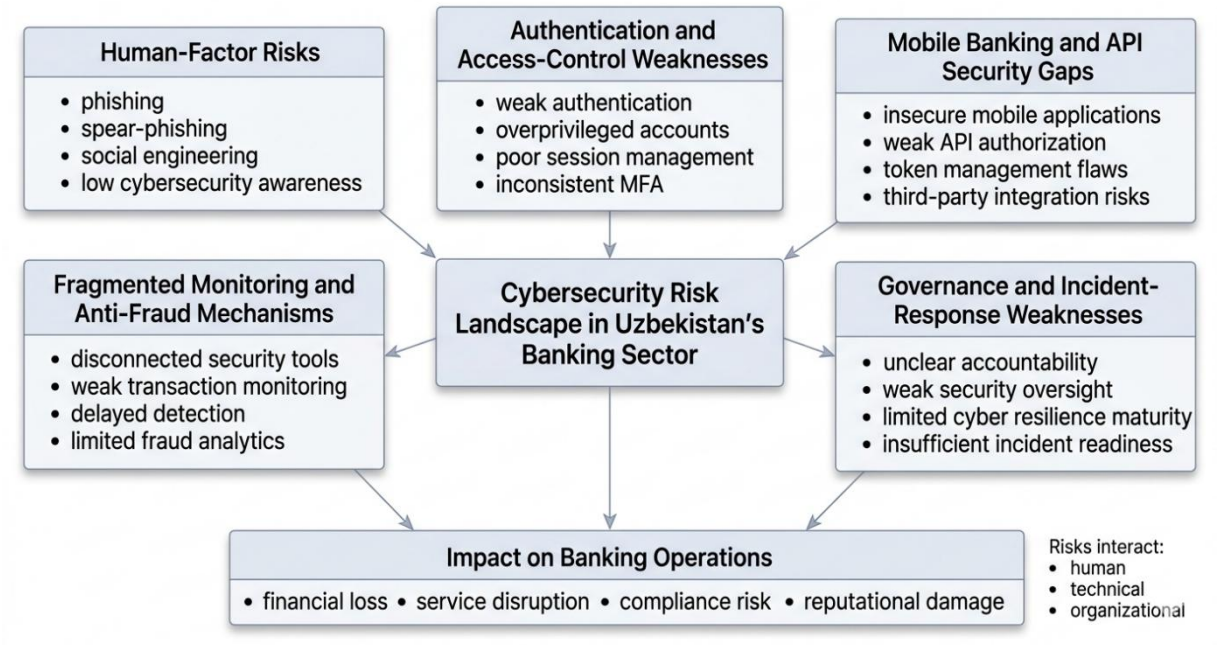

Figure 1. Integrated Cybersecurity Risk Landscape in Uzbekistan's Banking Sector

A second major area of vulnerability concerns authentication and access control. Excessive reliance on passwords, weak session management, overprivileged accounts, and the uneven implementation of multi-factor authentication increase the likelihood of unauthorized access and account compromise. In banking environments, these weaknesses are particularly serious because they affect not only data confidentiality, but also transaction integrity and operational continuity. The literature on mobile and digital banking also suggests that the practical use of stronger protective mechanisms, including biometric controls and enhanced user-verification measures, remains inconsistent across platforms and user groups [9], [10].

The analysis also points to mobile banking and API ecosystems as a growing source of exposure. As banks extend their services through mobile applications, digital platforms, and third-party integrations, the number of security-sensitive interfaces increases. Weak authorization logic, insecure token handling, flawed consent mechanisms, and business-logic weaknesses in APIs can create direct pathways to abuse [11]. This issue is becoming more important as banks place greater emphasis on interoperability, service speed, and customer convenience, sometimes faster than security governance can mature.

Another important weakness lies in the fragmentation of monitoring and anti-fraud mechanisms. Many institutions deploy a range of protective technologies, including logging systems, endpoint protection, IDS/IPS tools, and anti-fraud controls, yet these tools do not always operate as part of a unified monitoring architecture. When visibility remains fragmented, early signs of compromise may go unnoticed, suspicious patterns may be missed, and incident response may be delayed. This challenge is particularly relevant in digital payment environments, where fraud can evolve quickly and where delayed detection may translate directly into financial and reputational loss [7].

The findings further suggest that governance remains a critical but often underestimated dimension of banking cybersecurity. Security failures are not always caused by the absence of

Web of Technology: Multidimensional Research Journal
webofjournals.com/index.php/4

technical controls; in many cases, they persist because responsibilities are poorly defined, oversight is weak, audit findings are not translated into corrective action, or incident-response processes remain immature. In the banking sector, where cyber risk is closely tied to service continuity, customer trust, compliance, and institutional reputation, governance gaps can significantly weaken the effectiveness of otherwise reasonable technical measures [2]–[5]. Taken together, these findings show that cybersecurity vulnerabilities in banking rarely operate in isolation. They tend to interact across technical, human, and organizational layers, creating a risk environment in which one weakness can amplify the consequences of another. This means that the problem is not simply the existence of individual vulnerabilities, but the way they combine within the broader structure of digital banking operations.

Discussion

The findings suggest that cybersecurity weaknesses in banking should not be understood as separate technical problems. In practice, they form an interconnected risk environment in which one weakness often makes another more dangerous. A phishing message may expose credentials, weak authentication may allow unauthorized access, insecure integrations may widen the scope of compromise, and fragmented monitoring may delay detection until the incident has already produced financial or operational consequences. This layered pattern helps explain why isolated security measures rarely provide sufficient protection in digital banking environments. One important implication is that identity security has to be treated as a priority rather than as a supporting control. In a sector where employees, administrators, and customers interact with critical systems through digital channels, weak authentication can quickly turn a limited incident into a broader compromise. Stronger multi-factor authentication, stricter privilege management, and more disciplined control over administrative access are therefore not optional improvements; they are foundational requirements for reducing exposure in practice.

The same logic applies to mobile banking platforms and API ecosystems. As banks continue to expand customer-facing digital services and integrate with external platforms, security can no longer be treated as something added after functionality has already been built. It has to be embedded into the design, development, and governance of digital services from the beginning. Secure software development, API inventory control, source-code review, token protection, and transaction-level safeguards all become more important when service speed and interoperability are driving digital expansion.

The findings also underline the importance of integrated monitoring and anti-fraud capability. A bank may have multiple technical controls in place and still remain vulnerable if those controls do not produce coherent visibility across the environment. Detection is no longer only about identifying malware or unauthorized access. It is also about recognizing suspicious transaction behavior, unusual user activity, device anomalies, and patterns that may indicate fraud or account abuse. In this sense, resilience depends not only on prevention, but also on the ability to observe, interpret, and respond in real time.

Another important point is that governance remains central to cybersecurity effectiveness. Technical tools are unlikely to deliver strong results if ownership of cyber risk is unclear,

Web of Technology: Multidimensional Research Journal
webofjournals.com/index.php/4

incident-response procedures are weak, or security decisions are not supported at the management level. In banking, where compliance, service continuity, customer trust, and reputational stability are tightly connected, governance weaknesses can magnify even relatively ordinary technical risks. This makes cybersecurity not only an IT issue, but a broader institutional responsibility. The discussion also highlights the role of AI in banking security. AI-assisted fraud detection and anomaly analysis may significantly improve the speed and depth of detection, especially in high-volume digital environments. At the same time, AI should not be treated as an automatic solution to structural security problems. Without explainability, accountability, and operational oversight, such systems may introduce new difficulties, including false positives, opaque decisions, and reduced trust in the detection process. Their value depends on how well they are integrated into a broader security architecture rather than on the novelty of the technology itself.

Overall, the results point toward a simple but important conclusion: cybersecurity resilience in the banking sector depends less on individual tools than on how well technical controls, human awareness, monitoring capacity, and institutional governance work together. For Uzbekistan's banking system, this means that progress will depend not only on adopting stronger technologies, but also on building a more coordinated and mature security model across the sector.

Conclusion

Cybersecurity problems in Uzbekistan's banking system rarely come from one technical weakness alone. They tend to take shape when several gaps begin to overlap: human error, weak access control, insecure digital services, fragmented monitoring, and limited organizational preparedness. Once these weaknesses start interacting, even a minor issue can escalate into a much broader operational and security concern. The analysis makes one thing clear: banking security does not become stronger simply by adding more tools. It remains fragile when controls are introduced formally but do not work together in practice, when suspicious activity is noticed too late, when responsibilities are vague, or when both employees and customers are unprepared for real attack scenarios. The real issue is not the number of security measures in place, but whether they function as part of a coordinated and workable system.

In Uzbekistan's banking sector, this points to the need for a more consistent and layered model of protection. Stronger identity security, tighter access control, more secure development and management of digital services, and better coordination between monitoring, fraud detection, and incident response all matter here. AI-based detection may help, but only when it is used carefully, understood properly, and supported by clear operational oversight.

The main value of this article lies in bringing these vulnerability areas together instead of treating them as separate problems. Phishing, access-control weakness, mobile banking security, API exposure, anti-fraud capability, and governance are closely connected in practice, and they need to be understood that way if banking security is to improve in any meaningful sense. Looking at them as parts of a single risk environment makes it easier to see where the real pressure points are and where improvement is most needed. There is still room to take this

Web of Technology: Multidimensional Research Journal
webofjournals.com/index.php/4

work further. Future research could move toward more practical models for the sector, including expert-based risk prioritization, sector-specific maturity assessment, and AI-oriented detection approaches built on synthetic banking attack scenarios. That would help shift the discussion from general analysis to more applied security solutions that reflect the realities of Uzbekistan's banking environment.

References

1. UZCERT, Forecast of Major Cyber Threats in Uzbekistan for 2025. Available: https://uzcert.uz/en/forecast-of-major-cyber-threats-in-uzbekistan-for-2025/
2. S. Wang et al., "Data privacy and cybersecurity challenges in the digital banking sector," Computers & Security, 2024.
3. Central Bank of the Republic of Uzbekistan, About the CERT-CBU Cybersecurity Center of the Central Bank. Available: https://cbu.uz/uz/cert/about/
4. LEX.UZ, Regulation on Ensuring Information Security and Cybersecurity in the Payment Systems of Payment System Operators and Payment Service Providers, No. 3513, May 21, 2024. Available: https://lex.uz/docs/-6933268
5. LEX.UZ, Regulation on Minimum Information Security and Cybersecurity Requirements for Commercial Banks of the Republic of Uzbekistan, No. 3669, August 18, 2025. Available: https://lex.uz/uz/docs/-7689673
6. J. A. Jafri et al., A Systematic Literature Review of the Role of Trust and Security in FinTech and Banking Adoption, 2023.
7. V. Laxman et al., Emerging Threats in Digital Payment and Financial Crime: A Bibliometric Review, 2025.
8. R. C. Chanda et al., "Assessing cybersecurity awareness among bank employees: a multi-stage analytical approach," Computers & Security, 2025.
9. Y. Hanif et al., "Security factors on the intention to use mobile banking applications," 2021.
10. I. Riasat et al., "Strengthening cybersecurity resilience: adoption of emerging security tools in mobile banking apps," 2025.
11. P. Modesti et al., "Security analysis of open banking account and transaction APIs," 2025.
12. E. Mollik and F. Majeed, "AI-Driven Cybersecurity in Mobile Financial Services: Enhancing Fraud Detection and Privacy in Emerging Markets," 2025.
13. H. Yaseen et al., "Adoption of Artificial Intelligence-Driven Fraud Detection in Banking," 2025.

Web of Technology: Multidimensional Research Journal
webofjournals.com/index.php/4