PROBLEMS AND SOLUTIONS OF SCIENTIFIC AND INNOVATIVE RESEARCH
Volume 02, Issue 05, 2025

SECURITY MEASURES AND TECHNICAL REQUIREMENTS FOR DIGITAL BANKS

Sharipova Nigina Djurakulovna
Teacher of Samarkand Institute of Economics and Service

Annotation: This text explores the multifaceted approach required to ensure the security of digital banks. It analyzes how digital-only financial institutions must rely on advanced technological infrastructure, secure development practices, and regulatory compliance to protect sensitive customer data and maintain service continuity. The discussion includes the importance of encryption, authentication systems, fraud detection mechanisms, secure APIs, and cloud infrastructure configurations. Emphasis is placed on the necessity of integrating security throughout the system lifecycle, educating users and staff, managing third-party risks, and adhering to evolving legal standards. The text concludes that successful digital banking depends not only on technical excellence but also on building and maintaining customer trust through resilience, transparency, and proactive risk management.

Keywords: digital banking, cybersecurity, secure architecture, data protection, authentication, encryption, fraud prevention, secure APIs, cloud security, user awareness, cyber threats, compliance, zero-trust model, incident response, digital finance, financial technology, resilience, regulatory standards

Ensuring the security of digital banks is one of the most critical challenges in the modern financial landscape. As traditional banking services increasingly move online, the risks associated with cyber threats, data breaches, and unauthorized access grow accordingly. Digital banks rely entirely on information technology infrastructure to serve customers, manage transactions, and store sensitive data. This dependence means that any vulnerability in their systems can lead to serious consequences, including loss of trust, legal repercussions, and financial damage.

Security in digital banking is a combination of strong technological measures, organizational policies, and ongoing monitoring. At the core of digital bank security lies the protection of customer data. This includes safeguarding personal information, transaction records, account credentials, and all other forms of private communication between the bank and its users. Encryption is a fundamental part of this process, ensuring that data remains unintelligible to outsiders during storage and transmission. Alongside encryption, secure authentication mechanisms help verify

the identity of users before granting access to accounts. These often involve combinations of passwords, biometrics, and real-time verification methods that provide multiple layers of defense.

The technical requirements of digital banks extend beyond just strong authentication and data encryption. They include the development of secure mobile and web applications, robust back-end infrastructure, real-time fraud detection systems, and disaster recovery protocols. Applications must be designed to resist common attacks such as cross-site scripting, injection flaws, and session hijacking. Secure software development practices and regular code audits are essential to maintain the integrity of digital platforms. Moreover, digital banks must ensure their servers and databases are well-configured, updated, and protected from unauthorized access through firewalls and intrusion prevention systems. Another critical component of security in digital banking is continuous monitoring and threat intelligence. By analyzing traffic patterns and user behavior, banks can detect anomalies that suggest fraudulent activity or system compromise. Cybersecurity teams must respond quickly to incidents and apply patches and updates without delay.

Cloud security is also increasingly relevant, as many digital banks use cloud infrastructure to scale their operations. In such cases, it is vital to configure cloud environments securely, restrict access permissions, and maintain visibility over all assets. In addition to technical controls, regulatory compliance plays an important role. Digital banks must adhere to national and international standards on data protection, cybersecurity, and financial services. This includes compliance with laws concerning customer identity verification, anti-money laundering, and data privacy. Meeting these standards requires not only technical safeguards but also clear internal policies and staff training to ensure all employees understand their role in protecting information.

Since most digital banks operate with APIs to connect services such as payment processors, credit scoring systems, or identity verification platforms, they must ensure that these integrations do not create exploitable entry points for attackers. Authentication and identity management remain some of the most sensitive components in digital banking infrastructure. To reduce risks associated with password-based access, many banks implement biometric authentication such as fingerprint scans or facial recognition, especially on mobile devices. Device fingerprinting, behavioral analysis, and adaptive authentication mechanisms further help determine whether a user action is legitimate or potentially suspicious. For

example, changes in typing speed, geolocation, or transaction patterns can indicate compromised access or fraud attempts, prompting the system to request additional verification or temporarily block the transaction.

One of the most challenging aspects of digital bank security is ensuring data integrity and availability under constant external pressure. Distributed denial-of-service attacks, ransomware, and advanced persistent threats continue to evolve, targeting critical banking services. To withstand these attacks, digital banks often deploy redundant infrastructure, load balancing, and continuous data backups. These allow services to remain operational even during a breach or system failure. Logging, auditing, and forensic capabilities are built into the systems to ensure that any incident can be thoroughly analyzed and used to improve future defenses. Another key consideration is user education. Even the most robust digital banking platform can be undermined by user error, such as falling victim to phishing emails, downloading malicious apps, or sharing login information. As such, digital banks often provide customers with guidance on safe digital practices, regular reminders about current fraud techniques, and easily accessible help in case of suspicious activity.

In parallel, staff training is just as crucial. Employees who handle sensitive systems must understand social engineering risks, internal fraud scenarios, and how to respond to suspicious activity in real time. The operational environment of a digital bank must also be carefully segmented and monitored. Access to sensitive areas like core banking systems or encryption keys must be tightly controlled and granted only on a need-to-know basis. Zero-trust architecture, in which no internal or external device or user is automatically trusted, is increasingly adopted in digital finance to ensure that every action must be verified, regardless of origin. Moreover, automated tools continuously scan the network for signs of intrusion or unusual activity, reducing response time and limiting potential damage.

The legal and compliance landscape surrounding digital banking continues to grow more complex. Regulatory bodies require digital banks to demonstrate not only that they have strong cybersecurity policies in place, but also that they can prove ongoing compliance with data protection laws, financial transaction monitoring, and risk management protocols. Digital banks must produce detailed documentation and maintain audit trails to satisfy these obligations. Regulatory technologies, or RegTech, are often employed to help meet these demands through automation and analytics. Finally, public confidence in digital banks depends heavily on transparency, responsiveness, and demonstrated commitment to security. When data

breaches or technical failures occur, how a digital bank handles the situation—both technically and in terms of public communication—can either preserve or severely damage its reputation. Therefore, incident response planning, customer notification procedures, and legal preparedness must all be part of the overall security strategy.

References:

1. Anderson, Ross. Security Engineering: A Guide to Building Dependable Distributed Systems. 3rd ed., Wiley, 2020.
2. European Central Bank (ECB). Cyber Resilience Oversight Expectations for Financial Market Infrastructures. ECB, 2018.
3. Basel Committee on Banking Supervision. Sound Practices: Implications of Fintech Developments for Banks and Bank Supervisors. Bank for International Settlements, 2018.
4. National Institute of Standards and Technology (NIST). Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1, 2018.