HSR (LONDON),
HOUGHTON STREET REVIEW JOURNAL
ISSN: 2058-5519|Impact factor-15.9
http://houghtonstreetreview.com/index.php/hsr

THE ROLE OF MODERN DIGITAL TECHNOLOGIES IN ENSURING FINANCIAL INFORMATION SECURITY IN THE DIGITAL ECONOMY

Atakhanov Sanjarbek Anvarovich
International Institute of Food Technology and Engineering
Assistant Lecturer
Rajabov Jasurbek Rustamovich
1st-year student, Accounting International
Institute of Food Technology and Engineering
doi:https://doi.org/10.5281/zenodo.24523918

Abstract. This article examines the theoretical foundations and practical mechanisms for ensuring financial information security amid the rapid expansion of the digital economy. It systematizes contemporary cyber threats emerging from the widespread adoption of remote banking, Open Banking interfaces, and digital payment infrastructures. The study evaluates the effectiveness of Artificial Intelligence and Machine Learning (AI/ML), Blockchain and Distributed Ledger Technologies (DLT), Zero Trust Architecture (ZTA), multifactor biometric authentication, and post-quantum cryptography in safeguarding the confidentiality, integrity, and availability of financial assets. Practical recommendations are formulated for implementing a multi-layered cybersecurity ecosystem within financial institutions.

Keywords: digital economy, financial information security, cybersecurity, artificial intelligence, blockchain, Zero Trust architecture, biometric authentication, antifraud systems, cryptography.

1. Introduction

The digital transformation of the modern global economy has fundamentally reshaped the mechanisms of financial intermediation. The proliferation of electronic payment systems, mobile banking, Central Bank Digital Currencies (CBDCs), and Decentralized Finance (DeFi) platforms has accelerated capital velocity and significantly lowered transaction costs. However, the complete migration of financial assets and sensitive customer records into digital ecosystems has simultaneously made financial institutions primary targets for sophisticated cyberattacks.

Within the framework of the 'Digital Uzbekistan – 2030' strategy, comprehensive reforms are underway to digitize the banking and financial sector, expand cashless settlements, and foster a resilient fintech ecosystem. Yet, as digital infrastructure grows more interconnected, financial organizations face escalating risks stemming from social engineering, phishing, ransomware, API vulnerabilities, and insider threats.

HSR (LONDON),
HOUGHTON STREET REVIEW JOURNAL
ISSN: 2058-5519|Impact factor-15.9
http://houghtonstreetreview.com/index.php/hsr

The objective of this research is to identify key cyber risks threatening financial information systems in the digital economy and to substantiate the architectural application of advanced digital technologies to mitigate these vulnerabilities.

2. Materials and Methods

The study employs systemic analysis, comparative evaluation, threat modeling, and a review of international information security standards, including ISO/IEC 27001, PCI DSS 4.0, and the NIST Cybersecurity Framework. To identify structural vulnerabilities within financial information systems, the STRIDE threat modeling methodology and the MITRE ATT&CK adversarial tactics matrix were utilized.

The defensive efficacy of modern cybersecurity technologies was evaluated against the core CIA triad—Confidentiality, Integrity, and Availability—alongside the principle of Non-repudiation for financial transactions. The analytical scope encompasses the digital infrastructures of commercial banks, payment service providers, and fintech enterprises.

3. Results and Discussion

Our findings indicate that traditional perimeter-based defenses, such as legacy firewalls and signature-based antivirus software, are insufficient in an era dominated by cloud computing, microservices, and Open Banking APIs. Modern financial institutions must transition toward proactive, intelligence-driven security architectures.

Table 1 systematizes the primary digital technologies safeguarding financial information, detailing their operational mechanisms, mitigated threat vectors, and practical effectiveness.

Table 1

Functional Classification of Modern Digital Technologies for Financial Information Security

Technology	Core Functional Mechanism	Mitigated Cyber Threats	Practical Effectiveness
Artificial Intelligence & ML (SIEM / SOAR / Antifraud)	User and Entity Behavior Analytics (UEBA), real-time anomaly detection, automated response	Payment card fraud, Account Takeover (ATO), Advanced Persistent Threats (APT)	Transaction risk scoring in <50 ms; up to 70% reduction in fraud-related financial losses
Blockchain & Distributed Ledger Technologies (DLT)	Decentralized consensus, cryptographic hashing, immutable audit trails	Ledger tampering, double-spending, transaction repudiation	100% audit transparency and elimination of Single Points of Failure (SPOF)

HSR (LONDON),
HOUGHTON STREET REVIEW JOURNAL
ISSN: 2058-5519|Impact factor-15.9
http://houghtonstreetreview.com/index.php/hsr

Zero Trust Architecture & Micro-segmentation	Continuous per-request verification and strict least-privilege access control	Malicious insiders, lateral malware propagation across internal networks	Containment of potential data breaches within isolated micro-segments
Multifactor Biometrics & FIDO2 / Passkeys	Facial, voice, fingerprint recognition paired with hardware cryptographic keys	Credential phishing, password stuffing, SIM-swapping attacks	Passwordless secure authentication and high-assurance customer identity verification
Homomorphic Encryption & Post-Quantum Cryptography	Computation on encrypted data without decryption; quantum-resistant key exchange	Cloud data exposure, future quantum cryptanalysis ('harvest now, decrypt later')	Privacy-preserving interbank data sharing and long-term data confidentiality

Artificial Intelligence and Machine Learning (AI/ML) serve as the cornerstone of contemporary antifraud engines. Models built on gradient boosting (XGBoost, LightGBM) and deep neural networks analyze behavioral biometrics in real time (within milliseconds), evaluating device tilt angles, keystroke dynamics, geolocation patterns, and historical transaction profiles. This capability detects unauthorized transfers with 98–99% accuracy while substantially reducing false-positive declines that disrupt legitimate customer experiences.

Blockchain and Distributed Ledger Technologies (DLT) reinforce the immutability and auditability of financial records. Cryptographic hashing (SHA-256) combined with distributed consensus mechanisms prevents retroactive alteration of transaction histories. Furthermore, Smart Contracts automate settlement execution without intermediaries, minimizing operational risks in clearing and cross-border payments.

Adopting a Zero Trust Architecture ('never trust, always verify') effectively mitigates insider threats and lateral movement across corporate networks. Under this paradigm, every user, endpoint, and microservice is continuously authenticated and authorized via Multifactor Authentication (MFA) and the principle of least privilege, regardless of network location. Additionally, given advancements in quantum computing, preparing for migration to NIST-standardized post-quantum cryptographic algorithms (such as CRYSTALS-Kyber and CRYSTALS-Dilithium) is becoming essential for preserving long-term financial confidentiality.

HSR (LONDON),
HOUGHTON STREET REVIEW JOURNAL
ISSN: 2058-5519|Impact factor-15.9
http://houghtonstreetreview.com/index.php/hsr

4. Conclusion

Ensuring financial information security in the digital economy is not merely a technical IT function, but a strategic pillar of national economic resilience and public trust in the financial system. The research demonstrates that the synergistic integration of AI-driven antifraud analytics, distributed ledger technologies, Zero Trust architecture, and advanced cryptographic protocols establishes a robust defense-in-depth posture for financial assets.

Practically, financial institutions are advised to: first, upgrade Security Operations Centers (SOC) with AI-powered Security Orchestration, Automation, and Response (SOAR) platforms; second, enforce rigorous Open API security utilizing OAuth 2.0, mutual TLS (mTLS), and dynamic tokenization; and third, invest continuously in employee cyber hygiene training and customer digital financial literacy programs.

References

1. Atakhanov, S., & Turdimatova, R. (2023). Technology of Critical Thinking of Students on Biological Issues. Academia Repository, 4(12), 121-127.
2. Sanjarbek, A. (2023). The role of information technology in the treatment of cancer. Asian Journal Of Multidimensional Research, 12(4), 32-34.
3. Anvarovich, A. S., & Zavhiddinovich, J. A. (2026). BIG DATA AND MACHINE LEARNING IN ONCOLOGY EPIDEMIOLOGY: OPPORTUNITIES AND CONSTRAINTS IN CENTRAL ASIAN COUNTRIES. INNOVATION IN THE MODERN EDUCATION SYSTEM, 6(60), 16-21.
4. Anvarovich, A. S. (2026). ARTIFICIAL INTELLIGENCE IN SCREENING AND EARLY DIAGNOSIS OF GLAUCOMA AND DIABETIC RETINOPIA: A SYSTEMATIC REVIEW AND META-ANALYSIS FOR 2020-2025. SCIENTIFIC ASPECTS AND TRENDS IN THE FIELD OF SCIENTIFIC RESEARCH, 4(43), 65-68.
5. Anvarovich, A. S. (2025). MITOXONDRIAL DISFUNKTSIYA VA OKSIDATIV STRESSNING PARKINSON SINDROMI RIVOJLANISHIDAGI O ‘RNI. PEDAGOGICAL SCIENCES AND TEACHING METHODS, 6(51), 17-19.