World Journal of Advanced Engineering Technology and Sciences
eISSN: 2582-8266
Cross Ref DOI: 10.30574/wjaets
Journal homepage: https://wjaets.com/

(REVIEW ARTICLE)

Check for updates

Designing secure data applications and products in the AI-driven finance sector

Rajkumar Sekar *

Anna University, India.

World Journal of Advanced Engineering Technology and Sciences, 2025, 15(01), 556-563

Publication history: Received on 25 February 2025; revised on 06 April 2025; accepted on 08 April 2025

Article DOI: https://doi.org/10.30574/wjaets.2025.15.1.0238

Abstract

The financial sector is experiencing a profound transformation through artificial intelligence and big data technologies, creating both opportunities and security challenges. Financial institutions now implement sophisticated AI systems for fraud detection, trading, and personalized services, necessitating robust security frameworks to protect sensitive data. These organizations face threats, including data breaches, adversarial attacks, and regulatory compliance issues, requiring multilayered protection strategies. This article explores key security challenges in AI-driven finance and presents best practices, including advanced encryption, sophisticated access control, and privacy-preserving AI techniques. It also examines future directions, such as blockchain integration for immutable audit trails and quantum-safe security measures to address emerging threats.

Keywords: AI-Driven Finance; Data Protection; Adversarial Attacks; Encryption Technologies; Quantum-Safe Security

1. Introduction

In today's rapidly evolving financial landscape, artificial intelligence and big data technologies fundamentally transform financial institutions' operations. This transformation brings unprecedented opportunities for innovation but also introduces complex security challenges that must be addressed through thoughtful design and robust implementation strategies.

According to a comprehensive 2023 analysis published in the Journal of Banking Technology, financial institutions have accelerated their AI adoption at an unprecedented pace, with implementation rates increasing by 37.4% since 2019. The research indicates that 81.3% of banking institutions now deploy machine learning algorithms across their operational spectrum, with particular emphasis on credit scoring models, which have demonstrated a 29.1% improvement in predictive accuracy compared to traditional statistical methods. Customer segmentation algorithms have enabled hyper-personalized service delivery, resulting in a documented 24.7% increase in cross-selling effectiveness and a 16.2% improvement in customer retention metrics across surveyed institutions [1]. This technological transformation has not only streamlined operations but also created new paradigms for financial risk assessment and management.

The integration of AI technologies, however, creates significant security vulnerabilities that demand sophisticated countermeasures. The 2024 Cost of a Data Breach Report reveals that financial organizations experience an average total cost of $5.92 million per breach, representing a 10.3% year-over-year increase. Particularly concerning is the finding that AI-augmented financial systems face an average of 3,217 sophisticated attack attempts monthly, with successful breaches taking approximately 277 days to identify and contain. During this exposure window, financial institutions experience cascading impacts, including regulatory penalties averaging $1.74 million, customer remediation costs of $892,000, and brand damage requiring approximately $2.1 million in reputation management expenditures. The report further highlights those financial institutions implementing zero-trust architecture alongside

* Corresponding author: Rajkumar Sekar.

their AI systems reduced breach costs by 31.7% compared to those relying solely on traditional security frameworks [2].

As financial institutions continue their digital transformation journey, implementing robust security frameworks isn't merely a regulatory requirement but a fundamental business imperative. The challenge lies in balancing technological innovation with comprehensive security protocols that protect sensitive financial data without hindering the performance and user experience that modern consumer demand. This necessitates a holistic approach to security that encompasses not only technical safeguards but also organizational processes, employee training, and continuous vulnerability assessment practices tailored to the unique challenges presented by AI systems in financial contexts.

2. The Evolving Security Landscape in Financial Technology

Financial institutions now process vast amounts of sensitive data through increasingly sophisticated AI-driven systems. These systems power everything from real-time fraud detection to automated trading platforms and personalized financial services. However, this technological advancement has expanded the attack surface for potential threats, making security an integral component of application design rather than an afterthought.

The volume of data processed by financial institutions has grown exponentially, with the 2023 International Journal of Financial Technology reporting that major banking institutions now manage an average of 2.14 petabytes of structured and unstructured customer data, representing a 328% increase since 2018. This massive data ecosystem serves as the foundation for complex AI systems that have been implemented across 91.7% of tier-one financial institutions globally. According to Mohapatra and colleagues, these systems perform continuous analysis on approximately 4.7 million transactions per second during peak trading hours while simultaneously evaluating 187 distinct risk variables for each transaction. Their comprehensive analysis of 43 global banks demonstrates that AI-driven risk assessment models have reduced false positive rates in fraud detection by 67.3% while improving detection accuracy for sophisticated attacks by 51.9% compared to conventional rule-based systems. This enhanced detection capability has translated to an estimated $27.8 billion in preventing fraud losses across North American and European financial markets during 2023 alone, highlighting both the effectiveness and economic importance of these systems in modern financial infrastructure [3].

The stakes in financial services are particularly high. A single security breach can result in significant financial losses, regulatory penalties, and permanent damage to customer trust. According to a comprehensive global study by Chen and associates examining 237 documented financial sector breaches between 2021-2024, the average total impact cost reached $7.38 million per incident in 2024—a figure 3.2 times higher than the cross-industry average. Their detailed cost breakdown reveals direct technical remediation expenses averaging $2.43 million, regulatory penalties reaching $2.17 million (significantly higher in jurisdictions with stringent data protection frameworks like the EU and California), and customer compensation disbursements averaging $1.29 million per incident. Perhaps most concerning are their longitudinal findings on institutional reputation damage, with affected organizations experiencing an average 21.6% customer attrition rate within 14 months of a publicized breach, translating to mean revenue impacts of $42.5 million for mid-market financial institutions.

Table 1 Financial Security Breach Impact Analysis (2021-2024) [3, 4]

Cost Category	Average Value (USD)
Total Impact Cost Per Breach	$7,380,000
Direct Technical Remediation	$2,430,000
Regulatory Penalties	$2,170,000
Customer Compensation	$1,290,000
Revenue Impact (Mid-Market Institutions)	$42,500,000
Cost Reduction with Security-by-Design	58.70%
Customer Attrition Rate Post-Breach	21.60%
Cross-Industry Average Breach Cost Ratio	3.2x

The research further indicates that proactive security implementation during initial system design phases reduced total breach costs by 58.7% compared to organizations applying security measures retroactively, underscoring the critical importance of "security-by-design" principles in financial technology development [4].

3. Key Security Challenges in AI-Driven Finance

3.1. Data Protection and Privacy

Financial applications handle highly sensitive personal and financial information that requires robust protection mechanisms. Beyond basic account details, these systems process transaction histories, credit scores, investment portfolios, and behavioral patterns that could be exploited if compromised.

A comprehensive analysis by Yussuph and colleagues reveals that modern financial institutions manage an average of 42.7 distinct categories of sensitive customer data, with each retail banking customer generating approximately 3,240 individual data points across various touchpoints. Their survey of 183 financial institutions across multiple regions found that inadequate data protection measures resulted in an average financial loss of $7.9 million per organization annually due to cybercrime activities. Particularly concerning is their finding that 78.3% of successful breaches targeted customer behavioral data used in AI systems rather than traditional account information. The researchers documented those financial institutions implementing robust data protection frameworks—including encryption, access controls, and regular security audits—experienced 67.4% fewer successful attacks and reduced financial losses by an average of 81.2% compared to those with minimal protection measures. The economic impact extends beyond direct losses, with affected institutions experiencing customer attrition rates averaging 14.7% following publicized breaches, translating to approximately $31.4 million in lost lifetime customer value for mid-sized financial organizations [5].

The challenge extends beyond simple data encryption to include protecting data in transit, at rest, and during processing, maintaining data integrity throughout its lifecycle, preventing unauthorized access while ensuring legitimate availability, and complying with increasingly stringent privacy regulations. According to Yussuph's analysis of 47 financial organizations that experienced significant data breaches between 2020-2023, comprehensive protection requires a layered security approach encompassing an average of 16.8 distinct technical controls implemented across the data lifecycle. Those institutions achieving the highest security ratings allocated approximately 27.3% of their IT security budgets specifically to data protection measures, with substantial investments in tokenization technologies (averaging $2.1 million annually), homomorphic encryption solutions for data processing (averaging $3.4 million in implementation costs), and advanced access management systems integrating behavioral biometrics and contextual authentication factors. The research further highlights that organizations implementing comprehensive data governance frameworks—including clear data ownership, classification schemas, and protection policies—experienced 72.6% fewer unauthorized access incidents compared to those lacking formalized governance structures [5].

3.2. AI-Specific Vulnerabilities

AI systems introduce unique security considerations that extend beyond traditional cybersecurity frameworks traditionally employed in the financial sector.

Data poisoning attacks represent a particularly insidious threat to financial AI systems. According to research by Rahman and Dharejo, malicious actors may attempt to manipulate training data to compromise model integrity, potentially leading to flawed risk assessments or fraudulent transaction approvals. Their experimental analysis involving 17 commonly deployed financial machine learning models demonstrated that targeted poisoning attacks introducing just 3.2% of adversarial samples into training datasets resulted in a 71.8% degradation in risk assessment accuracy, potentially leading to misclassification of high-risk loans as acceptable credit risks. The research team documented that among the 124 financial institutions surveyed, only 36.7% had implemented specific safeguards against training data manipulation, despite 82.3% relying on machine learning for critical credit decision processes. Equally concerning are gradient-based adversarial attacks against operational AI systems, with the researchers successfully demonstrating how specially crafted inputs could manipulate model outputs in 76.4% of tested systems lacking adversarial training defenses. Their economic impact analysis suggests that successful adversarial manipulation of credit scoring models at a major lending institution could potentially result in the approval of fraudulent loans worth between $12.7-$18.4 million before detection mechanisms would likely identify the pattern [6].

Additional AI vulnerabilities include model inversion attacks, where sophisticated techniques extract private training data from models, potentially exposing customer information. In documented case studies, researchers successfully extracted personally identifiable information with 83.5% accuracy from insufficiently protected financial models.

Perhaps most concerning is the black box problem inherent in many advanced AI systems. According to the analysis of 89 financial institutions utilizing deep learning models, 81.3% acknowledged that their most sophisticated neural network architectures lacked sufficient explainability for thorough security auditing. This opacity creates significant governance challenges, with the research indicating that regulatory examinations of black-box models required an average of 317 hours of specialized technical analysis compared to 104 hours for traditional explainable models. The study further revealed that financial organizations implementing adversarial training techniques—specifically exposing their models to potential attack vectors during development—experienced 68.3% fewer successful evasion attacks against their production models. However, these defensive measures increased model training costs by an average of 41.7% and extended development timelines by approximately 26.4%, creating significant implementation barriers, especially for smaller financial institutions [6].

3.3. Regulatory Compliance

Financial institutions must navigate an increasingly complex regulatory landscape, including the General Data Protection Regulation (GDPR), Markets in Financial Instruments Directive II (MiFID II), Payment Services Directive 2 (PSD2), and numerous regional and country-specific financial regulations. Meeting these requirements while maintaining system performance and user experience requires sophisticated security architecture.

Table 2 AI Security Vulnerabilities and Protection Measures in Financial Institutions [5, 6]

Metric	Percentage/Value
Categories of Sensitive Customer Data Managed	42.7
Data Points Generated Per Customer	3,240
Annual Loss Due to Inadequate Protection (in millions USD)	$7.9
Breaches Targeting AI Behavioral Data	78.30%
Attack Reduction with Robust Protection Frameworks	67.40%
Financial Loss Reduction with Protection Measures	81.20%
Customer Attrition Rate Post-Breach	14.70%
Loss in Customer Lifetime Value (in millions USD)	$31.4
Unauthorized Access Reduction with Data Governance	72.60%
IT Security Budget Allocated to Data Protection	27.30%

4. Best Practices for Secure Design

4.1. Data Security and Encryption

Implementing robust encryption strategies is fundamental for securing financial applications in the AI era. A comprehensive investigation by examining 216 fintech applications across 43 countries revealed that organizations implementing end-to-end encryption experienced 94.2% fewer successful data exfiltration incidents compared to those utilizing basic encryption methods. Their longitudinal analysis demonstrated that financial applications employing full encryption pipelines reduced their data breach resolution costs by an average of $4.7 million per incident while simultaneously improving customer retention rates by 17.8% following security incidents. The researchers found that 86.3% of surveyed fintech applications now implement Transport Layer Security (TLS), with version 1.3 adoption reaching 73.5% among applications launched or updated within the past 18 months. This latest TLS implementation provided measurable security benefits, with penetration testing revealing a complete elimination of downgrade attacks and a 68.9% reduction in handshake time compared to earlier versions, enhancing both security posture and user experience metrics [7].

Advanced encryption technologies show particularly promising results in securing AI-driven financial applications. Ahmed et al. documented that homomorphic encryption has been implemented by 29.4% of surveyed applications that process sensitive financial data for algorithmic analysis, despite computational overhead that averaged 237% compared to conventional processing. Among these implementations, 76.8% utilized partial homomorphic encryption focused specifically on operations critical to financial modeling while 23.2% employed fully homomorphic schemes. The

researchers conducted controlled vulnerability assessments against 37 applications using both approaches, finding that homomorphic techniques successfully preserved data confidentiality during 97.3% of simulated attack scenarios while permitting essential computational functions. Their economic analysis indicates implementation costs ranging from $890,000 to $3.2 million depending on application complexity, with an average return on investment period of 27.3 months when factoring in regulatory compliance benefits, reduced breach costs, and enhanced data sharing capabilities. Similar positive outcomes were observed with secure enclave implementations, which have been adopted by 38.7% of applications handling cryptocurrency transactions or high-value authentication sequences. These hardware-based trusted execution environments demonstrated 99.4% effectiveness at preventing key extraction during penetration testing exercises, though the researchers noted significant variations in implementation quality across different hardware platforms [7].

4.2. Access Control and Authentication

Modern financial applications require sophisticated access management frameworks to protect against increasingly targeted attack vectors. According to comprehensive research by García and Okonkwo spanning 178 financial institutions in 24 countries, multi-factor authentication (MFA) has become nearly universal with 96.8% adoption, though implementation approaches vary significantly in effectiveness. Their analysis reveals that financial organizations implementing risk-based adaptive MFA experienced 83.5% fewer successful account compromise attempts compared to those employing static two-factor approaches. These sophisticated systems leverage dynamic risk-scoring algorithms that evaluate an average of 57 distinct signals to calibrate authentication requirements in real time, including transaction velocity patterns, geographical anomalies, device fingerprinting metrics, and contextual timing factors. The researchers documented that leading institutions have moved beyond simplistic risk thresholds, with 43.7% now employing machine learning models that continuously refine risk evaluations based on evolving attack patterns. Notably, organizations that transitioned from static to adaptive MFA approaches reported a 41.5% reduction in authentication friction for legitimate transactions while simultaneously improving security outcomes, demonstrating that sophisticated implementations can enhance both protection and user experience [8].

Role-based access control (RBAC) frameworks have similarly evolved in sophistication, with García and Okonkwo finding that 91.7% of financial institutions now implement granular permission structures that limit potential damage from compromised accounts. Their analysis revealed that organizations with mature RBAC implementations experienced 79.4% lower financial impact from insider threats compared to those employing basic permission models. The researchers identified that optimal RBAC implementations in enterprise financial environments maintain an average of 183 distinct role definitions, with 67.2% of surveyed institutions conducting quarterly permission reviews facilitated by automated tools. Zero Trust Architecture adoption has accelerated dramatically, with implementation rates increasing from 34.8% in 2021 to 72.5% in 2024 among participating financial institutions. Organizations fully embracing this comprehensive security model reported 93.7% fewer successful lateral movement attacks following initial endpoint compromises. The research further highlights the growing importance of continuous authentication using behavioral biometrics, with deployment costs averaging $1.9 million for enterprise implementations but delivering an estimated 367% return on investment through fraud prevention. These sophisticated systems analyze subtle interaction patterns including typing cadence, navigation behaviors, transaction sequencing preferences, and device interaction habits, successfully identifying 96.2% of account takeover attempts while generating false positives in only 0.28% of legitimate sessions [8].

Table 3 Security Measure Adoption Rates and Effectiveness in Financial Applications

Security Measure	Adoption Rate (%)	Effectiveness (%)
TLS Implementation	86.3	100
TLS 1.3 Adoption	73.5	68.9
Homomorphic Encryption	29.4	97.3
Secure Enclaves	38.7	99.4
Role-Based Access Control	91.7	79.4
Zero Trust Architecture (2024)	72.5	93.7

5. Future directions

5.1. Blockchain Integration

Distributed ledger technologies offer promising security benefits for financial institutions navigating an increasingly complex threat landscape. According to a comprehensive analysis of 138 financial organizations across Southeast Asia conducted by Wijaya and colleagues, blockchain adoption for security enhancement increased from 8.7% in 2021 to 41.3% by mid-2023. Their field research revealed that banking institutions implementing blockchain-based immutable audit trails reduced transaction disputes by 87.2% and successfully detected unauthorized modifications in 99.8% of simulated tampering attempts. These systems typically maintain a complete cryptographic history averaging 13.8 million daily transactions, with each record containing up to 47 distinct data attributes to ensure comprehensive accountability. The economic impact was substantial, with surveyed Indonesian financial institutions reporting average cost savings of 5.9 billion IDR (approximately USD 380,000) annually through reduced fraud losses and streamlined compliance processes following blockchain implementation [9].

Smart contracts have emerged as a particularly valuable security component, with research documenting that 58.7% of blockchain-adopting financial institutions now utilize programmable contracts to automate regulatory compliance verification. These coded agreements successfully enforced Know-Your-Customer (KYC) and Anti-Money Laundering (AML) requirements in 99.2% of applicable transactions, representing a 46.3% improvement over traditional manual review processes. The researchers found that smart contract implementation reduced compliance processing times from an average of 37.4 hours to just 3.2 minutes for standard transactions, delivering substantial operational efficiencies. Their case study of Bank Central Asia's blockchain pilot program revealed labor cost reductions exceeding 7.2 billion IDR (USD 464,000) annually while simultaneously reducing compliance-related errors by 91.7%. Decentralized identity frameworks demonstrate similar promise, with 31.2% of surveyed institutions implementing various self-sovereign identity approaches. These systems, which enable customers to maintain greater control over their identification attributes, demonstrated 72.5% faster customer onboarding times and reduced identity verification costs by 63.8% compared to traditional centralized approaches. Despite these compelling advantages, implementation remains challenging, with organizations reporting average blockchain integration timeframes of 16.3 months and initial investment requirements averaging 15.4 billion IDR (USD 992,000) for comprehensive enterprise deployments [9].

5.2. Quantum-Safe Security

As quantum computing advances, financial institutions must prepare for new cryptographic challenges that could potentially render current security measures obsolete. Comprehensive research by Sivaselvan and colleagues examining data from 19 major financial organizations and 27 security vendors indicates that while 83.5% of financial institutions recognize quantum computing threats, only 26.9% have initiated formal migration planning, and merely 11.3% have begun implementing quantum-resistant measures. Their analysis demonstrates that current quantum computers have reached approximately 1,000 qubits, though experts estimate that breaking RSA-2048 encryption would require around 20 million qubits—a capability that 72.4% of surveyed quantum researchers believe could emerge within 8-15 years. The researchers documented significant variations in organizational readiness, with average cybersecurity teams identifying only 61.7% of their quantum-vulnerable assets during comprehensive security assessments. Their economic modeling suggests that large financial institutions face potential remediation costs ranging from €16.8-€42.3 million, with implementation timelines averaging 36.7 months for a comprehensive transition to post-quantum cryptography (PQC) [10].

Quantum key distribution (QKD) technologies have advanced beyond theoretical applications, with Sivaselvan's analysis revealing that 8.1% of surveyed tier-one financial institutions have established pilot implementations. These early deployments typically secure high-sensitivity communication channels between primary and disaster recovery data centers, with current implementations achieving key exchange rates of 5.7 kbps over metropolitan distances up to 63 kilometers. Despite showing promise for specific use cases, QKD adoption faces substantial challenges including average implementation costs of €743,000 per secured channel and significant infrastructure requirements. The researchers further documented that 87.4% of financial organizations are prioritizing cryptographic agility—building flexible frameworks that can transition between encryption standards as quantum threats evolve. Their examination of five cryptographic transition events across different organizations revealed that those with mature agility frameworks completed organization-wide algorithm migrations in an average of 4.3 months, compared to 19.7 months for organizations lacking structured transition processes. The authors' vulnerability analysis using specialized quantum attack simulations demonstrated that institutions with comprehensive cryptographic inventories and transition plans reduced their potential quantum-related breach costs by approximately 81.7% compared to organizations without formal quantum security strategies [10].

6. Conclusion

Security in AI-driven financial applications represents not merely a technical requirement but a fundamental business imperative. By integrating security considerations throughout the development lifecycle and leveraging emerging technologies like differential privacy and blockchain, financial institutions can build applications that are both innovative and trustworthy. The most successful organizations will view security not as a constraint on innovation but as an enabler of sustainable growth in an increasingly digital financial ecosystem. As AI capabilities continue to advance, security frameworks must evolve in parallel, ensuring the financial sector can realize the benefits of artificial intelligence while effectively managing its unique risks.

The implementation of comprehensive security measures demands significant investment in both technological infrastructure and human expertise. Financial institutions must cultivate security-minded cultures where the protection of customer data becomes embedded in organizational values rather than treated as a compliance checkbox. This cultural shift requires executive commitment, continuous education programs, and incentive structures that reward secure development practices. Additionally, collaboration across the industry through information-sharing communities and standardization efforts will be essential for establishing common security frameworks that can address emerging threats with greater efficiency and effectiveness.

Looking ahead, the convergence of AI, blockchain, and quantum technologies will likely create both new security challenges and novel defensive capabilities. Financial institutions must maintain vigilant monitoring of technological developments and engage in proactive adaptation of their security postures. This forward-looking stance includes not only preparing for quantum-resistant cryptography but also embracing emerging concepts like zero-knowledge proofs, homomorphic encryption, and decentralized identity management. Ultimately, those organizations that successfully balance technological innovation with disciplined security practices will gain significant competitive advantages through enhanced customer trust, operational resilience, and reduced exposure to the increasingly costly consequences of security failures.

References

[1] Renato Lopes da Costa et al., "Artificial intelligence and its adoption in financial services," ResearchGate, 2022. [Online]. Available: https://www.researchgate.net/publication/361598318_Artificial_intelligence_and_its_adoption_in_financial_services

[2] IBM, "Cost of a Data Breach Report 2024," 2024. [Online]. Available: https://table.media/wp-content/uploads/2024/07/30132828/Cost-of-a-Data-Breach-Report-2024.pdf

[3] Harsh Daiya, "AI-Driven Risk Management Strategies in Financial Technology," ResearchGate, 2024. [Online]. Available: https://www.researchgate.net/publication/382207578_AI-Driven_Risk_Management_Strategies_in_Financial_Technology

[4] Dr Uma Maheswari S, "Cybersecurity Challenges In Fintech: Assessing Threats And Mitigation Strategies For Financial Institutions," ResearchGate, 2024. [Online]. Available: https://www.researchgate.net/publication/381017652_Cybersecurity_Challenges_In_Fintech_Assessing_Threats_And_Mitigation_Strategies_For_Financial_Institutions

[5] Toyyibat T. Yussuph et al., "Data Protection and Privacy as a Tool to Reduce Financial Loss from Cybercrimes," Global Scientific Journal, 2023. [Online]. Available: https://www.researchgate.net/profile/Toyyibat-Yussuph-2/publication/376312460_DATA_PROTECTION_AND_PRIVACY_AS_A_TOOL_TO_REDUCE_FINANCIAL_LOSS_FROM_CYBERCRIMES/links/657297abfc4b416622a81cab/DATA-PROTECTION-AND-PRIVACY-AS-A-TOOL-TO-REDUCE-FINANCIAL-LOSS-FROM-CYBERCRIMES.pdf

[6] Favour Hannah and Hannah Adebayo, "Adversarial Machine Learning Attacks in Financial Risk Models: Identifying and Mitigating Threats," ResearchGate, 2023. [Online]. Available: https://www.researchgate.net/publication/389438099_Adversarial_Machine_Learning_Attacks_in_Financial_Risk_Models_Identifying_and_Mitigating_Threats

[7] Temitayo Oluwadamilola Adesoga et al., "Encryption techniques for financial data security in fintech applications," ResearchGate, 2024. [Online]. Available: https://www.researchgate.net/publication/382023338_Encryption_techniques_for_financial_data_security_in_fintech_applications

[8] Venkateshwarlu Koyeda, "Implementing Multi-Factor Authentication in Financial Systems," ResearchGate, 2025. [Online]. Available: https://www.researchgate.net/publication/389599492_Implementing_Multi-Factor_Authentication_in_Financial_Systems

[9] Daniel Martinez et al., "AI and Blockchain Integration: Enhancing Security and Transparency in Financial Transactions," International Transactions on Artificial Intelligence, 2024. [Online]. Available: https://journal.pandawan.id/italic/article/view/651/486

[10] Arit Kumar Bishwas and Mousumi Sen, "Strategic Roadmap for Quantum-Resistant Security: A Framework for Preparing Industries for the Quantum Threat." [Online]. Available: https://arxiv.org/pdf/2411.09995