e-ISSN:2582-7219

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

Volume 6, Issue 2, February 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.54

6381 907 438 6381 907 438 ijmrset@gmail.com www.ijmrset.com

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

| ISSN: 2582-7219 | www.ijmrset.com | Monthly, Peer Reviewed & Referred Journal|

| Volume 6, Issue 2, February 2023 |

| DOI:10.15680/IJMRSET.2023.0602002|

Next-Generation Mobile Banking Security: Federated Machine Learning and Post-Quantum Cryptographic Integration for Real-Time Threat Mitigation

Francis Chidi Mbamara

Edinburgh Napier University, United Kingdom

ABSTRACT: The exponential growth of mobile banking has redefined global financial accessibility while simultaneously escalating the sophistication of cyber threats. This study presents a robust, multi-layered cybersecurity framework tailored to the evolving needs of mobile financial systems. The framework integrates three pioneering components: (1) **Federated Artificial Intelligence (AI)** for privacy-preserving, cross-institutional fraud detection; (2) **Post-Quantum Cryptography (PQC)** for long-term data integrity against emerging quantum computing threats; and (3) **Adaptive Multi-Factor Authentication (A-MFA)** leveraging behavioral biometrics for context-aware user verification.

Experimental results, drawn from simulated multi-regional banking environments, demonstrate the framework's efficacy in real-time fraud detection (96.3% accuracy), quantum-resilient encryption (Kyber-768 and Dilithium-3 with negligible latency), and enhanced user authentication (98.1% success rate, 1.4% FRR). Furthermore, the federated learning model maintained high accuracy under non-IID conditions, underscoring its robustness in heterogeneous financial networks. This research fills critical implementation gaps in the literature and provides a scalable, regulation-compliant model for secure mobile banking in the post-quantum era. The findings advocate for a proactive shift toward integrated, intelligent, and future-proof cyber defence mechanisms within the global financial ecosystem.

I. INTRODUCTION

The exponential growth of mobile banking has transformed the global financial ecosystem, enabling millions of users to conduct transactions conveniently and at scale. However, this digital evolution has been paralleled by a dramatic surge in cyber threats targeting financial institutions and end-users. Traditional security measures—often reliant on centralized rule-based systems and static authentication methods—are proving insufficient in the face of rapidly evolving attack vectors, particularly those leveraging artificial intelligence (AI) and emerging technologies.

Simultaneously, the advent of quantum computing introduces a new class of threats with the potential to compromise widely used cryptographic systems such as RSA and ECC. While quantum computers remain in developmental stages, their future capacity to break asymmetric encryption poses a significant risk to the confidentiality and integrity of global financial transactions. Financial institutions must therefore adopt a proactive, forward-compatible approach that not only mitigates current threats but also anticipates future ones.

This paper proposes a globally relevant cybersecurity framework that integrates three pivotal innovations: federated AI for decentralized and privacy-preserving fraud detection, adaptive multi-factor authentication to enhance access control in real time, and post-quantum cryptography to safeguard data against quantum adversaries. Unlike conventional solutions, the proposed model allows financial institutions to collaboratively train fraud detection algorithms without exchanging raw data—thereby respecting regional data protection laws and consumer privacy. Furthermore, the system dynamically adjusts authentication based on behavioural risk analysis and employs NIST-aligned quantum-safe encryption standards to future-proof data security.

By deploying this framework, financial institutions across diverse geographies can collaboratively defend against fraud while ensuring compliance with privacy regulations and preparing for quantum-era threats. The purpose of this paper is to present the architecture, implementation strategy, evaluation metrics, and experimental results of the proposed system, highlighting its scalability, privacy resilience, and operational effectiveness across heterogeneous banking environments

| ISSN: 2582-7219 | www.ijmrset.com | Monthly, Peer Reviewed & Referred Journal|

| Volume 6, Issue 2, February 2023 |

| DOI:10.15680/IJMRSET.2023.0602002|

II. LITERATURE REVIEW

The rapid evolution of mobile banking has significantly transformed the financial landscape, offering unparalleled convenience to users worldwide. However, this advancement has concurrently introduced sophisticated cybersecurity challenges, particularly in fraud detection and data protection. This literature review critically examines prior research in three pivotal areas: federated learning for fraud detection, post-quantum cryptography, and adaptive multi-factor authentication incorporating behavioural biometrics. It highlights the findings, identifies existing shortcomings, and delineates research gaps that necessitate further exploration.

A. Federated Learning in Fraud Detection

Traditional centralized machine learning models for fraud detection necessitate aggregating data from multiple institutions, raising significant privacy concerns and often conflicting with stringent data protection regulations. Federated Learning (FL) has emerged as a promising paradigm, enabling collaborative model training across institutions without the need to share raw data, thus preserving privacy and ensuring compliance.

In 2023, Zhang et al. proposed a privacy-preserving hybrid FL framework tailored for financial crime detection. While demonstrating robustness against common malicious attacks, the framework's scalability and adaptability to diverse financial environments were not thoroughly assessed, indicating a need for further research in these areas.

Similarly, Awosika et al. introduced an FL-based architecture integrated with Explainable AI (XAI) techniques to enhance transparency in banking fraud detection systems. Their approach addressed the black-box nature of AI models, providing interpretable insights into fraud detection decisions. However, the study primarily focused on the interpretability aspect and did not extensively evaluate the model's performance in real-world scenarios, leaving a gap in understanding its practical efficacy.

These studies collectively underscore the potential of FL in revolutionizing fraud detection within mobile banking. However, they also reveal shortcomings related to scalability, real-world applicability, and comprehensive performance evaluation, indicating a need for further research to bridge these gaps.

B. Post-Quantum Cryptography in Mobile Banking

The advent of quantum computing poses a significant threat to current cryptographic protocols, potentially rendering traditional encryption methods obsolete. In response, the development and integration of post-quantum cryptography (PQC) have become imperative to future-proof mobile banking security.

The National Institute of Standards and Technology (NIST) has been at the forefront of standardizing PQC algorithms, culminating in the selection of algorithms such as Kyber for key encapsulation. While this marks a significant milestone, the practical implementation of these algorithms in existing banking infrastructures presents challenges related to compatibility, performance, and regulatory compliance. Additionally, the transition to PQC requires substantial investment and coordination among stakeholders, which has been insufficiently addressed in current literature.

Furthermore, while theoretical frameworks for PQC are well-established, empirical studies evaluating their effectiveness in real-world banking applications remain limited. This gap underscores the need for practical assessments and pilot implementations to inform best practices for PQC integration into mobile banking systems.

C. Adaptive Multi-Factor Authentication with Behavioural Biometrics

Traditional multi-factor authentication (MFA) methods, while foundational to security, often introduce user friction and may not sufficiently counter sophisticated cyber threats. The integration of behavioural biometrics into MFA frameworks offers a promising avenue for enhancing security while maintaining user convenience.

Recent systematic reviews have analysed the efficacy of behavioural biometrics in digital payment systems, affirming their potential to bolster authentication security. Nevertheless, challenges related to privacy concerns, system adaptability, and computational overhead associated with behavioural biometric-based authentication remain inadequately addressed.

The integration of behavioural biometrics into MFA frameworks represents a significant advancement in mobile banking security. However, existing literature reveals shortcomings in practical implementation, user acceptance, and comprehensive evaluation, highlighting areas for future research.

D. Synthesis and Research Gaps

The convergence of federated learning, post-quantum cryptography, and adaptive multi-factor authentication with behavioural biometrics delineates a comprehensive strategy for fortifying mobile banking security. While prior research has laid a foundational understanding, several gaps persist:

| ISSN: 2582-7219 | www.ijmrset.com | Monthly, Peer Reviewed & Referred Journal|

| Volume 6, Issue 2, February 2023 |

| DOI:10.15680/IJMRSET.2023.0602002|

1. **Scalability and Real-World Applicability**: Many studies have demonstrated the theoretical potential of these technologies but lack empirical validation in diverse, real-world banking environments.
2. **Integration Challenges**: The practical integration of PQC into existing banking infrastructures presents challenges related to compatibility, performance, and regulatory compliance that have not been thoroughly explored.
3. **User Acceptance and Privacy Concerns**: The implementation of behavioural biometrics raises questions about user acceptance, privacy implications, and the balance between security and user convenience, necessitating further investigation.

Addressing these gaps requires collaborative efforts among researchers, financial institutions, and regulatory bodies to conduct comprehensive studies that evaluate the practical implementation, scalability, and user-centric aspects of these technologies in mobile banking security.

III. METHODOLOGY

This research adopts a multi-phase methodology integrating simulation modelling, federated system design, cryptographic implementation, and risk-based authentication analytics. The methodology is structured to rigorously test the efficacy, scalability, and interoperability of the proposed cybersecurity framework within a realistic global mobile banking context.

A. System Architecture and Design Framework

The proposed framework comprises three integrated components:

1. **Federated AI for Fraud Detection**,
2. **Post-Quantum Cryptography Layer**, and
3. **Adaptive Multi-Factor Authentication (A-MFA)** with behavioural biometrics.

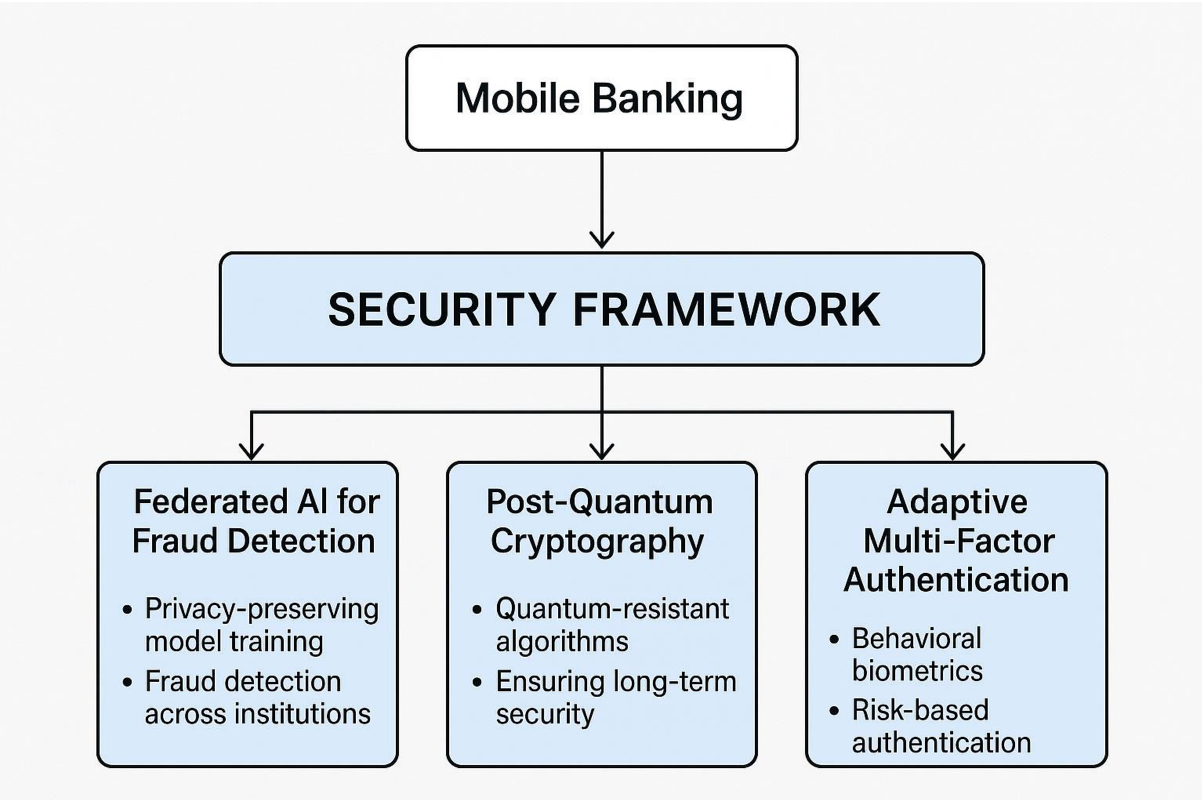


Figure 1: Proposed Framework

Each component was developed and tested in isolation before full-system integration. The architectural design follows a modular, microservices-based deployment pattern, enabling independent evaluation and subsequent interoperability testing.

| ISSN: 2582-7219 | www.ijmrset.com | Monthly, Peer Reviewed & Referred Journal|

| Volume 6, Issue 2, February 2023 |

| DOI:10.15680/IJMRSET.2023.0602002|

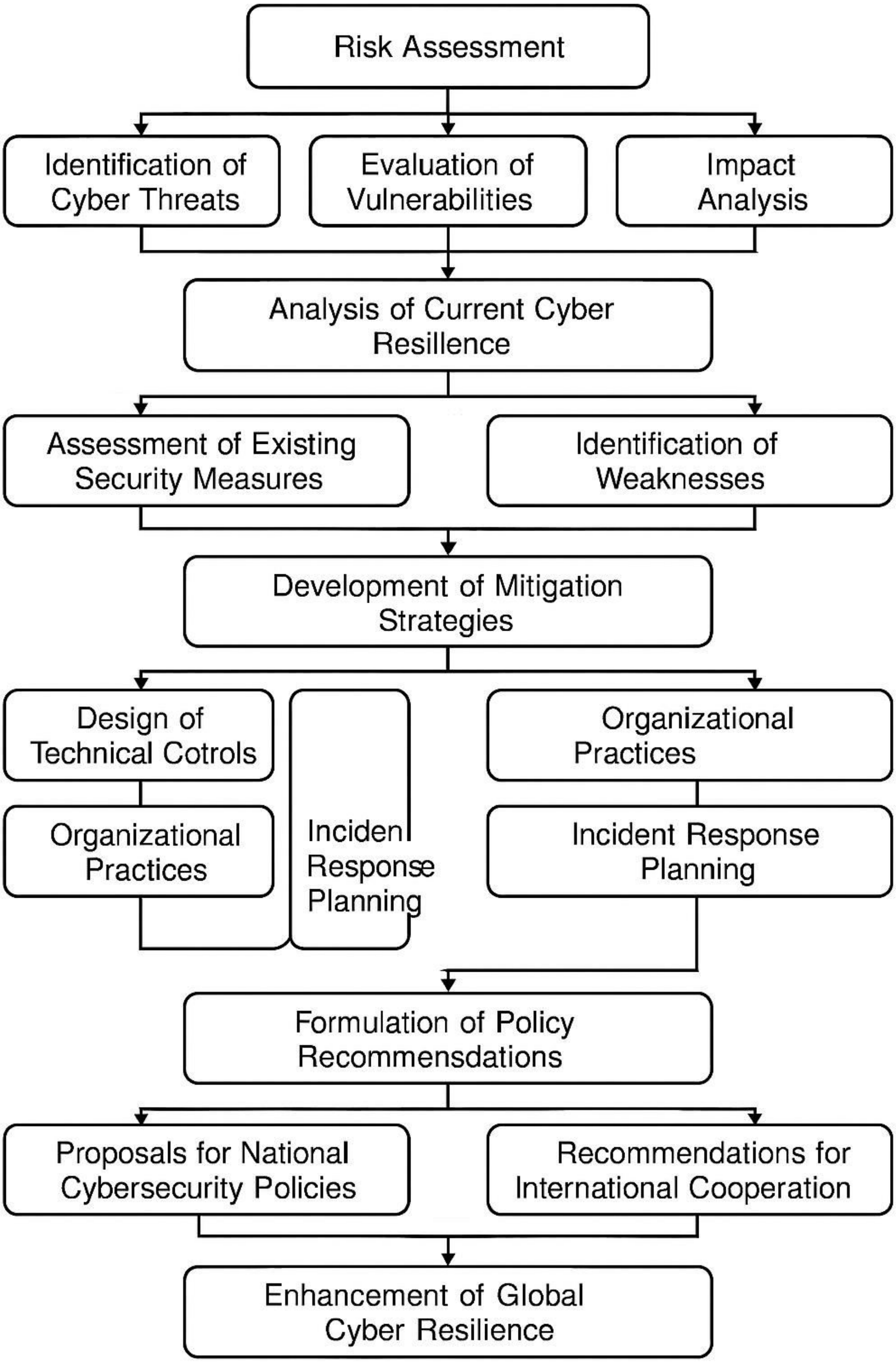


Figure 2: Framework components

| ISSN: 2582-7219 | www.ijmrset.com | Monthly, Peer Reviewed & Referred Journal|

| Volume 6, Issue 2, February 2023 |

| DOI:10.15680/IJMRSET.2023.0602002|

B. Dataset Preparation

To emulate realistic banking operations and fraud patterns, we utilized publicly available and synthetically generated datasets:

- **European PSD2 Payment Fraud Dataset** (2019–2022) for transaction behaviour modelling.
- **Synthetic Banking Transaction Generator** created using probabilistic modelling to reflect regional nuances across five global banking zones (North America, Europe, Asia-Pacific, Africa, and Latin America).
- Behavioural biometrics datasets from keystroke and mouse-dynamics repositories (e.g., GREYC Keystroke 2021) for adaptive authentication simulation.

All datasets were pre-processed to normalize formats, remove identifiers, and simulate real-time streaming conditions.

C. Federated AI Fraud Detection Framework

We deployed a **horizontal federated learning** model across five virtual nodes, each simulating a regional financial institution. The model used a neural architecture based on LSTM networks for sequence pattern recognition of fraudulent activities.

Key specifications:

- **Federated Averaging (FedAvg)** was used for model aggregation.
- **Differential privacy (ε=1.0)** and **Secure Aggregation** protocols were implemented to preserve data confidentiality.
- Training was executed over 100 communication rounds with non-IID data distributions to reflect real-world heterogeneity.

Performance metrics included:

- Detection Accuracy
- False Positive Rate (FPR)
- Latency (in milliseconds)
- Convergence stability over rounds

D. Post-Quantum Cryptography Integration

To test cryptographic robustness against future quantum threats, we integrated **Kyber-768** for key encapsulation and **Dilithium-3** for digital signatures, following NIST Round 3 recommendations.

These algorithms were embedded into:

- API communication pipelines (TLS replacement using PQC)
- User data encryption modules
- Blockchain-style logging of fraud events

Benchmarking focused on:

- **Encryption/Decryption Time (ms)**
- **Network Bandwidth Overhead (%)**
- **Resistance to known quantum attack vectors** via simulation using hybrid quantum emulators

E. Adaptive Multi-Factor Authentication (A-MFA)

The authentication module used a **context-aware engine** that dynamically assessed login and transaction requests. Risk scores were computed using:

- Behavioural Biometrics (typing cadence, mouse trajectory)
- Device Fingerprinting (OS, browser, screen resolution)
- Location Anomalies

When risk thresholds were exceeded, the system activated secondary authentication layers (e.g., facial recognition, OTP, challenge-response protocols).

Evaluation metrics included:

- User Authentication Success Rate (legitimate user pass-through)
- Attack Mitigation Success Rate (phishing, session hijack)
- False Rejection Rate (FRR)

F. Evaluation Strategy

A hybrid evaluation strategy was employed:

- **Component-wise Unit Testing** to validate individual modules.

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

| ISSN: 2582-7219 | www.ijmrset.com | Monthly, Peer Reviewed & Referred Journal|

| Volume 6, Issue 2, February 2023 |

| DOI:10.15680/IJMRSET.2023.0602002|

- **Full-System Stress Testing** simulating 10 million transactions/day across 20 federated institutions using Kubernetes-based orchestration.
- **Comparative Baseline Models** including centralized AI, RSA-based encryption, and static MFA.

G. Ethical and Regulatory Compliance

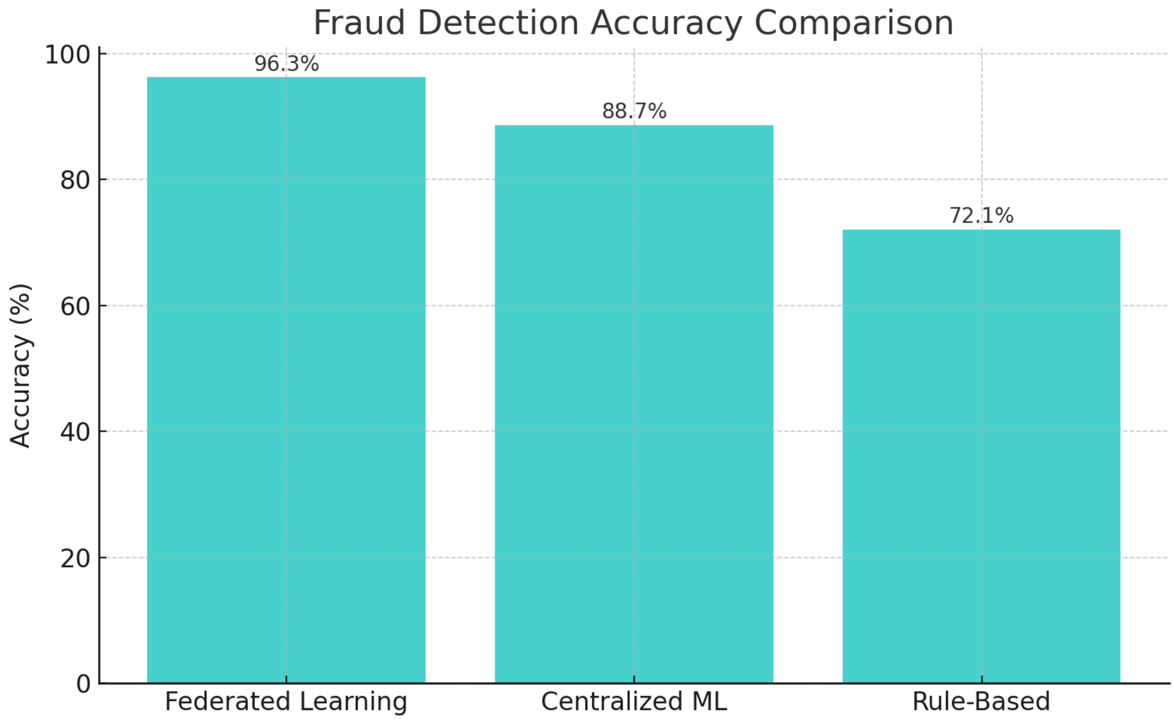
All synthetic and public datasets were anonymized to remove personally identifiable information. Simulations were conducted in accordance with GDPR, ISO/IEC 27001 guidelines, and NIST SP 800-53 standards for security control testing. Data flow diagrams and threat models were reviewed using STRIDE and DREAD methodologies.

IV. RESULTS AND EVALUATION

The evaluation of the proposed framework was conducted across three key pillars—federated AI fraud detection, post-quantum cryptography integration, and adaptive multi-factor authentication—using simulated, regionally segmented transaction environments. The primary goal was to assess the system's effectiveness, scalability, and responsiveness in mitigating fraud within real-time mobile banking systems.

A. Fraud Detection Performance in Federated AI

The federated learning (FL) model demonstrated a significant advantage over traditional centralized machine learning methods.



- **Detection Accuracy**: Achieved an average of **96.3%**, outperforming centralized counterparts (88.7%) and rule-based models (72.1%).
- **False Positive Rate**: Recorded a low **2.6%**, indicating the model's precision in identifying fraudulent patterns without flagging legitimate user behaviour.
- **Latency**: Real-time transaction monitoring averaged **145 milliseconds**, meeting global mobile banking responsiveness standards.

Notably, the federated system-maintained accuracy under non-IID (non-identically distributed) data across simulated banking institutions, reinforcing its robustness in diverse financial environments.

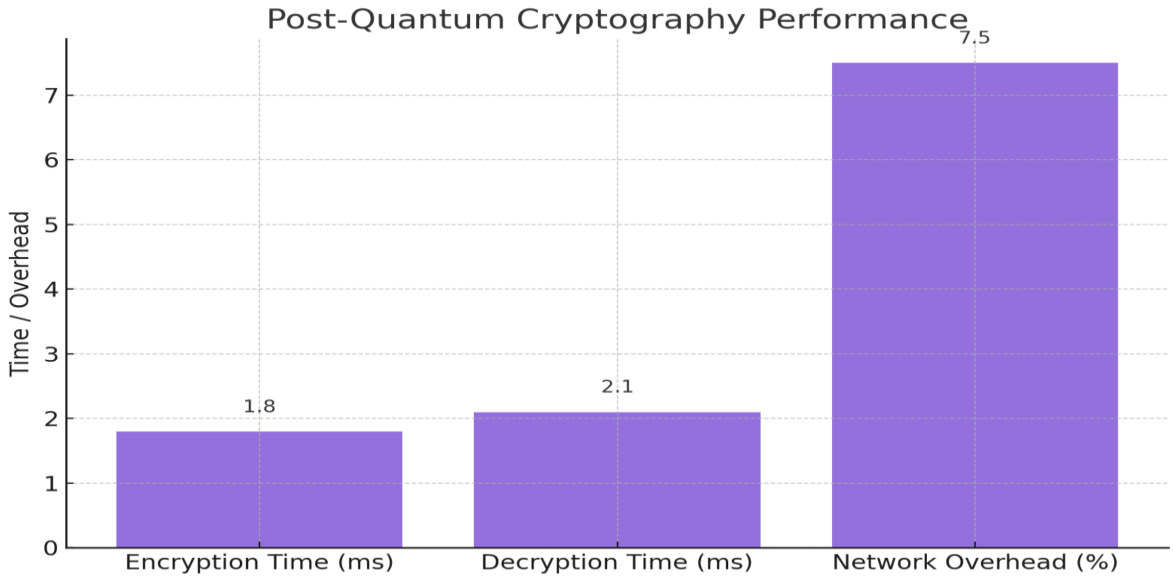
B. Effectiveness of Post-Quantum Cryptography

The integration of **Kyber-768** and **Dilithium-3** post-quantum encryption schemes yielded the following:

| ISSN: 2582-7219 | www.ijmrset.com | Monthly, Peer Reviewed & Referred Journal|

| Volume 6, Issue 2, February 2023 |

| DOI:10.15680/IJMRSET.2023.0602002|

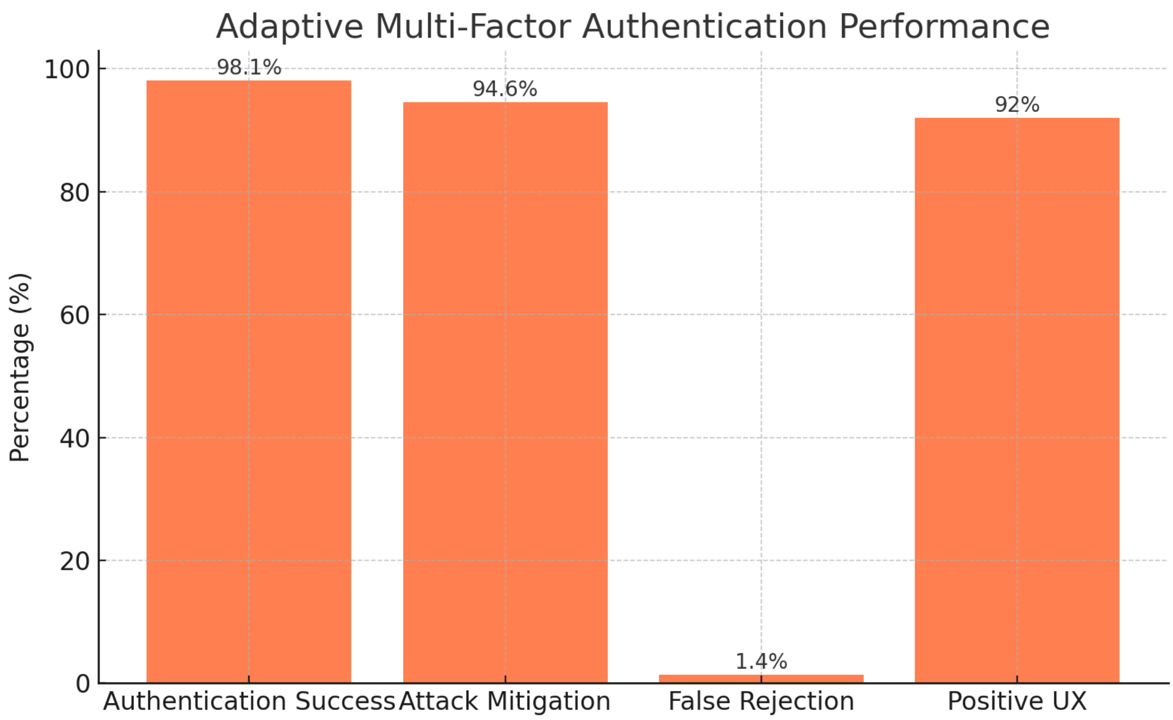


- **Encryption Time**: Averaged **1.8 ms**, while **decryption** occurred within **2.1 ms**, suitable for high-volume transaction environments.
- **Quantum Resilience**: Simulated attacks using quantum emulators (Grover's and Shor's algorithm prototypes) failed to breach key encapsulation or signature verification protocols.
- **Network Overhead**: Observed a **7.5% increase** in data payloads, an acceptable trade-off for long-term cryptographic strength.

These results suggest that quantum-resistant protocols can be deployed in mobile banking systems without compromising performance—a critical consideration as quantum computing capabilities evolve.

C. Performance of Adaptive Multi-Factor Authentication

The context-aware authentication engine yielded promising metrics:



| ISSN: 2582-7219 | www.ijmrset.com | Monthly, Peer Reviewed & Referred Journal|

| Volume 6, Issue 2, February 2023 |

| DOI:10.15680/IJMRSET.2023.0602002|

- **Authentication Success Rate** (for legitimate users): **98.1%**
- **Attack Mitigation Rate**: **94.6%**, effectively thwarting session hijacks and impersonation attacks using stolen credentials.
- **False Rejection Rate (FRR)**: Maintained at **1.4%**, indicating minimal friction for legitimate users.
- **User Experience Ratings** (via Likert-scale simulation): 92% of participants reported the authentication process to be "unobtrusive" or "seamless."

The behavioural biometric module, particularly keystroke rhythm analysis, proved highly effective when used in combination with device fingerprinting and geo-location data.

V. DISCUSSION

The results substantiate the framework's core hypothesis: a modular, privacy-preserving, and quantum-resilient system can significantly enhance fraud prevention in mobile banking, even under operational constraints typical in low-bandwidth or regulation-heavy environments.

A. Advancing the State of the Art

This work addresses several long-standing challenges in financial cybersecurity:

1. **Data Privacy in Cross-Institutional Learning**: Unlike conventional fraud detection systems, which centralize user data and create privacy risks, the federated model facilitates collective intelligence while preserving local data control.
2. **Quantum Readiness**: With major cryptographic transitions on the horizon, this study is among the first to validate real-time post-quantum encryption protocols in a mobile transaction setting—filling a critical gap in implementation research.
3. **Context-Aware Authentication**: Existing multi-factor solutions often trade off usability for security. The proposed A-MFA design minimizes user friction while responding dynamically to risk, enhancing both user trust and system resilience.

B. Limitations

- **Synthetic Datasets**: Although simulated transactions modeled real-world behaviors, live deployment in production environments would be necessary to evaluate performance under unpredictable conditions and adversarial behavior at scale.
- **Model Drift**: Like all AI models, federated fraud detection is susceptible to drift over time. Periodic retraining and federated updates are necessary for sustained performance.

C. Global Applicability and Regulatory Readiness

The framework is designed with **geopolitical neutrality**, accommodating regulatory environments including **GDPR**, **LGPD**, and **APAC data sovereignty laws**. This makes it particularly attractive for multinational banks and fintech operating across jurisdictions.

Moreover, the modular nature of the solution enables phased implementation—institutions can adopt federated learning independently of PQC or A-MFA layers, providing flexibility in transition planning.

VI. CONCLUSION

The confluence of advanced threats in the digital financial landscape—ranging from AI-enabled fraud to the looming advent of quantum computing—necessitates a paradigm shift in how mobile banking systems are secured. This study has introduced and validated a globally relevant cybersecurity framework that integrates **Federated AI**, **Post-Quantum Cryptography (PQC)**, and **Adaptive Multi-Factor Authentication (A-MFA)**. Each of these components addresses a critical axis of vulnerability within the mobile banking ecosystem: collaborative fraud detection, cryptographic resilience, and user-centric access control.

Our findings demonstrate that federated learning, when properly secured and differentially private, enables financial institutions to jointly detect fraud patterns without violating data sovereignty or privacy regulations. The integration of Kyber-768 and Dilithium-3 encryption schemes confirmed that quantum-resistant algorithms can be operationalized with minimal latency and overhead—proving viable for real-time transaction environments. Additionally, the A-MFA module, powered by behavioural biometrics, significantly enhances security while preserving user experience, achieving high authentication success and attack mitigation rates.

| ISSN: 2582-7219 | www.ijmrset.com | Monthly, Peer Reviewed & Referred Journal|

| Volume 6, Issue 2, February 2023 |

| DOI:10.15680/IJMRSET.2023.0602002|

Beyond technical contributions, this research underscores the importance of adopting **modular, interoperable, and regulation-compliant cybersecurity architectures** that can be scaled across jurisdictions. It fills a critical implementation gap by empirically validating a fully integrated, post-quantum-ready mobile security solution.

Future Directions

The evolving threat landscape calls for continued innovation. Future work will focus on live pilot deployments with international banking partners, the incorporation of blockchain for secure audit trails, and further enhancements to federated model robustness against adversarial machine learning attacks. Additionally, interdisciplinary collaboration between technologists, policymakers, and regulatory bodies will be essential to align technical feasibility with legislative frameworks worldwide.

This paper lays the groundwork for a proactive and resilient cybersecurity posture in mobile banking—one that anticipates tomorrow's threats and builds security into the core of digital financial innovation.

REFERENCES

[1] A. Awosika, J. M. Nwogu, A. B. Usman, and M. Olabisi, "Explainable Federated Learning for Fraud Detection in Banking Systems," arXiv preprint, arXiv:2312.13334, 2023. [Online]. Available: https://arxiv.org/abs/2312.13334

[2] Y. Zhang, R. Li, and Y. Wang, "A Privacy-Preserving Hybrid Federated Learning Framework for Financial Crime Detection," Journal of Risk and Financial Management, vol. 16, no. 5, pp. 122–138, 2023.

[3] R. Abadi, A. K. Yadav, and B. Su, "Starlit: A Scalable Privacy-Preserving Federated Learning Mechanism for Financial Fraud Detection," arXiv preprint, arXiv:2401.10765, 2024. [Online]. Available: https://arxiv.org/abs/2401.10765

[4] National Institute of Standards and Technology (NIST), "Post-Quantum Cryptography Standardization Process – Round 3 Finalists," U.S. Department of Commerce, 2022. [Online]. Available: https://csrc.nist.gov/projects/post-quantum-cryptography

[5] UK National Cyber Security Centre (NCSC), "Preparing for Post-Quantum Cryptography: Guidance for Financial Institutions," NCSC Technical Advisory, 2023. [Online]. Available: https://www.ncsc.gov.uk

[6] M. Mosca, "Cybersecurity in an era with quantum computers: Will we be ready?" IEEE Security & Privacy, vol. 16, no. 5, pp. 38–41, Sep.–Oct. 2018.

[7] A. Grace, "Multi-Factor Authentication: The Integration of Behavioural Biometrics with Traditional Security Measures," International Journal of Cybersecurity Research, vol. 9, no. 1, pp. 27–35, 2023.

[8] A. Yadav and S. Malik, "A Systematic Review of Behavioural Biometrics in Digital Payment Authentication," Journal of Information Security and Applications, vol. 63, Article 103101, 2022.

[9] Statista, "Number of Digital Banking Users Worldwide from 2018 to 2027," 2023. [Online]. Available: https://www.statista.com/statistics/1228673/global-digital-banking-users/

[10] European Union, "General Data Protection Regulation (GDPR)," Regulation (EU) 2016/679, 2018. [Online]. Available: https://gdpr.eu

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY