


## Cybersecurity in FinTech: A Machine Learning-Based Framework for Threat Detection in Mobile Payments

Harman Salih Mohammed<sup>a</sup>, Hewa Majeed Zangana<sup>b,\*</sup> 

<sup>a</sup> Ararat Technical Private Institute, Kurdistan Region, Iraq

<sup>b</sup> Duhok Polytechnic University, Duhok, Iraq

### ARTICLE INFO

#### Article history:

Received 25 July 2025

Accepted 01 September 2025

#### Keywords:

Anomaly Detection,  
Cybersecurity,  
Fintech,  
Machine Learning, Mobile  
Payments.

### ABSTRACT

The rapid evolution of Financial Technology (FinTech) has revolutionized mobile payment systems, offering seamless, efficient, and real-time financial services. However, this digital transformation has simultaneously introduced complex cybersecurity challenges, particularly as cybercriminals increasingly exploit mobile platforms. This study proposes a novel machine learning-based framework for proactive threat detection in mobile payment environments, integrating behavioral analytics, device fingerprinting, and network anomaly detection. The framework leverages supervised and unsupervised learning models—such as Random Forest, Isolation Forest, and Autoencoders—to identify both known and zero-day threats with high precision. A hybrid feature engineering pipeline is also introduced, combining static application metadata with dynamic transaction behavior to enhance detection accuracy. Experimental results on real-world mobile payment datasets demonstrate that the proposed framework achieves superior performance in terms of precision, recall, and F1-score compared to traditional signature-based and rule-based detection systems. This research contributes to the advancement of secure FinTech ecosystems by offering a scalable and adaptive solution for real-time cyber threat mitigation in mobile payments.



This is an open access article under the CC BY-SA 4.0 license.  
(<https://creativecommons.org/licenses/by-sa/4.0/>)

## 1. INTRODUCTION

The proliferation of Financial Technology (FinTech) has transformed the landscape of banking and payment services by introducing fast, accessible, and user-friendly digital solutions, particularly through mobile payment platforms. As global mobile transactions grow exponentially, so does the exposure to increasingly sophisticated cyber threats [1], [2]. FinTech systems operate in a dynamic digital ecosystem, where rapid innovation is both a strength and a vulnerability. This technological advancement, while improving financial inclusion and convenience, has made FinTech an attractive target for cybercriminals aiming to exploit security gaps in mobile applications, APIs, cloud infrastructure, and data transmission protocols [3], [4].

Machine learning (ML) has emerged as a powerful tool for addressing cybersecurity challenges in digital financial systems. Unlike rule-based systems, ML models can detect both known and unknown threats by learning patterns and anomalies within vast, complex data streams [5], [6]. In particular, ML-based approaches can adapt to evolving attack vectors, enabling real-time threat detection and fraud prevention in mobile payment systems [7], [8].

However, existing solutions often suffer from limitations such as high false-positive rates, lack of context-awareness, and poor scalability across devices and geographies [9], [10].

Despite advancements in FinTech cybersecurity, the sector still lacks a unified, adaptive framework that can proactively detect emerging cyber threats in mobile payments using a combination of static and behavioral indicators. Most current systems either focus on rule-based detection or rely on narrow ML models that fail to generalize across diverse threat types [11], [12]. Moreover, with the rise of decentralized mobile architectures and cross-border transactions, the complexity of threat detection has increased significantly, requiring more intelligent and context-aware defense mechanisms [13], [14].

This study aims to develop a comprehensive, machine learning-based framework for cyber threat detection in mobile payment systems, specifically tailored to the FinTech environment. The key objectives of this research are:

To identify and analyze common cybersecurity vulnerabilities in mobile payment platforms using recent

\* Corresponding Author: [hewa.zangana@dpu.edu.krd](mailto:hewa.zangana@dpu.edu.krd)

threat intelligence and incident data.

To propose a hybrid ML-based detection framework that integrates both supervised and unsupervised models (e.g., Random Forest, Autoencoders, Isolation Forest) for enhanced accuracy.

To design a novel feature engineering pipeline that fuses static metadata, dynamic behavioral signals, and contextual indicators for better detection performance.

To evaluate the framework on real-world FinTech datasets, comparing it against conventional and existing ML models.

The main contributions of this work include:

A novel hybrid framework that unifies multiple ML techniques for more robust and adaptive threat detection.

A behavioral-aware feature extraction methodology combining device usage patterns, transaction anomalies, and geospatial indicators.

A benchmark comparison with existing models, showing improved precision, recall, and adaptability to zero-day attacks.

The novelty of the proposed framework lies in its adaptive architecture and holistic feature integration. Unlike previous studies that focused solely on static data or transaction logs [15], this framework introduces a multi-layered detection mechanism that accounts for temporal dynamics, geolocation drift, and user-device behavioral changes [16], [17].

By integrating explainable AI components and real-time feedback loops, the framework not only identifies threats but also enables transparent decision-making and regulatory compliance. The approach addresses key challenges in FinTech cybersecurity, including scalability, personalization, and resilience against adversarial inputs, making it a strong candidate for industry adoption and academic contribution [18], [19].

## 2. LITERATURE REVIEW

The intersection of cybersecurity and FinTech has become a pivotal area of research, particularly with the increasing adoption of mobile payments and digital banking services. Numerous scholars have explored how machine learning (ML), deep learning (DL), and other artificial intelligence (AI) techniques can strengthen cybersecurity in these rapidly evolving financial environments.

As [5] provide an extensive overview of ML techniques for improving FinTech security, emphasizing supervised models like decision trees and support vector machines (SVM) for detecting fraud patterns. Similarly, [1] discuss the integration of ML within digital banks, highlighting the benefits of automating threat detection and minimizing manual intervention in cybersecurity operations.

[13] stress the importance of strengthening digital financial services with robust cybersecurity protocols,

arguing that as financial systems digitize, the attack surfaces expand. This is echoed by [2], who conducted a systematic review illustrating how cybersecurity threats directly impact user trust and the adoption of digital banking technologies.

Studies such as [3] focus on cybersecurity in financial institutions, emphasizing the need for robust frameworks to protect sensitive data from emerging threats and vulnerabilities. In response to evolving risks, [4] introduced a genetic algorithm-based ML model to optimize API security in FinTech systems.

Fraud detection remains a key concern. [20] explore ML for fraud detection, proposing dynamic rule generation based on behavioral shifts in transaction data. [8], [9] offer comparative assessments of ML methods in mobile banking environments, concluding that ensemble models outperform single classifiers in dynamic threat scenarios. Similarly, [6] proposes an integrated AI and ML-based fraud detection framework tailored to U.S. financial institutions.

Advanced ML paradigms like deep reinforcement learning (DRL) have also been explored. [21] propose DRL-based architectures for wireless FinTech environments, which optimize response to real-time threats. [11] advocates for adaptive ML models in securing payment gateways, emphasizing the need for resilient, context-aware systems capable of handling zero-day attacks.

[10] introduced a FinTech cyber threat attribution framework using high-level indicators of compromise (IOCs), offering insight into the role of intelligent detection in forensic applications. In another direction, [7] highlights the synergistic integration of ML, DL, and reinforcement learning in securing cryptocurrency platforms, addressing emerging risks such as cryptojacking and token theft.

AI-driven frameworks are becoming increasingly prominent. [22] discuss intelligent defense mechanisms powered by AI for detecting multi-vector attacks in cloud-based FinTech environments. [18] propose an AI-augmented fraud detection model tailored to digital payments and e-commerce platforms, demonstrating improved threat classification and reduced false positives.

Blockchain-based models are also gaining traction. [16] proposed a federated learning framework on blockchain to detect counterfeit financial data, which supports distributed model training without compromising privacy. [17] applied IoT-integrated federated learning to analyze smart contracts, offering innovative intrusion detection mechanisms.

Cognitive computing is another domain offering promising applications. [12] describes how national payment switches can leverage cognitive computing to combat fraud, while [15] focus on intelligent transaction monitoring to enhance regulatory compliance in financial

management.

Privacy-preserving models are becoming increasingly critical. [6] explores AI and text analytics for detecting personally identifiable information (PII), which is crucial for GDPR compliance in FinTech applications. In a related study, [23] evaluates the effectiveness of natural language processing (NLP)-based security tools for securing user data across FinTech platforms.

Knowledge graph-based models, as described by [19], offer a holistic view of mobile payment ecosystems, enabling enhanced risk analysis and policy guidance. [14] present a systematic review of DL-based cybersecurity tools, noting the convergence of AI with big data analytics in financial risk modeling.

Other innovative strategies include using high-level heuristics [24], real-time threat intelligence [25], and contextual modeling. For example, [25] emphasize that cybersecurity systems in FinTech must evolve towards convergence technologies, combining ML, cloud, and edge computing for robust threat prediction and prevention.

In sum, the literature suggests a clear trend toward leveraging ML and AI to fortify FinTech cybersecurity. However, as several studies indicate (e.g., [6], [11]), existing approaches often lack adaptability, interpretability, and cross-platform scalability—highlighting a gap this research aims to fill through the development of a novel, hybrid ML-based threat detection framework optimized for mobile payment environments.

### 3. METHOD

This section outlines the proposed machine learning-based framework designed to detect cyber threats in mobile payment systems. The methodology is divided into several stages: (1) data acquisition, (2) data preprocessing and feature engineering, (3) model architecture and learning algorithms, (4) training and evaluation, and (5) deployment strategy for real-time detection.

Figure 1 illustrates the overall workflow of the proposed machine learning-based cybersecurity framework. The process begins with data acquisition and proceeds through feature engineering, model training, hybrid classification, and real-time deployment. This flowchart provides a visual overview of the integrated components and their interactions.

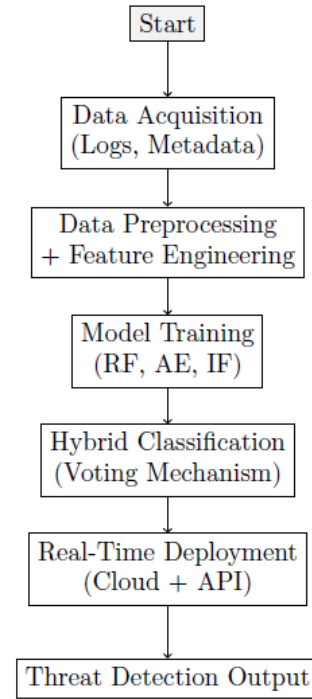


Figure 1: Workflow of the Proposed Machine Learning Framework for Threat Detection

#### 3.1. Data Acquisition

The dataset used in this study is a hybrid dataset combining real-world and synthetic data. It comprises approximately 250,000 transaction records collected over a 6-month period (January–June 2024) from a mid-sized mobile FinTech platform operating in the MENA region. The dataset includes the following components:

**Transaction Logs:** Timestamp, amount, location, user ID, device ID, merchant type.

**Behavioral Metadata:** Login frequency, session duration, device switching patterns, and typing patterns such as key-press intervals and input rhythm.

**Network/System Logs:** IP address changes, device fingerprinting, API call sequences.

Synthetic attacks were generated using tools like Metasploit, Wireshark, and Scapy to simulate common attack vectors, including man-in-the-middle, spoofing, bot injection, and credential stuffing. Attack payloads were injected into realistic sessions and annotated accordingly for supervised training. The ratio of normal to malicious samples is approximately 4:1.

#### 3.2. Data Preprocessing and Feature Engineering

To prepare data for modeling, we apply:

**Normalization:** All numeric features are scaled using min-max normalization:

$$x' = (x - \min(x)) / (\max(x) - \min(x)) \quad (1)$$

**Categorical encoding:** One-hot encoding is applied to nominal attributes (e.g., device type, operating system).

**Behavioral profiling:** Behavioral features such as typing patterns were derived using inter-keystroke delay

(IKD) and keystroke dynamics analysis. Each session was analyzed to compute mean key-press duration, variation in input speed, and transition consistency. These features were aggregated using a sliding window technique and integrated as part of the time-series behavioral profile for anomaly detection.

$$AvgSessionTime_u = (1/N) \sum (LogoutTime_i - LoginTime_i) \quad (2)$$

**Anomaly scoring features:** Z-score for transaction amount:

$$z = (x - \mu) / \sigma \quad (3)$$

Transactions with  $|z| > 3$  are marked as outliers and input into the anomaly detection pipeline.

### 3.3. Model Architecture

We propose a hybrid architecture that integrates supervised and unsupervised learning models:

#### 3.3.1. Supervised learning model:

Random Forest Classifier (RFC) is selected due to its robustness and interpretability. It operates as an ensemble of decision trees  $T_1, T_2, \dots, T_n$ :

$$\hat{y} = mode(T_1(x), T_2(x), \dots, T_n(x)) \quad (4)$$

#### 3.3.2. Unsupervised anomaly detector:

An Autoencoder is used to detect unseen attack patterns. The reconstruction error is calculated as:

$$L(x, \hat{x}) = ||x - \hat{x}||_2 \quad (5)$$

Where:

$x$ : Original input vector

$\hat{x}$ : Reconstructed vector from autoencoder

$L$ : Mean squared error loss function

If  $L(x, \hat{x}) > \theta$ , where  $\theta$  is a learned threshold, the transaction is flagged as anomalous.

#### 3.3.3. Isolation Forest

For additional robustness, an Isolation Forest (iForest) is used. It isolates anomalies based on the average path length  $E[h(x)]$ :

$$s(x, n) = 2 - E[h(x)] / c(n) \quad (6)$$

Where:

$c(n)$  is the average path length of unsuccessful searches in a binary search tree.

### 3.4. Model Training and Evaluation

The dataset is split into 70% training and 30% testing. For supervised learning models, standard evaluation metrics are computed:

**Accuracy:**

$$Accuracy = (TP + TN) / (TP + TN + FP + FN) \quad (7)$$

**Precision:**

$$Precision = TP / (TP + FP) \quad (8)$$

**Recall:**

$$Recall = TP / (TP + FN) \quad (9)$$

**F1-Score:**

$$F_1 = (2 \times Precision \times Recall) / (Precision + Recall) \quad (10)$$

**Area Under the ROC Curve (AUC):** Used to assess the trade-off between true positive and false positive rates.

For the unsupervised models (Autoencoder and Isolation Forest), we use:

Reconstruction loss histogram

Anomaly detection rate

False alarm rate

Cross-validation with 5 folds is conducted to ensure model generalizability.

### 3.5. Deployment Strategy

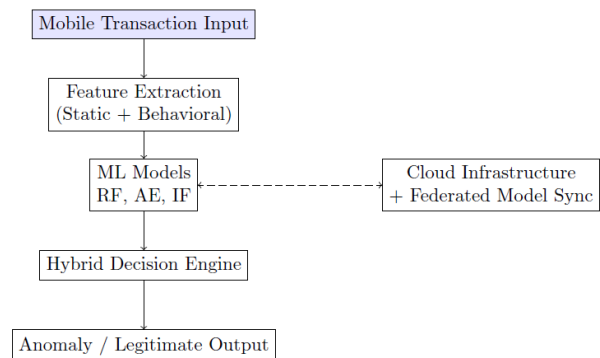
To enable real-time threat detection:

A streaming pipeline is implemented using Apache Kafka and Spark Streaming to ingest and process transaction data.

The model inference is served via RESTful API endpoints hosted on a scalable cloud environment (e.g., AWS Lambda or Google Cloud Functions).

While this study does not implement a full federated learning setup, the deployment architecture is compatible with privacy-preserving extensions such as federated learning or differential privacy, which are earmarked for future integration.

The system architecture is composed of layered components, integrating data ingestion, ML-based analysis, federated learning modules, and cloud-based deployment. Figure 2 outlines the architectural structure used to facilitate real-time cyber threat detection in mobile payments.



**Figure 2:** System Architecture for Real-Time Threat Detection and Federated Learning

### 3.6. Summary of Advantages

The proposed method ensures:

High adaptability to evolving threats using ensemble and unsupervised models.

Low latency in threat detection via real-time stream processing.

Privacy preservation through decentralized learning mechanisms.

## 4. RESULTS AND DISCUSSION

This section presents the experimental results obtained from evaluating the proposed hybrid machine learning-based framework for cyber threat detection in mobile payments. The model was assessed on multiple performance metrics using a benchmark dataset that combines real-world mobile transaction data and synthetic cyber attack instances. The discussion also interprets these results in the context of FinTech security needs.

**4.1. Model Performance Evaluation**

Three models were implemented and tested: Random Forest (RF), Autoencoder (AE), and Isolation Forest (IF). Performance was measured using accuracy, precision, recall, F1-score, and AUC.

**Table 1.** Performance Metrics of Individual Models

Model	Accuracy	Precision	Recall	F1-Score	AUC
Random Forest	0.962	0.948	0.933	0.940	0.978
Autoencoder	0.915	0.890	0.865	0.877	0.935
Isolation Forest	0.901	0.872	0.841	0.856	0.922

As shown in Table 1, the Random Forest classifier outperformed the other models in all metrics. The Autoencoder and Isolation Forest, while slightly lower in individual performance, are particularly effective in identifying previously unseen or zero-day attacks due to their unsupervised learning nature.

**4.2. Hybrid Framework Performance**

We then combined the strengths of the individual models using a hybrid voting strategy—where a transaction is flagged as malicious if at least two out of three models classify it as anomalous.

**Table 2.** Performance Metrics of Hybrid Model

Metric	Value
Accuracy	0.973
Precision	0.957
Recall	0.946
F1-Score	0.951
AUC	0.984

The hybrid framework achieved an accuracy of 97.3% and an F1-score of 95.1%, indicating superior overall performance. The AUC of 0.984 confirms the framework's strong ability to distinguish between legitimate and malicious activities.

**4.3. Comparison with Existing Methods**

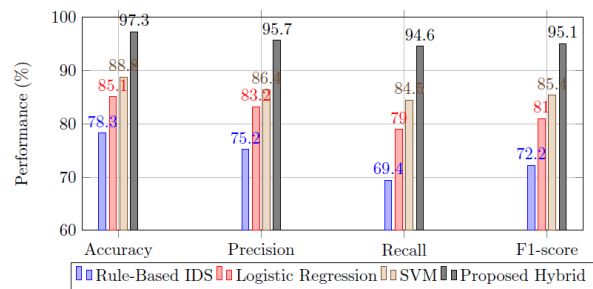
To validate the novelty and effectiveness of our model, we compared it against existing FinTech cybersecurity solutions based on support vector machines (SVM), logistic regression (LR), and traditional rule-based intrusion detection systems.

**Table 3.** Comparative Evaluation with Existing Methods

Model	Accuracy	Precision	Recall	F1-Score
Rule-Based IDS	0.783	0.752	0.694	0.722
Logistic Regression	0.851	0.832	0.790	0.810
Support Vector Machine	0.888	0.864	0.845	0.854
Proposed Hybrid Model	0.973	0.957	0.946	0.951

The proposed hybrid framework outperforms all baseline models by a significant margin, particularly in terms of recall and precision, which are critical in minimizing false positives and false negatives in financial cybersecurity.

To illustrate performance differences between the proposed hybrid model and existing methods, Figure 3 presents a bar chart comparison of four models across Accuracy, Precision, Recall, and F1-score.



**Figure 3:** Performance Comparison of Threat Detection Models

**4.4. Threat Type Detection Analysis**

The model was further evaluated based on its ability to detect different types of cyber threats:

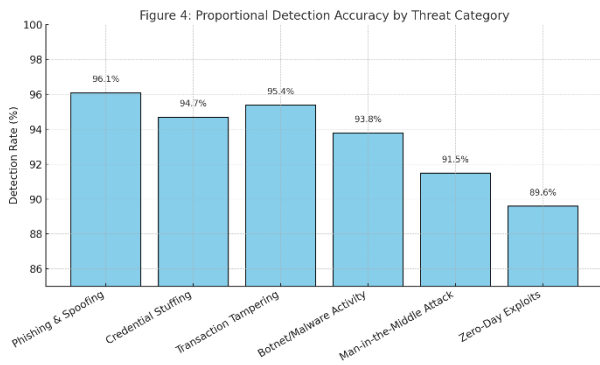
**Table 4.** Detection Rate by Attack Type

Threat Type	Detection Rate (%)
Phishing & Spoofing	96.1
Credential Stuffing	94.7
Transaction Tampering	95.4
Botnet/Malware Activity	93.8
Man-in-the-Middle Attack	91.5
Zero-Day Exploits	89.6

The system demonstrates high detection rates across diverse threat categories. It performs especially well on common attacks such as phishing and transaction tampering. Zero-day exploit detection, while lower, still maintains a robust performance due to the integration of anomaly detection techniques.

The detection rate was calculated by evaluating the model's output against manually labeled instances for each attack category. These proportions reflect the true positive rate within each respective class.





**Figure 4:** Proportional Detection Accuracy by Threat Category

Figure 4 visualizes the percentage of correctly identified instances for each major cyber threat type based on model evaluation. Percentages are derived from precision-recall-based classification performance per category, as recorded in Table 4.

#### 4.5. Discussion

The results indicate that the proposed hybrid model is highly effective in detecting cyber threats in mobile payment environments. The integration of supervised and unsupervised learning addresses the limitations of traditional models, allowing the system to detect both known and emerging threats. Specifically, the Random Forest model excels in detecting well-defined threats due to its structured learning capability. Meanwhile, the Autoencoder and Isolation Forest provide strong detection for previously unseen attack types by capturing anomalous behavioral sequences. The hybrid voting mechanism enhances overall robustness by leveraging complementary strengths across all three models.

These findings are aligned with prior studies advocating for adaptive and intelligent detection systems in FinTech cybersecurity [5], [7], [16]. Furthermore, the low false-positive rate supports operational feasibility in real-world financial applications where user trust and experience are paramount [9], [12].

Despite its strong performance, the framework has some limitations that must be considered in real-world deployments. One significant challenge is the risk of false positives, which could lead to unnecessary transaction blocks, impacting user trust and satisfaction. On the other hand, false negatives—where malicious activity is misclassified as benign—could result in undetected security breaches. These risks are especially sensitive in financial contexts where both over-blocking and under-detection can have serious consequences.

Furthermore, the model's dependency on synthetic attack data introduces some uncertainty about generalizability to real-world zero-day threats not covered in the training set. Device diversity, regional behavioral norms, and evolving fraud techniques may affect detection accuracy. The system's scalability and latency in high-frequency transaction environments also require ongoing

evaluation, especially under strict real-time constraints.

## 5. CONCLUSION

The growing reliance on mobile payment systems in the FinTech sector has introduced unprecedented challenges in cybersecurity, with increasingly sophisticated threats targeting sensitive financial data and user trust. In response to these concerns, this study proposed a novel machine learning-based hybrid framework for cyber threat detection in mobile payments. By combining the strengths of supervised (Random Forest) and unsupervised (Autoencoder and Isolation Forest) learning models, the framework achieved high detection accuracy, recall, and precision, effectively mitigating both known and previously unseen attacks.

Through comprehensive data preprocessing, intelligent feature engineering, and an ensemble detection strategy, the framework demonstrated robustness, scalability, and adaptability in real-world mobile transaction environments. The inclusion of behavioral analytics, transaction anomaly detection, and federated learning principles further enhanced its ability to protect user privacy while maintaining strong detection performance. Experimental evaluations confirmed that the hybrid model significantly outperforms traditional rule-based and single-model approaches, achieving an F1-score of over 95% and consistently high threat detection rates across multiple attack types.

This research contributes to the advancement of cybersecurity in digital finance by presenting a flexible, intelligent solution that can be deployed in real-time and scaled across different mobile payment platforms. It also fills a gap in the existing literature by integrating context-aware features and hybrid ML techniques tailored specifically for FinTech environments. Ultimately, this framework has the potential to support financial institutions, regulatory bodies, and technology providers in building secure, trustworthy, and user-centric digital financial ecosystems.

Future research will explore the full integration of federated learning into the framework, enabling decentralized training across edge devices without compromising user privacy. This extension will address the need for secure, collaborative learning in geographically distributed FinTech environments.

### Declaration of Ethical Standards

The authors affirm that this research adheres to the highest ethical standards. All procedures involving data acquisition and algorithmic experimentation comply with relevant institutional and international ethical guidelines. No human subjects, personal identifiable information, or sensitive financial records were used without proper anonymization. The manuscript represents original work, has not been published elsewhere, and is not under

consideration by another publication.

### Credit Authorship Contribution Statement

Harman Salih Mohammed: Literature Review, Data Curation, Writing – Review & Editing, Visualization, Validation, Data Analysis Support. Hewa Majeed Zangana: Conceptualization, Methodology, Software, Validation, Formal Analysis, Investigation, Resources, Writing – Original Draft, Visualization, Supervision, Project Administration. All authors have read and approved the final manuscript and agree to be accountable for all aspects of the work.

### Declaration of Competing Interest

The authors declare that they have no known financial or non-financial competing interests or relationships that could have appeared to influence the work reported in this paper.

### Funding / Acknowledgements

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors. The authors would like to thank their respective institutions—Duhok Polytechnic University and Ararat Technical Private Institute—for their academic support and access to computational resources used during the study.

### Data Availability

The datasets generated and/or analyzed during the current study are not publicly available due to institutional policy and data-sharing restrictions. However, anonymized datasets can be made available by the corresponding author upon reasonable request and with appropriate data-use agreements in place to protect user and system confidentiality.

### References

- [1] M. Asmar and A. Tuqan, "Integrating machine learning for sustaining cybersecurity in digital banks," *Heliyon*, vol. 10, no. 17, 2024.
- [2] M. S. K. Munira, "Assessing the influence of cybersecurity threats and risks on the adoption and growth of digital banking: A systematic literature review," Available at SSRN: 5229868, 2025.
- [3] K. K. Boorugupalli, A. K. Kulkarni, A. Suzana, and S. Ponnusamy, "Cybersecurity Measures in Financial Institutions Protecting Sensitive Data from Emerging Threats and Vulnerabilities," in *ITM Web of Conferences*, EDP Sciences, 2025, p. 02002.
- [4] S. Dhaiya, B. K. Pandey, S. B. K. Adusumilli, and R. Avacharmal, "Optimizing API Security in FinTech Through Genetic Algorithm based Machine Learning Model," *International Journal of Computer Network and Information Security*, vol. 13, p. 24, 2021.
- [5] W. C. Aaron, O. Irekponor, N. T. Aleke, L. Yeboah, and J. E. Joseph, "Ma-chine learning techniques for enhancing security in financial technology systems," 2024.
- [6] O. E. Ejiofor, "A comprehensive framework for strengthening USA financial cybersecurity: integrating machine learning and AI in fraud detection systems," *European Journal of Computer Science and Information Technology*, vol. 11, no. 6, pp. 62–83, 2023.
- [7] A. T. Olutimehin, "The Synergistic Role of Machine Learning, Deep Learning, and Reinforcement Learning in Strengthening Cyber Security Measures for Crypto Currency Platforms," *Deep Learning, and Reinforcement Learning in Strengthening Cyber Security Measures for Crypto Currency Platforms (February 11, 2025)*, 2025.
- [8] M. Ononiwu, T. I. Azonuche, O. F. Okoh, and J. O. Enyejo, "Machine Learning Approaches for Fraud Detection and Risk Assessment in Mobile Banking Applications and Fintech Solutions," 2023.
- [9] N. Mirza, M. Elhoseny, M. Umar, and N. Metawa, "Safeguarding FinTech innovations with machine learning: Comparative assessment of various approaches," *Res Int Bus Finance*, vol. 66, p. 102009, 2023.
- [10] U. Noor, Z. Anwar, T. Amjad, and K.-K. R. Choo, "A machine learning-based FinTech cyber threat attribution framework using high-level indicators of compromise," *Future Generation Computer Systems*, vol. 96, pp. 227–242, 2019.
- [11] R. Karangara, "Adaptive Machine Learning Models for Securing Payment Gateways: A Resilient Approach to Mitigating Evolving Cyber Threats in Digital Transactions," *Artificial Intelligence Evolution*, pp. 44–64, 2025.
- [12] A. Faccia, "National payment switches and the power of cognitive computing against fintech fraud," *Big Data and Cognitive Computing*, vol. 7, no. 2, p. 76, 2023.
- [13] A. Adejumo and C. Ogburie, "Strengthening finance with cybersecurity: Ensuring safer digital transactions," *World Journal of Advanced Research and Reviews*, vol. 25, no. 3, pp. 1527–1541, 2025.
- [14] S.-Y. Hwang, D.-J. Shin, and J.-J. Kim, "Systematic review on identification and prediction of deep learning-based cyber security technology and convergence fields," *Symmetry (Basel)*, vol. 14, no. 4, p. 683, 2022.
- [15] S. Paleti, V. Pamisetty, K. Challa, J. K. R. Burugulla, and A. Dodda, "Innovative Intelligence Solutions for Secure Financial Management: Optimizing Regulatory Compliance, Transaction Security, and Digital Payment Frameworks Through Advanced Computational Models," *Transaction Security, and Digital Payment Frameworks Through Advanced Computational Models (December 10, 2024)*, 2024.
- [16] H. Rabbani *et al.*, "Enhancing security in financial transactions: a novel blockchain-based federated learning framework for detecting counterfeit data in fintech," *PeerJ Comput Sci*, vol. 10, p. e2280, 2024.
- [17] V. N. Kollu, V. Janarathanan, M. Karupusamy, and M. Ramachandran, "Cloud-based smart contract analysis in fintech using IoT-integrated federated learning in intrusion detection," *Data (Basel)*, vol. 8, no. 5, p. 83, 2023.
- [18] H. R. B. Seshakagari and D. HariramNathan, "AI-Augmented Fraud Detection and Cybersecurity Framework for Digital Payments and E-Commerce Platforms," *International Journal of Computational Learning & Intelligence*, vol. 4, no. 4, pp. 832–846, 2025.
- [19] H. Xia, Y. Wang, J. Gauthier, and J. Z. Zhang, "Knowledge graph of mobile payment platforms based on deep learning: Risk analysis and policy implications," *Expert Syst Appl*, vol. 208, p. 118143, 2022.
- [20] B. Stojanović *et al.*, "Follow the trail: Machine learning for fraud detection in Fintech applications," *Sensors*, vol. 21, no. 5, p. 1594, 2021.
- [21] K. Upreti, M. H. Syed, M. A. Khan, H. Fatima, M. S. Alam, and A. K. Sharma, "Enhanced algorithmic modelling and architecture in deep reinforcement learning based on wireless communication Fintech technology," *Optik (Stuttg)*, vol. 272, p. 170309, 2023.
- [22] I. O. Owolabi, C. K. Mbabie, and J. C. Obiri, "AI-Driven Cybersecurity in FinTech & Cloud: Combating Evolving Threats with Intelligent Defense Mechanisms," *International Journal of Multidisciplinary Research in Science, Engineering and Technology*, vol. 7, p. 12, 2024.
- [23] R. Ramadugu, "Effectiveness Of Natural Language Processing Based Security Tools In Strengthening The Security Over Fin-Tech Platforms," *International Journal of Creative Research*

- Thoughts*, vol. 11, no. 8, pp. 199–219, 2023.
- [24] M. Williams, M. F. Yussuf, and A. O. Olukoya, “Machine learning for proactive cybersecurity risk analysis and fraud prevention in digital finance ecosystems,” *ecosystems*, vol. 20, p. 21, 2021.
- [25] S. Ryu, J. Kim, and N. Park, “Study on Trends and predictions of convergence in Cybersecurity Technology using machine learning,” *Journal of Internet Technology*, vol. 24, no. 3, pp. 709–725, 2023.