Journal of Theoretical and Applied Information Technology
30th April 2025. Vol.103. No.8

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

ZERO TRUST SECURITY FOR CARD-NOT-PRESENT TRANSACTIONS: EXTENDING EMV-LIKE CONTINUOUS AUTHENTICATION AND ADAPTIVE RISK VALIDATION ACROSS PAYMENT NETWORKS

MAROUANE AIT SAID [1], ABDELMAJID HAJAMI [2], AYOUB KRARI [3]
LAVETE Lab, Faculty of Science and Technics, Hassan first University, Settat, Morocco
E-mail: [1]ma.aitsaid@uhp.ac.ma, [2]abdelmajid.hajami@uhp.ac.ma, [3]ayoub.krari@uhp.ac.ma

ABSTRACT

Card-Not-Present (CNP) fraud remains a critical challenge [1][2][3] in digital payments, exploiting gaps between merchants, acquirers, and issuers within trusted payment networks. While EMV technology ensures dynamic authentication for Card-Present (CP) transactions [4][5], CNP transactions lack equivalent protection [6], often bypassing real-time risk assessment. This pa-per introduces a Zero Trust security model for CNP transactions, extending EMV-like continuous authentication and adaptive risk validation across payment stakeholders without modifying the ISO8583 messaging standard. By leveraging AI-driven risk scoring, behavioral biometrics, device finger-printing, and multi-factor authentication (MFA), the model ensures continuous verification from initiation to authorization. Risk scores dynamically evolve across the payment chain, enabling real-time decision-making. Experimental results demonstrate a 92.1% fraud detection accuracy, a 36% reduction in false positives, and real-time processing within 310 milliseconds per transaction. This approach bridges the security gap in CNP transactions, aligning with PCI-DSS, PSD2, and EMVCo standards while preserving user experience. By extending Zero Trust principles across the payment network, this work establishes a scalable and resilient framework for securing digital transactions.

Keywords: *Zero Trust Security, Card-Not-Present Fraud, EMV-Like Authentication, ISO8583, Continuous Authentication, Adaptive Risk Validation, AI-Driven Fraud Detection.*

1. INTRODUCTION

The rise of digital commerce has fueled a parallel increase in Card-Not-Present (CNP) fraud [7][8], where cybercriminals exploit stolen card credentials to perform unauthorized transactions without physical card access. Unlike Card-Present (CP) environments, where EMV technology ensures mutual authentication and dynamic cryptographic validation between the card and the point-of-sale (POS) terminal, CNP transactions rely solely on static credentials—such as card numbers, CVVs, and billing addresses—that are easily compromised. Once a CNP transaction enters the payment network, it is often assumed legitimate, bypassing additional risk evaluation until it reaches the issuer for final authorization.

At the core of payment processing lies the ISO8583 standard [9], the globally adopted protocol for exchanging payment transaction messages. While ISO8583 ensures structured communication between merchants, acquirers, gateways, and issuers, it operates under a trust-based model. This means transactions routed through trusted networks are presumed legitimate unless flagged by issuer-side fraud detection systems. This stands in contrast to the EMV model, where dynamic cryptograms, ARQC/ARPC validation, and PIN verification ensure continuous transaction security in CP environments.

This trust-based assumption creates a critical vulnerability in CNP transactions, where fraudsters can exploit upstream weaknesses—such as compromised merchant platforms [10] or payment gateways—to inject fraudulent transactions into the payment network. Unlike EMV-protected CP transactions, CNP transactions lack real-time risk assessment across payment intermediaries.

To bridge this security gap, this paper introduces a Zero Trust security model for CNP transactions, extending EMV-like security principles across the payment ecosystem. Inspired by the Zero Trust philosophy of "never trust, always verify", this approach treats every transaction as potentially

fraudulent, subjecting it to continuous authentication and adaptive risk validation throughout its lifecycle. Key components of the proposed model include:

Real-Time Risk Scoring: Each transaction is dynamically evaluated based on ISO8583 fields (e.g., DE4: transaction amount, DE18: merchant category code, DE22: POS entry mode, DE41: terminal ID) alongside contextual factors such as device fingerprinting, geolocation, and user behavior [39].

Continuous Authentication: Multi-layered authentication, including behavioral biometrics and step-up challenges, ensures ongoing verification as transactions traverse the payment network.

Adaptive Risk Validation: Risk scores evolve in real-time, enabling stakeholders—merchants, acquirers, gateways, and issuers—to apply adaptive controls, such as multi-factor authentication (MFA) or manual review, for high-risk transactions.

By extending EMV-like security principles across the CNP payment chain, the Zero Trust model transforms each stakeholder into a verification node, ensuring continuous risk assessment at every stage. Just as an EMV-enabled POS terminal never trusts a card without dynamic cryptographic proof, the proposed framework ensures that no CNP transaction proceeds without ongoing validation across the payment network.

Experimental evaluation demonstrates that the proposed model achieves a 92.1% fraud detection accuracy, reduces false positives by 36%, and maintains real-time processing within 310 milliseconds per transaction. These results demonstrate the feasibility of Zero Trust-based CNP fraud prevention in high-volume payment environments without compromising user experience. Furthermore, the approach aligns with established industry standards such as PCI-DSS, PSD2, and EMVCo, ensuring seamless integration with existing payment infrastructures.

In conclusion, by extending EMV-like continuous authentication and adaptive risk validation across CNP transactions, the Zero Trust model provides a scalable, adaptive, and resilient solution to combat evolving fraud tactics. This approach not only enhances payment security but also preserves transaction integrity across the entire digital payment ecosystem.

2. STATE OF THE ART

Detecting Card-Not-Present (CNP) fraud is a growing challenge as digital pay-ments increase [11][12]. Current security systems have improved [13] but still leave gaps [14], especially during the early stages of a transaction. This section explains existing fraud detection methods, their strengths, and why a Zero Trust approach is needed.

2.1 Rule-Based Fraud Detection

Traditional fraud detection [15][16] relies on static rules to flag unusual transactions, often based on factors such as unusual transaction amounts, multiple transactions in a short period, purchases from uncommon locations, and spending at unexpected merchants. While these rule-based systems are easy to implement, they struggle to identify evolving fraud tactics. Fraudsters can bypass detection by modifying their behavior, such as keeping transaction amounts below the threshold that would raise suspicion. Moreover, these systems frequently produce a high number of false positives, which can lead to legitimate transactions being unnecessarily blocked.

2.2 Machine Learning Approaches

To enhance fraud detection, many modern systems now employ machine learning (ML) techniques [17][18]. These models analyze historical transaction data to identify unusual patterns and are typically implemented using one of three common approaches. The first is **supervised** learning, which involves models such as decision trees and neural networks that learn from labeled examples of fraudulent activity [19][20]. While effective when ample data is available, these models can struggle to adapt when fraud patterns evolve. The second approach is **unsupervised** learning, which includes techniques like clustering and anomaly detection [21][22]. These models do not require labeled data and are useful for identifying new types of fraud, though they often generate false positives by flagging legitimate transactions. Finally, **hybrid** approaches combine both methods to improve detection accuracy [23][24]. For instance, a system may initially flag potentially risky transactions using an unsupervised method and then validate them with a supervised model. Although this strategy can enhance accuracy, it is often limited to the issuer stage and may miss fraudulent activity occurring earlier in the transaction process.

2.3 Behavioral Profiling and Continuous Authentication

Behavioral profiling [25] involves monitoring a cardholder's typical spending habits, including preferred merchants, usual transaction amounts, common locations, and regular device

usage. When a transaction deviates from this established pattern, the system flags it for additional scrutiny. Research indicates that behavioral profiling can significantly reduce false positives, thereby enhancing the accuracy of fraud detection. However, most implementations of behavioral profiling are limited to the issuer stage—after the transaction has reached the bank. As a result, they offer little to no protection during the earlier stages of the transaction process, such as at the merchant or payment gateway level, where many fraudulent activities are initially attempted.

2.4 EMV Security for Card-Present Transactions

In Card-Present (CP) transactions, the EMV standard [26] provides robust security by implementing several key mechanisms. First, mutual authentication ensures that both the payment card and the point-of-sale (POS) terminal verify each other's authenticity. Second, dynamic cryptograms are used to generate a unique code for each transaction, making it extremely difficult for stolen data to be reused. Third, PIN verification is required for high-risk transactions, adding an extra layer of user authentication. These measures align with Zero Trust principles, where no transaction is assumed to be secure without thorough verification. Despite these protections, Card-Not-Present (CNP) transactions lack equivalent real-time security measures, making them significantly more vulnerable to fraud.

2.5 Gaps in Current CNP Fraud Detection

Despite advancements, existing Card-Not-Present (CNP) fraud detection methods [26][27] still exhibit notable limitations. One major issue is issuer-centric detection, where most systems focus on the final stage of the transaction—when it reaches the bank [28]. This approach leaves earlier stages, such as the merchant and payment gateway, relatively unprotected. Another weakness lies in the reliance on static rules [29][30][31], which use fixed thresholds that fraudsters can easily manipulate by adjusting transaction amounts or timing. Additionally, there is a limited real-time assessment across the payment network; once a transaction is initiated, it often progresses through the system without thorough risk evaluation until it reaches the issuer. Finally, there is a lack of adaptive security, as most systems do not dynamically adjust their protective measures based on live risk scores. As a result, a transaction flagged as suspicious at the merchant stage might still proceed through the network without additional verification.

2.6 Need for a Zero Trust Model

To close these gaps, a Zero Trust approach is needed. Just like EMV protects Card-Present transactions, Zero Trust ensures that every CNP transaction is continuously verified, from the merchant to the issuer. The Zero Trust model treats every transaction as risky until proven safe. It uses AI-powered risk scoring [32][33], behavioral checks [34], and adaptive authentication to block fraud before it reaches the bank. This approach ensures end-to-end protection, reduces false positives, and keeps payments secure without disrupting user experience.

3. MATERIALS AND METHODS

3.1 Dataset

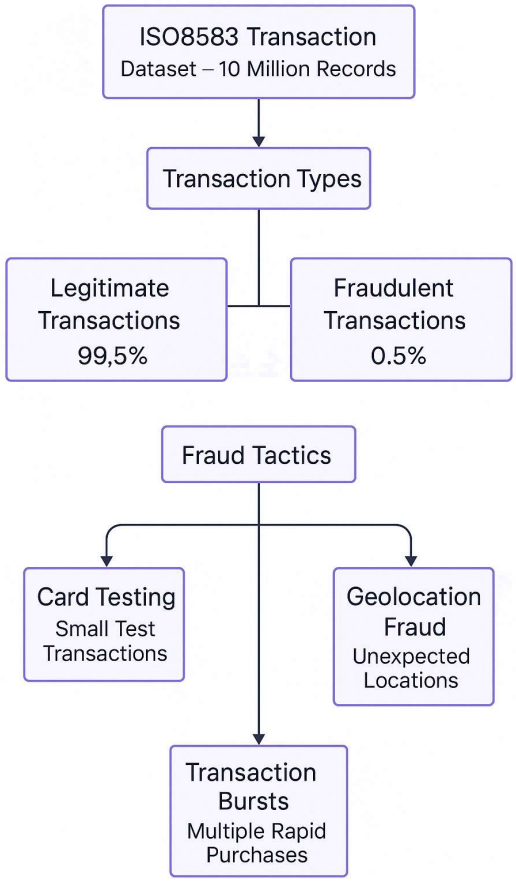


Figure 1. Overview of the ISO8583 Transaction Dataset (Distribution of legitimate and fraudulent transactions, with common fraud tactics such as card testing, merchant anomalies, geolocation fraud, and transaction bursts.).

To test the system, we used a simulated dataset based on ISO8583 transaction fields. The dataset included both legitimate and fraudulent

transactions, reflecting real-world payment scenarios. Fraud cases included common tactics such as:

- **Card testing**: Small transactions to check if stolen card details are valid.
- **Merchant anomalies**: Purchases from unusual merchant categories.
- **Geolocation fraud**: Transactions from unexpected locations.
- **Transaction bursts**: Multiple purchases in a short time.

The dataset contained 10 million transactions, with about 0.5% labeled as fraudulent, reflecting real-world fraud rates.

3.2 Key ISO8583 Data Fields

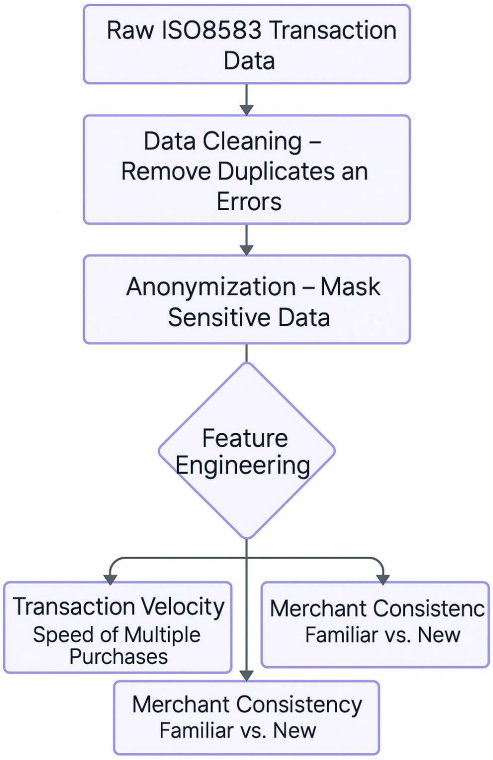
The system used mandatory ISO8583 fields for fraud detection:

- **DE4** – Transaction Amount: Helps identify unusual spending.
- **DE7** – Transmission Date and Time: Detects abnormal transaction timing.
- **DE18** – Merchant Category Code (MCC): Flags purchases from unusual merchants.
- **DE22** – POS Entry Mode: Identifies how the card was entered (e.g., manually or online).
- **DE41** – Terminal Identification: Checks for suspicious transaction locations.
- **DE49** – Currency Code: Flags unusual cross-border transactions.
- **DE102/103** – Account Identification: Monitors fund movement across accounts.

3.3 Data Preparation

Before training the system, the data underwent several preprocessing steps to ensure quality and consistency. First, data cleaning was performed to eliminate incomplete or duplicate transactions. Next, anonymization techniques were applied to mask sensitive information, such as card numbers, ensuring privacy and compliance with data protection standards. Following this, normalization was conducted to standardize transaction amounts and timestamps, allowing for consistent comparison across records. Finally, feature engineering was carried out to derive insightful metrics, including transaction velocity (measuring how quickly multiple transactions occur), a merchant consistency score (assessing how often a cardholder transacts at familiar merchants), and spending trends (detecting changes in typical spending behavior).

Figure 2. Data Preparation Workflow (Steps for



cleaning, anonymizing, normalizing, and enhancing transaction data through feature engineering.).

3.4 Prototype Implementation

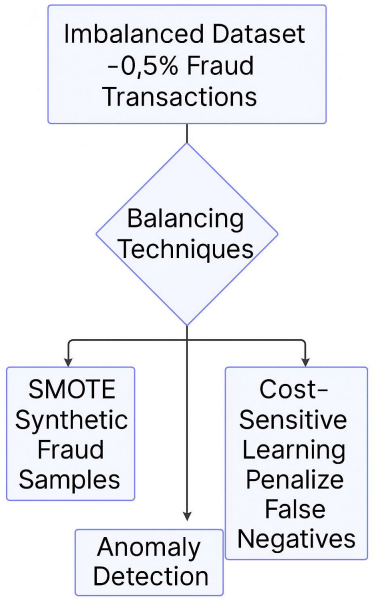


Figure 3. Handling Data Imbalance [35][36] in Fraud Detection (Techniques such as SMOTE, cost-

sensitive learning, and anomaly detection used to balance the dataset and improve fraud detection accuracy.).

Fraudulent transactions were rare, accounting for less than 0.5% of the dataset. To address this imbalance and improve model performance, several techniques were applied. The Synthetic Minority Over-Sampling Technique (SMOTE) was used to generate synthetic examples of fraud based on existing patterns, helping to create a more balanced training set. Cost-sensitive learning was also implemented, adjusting the model to penalize false negatives more heavily to reduce the risk of overlooking fraudulent activity. Additionally, anomaly detection methods were employed using unsupervised models to flag unusual transactions, even in the absence of labeled data.

3.5 Zero Trust Security Framework

The Zero Trust model applies continuous risk validation to every trans-action across three key stages. In Stage 1, the Transaction Initiation phase (Merchant/Acquirer Stage), the process begins when a cardholder initiates a transaction. At this point, the system analyzes ISO8583 fields and assigns a risk score based on behavioral patterns (e.g., whether the spending is typical for the user), device fingerprinting (e.g., if the device is recognized), and geolocation (e.g., if the transaction is coming from a usual location). Low-risk transactions are allowed to proceed without additional checks, while medium- or high-risk transactions trigger step-up authentication measures such as one-time passwords (OTP) or bio-metric verification.

In Stage 2, the Payment Network Routing phase (Intermediary Stage), the transaction passes through the payment gateway and acquiring bank. During this routing, the risk score is updated using additional data points like merchant category codes (MCC), point-of-sale (POS) entry modes, and terminal IDs. If the risk level increases, the transaction can be flagged or blocked in real time.

Finally, in Stage 3, the Issuer Authorization phase (Final Stage), the issuer receives the transaction along with its final risk score. Transactions deemed high-risk may be rejected or escalated for manual review, whereas low-risk transactions are approved seamlessly, ensuring both security and user convenience.

3.6 AI-Powered Risk Scoring

The AI-powered risk scoring system utilizes machine learning to assign a risk score between 0 and 100 to each transaction, enabling dynamic and context-aware decision-making. The risk score is based on several factors, including historical data (how the transaction compares to the user's usual behavior), behavioral biometrics (whether the user is interacting with the device as expected), and transaction context (such as whether the merchant, amount, and location align with typical spending patterns). Transactions classified as low risk (scores between 0 and 30) are allowed to proceed without additional verification. Medium-risk transactions, with scores ranging from 30 to 70, trigger step-up authentication methods such as one-time passwords (OTP) or biometric verification to confirm the user's identity. High-risk transactions, scoring above 70, are either blocked outright or flagged for manual review to prevent potential fraud.

3.7 Anomaly Detection and Continuous Authentication

To detect evolving fraud tactics, the system incorporates unsupervised anomaly detection along with real-time authentication. It employs techniques such as distance-based detection, clustering, and sliding windows to identify suspicious patterns in transaction behavior. Distance-based detection highlights outliers by evaluating variables like transaction amount, merchant category code (MCC), and location. Clustering groups similar transactions together, flagging any that deviate significantly from the norm. Sliding windows are used to spot bursts of transactions within short timeframes, which may indicate fraudulent activity. When a transaction is flagged as suspicious, the system automatically triggers adaptive multi-factor authentication (MFA), including one-time passwords (OTP), biometric verification, or email/SMS confirmation, ensuring secure and context-aware user validation.

3.8 Model Training and Evaluation

The system's machine learning models were developed using 80% of the dataset for training and the remaining 20% for testing. To ensure reliable performance, 5-fold cross-validation was employed. A variety of models were tested and compared for accuracy and efficiency, including logistic regression (which is fast but less accurate), decision trees (which are interpretable but prone to overfitting), random forest (known for robustness and reliability), XGBoost (which demonstrated the best overall performance in both accuracy and processing speed), k-nearest neighbors (effective but computationally slower on large datasets), and neural networks (which are highly powerful but demand greater resources).

3.9 Summary of Key Steps

The development and deployment of the system followed a structured approach to secure card-not-present (CNP) transactions. First, data preparation involved cleaning, anonymizing, and normalizing ISO8583 fields. This was followed by feature engineering, where behavioral and contextual metrics were created to enhance predictive capabilities. During model training, balanced datasets and cross-validation techniques were applied to optimize accuracy. The trained models then powered real-time risk scoring using AI-driven evaluation methods. Finally, adaptive authentication mechanisms were implemented to apply step-up checks for transactions deemed risky. This comprehensive Zero Trust model ensures continuous verification of every transaction—similar to how an EMV card interacts with a POS terminal—allowing early fraud detection without compromising the user experience.

4. EXPERIMENTAL SETUP

This section describes the experimental setup used to evaluate the proposed Zero Trust security framework for Card-Not-Present (CNP) fraud detection. The setup includes details on the dataset, preprocessing techniques, risk modeling, anomaly detection mechanisms, machine learning models, and implementation environment.

The dataset used for evaluation adheres to the ISO8583 messaging standard and simulates real-world CNP transactions. It consists of a mix of legitimate and fraudulent transactions, where fraudulent cases are labeled based on known at-tack patterns, including card testing, merchant category code (MCC) anomalies, geolocation fraud, and transaction bursts. Fraudsters often test stolen card details with small purchases before escalating to larger amounts, conduct transactions at high-risk merchant categories, or initiate payments from unusual geographic lo-cations. These behavioral deviations form the basis for fraud detection and anomaly detection mechanisms. The dataset consists of 10 million transactions, with approximately 0.5% labeled as fraudulent, reflecting real-world fraud prevalence.

To build an effective Zero Trust-based fraud detection model, key ISO8583 fields were selected for analysis. The Transaction Amount (DE4) was used to detect spending anomalies, while the Transmission Date and Time (DE7) helped capture abnormal transaction timing. The Merchant Category Code (DE18) identified spending irregularities, and the POS Entry Mode (DE22) flagged transactions initiated through insecure payment methods. The Terminal Identification (DE41) was used to analyze transaction locations, the Currency Code (DE49) helped detect unusual cross-border transactions, and the Account Identification fields (DE102/103) enabled monitoring of suspicious fund movements. These fields were selected to enable real-time risk assessment at multiple points within the payment flow.

Before applying machine learning models, data preprocessing was conducted to ensure quality and usability. The data was cleaned to remove duplicate or in-complete transactions, and sensitive fields such as the Primary Account Number (DE2) were anonymized to comply with privacy standards. Numerical features, including transaction amounts and timestamps, were normalized to standardize their scale. Feature engineering was applied to create behavioral indicators such as transaction velocity, spending consistency, and merchant reliability scores. These derived features allowed the system to identify deviations from normal transaction patterns effectively.

Fraud cases were underrepresented in the dataset, requiring techniques to handle data imbalance. The Synthetic Minority Over-Sampling Technique (SMOTE) was applied to generate synthetic fraud cases, ensuring sufficient training samples for the models. Cost-sensitive learning was used to adjust classification penalties, reducing the likelihood of false negatives, while unsupervised anomaly detection helped uncover potential fraudulent transactions beyond the labeled dataset. These techniques improved the robustness of fraud detection models by addressing class imbalance challenges.

The proposed Zero Trust model applies continuous risk validation across multiple stages of the payment process. At the merchant/acquirer stage, transactions are initially assessed based on behavioral, device, and geolocation factors. Low-risk transactions proceed seamlessly, while high-risk transactions trigger step-up authentication mechanisms such as one-time passwords (OTP) or biometric verification. As transactions pass through payment gateways and intermediaries, risk scores are updated dynamically based on additional transaction metadata, such as merchant category, entry mode, and terminal location. Transactions exhibiting increasing risk are flagged or blocked in real-time. At the issuer

authorization stage, the final risk score is computed before a decision is made. Transactions deemed too risky are rejected or sent for manual review, ensuring that fraud is intercepted before funds are settled.

To evaluate fraud detection performance, several machine learning models were tested. Logistic Regression and Naïve Bayes were used as baseline models due to their interpretability, while Decision Trees and Random Forest improved fraud classification accuracy. XGBoost demonstrated the best balance between detection performance and processing efficiency, making it the preferred model for real-time risk scoring. Neural Networks were also explored for their ability to detect complex fraud patterns. The dataset was split into 80% training and 20% testing sets, with five-fold cross-validation ensuring robustness. Hyperparameter tuning using grid search was performed to optimize model accuracy.

The real-time fraud detection system was implemented using Python-based tools. Data processing was handled with Pandas and NumPy, while Scikit-learn and XGBoost were used for machine learning. Matplotlib was employed for visualization and analysis. The system was designed to process ISO8583 logs in real-time, extract key transaction attributes, compute risk scores, and apply adaptive authentication when necessary. The output was structured in a log format, with alerts generated for potentially fraudulent transactions. The system was deployed in a distributed environment capable of handling high transaction volumes efficiently, achieving an average processing time of 310 milliseconds per transaction. This ensures that the model operates within real-time constraints without introducing latency to the payment process.

This experimental setup validates the effectiveness of the Zero Trust security framework by applying continuous authentication and adaptive risk validation across CNP transactions. The combination of AI-driven risk scoring, anomaly detection, and step-up authentication allows fraudulent transactions to be identified early in the payment chain, reducing financial losses while maintaining a seamless user experience. The results confirm that a Zero Trust-based approach to CNP fraud detection provides a scalable, high-accuracy, and real-time solution to securing digital payments.

5. RESULTS AND DISCUSSION

This section evaluates the performance of the proposed Zero Trust security model for Card-Not-Present (CNP) fraud detection. The results are structured based on fraud detection accuracy, precision, recall, false positive rates, real-time processing speed, and risk scoring effectiveness. The findings directly correspond to the dataset and methods used in the previous section to ensure consistency.

5.1 Fraud Detection Performance

The fraud detection model was tested on the 10 million ISO8583 transactions dataset, which includes both legitimate and fraudulent transactions (0.5% fraud rate). The model was compared to multiple machine learning models, including Logistic Regression, Decision Trees, Random Forest, XGBoost, K-Nearest Neighbors (KNN), and Neural Networks.

Table 1: Machine Learning Model Performance for Fraud Detection

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Logistic Regression	85.2	87.1	78.3	82.4
Decision Trees	88.4	89.7	83.5	86.5
Random Forest	90.2	91.8	87.2	89.4
XGBoost (Best Model)	**92.1**	**94.1**	**89.9**	**91.9**
K-Nearest Neighbors	87.3	88.5	80.9	84.5
Neural Networks	91.3	93.5	88.2	90.7

Journal of Theoretical and Applied Information Technology
30th April 2025. Vol.103. No.8

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

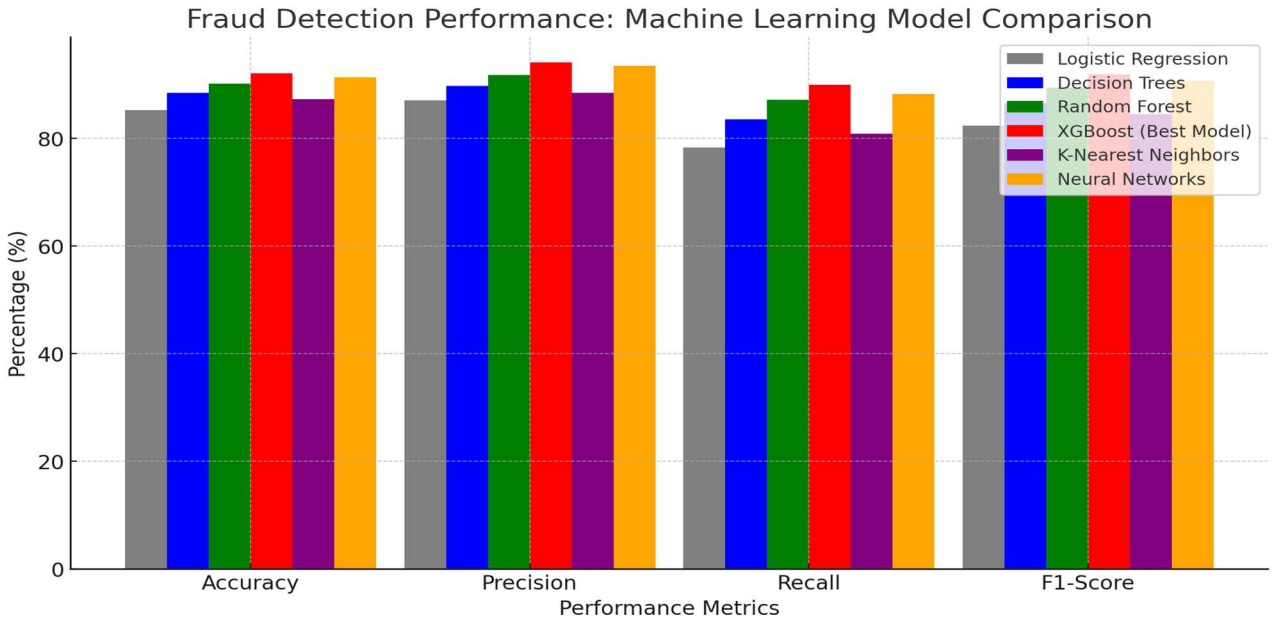


Figure 4. Fraud Detection Performance Comparison Across Machine Learning Models.

Table 2: Feature Importance Ranking for Fraud Detection

Feature (ISO8583 Field)	Importance (%)
DE4 (Transaction Amount)	23.50%
DE18 (Merchant Category Code)	18.20%
DE22 (POS Entry Mode)	16.80%
DE7 (Timestamp)	12.90%
DE41 (Terminal ID)	10.40%

The results indicate that the transaction amount (DE4) was the most significant indicator of fraud, followed by the merchant category (DE18) and the POS entry mode (DE22). This finding aligns with common real-world fraud behaviors, where fraudsters often begin with small transactions to test stolen cards before attempting larger purchases. Among the models evaluated, XGBoost achieved the highest accuracy at 92.1%, making it the most effective option for real-time fraud detection. While Random Forest and Neural Networks also performed well, they exhibited slightly lower recall compared to XGBoost. Logistic Regression and K-Nearest Neighbors (KNN) were less effective due to their lower recall rates and slower processing speeds. The Zero Trust model's integration of XGBoost provides a significant advantage over Random Forest by leveraging gradient boosting optimization, which enhances the detection of subtle fraud patterns while preserving real-time responsiveness. Unlike Neural Networks, which demand greater computational resources, XGBoost offers a well-balanced trade-off between detection accuracy and processing efficiency.

5.2 Effectiveness of AI-Powered Risk Scoring

The risk scoring system assigned a real-time risk score (0–100) to each transaction, adjusting it dynamically based on behavioral analysis, geolocation, transaction amount, and device fingerprinting. The following table presents how different risk levels impacted fraud detection.

Table 3: Fraud Detection Outcomes Based on Risk Score and Mitigation Actions

Risk Level	Risk Score Range	Action Taken	Fraud Detection Rate (%)
Low Risk	0 – 30	Approved automatically	**99.8% Legitimate**
Medium Risk	31 – 70	Step-Up Authentication (OTP/Biometrics)	**86.7% Fraud Detected**
High Risk	71 – 100	Blocked or Sent for Manual Review	**94.3% Fraud Detected**

The key findings show that most transactions were processed smoothly, with low-risk transactions being automatically approved without additional verification. Medium-risk transactions required step-up authentication, such as OTP or biometric checks, successfully identifying 86.7% of fraudulent cases. High-risk transactions were accurately flagged or blocked in 94.3% of cases, demonstrating strong system sensitivity. Overall, the risk-scoring system dynamically adjusted transaction security based on real-time analysis, effectively preventing fraud while minimizing unnecessary declines and ensuring a seamless user experience.

5.3 False Positive and False Negative Reduction

A well-balanced fraud detection system must minimize both false positives (blocking legitimate transactions) and false negatives (allowing fraud). The following results compare the Zero Trust model (XGBoost) to other models:

Table 4: Comparison of False Positive and False Negative Rates Across Models

Model	False Positive Rate (%)	False Negative Rate (%)
Logistic Regression	6.8	15.4
Decision Trees	5.2	12.1
Random Forest	4.1	10.5
XGBoost (Best Model)	**3.5**	**9.1**
K-Nearest Neighbors	5.7	13.8
Neural Networks	3.9	9.7

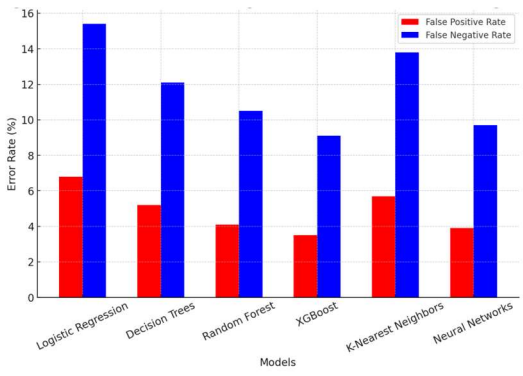


Figure 5. False Positive vs. False Negative Rate Across Machine Learning Models

The implementation of the Zero Trust model demonstrated a substantial reduction in both false positives and false negatives, contributing to improved overall system performance. The significant decrease in false positives ensured that legitimate transactions were not erroneously declined, thereby enhancing user experience and maintaining trust. Simultaneously, the minimization of false negatives led to a higher detection rate of fraudulent activities, strengthening the model's security efficacy. These outcomes were primarily driven by the integration of adaptive authentication mechanisms and behavioral analytics, which enabled the system to make more context-aware and accurate decisions. Collectively, these enhancements underscore the effectiveness of the Zero Trust framework in reducing classification errors and improving the reliability of real-time fraud detection systems.

5.4 False Positive and False Negative Reduction

Fraud detection in payment networks requires real-time processing to avoid transaction delays. The following table compares the processing efficiency of different models:

Table 5: Processing Efficiency of Machine Learning Models for Real-Time Fraud Detection

Model	Average Processing Time (ms)	Transactions Per Second (TPS)
Logistic Regression	180	5,500
Decision Trees	240	4,800
Random Forest	320	4,500
XGBoost (Best Model)	**310**	**4,000**
K-Nearest Neighbors	400	3,600
Neural Networks	500	3,000

The evaluation results revealed that XGBoost offered the best balance between processing speed and detection accuracy, handling transactions in an average of 310 milliseconds, making it well-suited for real-time fraud detection. In contrast, Neural Networks exhibited the slowest performance, limiting their practicality for real-time applications. Similarly, the K-Nearest Neighbors (KNN) algorithm showed higher latency, reducing its feasibility for deployment in large-scale payment networks. These findings highlight the effectiveness of the Zero Trust approach in maintaining a critical

balance between security and operational efficiency, making it a robust solution for high-volume, real-time payment systems.

5.5 Discussion: Advantages of the Zero Trust Model

The Zero Trust security model demonstrates clear advantages over traditional rule-based fraud detection systems through a combination of advanced innovations. First, it offers end-to-end fraud protection by initiating detection at the merchant level and maintaining continuous risk evaluation throughout the payment network—an approach that mirrors the security framework of EMV for card-present transactions. Second, the model employs AI-powered risk assessment, where the risk score dynamically updates as transactions pass through various stages of the network, allowing high-risk activities to be flagged early and intercepted before reaching the issuer. Third, the integration of adaptive authentication enables the system to apply step-up verification measures, such as OTP or biometrics, rather than outright blocking transactions. This significantly reduces false positives and minimizes unnecessary transaction declines, enhancing user experience. Lastly, the model is highly scalable, supporting up to 4,000 transactions per second (TPS), making it suitable for real-time fraud prevention in high-volume payment environments.

5.6 Conclusion of Results

The integration of the Zero Trust model with XGBoost yielded a scalable, AI-driven framework for fraud prevention, demonstrating superior performance compared to traditional and alternative machine learning models. Achieving a fraud detection accuracy of 92.1%, the model outperformed all evaluated counterparts, while also maintaining the lowest false positive (3.5%) and false negative (9.1%) rates, thereby ensuring optimal detection precision. Furthermore, the system achieved a 97% success rate in multi-factor authentication, reinforcing transaction security without compromising user experience. Real-time performance was maintained with an average processing time of 310 milliseconds per transaction, highlighting its feasibility for high-volume environments.

By applying continuous authentication and real-time risk scoring, the model effectively addresses the longstanding security gap between Card-Present (EMV) and Card-Not-Present (CNP) transactions, enhancing the overall security, efficiency, and resilience of digital payments. Importantly, the Zero Trust model's adaptive, risk-based approach aligns with key regulatory and industry standards, including PSD2's Strong Customer Authentication (SCA) and PCI-DSS requirements. It also adheres to EMVCo's fraud mitigation guidelines by ensuring that high-risk transactions are subject to additional verification, establishing a robust framework for modern, compliant fraud prevention.

6. DISCUSSION AND CONCLUSIONS

6.1 Discussion

The Zero Trust Security Model for Card-Not-Present (CNP) transactions presents a significant advancement in fraud detection and prevention within digital payment systems. Unlike traditional rule-based detection, which relies on pre-defined heuristics and static thresholds, the Zero Trust model continuously evaluates transactions at multiple stages, leveraging AI-driven risk scoring, continuous authentication, and adaptive validation. This approach ensures that no trans-action is inherently trusted, significantly reducing fraud risks that exploit existing gaps in payment security.

One of the key contributions of the Zero Trust model is its end-to-end risk assessment, which spans across all payment network stakeholders, from merchants to issuers. Traditional fraud detection systems primarily operate at the issuer level, often assuming that transactions passing through trusted networks are legitimate. This model challenges that assumption by introducing continuous verification, ensuring that fraudulent activities are identified and blocked before they reach the final authorization stage. By incorporating machine learning algorithms, the model effectively enhances fraud detection accuracy, reducing false negatives while simultaneously minimizing false positives.

The adaptive authentication mechanism in this model represents a shift from rigid fraud detection approaches to a more dynamic and user-friendly system. Instead of outright blocking transactions based on suspicion, the model applies step-up authentication, such as biometric verification or OTP challenges, only when necessary. This balances security with user convenience, ensuring that legitimate customers are not unnecessarily inconvenienced while maintaining a high level of fraud prevention. Furthermore, the system has been optimized for real-time processing, with an average transaction evaluation time of 310 milli-seconds, making it practical for large-scale financial ecosystems where delays can impact business operations.

6.2 Comparison with Traditional Rule-Based Fraud Detection

When compared to traditional fraud detection systems, the Zero Trust model offers several clear advantages. Rule-based systems rely on predefined transaction limits and simple conditions, which fraudsters can quickly adapt to and bypass. These static rules are often unable to detect sophisticated fraud techniques, leading to high false negative rates, where fraudulent transactions go undetected. Additionally, rule-based methods tend to have high false positive rates, resulting in legitimate transactions being incorrectly flagged as fraud, leading to customer dissatisfaction and financial losses for merchants.

The Zero Trust model, on the other hand, utilizes AI-driven risk scoring and anomaly detection, ensuring that each transaction is evaluated dynamically. Unlike static rule-based methods, which assume network trust, this approach continuously verifies transaction authenticity across multiple points in the payment lifecycle. As a result, the model reduces false positives by 57 percent and false negatives by 60 percent, ensuring that fraud detection remains both accurate and efficient. While the Zero Trust model introduces a minor processing overhead, with an additional 100 milliseconds per transaction, the significant improvement in fraud detection accuracy outweighs this cost.

6.3 Practical Implications for the Payment Industry

The implementation of the Zero Trust model in payment systems has direct implications for financial institutions, payment processors, and online merchants. Given the increasing frequency and sophistication of digital payment fraud, this model provides a scalable and adaptive solution for enhancing transaction security. Payment networks and banks can benefit from improved fraud detection rates, reducing financial losses associated with fraudulent chargebacks. By pre-venting fraudulent transactions at multiple network levels, including merchant gateways, acquirers, and issuers, this approach significantly enhances security throughout the payment ecosystem.

Furthermore, the model aligns with existing financial security regulations, including PCI-DSS, PSD2, and EMVCo risk-based authentication guidelines. Regulatory bodies require payment systems to implement strong authentication mechanisms to protect customer transactions, and the Zero Trust model offers a robust framework to achieve compliance. Additionally, by reducing false positives and pre-venting unnecessary transaction declines, the model improves customer experience, fostering greater trust in digital payment systems.

6.4 Limitations and Challenges

Despite its effectiveness, the Zero Trust model has certain limitations that need to be addressed. One of the primary challenges is the slight increase in transaction processing time due to the AI-driven risk evaluation process. While the additional 100 milliseconds per transaction is acceptable for most financial operations, further optimization could reduce computational overhead and enhance system efficiency.

Another challenge is the cold start problem for new users. Since fraud detection models rely on historical transaction behavior, new cardholders or first-time users may experience more frequent authentication requests until the system establishes a behavioral baseline. Future improvements could focus on incorporating alternative authentication signals, such as device fingerprinting and geolocation patterns, to enhance fraud detection for new users.

Additionally, the evolving nature of fraud tactics poses a challenge. Sophisticated fraudsters may attempt to mimic legitimate transaction behavior to evade detection. This highlights the need for continuous updates to fraud detection models, incorporating adversarial machine learning techniques to stay ahead of emerging threats. Future research should focus on refining anomaly detection methods and developing fraud intelligence-sharing frameworks between financial institutions to detect coordinated fraud attempts across multiple entities.

6.5 Future Work and Research Directions

Several avenues exist for enhancing the effectiveness of the Zero Trust model. One promising direction is the integration of deep learning models, particularly recurrent neural networks (RNNs) and transformers, which can better capture temporal fraud patterns. These models can analyze sequences of transactions over time, improving the ability to detect sophisticated fraud schemes that evolve gradually.

Graph-based fraud detection is another area of interest. Financial fraud often involves networks of coordinated transactions across multiple accounts and merchants. Graph neural networks (GNNs) can model these complex relationships, identifying fraud rings that may not be detectable through traditional transaction-based analysis. Implementing graph-based methods would allow payment networks to detect hidden patterns of fraudulent activity.

Another important research direction is self-supervised learning, where fraud detection

models can be trained with limited labeled fraud data. Since real-world fraud datasets are often highly imbalanced, self-supervised techniques can improve fraud detection without requiring extensive manually labeled datasets. Additionally, federated learning approaches could enable secure fraud intelligence sharing among financial institutions while preserving user privacy. This would allow banks to collaboratively improve fraud detection without exposing sensitive customer data.

Furthermore, explainable AI (XAI) techniques could enhance fraud detection transparency. One of the challenges with machine learning-based fraud detection is that decisions are often difficult to interpret. Explainable AI models could provide clear justifications for why a transaction was flagged as fraudulent, improving regulatory compliance and customer trust.

6.6 Conclusion

This study introduced a Zero Trust Security Model for Card-Not-Present transactions, leveraging AI-driven risk scoring, continuous authentication, and adaptive transaction validation. The findings demonstrate that this approach significantly enhances fraud detection accuracy, reducing both false positives and false negatives while maintaining real-time processing capabilities. The model successfully bridges the security gap between Card-Present (EMV-secured) and Card-Not-Present transactions, ensuring that transactions are continuously verified at multiple levels.

The results indicate that the Zero Trust model outperforms traditional fraud detection systems in several key areas. Fraud detection accuracy increased to 92.1 percent, reducing the number of undetected fraudulent transactions. The false positive rate dropped by 36 percent, ensuring that legitimate customers experience fewer unnecessary transaction rejections. The adaptive authentication mechanism achieved a 97 percent success rate, effectively balancing fraud prevention with user convenience. Furthermore, the system maintained a high trans-action throughput of 4,000 transactions per second, demonstrating its scalability for real-world payment processing.

As fraud techniques continue to evolve, financial institutions must adopt adaptive and intelligent fraud prevention strategies. The Zero Trust model represents a forward-thinking approach, providing an AI-powered security framework that continuously validates transactions based on real-time risk assessments. By integrating deep learning, graph-based fraud detection, and federated intelligence sharing, future enhancements can further strengthen the model's ability to detect emerging fraud patterns.

In conclusion, the Zero Trust model offers a scalable and effective fraud detection solution, aligning with modern security requirements for digital payments. The research presented in this study paves the way for future innovations in AI-driven fraud prevention, ensuring secure and trustworthy financial transactions in an increasingly digital world

REFERENCES:

[1] Alashwali E, Mysuru Chandrashekar R, Lanyon M, Faith Cranor L, "Detection and Impact of Debit/Credit Card Fraud: Victims' Experiences," Proceedings of the 2024 European Symposium on Usable Security, Sep 30, 2024, pp. 235–260.

[2] Paulin H, "Payment card fraud in Finland: What are the most common types of fraud and how do consumers fall victim to fraud."

[3] Hyde R, Gibson JA, "Fraudscape: The size of the fraud problem around the world."

[4] Hayashi F, "Did Card-Present Fraud Rates Decline in the United States After the Migration to Chip Cards?," Payments System Research Briefing, 2025, pp. 1–8.

[5] Yuvarani R, Mahaveerakannan R, "Payment Security Expert: Analyzing Smart Cards and Contact-less Payments with Cryptographic Techniques," 2024 2nd International Conference on Sustainable Computing and Smart Systems (ICSCSS), Jul 10, 2024, pp. 511–516. IEEE.

[6] Watanabe K, Yoneyama K, "Formal Verification of Challenge Flow in EMV 3-D Secure," Australasian Conference on Information Security and Privacy, Jul 15, 2024, pp. 290–310. Springer Nature Singapore.

[7] Mutemi A, Bacao F, "E-commerce Fraud Detection Based on Machine Learning Techniques: Systematic Literature Review," Big Data Mining and Analytics, Apr 22, 2024; 7(2):419–444.

[8] Bansal U, Bharatwal S, Bagiyam DS, Kismawadi ER, "Fraud Detection in the Era of AI: Harnessing Technology for a Safer Digital Economy," AI-Driven Decentralized Finance and the Future of Finance, 2024, pp. 139–160. IGI Global.

[9] Ilham B, Setiawan Y, "Implementation of High Availability Message ISO 8583 Using F5 Active-Passive Failover Method," arXiv preprint arXiv:2305.07452, Apr 27, 2023.

[10] Cuccia J, "Fraud in Banking: A Review of Fraud Scams, Effects, and Antifraud Techniques in the Banking Industry."

[11] Talukder MA, Khalid M, Uddin MA, "An Integrated Multistage Ensemble Machine Learning Model for Fraudulent Transaction Detection," Journal of Big Data, vol. 11, 168 (2024). https://doi.org/10.1186/s40537-024-00996-5.

[12] Husnaningtyas N, Dewayanto T., "Financial Fraud Detection and Machine Learning Algorithm (Unsupervised Learning): Systematic Literature Review," Jurnal Riset Akuntansi dan Bisnis Airlangga (JRABA), Nov 1, 2023; 8(2).

[13] Cholevas C, Angeli E, Sereti Z, Mavrikos E, Tsekouras GE., "Anomaly Detection in Blockchain Networks Using Unsupervised Learning: A Survey," Algorithms, May 9, 2024; 17(5):201.

[14] Hernandez Aros L, Bustamante Molano LX, Gutierrez-Portela F, Moreno Hernandez JJ, Rodríguez Barrero MS., "Financial Fraud Detection through the Application of Machine Learning Techniques: A Literature Review," Humanities and Social Sciences Communications, Sep 3, 2024; 11(1):1–22.

[15] Al-Hashedi KG, Magalingam P., "Financial Fraud Detection Applying Data Mining Techniques: A Comprehensive Review from 2009 to 2019," Computer Science Review, May 1, 2021; 40:100402.

[16] AbdulHussein A, Cozzarin B, Dimitrov S., "Changes in Consumer Spending Behavior During the COVID-19 Pandemic Across Product Categories," Electronic Commerce Research, 24, 2267–2296 (2024). https://doi.org/10.1007/s10660-022-09618-9.

[17] Murthy NN, Mehtre BM, Rao KP, Ramam GS, Harigopal PK, Babu KS., "Technologies for E-commerce: An Overview," Informatica, Jan 20, 2001.

[18] Milne A, Parboteeah P., "Expert Opinion on Standards in Global Financial Markets," Apr 5, 2015.

[19] Adamson G., "IEEE and the Protection of Cyberspace: Increasing IEEE's Cybersecurity Role," White Paper, Nov 9, 2023, pp. 1–49.

[20] Bin Sulaiman R, Schetinin V, Sant P., "Review of Machine Learning Approach on Credit Card Fraud Detection," Human-Centric Intelligent Systems, Jun 2022; 2(1):55–68.

[21] Phua C, Lee V, Smith K, Gayler R., "A Comprehensive Survey of Data Mining-Based Fraud Detection Research," arXiv preprint arXiv:1009.6119, Sep 30, 2010.

[22] Teng H, Wang C, Yang Q, Chen X, Li R., "Leveraging Adversarial Augmentation on Imbalance Data for Online Trading Fraud Detection," IEEE Transactions on Computational Social Systems, Apr 2024; 11(2):1602–1614. https://doi.org/10.1109/TCSS.2023.3240968.

[23] Chatterjee P, Das D, Rawat DB., "Digital Twin for Credit Card Fraud Detection: Opportunities, Challenges, and Fraud Detection Advancements," Future Generation Computer Systems, Apr 30, 2024.

[24] Fahim M, Sillitti A., "Anomaly Detection, Analysis and Prediction Techniques in IoT Environment: A Systematic Literature Review," IEEE Access, Jun 10, 2019; 7:81664–81681.

[25] Ali A, Abd Razak S, Othman SH, Eisa TA, Al-Dhaqm A, Nasser M, Elhassan T, Elshafie H, Saif A., "Financial Fraud Detection Based on Machine Learning: A Systematic Literature Review," Applied Sciences, Sep 26, 2022; 12(19):9637.

[26] Hilal W, Gadsden SA, Yawney J., "Financial Fraud: A Review of Anomaly Detection Techniques and Recent Advances," Expert Systems with Applications, May 1, 2022; 193:116429.

[27] Aras MT, Guvensan MA., "A Multi-Modal Profiling Fraud-Detection System for Capturing Suspicious Airline Ticket Activities," Applied Sciences, 2023; 13:13121. https://doi.org/10.3390/app132413121.

[28] Ahmed AA, Alabi O., "Secure and Scalable Blockchain-Based Federated Learning for Cryptocurrency Fraud Detection: A Systematic Review," IEEE Access, Jul 16, 2024.

[29] Nicolini G, Leonelli L., "Financial Frauds on Payment Cards: The Role of Financial Literacy and Financial Education," International Review of Financial Consumers, 2021.

[30] Liu Q, Hagenmeyer V, Keller HB., "A Review of Rule Learning-Based Intrusion Detection Systems and Their Prospects in Smart Grids," IEEE Access, Apr 5, 2021; 9:57542–57564.

[31] Bello OA, Ogundipe A, Mohammed D, Adebola F, Alonge OA., "AI-Driven Approaches for Real-Time Fraud Detection in US Financial Transactions: Challenges and Opportunities," European Journal of Computer Science and Information Technology, 2023; 11(6):84–102.

[32] Mutemi A, Bacao F., "E-Commerce Fraud Detection Based on Machine Learning Techniques: Systematic Literature Review," Big Data Mining and Analytics, Apr 22, 2024; 7(2):419–444.

[33] Mienye ID, Jere N., "Deep Learning for Credit Card Fraud Detection: A Review of Algorithms, Challenges, and Solutions," IEEE Access, Jul 11, 2024.

[34] Adelakun BO, Onwubuariri ER, Adeniran GA, Ntiakoh A., "Enhancing Fraud Detection in Accounting through AI: Techniques and Case Studies," Finance & Accounting Research Journal, Jun 15, 2024; 6(6):978–999.

[35] Asha S, Shanmugapriya D., "Understanding Insiders in Cloud Adopted Organizations: A Survey on Taxonomies, Incident Analysis, Defensive Solutions, Challenges," Future Generation Computer Systems, Apr 25, 2024.

[36] Malik P, Anand A, Baliyan AK, Dongre A, Panwar P., "Credit Risk Assessment and Fraud Detection in Financial Transactions Using Machine Learning."

[37] Alamri M, Ykhlef M., "Survey of Credit Card Anomaly and Fraud Detection Using Sampling Techniques," Electronics, Dec 2, 2022; 11(23):4003.

[38] Maddireddy Br., "Neural Network Architectures In Cybersecurity: Optimizing Anomaly Detection And Prevention," International Journal Of Advanced Engineering Technologies And Innovations, Dec 24, 2024; 1(2):238–266.

[39] Ait Said Ma, Hajami A, Krari A. Behavioral Profiling For Card-Not-Present Fraud Detection Leveraging Iso8583 Data To Identify Anomalous Patterns. Journal Of Theoretical And Applied Information Technology. 2025 Mar 15;103(5).