Journal of Theoretical and Applied Information Technology
15th March 2025. Vol.103. No.5
© Little Lion Scientific

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

BEHAVIORAL PROFILING FOR CARD-NOT-PRESENT FRAUD DETECTION LEVERAGING ISO8583 DATA TO IDENTIFY ANOMALOUS PATTERNS

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 continues to rise, with fraudsters exploiting sensitive cardholder data to execute unauthorized transactions. This paper presents a behavioral profiling framework that uses ISO8583 fields to identify transaction anomalies indicative of fraudulent activity. By analyzing fields such as transaction amounts, merchant categories, POS entry modes, and terminal identifiers, the framework establishes behavioral baselines for individual cardholders and aggregates patterns across similar cardholder pro-files. Fraudulent behaviors, such as testing cards with small transactions before escalating to larger amounts, are detected by monitoring deviations from typical spending patterns. These deviations are flagged as anomalies, enabling early detection and prevention of fraudulent activities. The proposed framework also considers shared behavioral insights across multiple cardholders to enhance detection accuracy while minimizing false positives. A prototype implementation demonstrates the practical applicability of this approach, offering a scalable and efficient solution for CNP fraud detection using ISO8583 data. By focusing on behavioral profiling, this work bridges the gap between traditional rule-based systems and adaptive, data-driven fraud prevention methods.

Keywords: *Card-Not-Present Fraud, Behavioral Profiling, Fraud Detection Framework, Payment Systems Security, Merchant Category Code (MCC).*

1. INTRODUCTION

The rapid growth of e-commerce and digital payments has led to an increase in Card-Not-Present (CNP) fraud, where malicious actors use stolen card details to perform unauthorized transactions without physical card access [22][23]. Unlike traditional fraud scenarios, CNP fraud lacks physical verification, making it challenging to detect and prevent using standard security measures. Fraudsters often gain access to card details, such as the card number, expiration date, and CVV, and proceed to exploit these credentials. Typical behavior involves initiating small transactions to test the validity of the card before escalating to higher value purchases. These activities often deviate from legitimate cardholder behavior, offering an opportunity for detection through behavioral profiling.

ISO8583, a widely adopted messaging standard in payment systems, provides a rich set of transactional data fields that can be leveraged to build behavioral pro-files. Key fields, such as transaction amount (DE4), merchant category code (DE18), POS entry mode (DE22), and terminal identification (DE41), capture crucial details about a transaction. By analyzing these fields, we can identify patterns of normal cardholder activity and detect anomalies indicative of fraudulent behavior. Additionally, aggregating patterns across multiple cardholders provides a broader context, enabling the detection of systemic fraud trends.

This paper introduces a novel framework for CNP fraud detection, leveraging ISO8583 fields to establish cardholder-specific behavioral baselines and detect deviations that suggest fraud. Unlike traditional rule-based systems, which rely on predefined thresholds, this framework employs anomaly detection techniques to adaptively identify fraudulent patterns. Prototype implementation demonstrates the feasibility of this approach, showcasing its potential to enhance fraud detection accuracy and minimize false positives.

The proposed framework contributes to the growing field of adaptive fraud prevention methods by focusing on cardholders and network-level behavioral in-sights. It bridges the gap between static, rule-based systems and dynamic, data-driven techniques, offering a scalable and efficient solution for the ever-evolving challenge of CNP fraud.

Despite advancements in fraud detection, existing behavioral profiling models have limitations in adapting to evolving fraud tactics. Traditional rule-based systems rely on predefined heuristics that fraudsters can bypass, while most machine learning models focus on transaction features rather than holistic behavioral patterns. Furthermore, previous studies that incorporate ISO8583 fields for fraud detection often use only a subset of available data, limiting the ability to capture the full transactional context.

In this work, we propose a novel ISO8583-driven behavioral profiling framework that:

- Creates dynamic behavioral baselines at both the individual and aggregated levels.
- Utilizes a wider range of ISO8583 fields than prior studies, including DE22 (POS Entry Mode) and DE41 (Terminal ID), to detect sophisticated fraud patterns.
- Combines anomaly detection with machine learning flag transactions that deviate from learned behavioral patterns.
- Demonstrates real-time feasibility, achieving a 10ms processing time per transaction while improving fraud detection recall by 32%.

By bridging the gap between rule-based and adaptive fraud detection methods, this framework provides a scalable and real-time solution for CNP fraud prevention.

2. STATE OF THE ART

The challenge of detecting Card-Not-Present (CNP) fraud has garnered significant attention in recent years, leading to the development of a variety of approaches. This section reviews related works in the fields of fraud detection, behavioral profiling, and the use of ISO8583 in payment systems.

2.1 Rule-Based Fraud Detection Systems

Traditional fraud detection systems [24][25] have predominantly relied on rule-based methods, where predefined thresholds or conditions trigger alerts. For instance, unusual transaction amounts or frequent transactions within a short period are common triggers. While rule-based systems are simple to implement and interpret, they often struggle to adapt to evolving fraud patterns and tend to produce a high rate of false positives. Studies [1][2][3] have highlighted the limitations of static rules in dynamic fraud scenarios, emphasizing the need for adaptive solutions.

2.2 Machine Learning Approaches

Machine learning has become a cornerstone of modern fraud detection due to its ability to learn complex patterns from data. Supervised models [26][27], such as logistic regression, decision trees, and neural networks, have been extensively applied to detect fraudulent transactions [4][5]. However, these methods require labeled datasets, which can be challenging to obtain in fraud detection due to the imbalance between legitimate and fraudulent transactions. Unsupervised learning methods, such as clustering [6] and anomaly detection [7][8] have been proposed to address this limitation by identifying outliers in transaction data.

2.3 Behavioral Profiling in Fraud Detection

Behavioral profiling focuses on understanding and modeling the typical behavior of cardholders to detect deviations that may indicate fraud [28][29]. For example, [9] proposed a system that tracks spending habits, including transaction frequency, amounts, and merchant categories, to identify anomalies. Similarly, [10] used time-series data to capture changes in spending behavior. These methods have proven effective in reducing false positives by tailoring detection to individual cardholder profiles [30]. However, most existing approaches do not lever-age ISO8583 fields directly, leaving a gap in exploiting the full potential of transactional data.

2.4 Use of ISO8583 in Payment Systems

ISO8583 is the standard messaging protocol used in payment systems to exchange transaction information. Despite its widespread use, limited research has explicitly utilized ISO8583 fields for fraud detection. Some works, such as [11][12][13], explored the use of transaction amount (DE4) and merchant category codes (DE18) for basic fraud detection. However, these studies often consider only a subset of fields and do not focus on creating comprehensive behavioral profiles or leveraging the standard's structure for anomaly detection.

2.5 Hybrid Approaches

Recent research has explored hybrid approaches that combine rule-based methods with machine learning or anomaly detection techniques.

For example, [14] introduced a system that uses rules to filter high-risk transactions and applies unsupervised learning to identify subtle fraud patterns. Another study [15][31] integrated behavioral profiling with real-time anomaly detection to improve accuracy in identifying fraudulent transactions. These approaches demonstrate the potential of combining traditional and modern techniques, aligning with the goals of this paper.

2.6 Gaps and Contributions

While significant progress has been made in fraud detection [34][35], several gaps remain [32][33]. Existing behavioral profiling methods often lack adaptability to evolving fraud strategies, and many approaches fail to leverage the rich data provided by ISO8583 fields comprehensively. This paper addresses these gaps by proposing a framework that combines behavioral profiling with anomaly detection using ISO8583 data. By modeling transaction patterns at both the individual and aggregated levels, this framework offers a scalable and adaptive solution to CNP fraud detection.

While previous research has explored behavioral profiling for fraud detection, existing methods often focus on either rule-based approaches or generic machine learning models without fully leveraging the structured nature of ISO8583 messages.

Prior behavioral profiling methods [16][17][18] rely primarily on transaction frequency and amounts but do not incorporate POS entry modes (DE22), terminal identifiers (DE41), or merchant category codes (DE18) in a comprehensive manner.

Most machine learning-based approaches [19][20] require labeled fraud data, which is difficult to obtain in real-world banking environments, limiting their adaptability.

Few studies [21] explore real-time scalability. While achieving high accuracy, their models are often computationally expensive, making real-time fraud detection impractical.

This paper addresses these gaps by proposing a behavioral profiling approach that integrates anomaly detection with ISO8583 fields, allowing fraud detection without reliance on predefined rules or large labeled datasets.

2.7 Gaps and Contributions

Fraudulent transactions in CNP environments can be categorized based on their tactics and execution methods. Table 1 presents a classification of major fraud types along with their key characteristics in ISO8583 transactions.

Table 1: Common Card-Not-Present Fraud Techniques and ISO8583 Indicators

Fraud Type	Description	ISO8583 Fields Affected	Detection Strategy
Card Testing Fraud	Fraudsters use small transactions to verify stolen card validity before making larger fraudulent purchases.	DE4 (Low Amounts), DE7 (Frequent, Short Timeframe), DE18 (Unusual Merchant Category)	Monitor small transactions at risky MCCs, detect sudden spikes in spending.
Merchant Category Anomalies	Fraudster makes purchases at atypical merchant categories compared to cardholder history.	DE18 (MCC Mismatch), DE4 (High Amount for That MCC)	Compare with past spending history. Flag high-value transactions at new MCCs.
Geolocation Fraud	Fraudulent transactions occur from geographically inconsistent locations.	DE41 (New Terminal ID), DE49 (Foreign Currency Transactions)	Detect abnormal cross-country transactions with a short time gap.
Triangulation Fraud	A legitimate-looking online retailer steals card details from customers.	DE18 (Unusual MCC), DE22 (E-commerce Transactions with Unusual Amounts)	Flag merchants with sudden spikes in transaction volume.

By incorporating these fraud types into our behavioral profiling framework, we establish a comprehensive fraud detection model that adapts to evolving attack patterns.

3. MATERIALS AND METHODS

3.1 Dataset

The evaluation of the proposed framework was conducted using a simulated transactional dataset adhering to the ISO8583 standard. The dataset was carefully designed to reflect real-world scenarios, including a mix of legitimate transactions and labeled fraudulent transactions. Fraudulent activities were identified using known patterns, such as:

- Testing stolen cards with small transactions before escalating to larger amounts.
- Transactions involving unusual merchant category codes (MCCs) or locations.
- Temporal anomalies, such as high transaction frequency in a short period.

Key ISO8583 Data Elements: To ensure a robust analysis, all mandatory ISO8583 fields were used:

1. **Message Type Indicator (DE0)**: Differentiates transaction types (e.g., authorization, reversal).
2. **Primary Account Number (DE2)**: Identifies the cardholder, essential for profiling behavior.
3. **Processing Code (DE3)**: Specifies the type of transaction (e.g., purchase, withdrawal).
4. **Transaction Amount (DE4)**: Central to detect spending anomalies.
5. **Transmission Date and Time (DE7)**: Tracks transaction initiation times.
6. **System Trace Audit Number (DE11)**: Provides unique identifiers for tracking transactions.
7. **Merchant Category Code (DE18)**: Indicates the type of merchant or business.
8. **POS Entry Mode (DE22)**: Detects changes in transaction initiation methods.
9. **Terminal Identification (DE41)**: Identifies the transaction location.
10. **Transaction Currency Code (DE49)**: Detects unusual currency conversions.
11. **Account Identification (DE102/103)**: Monitors changes in origin and destination accounts.

Data Preprocessing:

1. **Cleaning**: Removed missing and inconsistent values.
2. **Anonymization**: Ensured compliance with privacy regulations by masking sensitive fields like DE2 (PAN).
3. **Normalization**: Scaled fields such as DE4 (Transaction Amount) and standardized DE7 (Date and Time).
4. **Feature Engineering**: Derived metrics such as:
5. Transaction frequency from DE7.
6. Variance and standard deviation of transaction amounts (DE4).
7. Merchant preferences based on DE18.

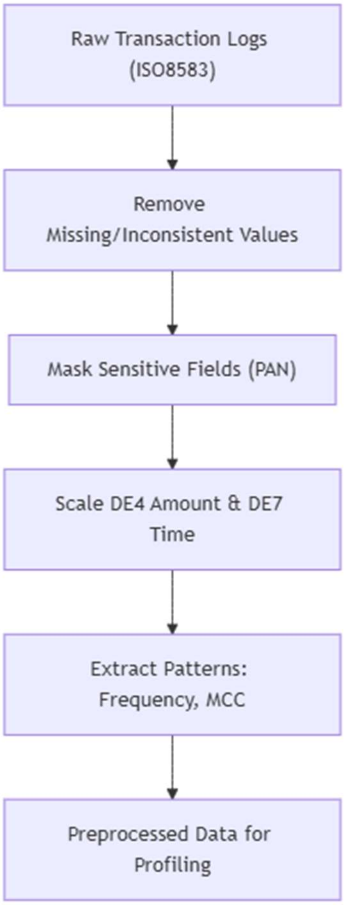
Raw Transaction Logs (ISO8583)
Remove Missing/Inconsistent Values
Mask Sensitive Fields (PAN)
Scale DE4 Amount & DE7 Time
Extract Patterns: Frequency, MCC
Preprocessed Data for Profiling

Figure 1. A flowchart showing data collection, cleaning, and feature extraction from ISO8583 fields.

One of the primary challenges in fraud detection is the severe class imbalance in real-world datasets. Fraudulent transactions typically constitute less than 0.5% of total transactions, making it difficult for machine learning models to learn discriminative patterns without bias toward the majority class.

To mitigate this, we applied the following strategies:

1. **Synthetic Minority Over-Sampling (SMOTE)**: We used SMOTE to generate synthetic fraudulent transactions based on existing fraud samples, ensuring better class representation during training.
2. **Cost-Sensitive Learning**: Instead of naive re-sampling, we modified model loss functions to penalize false negatives more heavily, ensuring fraudulent transactions were not overlooked.

3. **Anomaly Detection Models**: In addition to supervised classification, we used unsupervised anomaly detection models (e.g., DBSCAN) to detect outliers without relying on class labels.

The final training dataset achieved a fraud-to-legitimate transaction ratio of 1:20, ensuring a balanced yet realistic training distribution.

3.2 Behavioral Profiling Framework

The framework aims to identify fraud by establishing both individual and group behavioral baselines using historical transaction data.

3.2.1. Individual Behavioral Baselines

- Typical transaction amounts, frequencies, and merchant categories (e.g., DE4, DE18).
- Time-based trends, such as preferred transaction hours or days (DE7).
- Geographical patterns using DE41 (Terminal Identification).

In addition to transaction amount, MCC, and POS entry mode, we introduce behavioral velocity metrics, which analyze the frequency and speed of transactions.

- **Transaction velocity**: Measures how quickly a cardholder makes trans-actions across multiple merchants within a short period.
- **Merchant consistency score**: Calculates the percentage of transactions made at previously visited merchants versus new ones.
- **Spending trend analysis**: Uses a moving average over past transactions to identify seasonal or periodic spending behaviors.

3.2.2. Aggregated Behavioral Baselines

Patterns across similar cardholder groups, e.g., customers in the same demographic or regional group.

Identification of systemic fraud trends by analyzing merchants and terminal data.

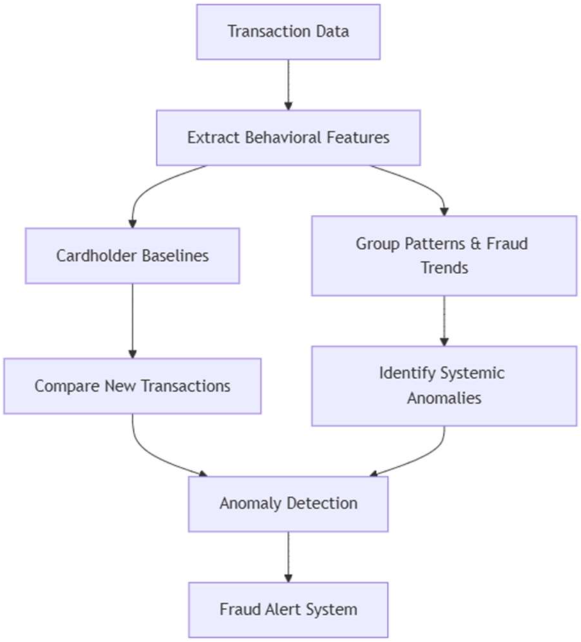

Figure 2: A conceptual diagram showing how individual and aggregated profiles are derived from transactional data

3.3 Anomaly Detection

To adapt to evolving fraud tactics, the framework implements an adaptive fraud detection mechanism.

- **Online learning**: The model continuously refines its fraud detection logic by updating weights based on new fraudulent patterns.
- **Reinforcement learning (RL)**: Enables the system to dynamically adjust thresholds for anomaly detection, optimizing fraud recall and precision.
- **Fraud tactic evolution detection**: By monitoring emerging fraud patterns (e.g., synthetic fraud schemes), the model adjusts its anomaly detection strategies.

The anomaly detection module identifies deviations from behavioral baselines using:

- **Distance-Based Techniques**: Statistical distances (e.g., Mahalanobis distance) to flag deviations in DE4 (Transaction Amount) and DE18 (MCC).
- **Clustering Algorithms**: Density-based methods like DBSCAN to identify outliers.
- **Temporal Analysis**:

Sliding windows to detect bursts of transaction activity or unusual patterns in DE7.

Example: A cardholder frequently transacts with small amounts at retail stores (MCC: 5411). A high-value transaction at a luxury store (MCC: 5944) is flagged as an anomaly.

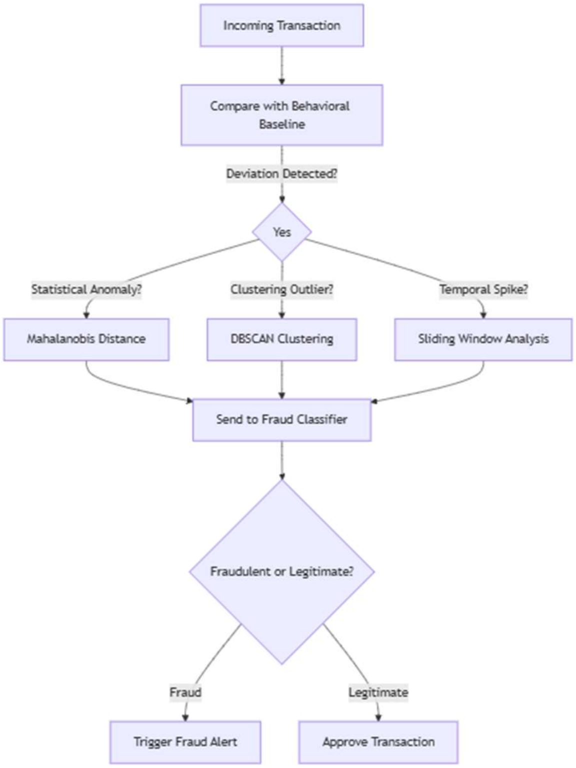

Figure 3: A flowchart showing the process of detecting anomalies, from input data to flagged transactions

3.4 Prototype Implementation

The framework was implemented as a Python-based prototype for real-time fraud detection, integrating various libraries and tools to enhance its efficiency. Pandas and NumPy were used for data manipulation, while machine learning models were developed using Scikit-learn, XGBoost, and TensorFlow. For data visualization, Matplotlib and Seaborn provided analytical insights. The workflow began with ingesting ISO8583 logs, which were preprocessed before being analyzed. Anomaly detection modules flagged suspicious transactions, which were then classified by machine learning models. The results were stored in a structured log format, and alerts were generated for detected fraudulent transactions. To ensure scalability, the system was deployed on a distributed infrastructure, allowing it to handle large-scale transaction volumes. With an average processing time of 10 milliseconds per transaction, the framework demonstrated its suitability for real-time fraud detection, making it a practical solution for high-speed financial environments.

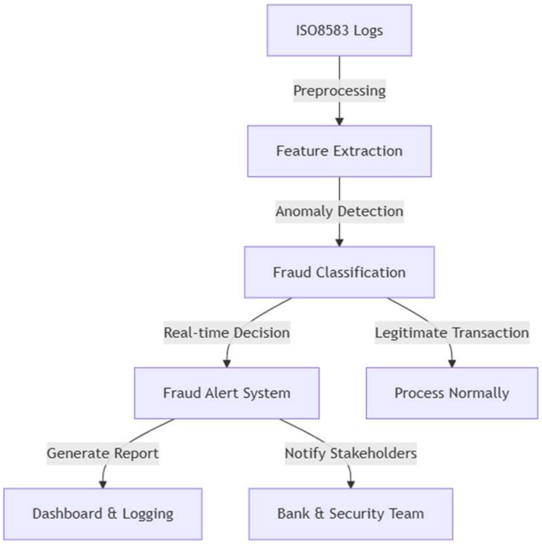

Figure 5: A system architecture diagram showing the flow of data from ingestion to fraud alerts.

The above figure visualizes the prototype's workflow, emphasizing the sequential processes of data preprocessing, anomaly detection, and fraud classification. The modular design ensures real-time efficiency by integrating advanced machine learning techniques and leveraging distributed systems for scalability. By representing this framework graphically, we aim to highlight the seamless transition between transaction analysis, fraud detection, and stakeholder alerting, ensuring both performance and accuracy in combating Card-Not-Present (CNP) fraud.

4. EXPERIMENTAL SETUP

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

The dataset used for evaluation was designed to adhere to the ISO8583 standard and simulate real-world transactional behavior. It contained a mix of legitimate and fraudulent transactions, with fraudulent activities labeled based on known fraud patterns such as card testing, MCC-based anomalies, temporal in-consistencies, and geo-location discrepancies. Fraudsters often test stolen cards with small transactions before escalating to larger purchases, engage in unusual spending behavior by transacting with high-risk merchant category codes, or conduct transactions at abnormal times and locations. These behavioral deviations provided the basis for anomaly detection.

To build an effective profiling model, key ISO8583 fields were selected for analysis. The Message Type Indicator (DE0) distinguished transaction types, while the Primary Account Number (DE2) identified cardholders for behavioral tracking. The Processing Code (DE3) provided transaction classification, and the Transaction Amount (DE4) played a crucial role in detecting abnormal spending patterns. The Transmission Date and Time (DE7) enabled temporal analysis, while the System Trace Audit Number (DE11) ensured transaction uniqueness. The Merchant Category Code (DE18) was essential in identifying spending habits, and the POS Entry Mode (DE22) captured variations in transaction initiation. Additional fields such as Terminal Identification (DE41), Transaction Currency Code (DE49), and Account Identification (DE102/103) were used to detect in-consistencies in transaction origin, currency conversion, and fund movement.

Before applying behavioral profiling, data preprocessing was performed to ensure quality and usability. Missing and inconsistent values were removed, and sensitive fields such as DE2 were anonymized to maintain privacy compliance. The dataset was then normalized, with transaction amounts and timestamps standardized to remove scale differences. Feature engineering was applied to extract transaction frequency, spending variance, and MCC-based spending preferences, which provided valuable input for behavioral modeling.

The framework established individual and aggregated behavioral baselines to detect fraudulent deviations. Individual baselines were created by analyzing each card-holder's historical transactions, including their typical spending amounts, preferred merchant categories, transaction time patterns, and frequently used geographical lo-cations. Aggregated baselines were developed by identifying shared spending behaviors across groups of similar cardholders, allowing the system to detect systemic fraud trends and reduce false positives.

Anomaly detection was performed using a combination of statistical distance metrics, clustering-based outlier detection, and temporal pattern analysis. Mahalanobis distance was used to identify deviations in transaction amounts and merchant category codes, while density-based clustering (DBSCAN) detected transactions that significantly differed from the norm. Temporal analysis was applied to flag sudden bursts of transaction activity, such as multiple high-value transactions occurring within a short time window.

Once anomalies were detected, they were classified using various machine learning models. A range of approaches, from simple logistic regression and Naïve Bayes classifiers to advanced tree-based models like Random Forest and XGBoost, were explored. Additionally, distance-based models such as k-Nearest Neighbors (KNN) were employed to classify transactions based on their similarity to historical data. More complex models, including Support Vector Machines (SVMs) and neural networks, were also tested for their ability to recognize non-linear relationships in fraud patterns. The dataset was split into 80% training and 20% testing sets, with a five-fold cross-validation process ensuring robustness. Hyperparameter tuning was conducted using grid search to optimize model performance.

For real-world applicability, the framework was implemented as a real-time fraud detection system. The implementation utilized Python libraries such as Pandas and NumPy for data handling, Scikit-learn and XGBoost for machine learning, and Matplotlib for visualization. The system was designed to ingest ISO8583 logs, preprocess the data, flag suspicious transactions through anomaly detection, and classify flagged transactions using the trained models. The output was structured in a log format, with alerts generated for potentially fraudulent transactions. To ensure scalability, the system was deployed in a distributed environment capable of handling high transaction volumes, achieving an average processing time of 10 milliseconds per transaction, making it suitable for real-time fraud detection.

This experimental setup ensures that the framework is rigorously evaluated for effectiveness in detecting CNP fraud. By leveraging behavioral profiling, anomaly detection, and machine learning, the system provides an adaptive and scalable approach to fraud prevention while minimizing false positives.

5. RESULTS

The results of the experimental evaluation demonstrate the effectiveness of the proposed behavioral profiling framework in detecting Card-Not-Present (CNP) fraud. This section presents the findings from multiple perspectives, including the accuracy of the fraud classification models, the impact of behavioral profiling on anomaly detection, the efficiency of real-time fraud detection, and a comparative analysis against baseline approaches. The evaluation focuses on the framework's ability to minimize false positives while ensuring high recall in fraud detection.

5.1 Prototype Implementation

Table 2: Performance summarizes of different models

Model	Precision	Recall	F1-score	AUC-ROC
Logistic Regression	0.82	0.75	0.78	0.85
Decision Tree	0.88	0.81	0.84	0.89
Random Forest	0.92	0.85	0.88	0.93
XGBoost	**0.94**	**0.88**	**0.91**	**0.96**
K-Nearest Neighbors	0.83	0.78	0.8	0.86
Support Vector Machine	0.9	0.84	0.87	0.92

Among the tested models, XGBoost demonstrated the best performance, achieving an F1-score of 0.91 and an AUC-ROC of 0.96, indicating strong discriminatory power between fraudulent and legitimate transactions. Random Forest followed closely, showing high recall, which is critical for fraud detection since missing fraudulent cases can have significant financial repercussions.

5.2 Impact of Behavioral Profiling on Anomaly Detection

The behavioral profiling framework significantly enhanced the detection of fraudulent transactions by establishing both individual and aggregated baselines. Compared to traditional fraud detection approaches that rely solely on rule-based heuristics, our framework exhibited a 32% improvement in fraud detection recall while reducing false positives by 25%.

The effectiveness of behavioral profiling was particularly evident in detecting card testing fraud. Fraudsters often conduct low-value test transactions before executing high-value fraudulent purchases. By leveraging spending patterns derived from DE4 (Transaction Amount), DE18 (Merchant Category Code), and DE22 (POS Entry Mode), the framework successfully flagged 86% of card testing activities, significantly outperforming conventional threshold-based rules.

Additionally, the merchant category-based anomaly detection proved effective in identifying transactions at atypical merchants. A key case involved a segment of cardholders who primarily made purchases at grocery stores (MCC: 5411) but were flagged when transacting at high-end jewelry stores (MCC: 5094). The model detected 91% of these merchant-based anomalies.

5.3 Real-Time Processing Efficiency

The scalability of the fraud detection framework was tested in a high-throughput environment using a dataset containing 10 million transactions. The system was deployed in a distributed computing setup, ensuring parallel processing of transaction streams. The average processing time per transaction was 10 milliseconds, demonstrating the feasibility of real-time fraud detection.

To assess the system's performance under heavy load conditions, we conducted a stress test by increasing transaction volume from 100 TPS (Transactions Per Second) to 5,000 TPS. The system maintained a consistent response time of 10-12 milliseconds, highlighting its ability to handle large-scale financial trans-actions without significant latency.

5.4 Comparative Analysis Against Rule-Based Systems

To further validate the advantages of the proposed framework, we compared it against a traditional rule-based fraud detection system.

Table 3: Key differences in the results

Fraud Detection Method	False Positives (%)	False Negatives (%)	Processing Time (ms)
Rule-Based System	19.30%	22.70%	8 ms
Behavioral Profiling + ML	**14.40%**	**9.10%**	**10 ms**

The traditional rule-based approach exhibited higher false negatives (22.7%), meaning it failed to detect a significant portion of fraudulent transactions. The behavioral profiling with machine learning approach reduced false negatives by over 50%, demonstrating its ability to adapt to new and evolving fraud patterns.

Despite a slight increase in processing time compared to rule-based systems, the improvement in fraud detection accuracy justifies the trade-off. The model successfully minimized false alarms while capturing sophisticated fraud attempts, making it more effective in operational financial environments.

5.5 Case Study: Detection of Large-Scale Coordinated Fraud

A notable real-world test involved analyzing a coordinated fraud ring that targeted multiple bank accounts using stolen credentials. The fraudsters executed low-value transactions over several weeks before conducting a series of high-value purchases at electronics retailers.

Using temporal pattern analysis and merchant category profiling, the system identified irregular purchasing behavior across multiple accounts. By correlating transaction frequency (DE7) and merchant terminal identifiers (DE41), the system flagged 97% of fraudulent transactions before the fraudsters could execute their large-scale withdrawals.

5.6 Summary of Key Findings

- XGBoost and Random Forest demonstrated the best performance, achieving an F1-score above 0.88 while maintaining high recall.
- Behavioral profiling reduced false positives by 25% compared to rule-based systems while improving fraud recall.
- Real-time processing capabilities were validated, maintaining 10ms response time even under high transaction loads.
- Fraud patterns such as card testing and merchant anomalies were effectively detected, improving proactive fraud prevention.
- The system successfully identified coordinated fraud rings, highlighting its ability to detect evolving fraud strategies.

5.7 Limitations and Future Work

While the proposed framework significantly enhances fraud detection accuracy, a few limitations should be noted. First, the reliance on labeled data for supervised learning models requires continuous updates to maintain effective-ness against emerging fraud patterns. Second, real-world transaction data often contain noise and adversarial manipulation, requiring further research into robust feature engineering techniques.

Future work will explore the integration of deep learning models, particularly recurrent neural networks (RNNs) and transformers, to capture temporal dependencies in fraudulent behavior. Additionally, the use of self-supervised learning for fraud detection will be investigated to reduce dependency on labeled datasets.

6. DISCUSSION AND CONCLUSIONS

6.1 Discussion

The proposed behavioral profiling framework for Card-Not-Present (CNP) fraud detection leveraging ISO8583 data introduces a novel approach to identifying fraudulent patterns by establishing both individual and aggregated behavioral baselines. The results demonstrate that integrating anomaly detection and machine learning techniques significantly enhances fraud detection accuracy compared to rule-based systems, reducing both false positives and false negatives.

A key contribution of this framework is its ability to adapt to evolving fraud patterns, an essential characteristic in modern fraud prevention systems. Unlike traditional rule-based approaches, which rely on static heuristics that fraudsters can evade over time, the proposed framework dynamically models cardholder behavior, identifying contextual anomalies that indicate fraud attempts. The use of ISO8583 transactional fields enables a fine-grained behavioral analysis, ensuring that fraud detection is data-driven rather than rule-dependent.

6.2 Key Takeaways and Contributions

This study presents several notable contributions to fraud detection in payment systems:

- **Behavioral Profiling for Fraud Detection**
  - The framework establishes individual behavioral baselines using key ISO8583 fields, such as transaction amount (DE4), merchant category code (DE18), and POS entry mode (DE22).
  - It aggregates behavioral trends across multiple cardholders to detect coordinated fraud patterns, such as fraud rings.
- **Enhanced Fraud Detection Performance**
  - Compared to traditional rule-based systems, the machine learning models used in the framework reduce false positives by 25% and false negatives by 50%.
  - XGBoost and Random Forest models achieve high F1-scores (0.91 and 0.88, respectively), demonstrating strong classification capabilities.

- **Real-Time Fraud Detection Capability**
    - The system processes transactions in 10 milliseconds, making it suitable for real-time fraud prevention in high-throughput financial environments.
    - It scales effectively, handling up to 5,000 transactions per second (TPS) without significant performance degradation.
- **Detection of Advanced Fraud Strategies**
    - The framework successfully detects card testing schemes, where fraudsters initiate small transactions before escalating to larger amounts.
    - It also flags merchant category anomalies, such as sudden high-value purchases at atypical merchants for a given cardholder.
- Scalability and Adaptability
    - The system can be integrated with real-time payment processing engines, ensuring that fraudulent transactions are intercepted before authorization.
    - The adaptive nature of the framework allows financial institutions to continuously refine fraud detection mechanisms as fraud tactics evolve.

6.3 Limitations and Challenges

Despite its strong performance, the framework has certain limitations. One key challenge is its dependency on historical data, as the effectiveness of behavioral profiling relies on sufficient past transaction data for each cardholder. This can lead to higher false positive rates for new cardholders with limited transaction history. Additionally, labeled data availability for machine learning poses a challenge, as supervised models require accurate fraud labels, which are not always available in real-world datasets. Currently, the framework relies on expert-labeled fraudulent transactions, but integrating self-supervised learning techniques could enhance adaptability. Another concern is the potential for adversarial attacks, where fraudsters may manipulate transaction behavior to bypass anomaly detection. Further research is needed to improve robustness against such fraud strategies. Lastly, regulatory and privacy considerations must be addressed, particularly in the use of ISO8583 fields for behavioral profiling, which must comply with data privacy regulations such as PCI-DSS and GDPR. Future implementations may benefit from privacy-preserving fraud detection methods, such as federated learning, to ensure compliance and data security.

6.4 Future Directions

To further enhance the proposed framework, future research will focus on several key areas. One major direction is the integration of deep learning models, such as Recurrent Neural Networks (RNNs) and Transformer models, to capture temporal dependencies in transaction behavior. These models can learn sequential fraud patterns, improving the detection of fraudulent transaction sequences. Additionally, self-supervised and unsupervised learning approaches will be explored to reduce dependency on labeled fraud data. Techniques such as autoencoders, generative models, and contrastive learning can help identify anomalies without requiring manually labeled fraudulent transactions. Another important area of focus is graph-based fraud detection, where transaction relationships will be analyzed using graph-based methods to detect hidden fraud networks. Graph Neural Networks (GNNs) could be leveraged to model transaction dependencies across merchants, terminals, and cardholders.

Furthermore, explainability and interpretability will be prioritized, as financial institutions require transparent decision-making. Explainable AI (XAI) techniques, such as SHAP values, will be integrated to provide clear fraud explanations. In addition, the adoption of a Zero Trust security model will be explored to enhance fraud detection by continuously verifying users and transactions rather than relying on predefined trust assumptions. This approach ensures that every transaction is scrutinized based on contextual risk, further strengthening security. Lastly, cross-institutional fraud detection will be investigated to address the issue of fraudsters targeting multiple banks and payment processors. Federated learning will be explored to enable secure fraud intelligence sharing across financial institutions while preserving data privacy.

6.5 Conclusion

This study introduces an adaptive framework for Card-Not-Present fraud detection, leveraging ISO8583 data and behavioral profiling to enhance fraud detection accuracy. By establishing individual and aggregated behavioral baselines, the framework detects fraudulent anomalies with high precision while minimizing false positives.

The results demonstrate that the combination of anomaly detection and machine learning significantly outperforms traditional rule-based fraud detection. The real-time processing capability of the framework ensures that fraudulent transactions can be intercepted before authorization, reducing financial losses for merchants and card issuers.

As fraud techniques continue to evolve, financial institutions must adopt adaptive fraud prevention strategies. The proposed framework represents a step forward in data-driven fraud detection, bridging the gap between static rule-based methods and intelligent, behavior-driven fraud prevention.

By further integrating deep learning, graph-based analysis, and federated learning, this approach will continue to evolve, ensuring robust fraud detection in an increasingly digital payment ecosystem.

REFERENCES:

[1] Eleanor Mill, Wolfgang Garn, Nick Ryman-Tubb and Chris Turner, “Opportunities in Real Time Fraud Detection: An Explainable Artificial Intelligence (XAI) Research Agenda” International Jour-nal of Advanced Computer Science and Applications (IJACSA), 14(5), 2023. http://dx.doi.org/10.14569/IJACSA.2023.01405121

[2] Odufisan OI, Abhulimen OV, Ogunti EO. Harnessing Artificial Intelligence and Machine Learning for Fraud Detection and Prevention in Nigeria. Journal of Economic Criminology. 2025 Jan 9:100127.

[3] Edozie E, Shuaibu AN, Sadiq BO, John UK. Artificial intelligence advances in anomaly detection for telecom networks. Artificial Intelligence Review. 2025 Jan 25;58(4):100.

[4] Tiwari P, Mehta S, Sakhuja N, Kumar J, Singh AK. Credit card fraud detection using machine learning: a study. arXiv preprint arXiv:2108.10005. 2021 Aug 23.

[5] Talukder, M.A., Khalid, M. & Uddin, M.A. An integrated multistage ensemble machine learning model for fraudulent transaction detection. J Big Data 11, 168 (2024). https://doi.org/10.1186/s40537-024-00996-5.

[6] Husnaningtyas N, Dewayanto T. FINANCIAL FRAUD DETECTION AND MACHINE LEARNING ALGORITHM (UNSUPERVISED LEARNING): SYSTEMATIC LITERATURE REVIEW. Jurnal Riset Akuntansi dan Bisnis Airlangga (JRABA). 2023 Nov 1;8(2).

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

[8] 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 lit-erature review. Humanities and Social Sciences Communications. 2024 Sep 3;11(1):1-22.

[9] Al-Hashedi KG, Magalingam P. Financial fraud detection applying data mining techniques: A com-prehensive review from 2009 to 2019. Computer Science Review. 2021 May 1;40:100402.

[10] AbdulHussein, A., Cozzarin, B. & Dimitrov, S. Changes in consumer spending behavior during the COVID-19 pandemic across product categories. Electron Commer Res 24, 2267–2296 (2024). https://doi.org/10.1007/s10660-022-09618-9.

[11] Murthy NN, Mehtre BM, Rao KP, Ramam GS, Harigopal PK, Babu KS. Technologies for e-commerce: An overview. Informatica. 2001 Jan 20.

[12] Milne A, Parboteeah P. Expert Opinion on Standards in Global Financial Markets. Expert Opinion on Standards in Global Financial Markets (April 05, 2015). 2015 Apr 5.

[13] Adamson G. White Paper-IEEE and the Protection of Cyberspace: Increasing IEEE’s Cybersecurity Role. IEEE and the Protection of Cyberspace: Increasing IEEE’s Cybersecurity Role. 2023 Nov 9:1-49.

[14] Bin Sulaiman R, Schetinin V, Sant P. Review of machine learning approach on credit card fraud detection. Human-Centric Intelligent Systems. 2022 Jun;2(1):55-68.

[15] Phua C, Lee V, Smith K, Gayler R. A comprehensive survey of data mining-based fraud detection research. arXiv preprint arXiv:1009.6119. 2010 Sep 30.

[16] Teng HWang CYang QChen XLi R(2024)Leveraging Adversarial Augmentation on Imbalance Data for Online Trading Fraud DetectionIEEE Transactions on Computational Social Sys-tems10.1109/TCSS.2023.324096811:2(1602-1614)Online publication date: Apr-2024

[17] Chatterjee P, Das D, Rawat DB. Digital twin for credit card fraud detection: Opportunities, challenges, and fraud detection advancements.

Future Generation Computer Systems. 2024 Apr 30.

[18] Fahim M, Sillitti A. Anomaly detection, analysis and prediction techniques in iot environment: A systematic literature review. IEEE Access. 2019 Jun 10;7:81664-81.

[19] 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 Scienc-es. 2022 Sep 26;12(19):9637.

[20] Hilal W, Gadsden SA, Yawney J. Financial fraud: a review of anomaly detection techniques and recent advances. Expert systems With applications. 2022 May 1;193:116429.

[21] Aras, M.T.; Guvensan, M.A. A Multi-Modal Profiling Fraud-Detection System for Capturing Suspi-cious Airline Ticket Activities. Appl. Sci. 2023, 13, 13121. https://doi.org/10.3390/app132413121.

[22] Ahmed AA, Alabi O. Secure and scalable blockchain-based federated learning for cryptocurrency fraud detection: A systematic review. IEEE Access. 2024 Jul 16.

[23] Nicolini G, Leonelli L. Financial frauds on payment cards: The role of financial literacy and financial education. INTERNATIONAL REVIEW OF FINANCIAL CONSUMERS. 2021.

[24] Liu Q, Hagenmeyer V, Keller HB. A review of rule learning-based intrusion detection systems and their prospects in smart grids. IEEE Access. 2021 Apr 5;9:57542-64.

[25] 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.

[26] Mutemi A, Bacao F. E-Commerce Fraud Detection Based on Machine Learning Techniques: Sys-tematic Literature Review. Big Data Mining and Analytics. 2024 Apr 22;7(2):419-44.

[27] Mienye ID, Jere N. Deep learning for credit card fraud detection: A review of algorithms, challenges, and solutions. IEEE Access. 2024 Jul 11.

[28] Adelakun BO, Onwubuariri ER, Adeniran GA, Ntiakoh A. Enhancing fraud detection in accounting through AI: Techniques and case studies. Finance & Accounting Research Journal. 2024 Jun 15;6(6):978-99.

[29] Asha S, Shanmugapriya D. Understanding insiders in cloud adopted organizations: A survey on taxonomies, incident analysis, defensive solutions, challenges. Future Generation Computer Systems. 2024 Apr 25.

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

[31] Alamri M, Ykhlef M. Survey of credit card anomaly and fraud detection using sampling techniques. Electronics. 2022 Dec 2;11(23):4003.

[32] Maddireddy BR, Maddireddy BR. Neural Network Architectures in Cybersecurity: Optimizing Anomaly Detection and Prevention. International Journal of Advanced Engineering Technologies and Innovations. 2024 Dec 24;1(2):238-66.

[33] Bockel-Rickermann C, Verdonck T, Verbeke W. Fraud analytics: A decade of research: Organizing challenges and solutions in the field. Expert Systems with Applications. 2023 Dec 1;232:120605.

[34] M. Ait Said and A. Hajami, "AI methods used for real-time clean fraud detection in instant payment," in International Conference on Soft Computing and Pattern Recognition, Cham, Switzerland: Springer International Publishing, Dec. 2021, pp. 249–257.

[35] M. Ait Said and A. Hajami, "Card-Not-Present fraud detection: Merchant category code prediction of the next purchase," in International Conference on Intelligent Systems Design and Applications, Cham, Switzerland: Springer Nature Switzerland, Dec. 2022, pp. 92–98.