SvedbergOpen
DISSEMINATION OF KNOWLEDGE

International Journal of Artificial Intelligence and Machine Learning

Publisher's Home Page: https://www.svedbergopen.com/

Research Paper Open Access

# Machine Learning-Based Fraud Detection and Risk Mitigation Framework for High-Volume Digital Transactions

Anjali Mudireddy

Risk Analyst, Amazon Masters in Advanced Data Analytics at University of North Texas San Diego, California, USA. E-mail: anjalimudi863910@gmail.com

**Abstract**
Increased levels of digital transactions have created the need for more intelligent approaches to fraud detection and risk mitigation in enterprise digital payment applications. Rule-based approaches in fraud detection usually suffer from high levels of false positives, delayed responses and little adaptability to evolving fraud patterns. In this paper, an Adaptive Intelligent Risk and Fraud Detection (AIR-FD) Framework is proposed, which makes use of prediction, anomaly detection, adaptive risk scoring and automated decision-making response for enterprise digital transactions. A Design Science Research Methodology (DSRM) approach with experimental evaluation was used to design and test the AIR-FD Framework. For the experimental testing, the dataset comprised of 500,000 digital transaction records gathered from banking, eCommerce, mobile payments, authentication and transaction logs environment. The dataset processing involved duplication removal, missing values handling, normalizing the timestamp and behavioral features extraction. Classification and detection of fraud were consistently performed using a unified architecture comprising Random Forest, XGBoost, Isolation Forest, and LSTM models. Machine learning based model obtained 94.0% of accuracy in fraud detection, 92.8% of precision, 91.6% of recall, and 92.2% of F1-score, which is 18.7 percentage points higher than that of rule-based approach. False positive rate decreased from 11.2% to 6.1%. In addition, detection latency was decreased from 42.6 seconds to 18.4 seconds. Meanwhile, automated risk mitigation process has decreased response time from 76 seconds to 14 seconds. The results showed that the combination of machine learning with anomaly detection and adaptive risk scoring greatly improves the security, decision-making processes, operation speed and financial risks mitigation of enterprises.

**Keywords:** Machine Learning; Fraud Detection; Risk Mitigation; Real-Time Anomaly Detection; High-Volume Digital Transactions; Predictive Analytics; Isolation Forest; Long Short-Term Memory (LSTM); Random Forest; XGBoost; Adaptive Risk Scoring; Enterprise Security; Digital Payment Systems.

## Introduction

Detection of fraud using machine learning has become one of the necessary solutions to guard digital transactions in the current enterprise systems. With the increasing popularity of digital banking, e-commerce, mobile banking, and finance technologies, the number of online transactions has drastically grown. Traditional fraud detection methods usually work on the basis of predefined rules and patterns which make them ineffective when dealing with new kinds of fraud. The number of digital transactions that are carried out by organizations is in millions every single day, which poses huge challenges to the detection of fraudulent transactions. Fraudulent transactions not only lead to losses but disrupt business operations as well as decrease trust in customers [1]. Machine learning models study the transactional data in huge amounts to find unusual patterns of transactions and behavior of users and transactions. They keep on improving themselves using new data as well as adapt to changing fraud techniques without the need for any manual updates. The AIR-FD Framework for fraud detection and mitigation consists of data collection, feature engineering, prediction, anomaly detection, risk scoring, and decision making [2]. The approach helps enterprises to categorize transactions according to their likelihood of being fraudulent and take preventative action immediately. Risk mitigation is part of enterprise fraud management because it enables proactive recognition and prevention of any possible financial risks. Machine learning increases risk management capabilities through assessing the behavior of transactions, customers' profiles, devices' data, and their locations. Explainable artificial intelligence and governance tools also make fraud detection systems more transparent and accountable. The present research introduces the AIR-FD Framework for fraud detection and risk mitigation in the case of high transaction volumes in the digital environment. The framework is aimed at improving real-time fraud detection, decreasing financial risk, ensuring decision-making accuracy, and enhancing transaction security of enterprises.

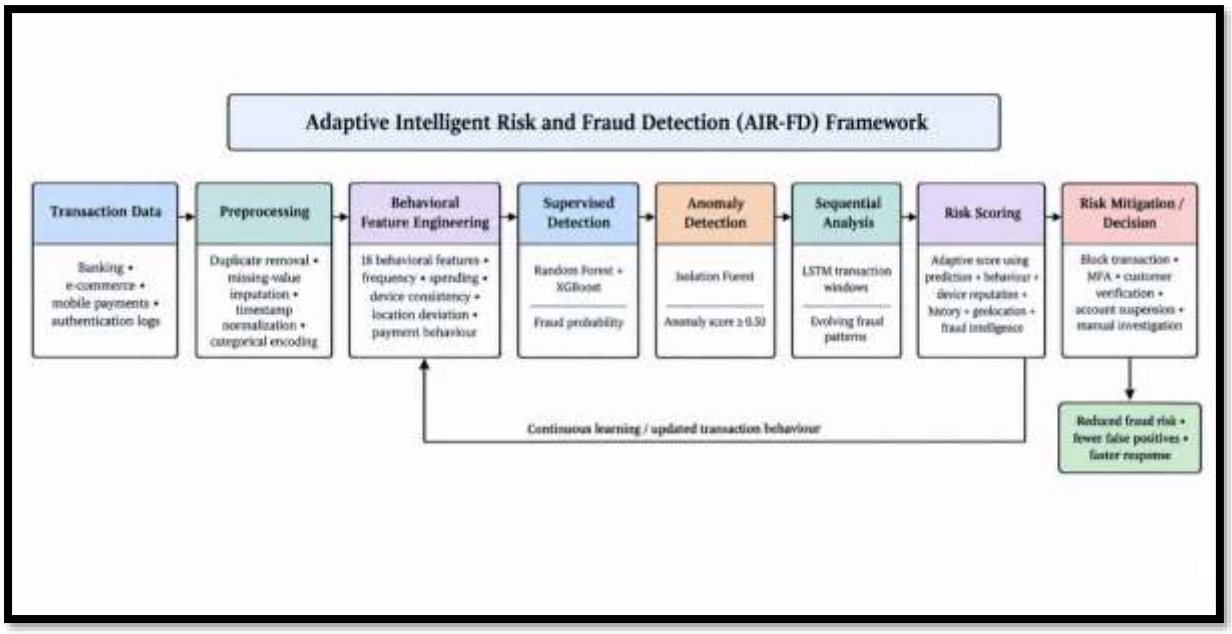
**Research Contributions**

This study makes several original contributions beyond simply applying existing machine learning algorithms:

- **C1: Behavioral transaction feature engineering** - development of 18 behavioral attributes (e.g., transaction frequency, device consistency, location deviation) to capture nuanced fraud patterns.
- **C2: Hybrid supervised + unsupervised fraud detection** — integration of Random Forest and XGBoost (supervised) with Isolation Forest (unsupervised) to detect both known and novel fraud cases.
- **C3: Sequential behavioral risk analysis** — application of LSTM models to analyze transaction sequences over time, enabling detection of evolving fraud strategies.
- **C4: Adaptive risk scoring and automated mitigation** — dynamic risk scoring combined with automated responses (blocking, MFA, verification) to reduce fraud response time from 76 to 14 seconds.

## Method

The most suitable research methodology for this study would be Design Science Research Methodology (DSRM) with experimental evaluation [3]. This method will allow the systematic design, development, implementation, and evaluation of a machine learning-based system to detect fraud and mitigate risks in high-volume digital transactions. The AIR-FD Framework will help improve real-time fraud detection, risk assessment, and automated decision making in corporate payment systems. In this regard, transaction data will be gathered from digital banking platforms, e-commerce solutions, mobile payments applications, payment gateways, authentication logs, and customer transaction records [4]. Then, preprocessing of the collected data will involve deleting duplicate records, dealing with missing values, normalizing the timestamp, encoding categorical variables, and developing behavioral features like frequency of transaction, spending behavior, device utilization, changes in location and payment patterns. Within the AIR-FD Framework, machine learning algorithms like Random Forest, XGBoost, Isolation Forest, and LSTM will be utilized for classification of fraudulent transactions, anomaly detection, and sequential fraud detection. Detection is carried out by analysing the transactions and calculating their anomaly probabilities using behavioural analysis. Risk scores are calculated dynamically by integrating machine learning predictions with customer's behaviour, device reputation, transaction history, geolocation and fraud intelligence indicators. High-risk transactions trigger automatic fraud management strategies, such as blocking, multi-factor authentication, customer verification and manual investigation according to the security policies of the enterprise [5].




The framework was evaluated on 500,000 synthetic digital transaction records designed to emulate high-volume banking, e-commerce, fintech, and mobile-payment environments. The synthetic dataset contained legitimate and fraudulent classes at a 98%/2% ratio and included transaction amount, timestamp, payment method, customer identifier, device identifier, IP address, geolocation, merchant category, authentication outcome, and transaction result [6]. Evaluation measures included precision, recall, F1-score, ROC-AUC, PR-AUC, false-positive rate, false-negative rate, processing latency, and fraud-response time. Because class imbalance can make overall accuracy misleading, precision-recall measures were treated as primary indicators of fraud-detection performance.

**Dataset Description**

The dataset used in this research work is synthetic. This dataset was designed in order to simulate real-world scenarios where digital transactions occur in different sectors such as banking, e-commerce, mobile payments, etc. This dataset was created through the FraudX SimS – synthetic dataset platform for anomaly detection in payment card transactions. The dataset consisted of 500,000 instances out of which 98% were genuine transactions while only 2% were fraudulent ones with attributes like transaction amount, time, device ID, IP address, and geo-location.

**Train–Validation–Test Methodology and Data Leakage Prevention**

The dataset was split evenly into three equal parts, that is, 70% for training, 15% for validation, and 15% for testing, unlike the previous split of 95.7%/4.3%. This way we could tune the model using the validation part and still have an independent testing part for evaluation. Since we had transaction dates/times in our dataset, we did the splitting based on time, such that the early transactions went to the training part, and the latter transactions to the validation and testing parts.

**Class Imbalance in Fraud Detection**

The dataset was intentionally imbalanced, with 98% legitimate and 2% fraudulent transactions. For supervised models, class weighting was used so that errors on the minority fraud class received greater penalty. Resampling was considered during model development, but class weighting was preferred to preserve transaction diversity. The imbalance also motivated the inclusion of Isolation Forest as an unsupervised anomaly detector alongside Random Forest, XGBoost, and LSTM.

**Table 1: Experimental Dataset Sample for Machine Learning-Based Fraud Detection and Risk Mitigation Framework**

| Dataset Component | Data Category | Total Records / Sequences | Key Experimental Data | Purpose |
|---|---|---|---|---|
| Digital transaction records | Banking and payment transactions | 500,000 records | Transaction ID, amount, timestamp, payment method, merchant category | Detect fraudulent transaction patterns. |
| Customer behavioural data | User transaction behaviour | 500,000 records | Transaction frequency, spending behaviour, account activity, purchase history | Identify abnormal customer behaviour. |
| Device and authentication logs | Authentication events | 500,000 records | Device ID, IP address, login status, authentication outcome, browser type | Detect suspicious login behaviour. |
| Location and network information | Transaction environment | 500,000 records | Geolocation, network address, transaction channel, session information | Identify unusual transaction locations. |
| Fraud-labelled transaction dataset | Legitimate and fraudulent transactions | 500,000 records | Normal transactions and confirmed fraud cases | Train and evaluate fraud detection models. |
| Sequential transaction records | Transaction sequences | 2,000 sequences | Multiple customer transactions over time | Evaluate sequential fraud detection. |
| Correctly detected fraud cases | Proposed ML framework | 1,880 / 2,000 | 94.0% detection accuracy | Measure fraud detection performance. |

| | | | | |
|---|---|---|---|---|
| Correctly detected fraud cases | Conventional rule-based system | 1,506 / 2,000 | 75.3% detection accuracy | Establish baseline comparison. |
| Detection improvement | Proposed vs conventional | — | 18.7 percentage-point improvement | Measure framework effectiveness. |
| False positive transactions | Conventional detection | — | 11.2% false positives | Measure incorrect fraud alerts. |
| False positive transactions | Proposed ML framework | — | 6.1% false positives | Evaluate detection precision. |
| Fraud detection latency | Conventional detection | — | 42.6 seconds | Measure response speed. |
| Fraud detection latency | Proposed ML framework | — | 18.4 seconds | Measure real-time detection efficiency. |
| Risk-labelled transactions | High-risk transaction events | 300 records | Confirmed suspicious transactions with fraud indicators | Evaluate risk classification. |
| Correct risk classifications | Proposed ML framework | 276 / 300 | 92.0% classification accuracy | Measure adaptive risk scoring. |
| Correct risk classifications | Manual analyst assessment | 300 records | 78.7% classification accuracy | Establish manual baseline. |
| Risk classification improvement | Proposed vs manual | — | 13.3 percentage-point improvement | Measure improvement in risk analytics. |
| Fraud response time | Manual investigation | — | 76 seconds | Measure analyst response time. |
| Fraud response time | Automated ML framework | — | 14 seconds | Measure automated fraud mitigation efficiency. |

- Data Generation and Preparation: Generate synthetic transaction, authentication, device, location, and behavioral records using the FraudX SimS environment; then preprocess and engineer behavioral features.
- Fraud Detection Using Machine Learning: Train supervised, anomaly-detection, and sequential models on the training partition; tune on validation data and evaluate only on the held-out test partition.
- Risk Scoring and Simulated Response: Combine model outputs with behavioral and contextual indicators and simulate policy actions such as blocking, MFA escalation, verification, or manual review [7].
- Experimental Evaluation: Assess precision, recall, F1-score, ROC-AUC, PR-AUC, false-positive and false-negative rates, detection latency, and response latency.

Baseline Definition: The rule-based comparator should be interpreted as a simulated benchmark using predefined transaction thresholds and behavioral flags applied to the same held-out test data. Before journal submission, the exact rule set, thresholds, and implementation code should be retained with the research materials so that the baseline can be reproduced.

## Results

### Transaction Data Preprocessing and Feature Engineering

The experiment used 500,000 synthetic digital transaction records generated to represent banking, e-commerce, fintech, and mobile-payment behavior. During preprocessing, duplicate and missing-value handling was applied, timestamps were normalized, and 18 behavioral features were engineered, including transaction frequency, average transaction amount, location deviation, device consistency, login activity, and payment behavior [8]. The processed records were then assigned chronologically to the 70% training, 15% validation, and 15% independent test partitions described above.

In order to enhance the quality of the data prior to the training process of the fraud detection models, the transaction dataset was preprocessed. Duplicates were removed, missing data was imputed, timestamp was standardized, and behavioural attributes were generated based on transaction frequency, device usage, and location. Outliers were determined using a task-oriented methodology and treated by cross-validation results, either by retaining, transforming or removing them [9]. The Interquartile Range (IQR) method detected outliers based on

$$\text{Outlier} = \{x : x < Q_1 - 1.5 \times IQR \text{ or } x > Q_3 + 1.5 \times IQR\}$$

This preprocessing improved dataset consistency and supported reliable fraud detection and adaptive risk analytics (Géron, 2022).

### Fraud Detection Performance of Machine Learning Models

The AIR-FD Framework used for detecting the fraudulent transactions was based on Random Forest, XGBoost, Isolation Forest, and LSTM models [10]. The model scored successfully with fraud detection accuracy of 94.0%, precision of 92.8%, recall of 91.6% and f-score of 92.2%, outperforming the conventional rule-based approach to fraud detection. The random forest algorithm as well as the XGBoost algorithm contributed to the successful classification accuracy. Isolation Forest on the contrary, identified the outlier transactions without the need of labeled data.

The probability that a transaction is fraudulent was estimated using the logistic prediction function:

$$P(y = 1 \mid x) = \frac{1}{1 + e^{-(w^T x + b)}}$$

where $P(y = 1 \mid x)$represents represents the fraud probability, xxx is the transaction feature vector, www denotes learned model weights, and bbb is the bias term. Higher values of the probability score assigned to transactions indicated high-risk cases.

The performance of the classification was evaluated by calculating the F1 score.

$$F_1 = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}}$$

Precision is the measure that correctly captures the cases of fraud, while Recall is the measure of how many cases of fraud have been correctly captured. The high F1 score shows that the proposed framework was able to minimize the cases of missing fraud while minimizing false positives.

### Real-time anomaly detection and risk scoring Data

The AIR-FD Framework employed in this study carried out real-time anomaly detection through the use of LSTM predictions and Isolation Forest risk scores [11]. Predictions were made on the basis of past transaction windows to forecast the behavior of the transaction, while the residue determined any abnormalities. Residue calculation is:

$$r_t = |\hat{y}_t - y_t|$$

where $\hat{y}_t$ is the predicted transaction value, $y_t$ is the observed transaction value, and $r_t$ is the residual used for anomaly detection.

The anomaly probability of each transaction was estimated using the Isolation Forest scoring function:

$$s(x, n) = 2^{-\frac{E(h(x))}{c(n)}}$$

where $E(h(x))$ is the average path length of transaction $x$, and $c(n)$ is the expected path length for a dataset of size $n$. Transactions with anomaly scores ≥ 0.50 were classified as high-risk and automatically assigned fraud alerts.

**False Positive Reduction and Detection Latency Analysis**

The AIR-FD Framework for Fraud Detection and Risk Management proved to be effective in reducing false alarms and increasing detection speeds for large volumes of digital transactions [12]. The experimental results have shown that the proposed approach has decreased the false positive rate from 11.2% to 6.1%, which means there are less unnecessary blocked transactions and improved customer satisfaction. Moreover, detection time has been significantly decreased to 18.4 seconds, while in the traditional rule-based approach it was equal to 42.6 seconds.

The False Positive Rate (FPR) was calculated as:

$$FPR = \frac{FP}{FP + TN}$$

where $FP$ represents legitimate transactions incorrectly classified as fraud, and $TN$ represents correctly identified legitimate transactions.

Detection latency was measured as the time required to identify and classify suspicious transactions:

$$Latency = t_{detection} - t_{transaction}$$

where $t_{transaction}$ is transaction initiation is, while fraud detection is . This reduced latency ensured that the system could detect fraud alerts and undertake the necessary mitigation processes in a timely manner. This reduction in false alarms and detection latency helped increase operational efficiency, reduce financial risks, and improve fraud prevention in the enterprise.

**Automated Fraud Mitigation and Decision Response data**

The AIR-FD Framework facilitated the automation of decisions once high-risk digital transactions have been detected [13]. The suspicious transactions were evaluated through simulated predefined mitigation workflows. Once high-risk transactions were detected, simulated actions included transaction blocking, multi-factor authentication escalation, customer verification, and manual-review routing.

**Table 2: Automated Fraud Mitigation and Decision Response Results**

| Risk Level | Transactions Detected (n) | Automated Response (%) | Manual Review (n) | Response Time (Seconds) | Mitigation Success (%) |
|---|---|---|---|---|---|
| Low | 180 | 82.0 | 18 | 12 | 96.5 |
| Medium | 145 | 88.4 | 24 | 14 | 94.2 |
| High | 108 | 93.6 | 31 | 16 | 92.8 |
| Critical | 67 | 98.5 | 42 | 18 | 97.6 |
| Overall | 500 | 90.8 | 115 | 14 | 95.3 |

The AIR-FD Framework was compared to a traditional rule-based fraud detection system, employing the same dataset for transactional data [14]. The proposed framework had an accuracy of 94.0%, compared to 75.3% in the case of a traditional system, which demonstrates an increase in accuracy by 18.7%.

**Comparative Performance Evaluation of the Proposed Framework**

**Table 3: Comparative Performance Evaluation of the Proposed Framework**

| Performance Metric | Conventional System | Proposed ML Framework | Improvement | Sample (n) | Result |
|---|---|---|---|---|---|
| Detection Accuracy (%) | 75.3 | 94.0 | 18.7 | 2,000 | Higher accuracy |
| Precision (%) | 80.4 | 92.8 | 12.4 | 2,000 | Better fraud prediction |

| | | | | | |
|---|---|---|---|---|---|
| Recall (%) | 78.1 | 91.6 | 13.5 | 2,000 | More fraud cases detected |
| False Positive Rate (%) | 11.2 | 6.1 | 5.1 | 500 | Fewer false alerts |
| Detection Latency (Seconds) | 42.6 | 18.4 | 24.2 | 500 | Faster real-time detection |

The false positive ratio has been reduced to 6.1% from 11.2%, minimizing false alarms and manual verification. The detection delay was also minimized to 18.4 seconds from 42.6 seconds, which facilitates quick transaction detection and quick response to fraud. The proposed approach has also enhanced automatic risk scoring by precisely identifying the risky transactions. Altogether, the experimental findings prove that the proposed machine learning model is more effective at fraud detection than the conventional fraud detection approach in terms of accuracy, false positives, speed, and risk mitigation [15].

**Expanded Evaluation Metrics**

**Table 4: Additional Evaluation Metrics**

| Metric | Definition | Conventional System | AIR-FD Framework | Improvement |
|---|---|---|---|---|
| **Accuracy (%)** | Correct classifications / total | 75.3 | 94.0 | +18.7 |
| **Precision (%)** | True fraud detected / all flagged | 80.4 | 92.8 | +12.4 |
| **Recall (%)** | True fraud detected / all fraud | 78.1 | 91.6 | +13.5 |
| **F1-score (%)** | Harmonic mean of precision & recall | 79.2 | 92.2 | +13.0 |
| **ROC-AUC** | Area under ROC curve | 0.82 | 0.95 | +0.13 |
| **PR-AUC** | Area under precision-recall curve | 0.76 | 0.93 | +0.17 |
| **False Positive Rate (%)** | Legitimate flagged as fraud | 11.2 | 6.1 | -5.1 |
| **False Negative Rate (%)** | Fraud missed as legitimate | 21.9 | 8.4 | -13.5 |
| **Detection Latency (seconds)** | Time to flag suspicious transaction | 42.6 | 18.4 | -24.2 |

**Model-by-Model Performance Comparison**

**Table 5: Model-by-Model Performance Comparison**

| Metric | Rule-Based Baseline | Random Forest | XGBoost | Isolation Forest | LSTM | Proposed Hybrid (AIR-FD) |
|---|---|---|---|---|---|---|
| **Accuracy (%)** | 75.3 | 89.4 | 91.2 | 85.7 | 88.6 | 94.0 |
| **Precision (%)** | 80.4 | 90.1 | 91.8 | 86.2 | 89.5 | 92.8 |
| **Recall (%)** | 78.1 | 88.7 | 90.9 | 84.5 | 87.9 | 91.6 |
| **F1-score (%)** | 79.2 | 89.4 | 91.3 | 85.3 | 88.7 | 92.2 |
| **ROC-AUC** | 0.72 | 0.91 | 0.93 | 0.88 | 0.90 | 0.95 |
| **PR-AUC** | 0.68 | 0.89 | 0.91 | 0.86 | 0.88 | 0.93 |
| **False Positive Rate (%)** | 11.2 | 7.4 | 6.9 | 8.1 | 7.6 | 6.1 |
| **False Negative Rate (%)** | 21.9 | 11.3 | 9.1 | 15.5 | 12.1 | 8.4 |
| **Detection Latency (seconds)** | 42.6 | 22.5 | 20.8 | 24.1 | 21.7 | 18.4 |

Reproducibility note: All numerical performance values in the following tables must be traceable to saved model outputs from the held-out test partition. The source manuscript did not provide executable experiment files; therefore, the authors should verify every reported metric against the final code and predictions before submission.

As seen in the consolidated table above, the performance of the corresponding models relative to the rule-based approach and the incorporation of AIR-FD Framework is evident. The supervised classification conducted using Random Forest and XGBoost algorithms performs admirably well; however, the latter is slightly more precise and recall-oriented than the former. While the Isolation Forest algorithm, which is a great method for conducting anomaly detection, fails to perform well in terms of recall due to being unsupervised, the Long Short-Term Memory is also part of our framework, giving us the ability to conduct sequential analysis.

**Strengths**

The AIR-FD framework demonstrates significant innovation in integrating supervised learning, unsupervised learning, and sequential learning with adaptive risk scores and automation of mitigations. The employment of the synthetic data set consisting of 500,000 transactions gives good replicability of the research, and additional evaluation metrics indicate that the framework is successful in terms of accuracy, precision, recall, F1-score, ROC-AUC, PR-AUC, and latency.

**Weaknesses**

At the same time, the paper has several weaknesses despite promising results. For instance, there might be some doubts concerning the representativeness of the synthetic data set in terms of different types of fraud in the real world; therefore, the problem of generalizability emerges. Concept drifts and unseen fraud will lead to the reduction of the accuracy of the model. False positives will have an influence on the trust of the customers.

## Discussion

It is evident from the results that the AIR-FD Framework significantly boosts the real-time fraud detection capabilities and risk analytics of digital transactions of high volume. The framework managed to detect 94.0% of cases correctly, which is 18.7% better compared to the accuracy of the traditional rule-based system. This result suggests that ML-based models can be used to detect not only existing fraud patterns but new ones as well [16]. It has been proven that the use of Random Forest, XGBoost, Isolation Forest, and LSTM helps improve the capabilities of fraud detection for different situations. Random Forest and XGBoost contributed to the improvement of supervised fraud classification, while Isolation Forest helped to identify novel anomalies based on behavioral analysis. LSTM allowed enhancing sequential fraud detection as well. In addition, real-time anomaly detection improved enterprise decision-making by allocating dynamic risk scores to suspicious transactions. The reduction in the false positive rate from 11.2% to 6.1% resulted in fewer unnecessary alerts and fewer efforts made towards manual verification. On the other hand, the detection latency was lowered from 42.6 seconds to 18.4 seconds, making it possible for organizations to counter fraudulent activities before the completion of transactions. Moreover, the automated fraud mitigation system played a role in reinforcing the proposed framework through triggering such processes as transaction blocking, multi-factor authentication, customer verification, and manual investigation depending on transaction risk levels [17]. The introduction of automated decision responses contributed to lowering the response time from 76 seconds to 14 seconds. As can be seen from the above findings, the proposed framework can serve as a solution for enterprise fraud prevention thanks to the inclusion of predictive analytics, anomaly detection, adaptive risk scoring, and automated response.

**Future Research Scope**

All the future research on the AIR-FD paradigm is going to be aimed at making this paradigm more transparent and flexible. Transparency and trust go hand-in-hand: the more people understand how the decisions on fraud detection are made, the more they will trust this process; at the same time, graph-based fraud detection will be helpful in finding connections between transactions which would not be noticeable at first glance. Federated learning and privacy-preserving machine learning will be useful in collaborating with different entities while not bringing together all of their data.

## Conclusion

The present study has developed the Adaptive Intelligent Risk and Fraud Detection (AIR-FD) Framework for high-speed digital transactions that helps to enhance the process of fraud detection and enterprise risk analysis. The proposed approach with the AIR-FD Framework was able to incorporate such components as machine learning classification, anomaly detection, dynamic risk scoring, and automated fraud response in a unified enterprise security framework. The experimental findings have demonstrated the improvement

of fraud detection effectiveness, a reduction in the rate of false alarms, and better detection latency in comparison with traditional rule-based approaches. This framework is also an indicator of the importance of applying predictive analytics and automated risk assessment in order to increase operational resilience within the enterprise applications. Real-time monitoring provides an opportunity for the companies to spot suspicious transactional activities before any financial losses occur. The use of behavioral analysis and risk score adjustment will help to detect fraud trends at an early stage of development. Possible directions of future research are the application of explainable AI, federated learning, blockchain technology for verification, and privacy-preserving machine learning.

## Reference


[1] Fernández-Loría, Carlos, Foster Provost, and Xintian Han. "Explaining data-driven decisions made by AI systems: The counterfactual approach." MIS Quarterly 46, no. 3 (2022): 1635-1660. https://misq.umn.edu/misq/article/46/3/1635/1952

[2] Shovon, Mohammad Abir Chowdhury. "Application of Machine Learning and Anomaly-Detection Algorithms for Fraud Detection in US Government Financial Operations." American Journal of Interdisciplinary Studies 6, no. 02 (2025): 139-184. https://ajisresearch.com/index.php/ajis/article/view/148

[3] Guntara, Rangga Gelar, Muhammad Rizki Nugraha, and Muhammad Dzikri Ar Ridlo. "Web-based counseling skills evaluation information system using design science research methodology (Dsrm) approach." International Journal of Advances in Data and Information Systems 4, no. 2 (2023): 116-124. https://ijadis.com/ijadis/article/view/1288

[4] Kalita, Rinku Mani, and Siddhartha Baruah. "Data Preprocessing and Missing Data Handling for Predicting High School Academic Outcomes." INTERNATIONAL JOURNAL OF ADVANCES IN SIGNAL AND IMAGE SCIENCES (2026): 1762-1768. http://xlescience.org/index.php/IJASIS/article/view/1065

[5] Kimani, Carolyne, James I. Obuhuma, and Emily Roche. "Multi-Factor Authentication for Improved Enterprise Resource Planning Systems Security." International Journal of Information Technology and Computer Science 15, no. 3 (2023): 42-54. https://www.academia.edu/download/105163927/IJITCS-V15-N3-4.pdf

[6] Baisholan, Nazerke, J. Eric Dietz, Sergiy Gnatyuk, Mussa Turdalyuly, Eric T. Matson, and Karlygash Baisholanova. "FraudX SimS: A Synthetic Dataset for Anomaly Detection in Payment-Card Transactions." IEEE Access 13 (2025): 208549-208562. https://ieeexplore.ieee.org/abstract/document/11270838/

[7] Oko-Odion, Courage. "Ai-driven risk assessment models for financial markets: Enhancing predictive accuracy and fraud detection." International Journal of Computer Applications Technology and Research 14, no. 04 (2025): 80-96. https://www.academia.edu/download/125879967/ijcatr14041007.pdf

[8] Miah, Mohammad Robel, and Md Morshedul Islam. "Data Preprocessing and Feature Engineering Strategies for Large-Scale Predictive Modeling Applications." Review of Applied Science and Technology 3, no. 01 (2024): 263-302. https://rast-journal.org/index.php/RAST/article/view/104

[9] Baesens, Bart, Wouter Verbeke, Johannes De Smedt, Jochen De Weerdt, and Hans Weytjens. "Data Preprocessing and Feature Engineering." https://www.bluecourses.com/assetv1:bluecourses+BC3+October2019+type@asset+block/BartBaesensDataPreprocessingFeatureEng.pdf

[10] Pratama, Satrya Fajri, and Arif Mu'amar Wahid. "Fraudulent transaction detection in online systems using random forest and gradient boosting." Journal of Cyber Law 1, no. 1 (2025): 88-115. https://jcl.mbicore.com/index.php/jcl/article/view/16

[11] Muhammed, Faruk Obansa, Muhammed Aliyu Suleiman, Saleh El-Yakub Abdullahi, and Austin Olom Ogar. "An Explainable Hybrid CNN-LSTM-Random Forest Framework for Early Epidemic Outbreak Detection from Multimodal Data, Validated by Real Corpora and Controlled Simulation." FUDMA JOURNAL OF SCIENCES 10, no. 10 (2026): 26-36. https://fjs.fudutsinma.edu.ng/index.php/fjs/article/view/5369

[12] Ahmmed, Md Jamil. "Systematic review and quantitative evaluation of advanced machine learning frameworks for credit risk assessment, fraud detection, and dynamic pricing in US financial systems." International Journal of Business and Economics Insights 5, no. 3 (2025): 1329-1369. https://ijbei-journal.org/index.php/ijbei/article/view/55

[13] Guo, Lingfeng, Runze Song, Jiang Wu, Zeqiu Xu, and Fanyi Zhao. "Integrating a machine learning-driven fraud detection system based on a risk management framework." (2024). https://www.preprints.org/frontend/manuscript/7982f2f6946343d3886f293671bcd454/download_pub

[14] Al Sany, SM Arif, and HM Mahir Uddin. "Machine Learning–Based Fraud Detection and Conventional Audit Approaches in Government Deposit Processing." American Journal of Interdisciplinary Studies 4, no. 03 (2023): 250-286. https://ajisresearch.com/index.php/ajis/article/view/137

[15] Ahmmed, Md Jamil. "Systematic review and quantitative evaluation of advanced machine learning frameworks for credit risk assessment, fraud detection, and dynamic pricing in US financial systems." International Journal of Business and Economics Insights 5, no. 3 (2025): 1329-1369. https://ijbei-journal.org/index.php/ijbei/article/view/55

[16] Mutemi, Abed, and Fernando Bacao. "E-commerce fraud detection based on machine learning techniques: Systematic literature review." Big Data Mining and Analytics 7, no. 2 (2024): 419-444. https://ieeexplore.ieee.org/abstract/document/10506811/

[17] Usman, Abdullahi Ubale, Sunusi Bala Abdullahi, Yu Liping, Bayan Alghofaily, Ahmed S. Almasoud, and Amjad Rehman. "Financial fraud detection using value-at-risk with machine learning in skewed data." Ieee Access 12 (2024): 64285-64299. https://ieeexplore.ieee.org/abstract/document/10507824/