JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue

JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

AI-POWERED FRAUD DETECTION IN DIGITAL PAYMENTS

[1]Anchal, [2]Sheetal, [3]Shreya G, [4]Spoorti
Student, Guru Nanak Dev Engineering College Bidar
Department of Computer Science and Engineering,
Guru Nanak Dev Engineering College Bidar, Department of Computer Science and Engineering,
Visvesvaraya Technological University (VTU), Belagavi-590018, Karnataka, India.

Abstract: Online banking fraud occurs whenever a criminal can seize accounts and transfer funds from an individual's online bank account. Successfully preventing this requires the detection of as many fraudsters as possible, without producing too many false alarms. This is a challenge for machine learning owing to the extremely imbalanced data and complexity of fraud. In addition, classical machine learning methods must be extended, minimizing expected financial losses. Finally, fraud can only be combated systematically and economically if the risks and costs in payment channels are known. We define three models that overcome these challenges: machine learning-based fraud detection, economic optimization of machine learning results, and a risk model to predict the risk of fraud while considering countermeasures. The models were tested utilizing real data. Our machine learning model alone reduces the expected and unexpected losses in the three aggregated payment channels by 15% compared to a benchmark consisting of static if-then rules. Optimizing the machine-learning model further reduces the expected losses by 52%. These results hold with a low false positive rate of 0.4%. Thus, the risk framework of the three models is viable from a business and risk perspective.

Keywords: Payment fraud risk management, Anomaly detection, Ensemble models, Integration of machine learning and statistical risk modelling, Economic optimization machine learning Outputs.

Introduction

The landscape of financial transactions in India has undergone a remarkable transformation with the advent of Digital Payment systems, among which the Unified Payments Interface Digital Payments stands as a hallmark of innovation and convenience. conceived and implemented by the National Payments Corporation of India (NPCI), has democratized financial inclusion by providing a seamless, interoperable, and instant platform for transferring funds between individuals, businesses, and institutions. Its widespread adoption, fuelled by the proliferation of smartphones and internet connectivity, has catalyzed a paradigm shift towards a cashless economy, empowering millions of users to conduct transactions with unprecedented ease and efficiency. Yet, amidst the rapid digitization of financial services, the specter of fraud looms large, casting a shadow of uncertainty over the security and integrity of Digital Payment ecosystems. The exponential growth of digital payments transactions has inadvertently provided fertile ground for fraudsters to exploit vulnerabilities and perpetrate various forms of financial malfeasance, ranging from account takeovers and identity theft to sophisticated phishing scams and social engineering tactics. These nefarious activities not only jeopardize the hard-earned savings of unsuspecting individuals but also erode the trust and confidence essential for the sustained growth of Digital Payments in India.

2. Objectives

- Develop Machine Learning Models: -Train and optimize machine learning models using historical UPI transaction data to accurately classify transactions as legitimate or fraudulent. Implement Real-Time Monitoring: Develop a real-time monitoring system capable of continuously evaluating incoming UPI transactions.
- Design Alert Mechanism: - Create an alert mechanism to promptly notify users and relevant stakeholders about potential fraudulent transactions.
- Ensure Regulatory Compliance: -Ensure compliance with regulatory frameworks and data privacy regulations governing financial transactions. - Incorporate mechanisms to maintain transparency and accountability in all aspects of the fraud detection process.

Methodology

3.1 System Design

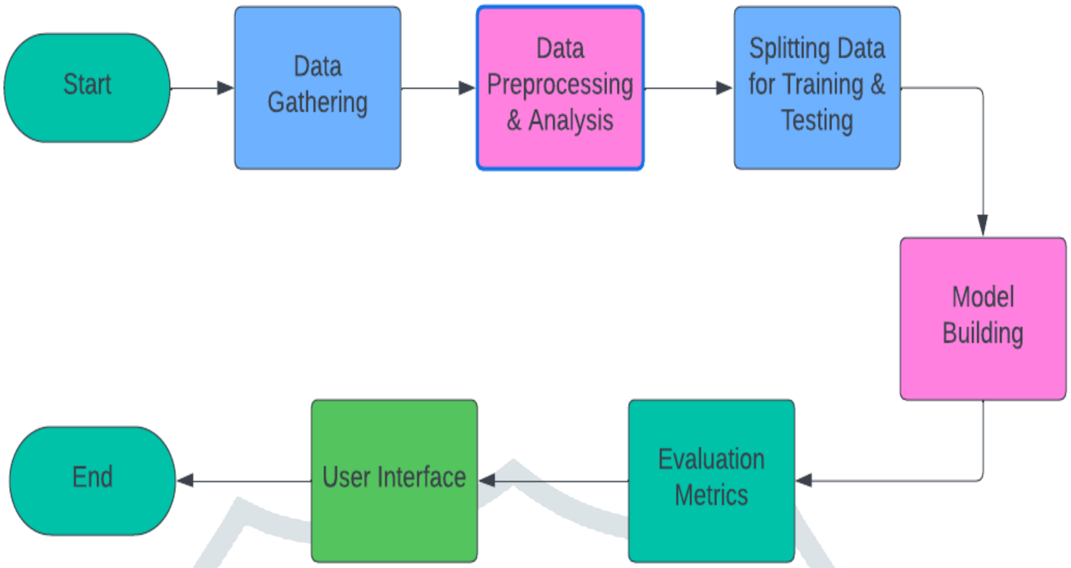


Fig 1 - System Architecture

Simplified System Design for Fraud Detection

1. **Architecture and Data Pipeline**
Adopt a microservices architecture using containerization (e.g., Docker) and orchestration platforms (e.g., Kubernetes).Design a data pipeline for real-time and batch processing of transactional data, leveraging frameworks like Apache Kafka or Flink for streaming.

2. Machine Learning and Monitoring
Develop and optimize machine learning models (e.g., ensemble methods, deep learning) for fraud detection with feature selection and dimensionality reduction techniques. Implement real-time anomaly detection and integrate monitoring tools to identify suspicious activities effectively.

3. Deployment and Maintenance
Deploy on scalable cloud platforms (e.g., AWS, GCP), with robust security and real-time alerting systems.
Ensure continuous monitoring, regular updates, and performance optimization through automated logging and alert mechanisms**.**

3.2 Training and Evaluation

Fraud detection in digital payments involves training machine learning models on historical transaction data to identify fraudulent patterns while minimizing false positives and negatives. The process begins with data preparation, including feature engineering (e.g., transaction velocity, location anomalies), handling imbalanced datasets (using SMOTE or under-sampling), and normalization. Models such as logistic regression, decision trees, or advanced methods like XGBoost and neural networks can be trained on labeled data split into training and test sets. Evaluation metrics like precision, recall, F1-score, and area under the ROC curve (AUC) are used to assess performance. Ensuring scalability, low latency, and robust feature selection is critical for real-time fraud detection systems.

3.3 Performance Metrics

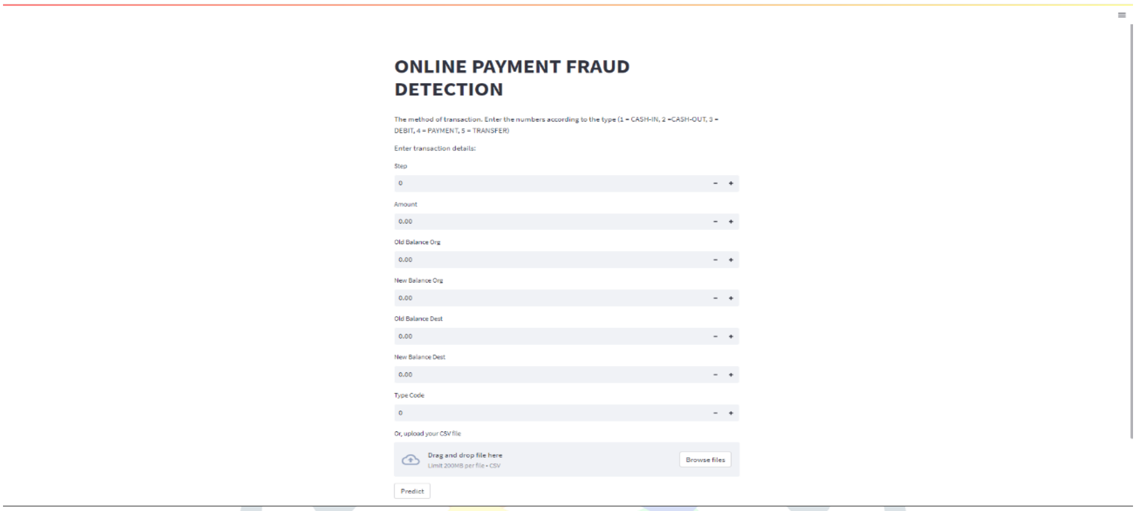
Evaluate model performance using metrics such as accuracy, precision, recall, F1 score, and area under the ROC curve (AUC-ROC). Cross-Validation: Perform cross-validation to validate model generalization performance and mitigate overfitting. Continuous Learning: Implement mechanisms for continuous learning and model adaptation to keep pace with evolving fraud tactics and patterns. Feedback Loop: Gather feedback from users and stakeholders to improve model performance and enhance system effectiveness over time.

4. Results and Discussion

The simulation results for online banking are presented in Table 6. The table shows the simulation results without applying fraud detection utilizing a constant FPR level of 0.4% and the triage model for an integrated FPR of 0.4%, respectively.

No additional recovery was applied. The above table shows the strong mitigation of risk due to fraud detection. The triage model performs better than the constant FPR benchmark in all submodels, particularly for the GPD submodel. Recall that the triage model places strong emphasis on detecting large fraudulent transactions, even flagging all transactions larger than CHF 192′000. As a second application, we compare the results of this risk model for the three e-channels with the bank's overall 2019 risk policy. This means that we compare the capital-at-risk (CaR) limits for market and credit risks with operational risk limits, where the e-channel part is now calculated in our model. The following allocation of CaR holds according to the annual report of the bank1: Credit Risk, 69%; operational risk, 11%; market risk trading, 4%; market risk treasury, 11%; market risk real estate, 2%; and investment, 4%. Approximately 1% of operational risk capital can be attributed to these three channels.

Even if we add another 4–5% of the total volume to all payment services, including corporate banking and interbank payments, less than 10% of the operational risk capital is attributed to payment systems. As payment systems account for a significant portion of operational risk, our results confirm serious doubts about the accuracy of the chosen operational risk capital in banks. Without reliable models and data, capital is determined by utilizing dubious business indicators. Our models, which represent a micro-foundation of risk, show that, at least in payment systems, trustworthy risk quantities can be derived by combining machine learning and statistics



ONLINE PAYMENT FRAUD DETECTION

The method of transaction. Enter the numbers according to the type (1 = CASH-IN, 2 =CASH-OUT, 3 = DEBIT, 4 = PAYMENT, 5 = TRANSFER)

Enter transaction details:

Step: 0

Amount: 0.00

Old Balance Org: 0.00

New Balance Org: 0.00

Old Balance Dest: 0.00

New Balance Dest: 0.00

Type Code: 0

Or, upload your CSV file

Drag and drop file here
Limit 200MB per file • CSV

5. Conclusion and Future Scope

In conclusion, fraud detection in digital payments is an ever-evolving challenge due to the increasing sophistication of fraudulent schemes and the growing volume of transactions. While current systems leveraging machine learning, artificial intelligence, and behavioral analytics have significantly improved detection rates, challenges like false positives, real-time processing, and adaptability to new fraud patterns persist. Future work should focus on enhancing the scalability and accuracy of fraud detection systems through the integration of advanced technologies such as deep learning, blockchain, and federated learning. Additionally, collaboration between financial institutions, regulators, and technology providers will be crucial to developing robust, transparent, and standardized approaches that can adapt to emerging threats while ensuring user privacy and compliance with regulations.

5.1 Adaptability to Diverse Scenarios:

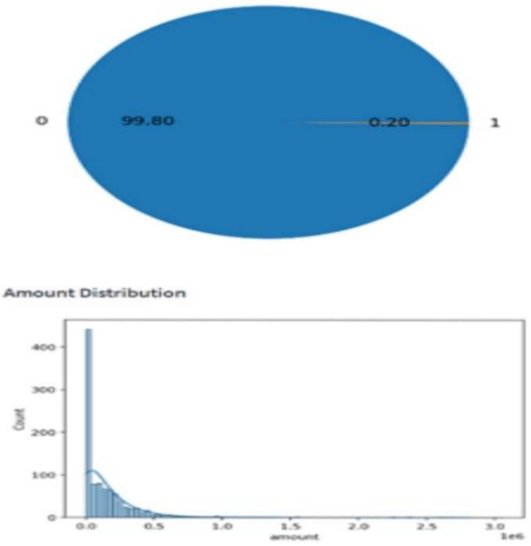


Figure 2: Fraud and Non-Fraud Transactions (Pie-chart) And Amount Distribution (Histogram)

Pie chart gives represents proportion of fraudulent transaction compared to non-fradulent. The larger blue portion represents the non-fradulent transactions while smaller yellow portion represents fraudulent transaction.

Histogram shows the distribution of the transaction amounts. The x-axis represents the transaction amount while the y-axis represents the frequency of transaction with range.
The height of each bar indicates the frequency of that transaction type.

5.2 Future Enhancements

1. **Advanced Machine Learning Techniques**:- Explore advanced machine learning techniques such as deep learning, reinforcement learning, and anomaly detection algorithms to further improve fraud detection accuracy and robustness.
2. **Enhanced Real-Time Monitoring**: - Integrate advanced data streaming and processing technologies to enhance real-time monitoring capabilities, enabling faster detection and response to fraudulent activities.
3**. Behavioral Analysis and Biometrics**:- Incorporate behavioral analysis and biometric authentication techniques to add an extra layer of security, leveraging user-specific patterns and biometric data for fraud detection.
4**. Explainable AI and Model Interpretability**:- Enhance model interpretability and transparency through explainable AI techniques, enabling users and stakeholders to understand the reasoning behind model predictions and decisions.

6. Reference

1. Keerthi, M. N., & Nalini, S. Online payment fraud detection using machine learning. International Journal of Creative Research Thoughts (IJCRT), (2024), 12(4).

2. Namani, S., Mordharia, H., Gajare, N., & Bemila, T. Online payment fraud detection: An integrated approach. International Research Journal of Modernization in Engineering Technology and Science (IRJMETS), (2024), 6(4), 7648.

3. Pachhala, N., Sai, M. D. S., Prudhvi, P., Gopi, G. M. N. V. S., Sai Ram, I. G. N., & Sandeep, M. R . Online payment fraud detection. International Journal of Innovative Science and Research Technology (IJISRT), (2023), 8(10), 1191.

4. Babu, C. M., SweeHoney, B., Prathyusha, P., Reddy, B. D., & Sathvika, M. Online payment fraud detection. International Journal of Early Childhood Special Education (INT-JECSE), (2023), 15(4), 778. https://doi.org/10.48047/INTJECSE/V15I4.86

5. Venkatesh, M., Bai, B. K., Bhargavi, B., Manasa, C., & Mokshitha, D. Online payment fraud detection using machine learning. Vasireddy Venkatadri Institute of Technology, Andhra Pradesh, India, (2023).

6. Almazroi, A. A., & Ayub, N. Online fraud detection model using machine learning technique(2023). IEEE Access. https://doi.org/10.1109/ACCESS.2023.3339226

7. Chawla, T. S. Online payment fraud detection using machine learning techniques (MSc Research Project) National College of Ireland (2022).

8. Madabhattula, L., Manikanta, M., & Kumar, P. Online transaction fraud detection. International Journal of Creative Research Thoughts (IJCRT), (2021), 9(5), 117-161.