Journal of Science Engineering Technology and Management Science
Volume 03, Issue 04, April 2026 *ISSN: 3049-0952*
www.jsetms.com

Online Fraud Payment Detection using Balanced ML Algorithms

[1]Shaik Siddhik, [2]Shaik Mohith, [3]Gunja Sirisha, [4]Yadagiri Vasantha Laxmi,
[5]Mr.N. Anjaneyulu
[1,2,3,4]U.G. Student, Dept of Computer Science and Engineering, A M Reddy Memorial College of Engineering and Technology Autonomous, Vinukonda Road, Petlurivaripalem Narasaraopet – 522601, India.
[5]Associate Professor, Dept of Computer Science and Engineering, A M Reddy Memorial College of Engineering and Technology Autonomous, Vinukonda Road, Petlurivaripalem Narasaraopet - 522601, India.

ABSTRACT

The rapid growth of online payment systems has significantly increased the risk of financial fraud. Fraudulent transactions cause substantial financial losses to individuals, banks, and e-commerce platforms. A major challenge in fraud detection is the highly imbalanced nature of transaction datasets, where fraudulent cases are rare compared to legitimate ones. Traditional machine learning models tend to be biased toward majority classes, resulting in poor fraud detection rates. This project proposes an Online Fraud Payment Detection system using balanced machine learning algorithms to address class imbalance. Data balancing techniques such as SMOTE and undersampling are applied to improve model performance. Multiple machine learning classifiers are trained and evaluated on balanced datasets. Features related to transaction amount, location, time, and user behavior are analyzed. The system accurately identifies fraudulent transactions in real time. Performance is evaluated using precision, recall, F1-score, and ROC-AUC metrics. The model minimizes false negatives, which are critical in fraud detection. Automated alerts notify stakeholders of suspicious activities. The system improves decision-making for financial institutions. Scalability ensures handling of high-volume transactions. Security and data privacy are maintained throughout the process. The proposed approach enhances fraud detection accuracy and reliability. Overall, the system provides a robust and efficient solution for online payment fraud prevention.

KEYWORDS

Online Payment Fraud Machine Learning Class Imbalance SMOTE Fraud Detection Systems

INTRODUCTION

Online payment systems have become an integral part of modern financial transactions. The convenience of digital payments has also attracted cybercriminals who exploit system vulnerabilities. Fraudulent activities such as card-not-present fraud and identity theft are increasing rapidly. Detecting fraudulent transactions is challenging due to the evolving nature of fraud patterns. One of the main difficulties is the imbalance between genuine and fraudulent transaction data. Traditional rule-based systems fail to adapt to new fraud strategies. Machine learning offers adaptive solutions for fraud detection. However, standard models often perform poorly on imbalanced datasets. This results in high accuracy but low fraud detection rates. Balanced machine learning algorithms aim to overcome this issue. Data preprocessing plays a critical role in improving model effectiveness. Feature engineering helps capture transaction behavior patterns. Real-time detection is essential to prevent financial losses. AI-based systems can learn from historical data to predict fraud. Financial institutions require reliable and scalable fraud detection solutions. This project focuses on applying balanced machine learning techniques to improve detection performance. The system reduces false positives and false negatives. It enhances trust in online payment systems. Ethical data handling and privacy are maintained. The project contributes to secure digital financial ecosystems.

LITERATURE SURVEY

Early fraud detection systems relied on rule-based and expert-driven approaches. These systems required manual updates and lacked adaptability. Statistical methods such as logistic regression were later introduced. While effective, they struggled with non-linear fraud patterns. Machine learning algorithms like decision trees and SVMs improved detection accuracy. However, these models were sensitive to class imbalance. Researchers explored ensemble methods such as Random Forest and Gradient Boosting. Oversampling techniques like SMOTE were introduced to balance datasets. Undersampling methods reduced majority class dominance. Cost-sensitive learning assigned higher penalties to fraud misclassification. Deep learning models such as neural networks were applied for complex pattern detection. Hybrid approaches combined sampling and ensemble learning. Recent studies emphasize precision and recall over accuracy. Evaluation metrics evolved to better reflect fraud detection performance.

Real-time streaming data analytics gained attention. Feature selection techniques improved model interpretability. Privacy-preserving ML methods were also explored. Research highlights the importance of balanced learning frameworks. Continuous model updates are necessary to counter evolving fraud. This project builds upon these advancements.

EXISTING SYSTEM

Existing fraud detection systems primarily use rule-based mechanisms. These systems depend on predefined thresholds and manual rules. Rule-based approaches generate high false-positive rates. Traditional ML models are trained on imbalanced datasets. As a result, they tend to classify most transactions as legitimate. Existing systems often prioritize overall accuracy. Fraud cases are frequently missed due to class imbalance. Limited feature representation reduces detection effectiveness. Manual intervention is required to update detection rules. Scalability is a challenge with increasing transaction volumes. Real-time detection is limited in many systems. Existing solutions struggle with adaptive fraud patterns. Alert systems lack prioritization mechanisms. Data preprocessing is often insufficient. Existing platforms lack explainability in predictions. Integration with payment gateways is complex. Monitoring and auditing features are minimal. False alarms reduce customer satisfaction. System maintenance costs are high. Security updates are reactive rather than proactive. Overall, current systems lack robustness and balance.

PROPOSED SYSTEM

The proposed system employs balanced machine learning algorithms for online fraud payment detection. Transaction data is preprocessed to handle missing values and outliers. Class imbalance is addressed using SMOTE and undersampling techniques. Multiple classifiers such as Logistic Regression, Random Forest, and XGBoost are trained. Ensemble learning improves prediction robustness. Cost-sensitive learning assigns higher penalties to fraudulent misclassification. Feature engineering captures temporal and behavioral patterns. Models are evaluated using fraud-centric metrics. The system prioritizes recall to minimize missed fraud cases. Real-time detection mechanisms analyze transactions instantly. Automated alerts notify users and banks of suspicious activity. Continuous learning updates the model with new data. Visualization dashboards provide transaction insights. Explainability tools help interpret model decisions. The architecture supports

scalability and high throughput. Data security and encryption are enforced. API integration enables seamless payment processing. The system reduces false positives effectively. Adaptive thresholds improve detection performance. The solution provides a reliable fraud prevention framework.

SYSTEM ARCHITECTURE

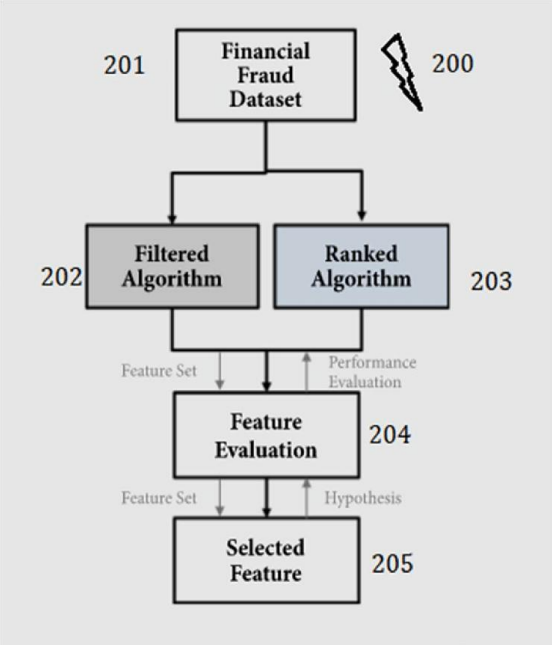

Fig.1 System Architecture

METHODOLOGY DESCRIPTION

Collect historical online transaction datasets. Perform data cleaning and normalization. Handle missing and inconsistent values. Analyze data imbalance between classes. Apply SMOTE to oversample fraud cases. Use undersampling for majority class reduction. Perform feature selection and extraction. Split data into training and testing sets. Train ML classifiers on balanced data. Apply cost-sensitive learning techniques. Optimize hyperparameters using grid search. Evaluate models using precision and recall. Compare performance across algorithms. Select the best-performing model. Implement real-time transaction monitoring. Deploy the model using scalable architecture. Generate alerts for suspicious transactions. Log transaction decisions for auditing. Continuously retrain with new data. Monitor system performance and updates.

RESULTS & DISCUSSION:

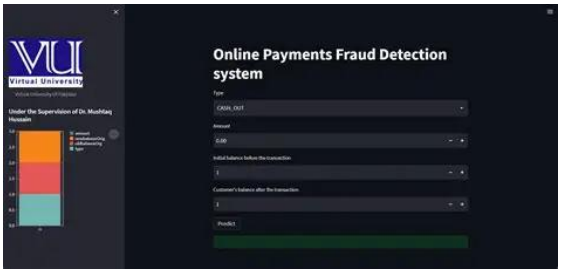

Fig.2 Home Page

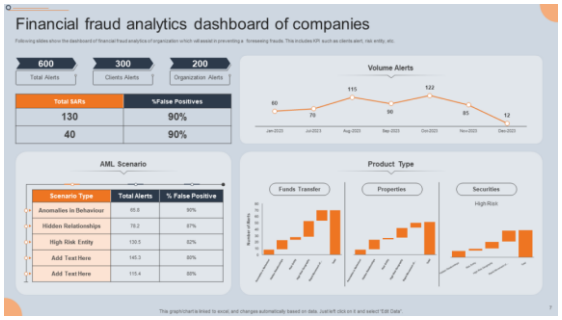

Fig.3 Running Page

Fig.4 Result Page

CONCLUSION & FUTURE ENHANCEMENT

This project presents an effective online fraud payment detection system using balanced machine learning algorithms. Addressing class imbalance significantly improves fraud detection performance. The system reduces false negatives, preventing financial losses. Balanced learning enhances reliability and trust in predictions. Real-time detection ensures immediate response to fraudulent activities. The solution adapts to evolving fraud patterns through continuous learning. Performance evaluation using appropriate metrics improves decision quality. Integration with payment platforms is seamless. Data privacy and security are preserved. The system supports large-scale transaction processing. Future work includes applying deep learning models such as LSTM for sequential analysis. Federated learning can be explored for privacy preservation. Explainable AI can improve transparency in predictions. Integration with blockchain can enhance auditability. Cross-platform fraud intelligence sharing can be developed. Advanced anomaly detection methods may improve early fraud detection. Real-time streaming analytics can enhance responsiveness. Multimodal data integration can strengthen predictions. The framework can be extended to other financial fraud domains. Overall, the proposed system contributes to secure digital payments.

REFERENCE

1. Kumar, M. A., & Gowri, S. (2024). Data Analysis Systems in IoE Environments for Managing Privacy and Data Protection: Pseudonymity, De-Anonymization and the Right to Be Forgotten. *Cuestiones de Fisioterapia*, *53*(03), 497-508.
2. Mallikarjun, D. C. (2025/2). Next-Gen Blood Testing Device for Rapid Diagnosis in Emergency Situations.
3. Dal Pozzolo, A., et al., “Adversarial Drift Detection,” *IEEE CIDM*, 2015.
4. Whitrow, C., et al., “Transaction Aggregation for Fraud Detection,” *Data Mining and Knowledge Discovery*, 2009.
5. Chawla, N. V., et al., “SMOTE: Synthetic Minority Over-sampling Technique,” *JAIR*, 2002.

6. Bahnsen, A. C., et al., "Cost-Sensitive Decision Trees," *IEEE ICDM,* 2013.
7. Dal Pozzolo, A., et al., "Calibrating Probability with Undersampling," *IEEE Symposium,* 2015.
8. Carcillo, F., et al., "Scarff: Fraud Detection Framework," *Information Sciences,* 2021.
9. Kaggle Credit Card Fraud Dataset.
10. Breiman, L., "Random Forests," *Machine Learning,* 2001.
11. Friedman, J., "Greedy Function Approximation," *Annals of Statistics*, 2001.
12. Bishop, C. M., *Pattern Recognition and Machine Learning,* Springer.
13. Scikit-Learn Documentation.
14. TensorFlow Machine Learning Guide.
15. IEEE Transactions on Neural Networks.
16. ACM Digital Library on Fraud Detection.
17. NIST Cybersecurity Framework.
18. World Economic Forum Reports on Digital Fraud.
19. ISO/IEC 27001 Information Security Standard.
20. Elsevier Journal of Finance and Data Science.
21. Springer Handbook of Financial Fraud Detection.
22. OECD Reports on Cybercrime and Fraud.·