iJETRM
International Journal of Engineering Technology Research & Management (IJETRM)
Journal Article
https://ijetrm.com/issue/

ONLINE FRAUD DETECTION USING MACHINE LEARNING AND DEEP LEARNING ALGORITHMS

K. Upendra, J. Sravan, A. Vishwa Teja
Final Year Students, Department of Computer Science & Engineering (Data Science),

Guide: Mrs. V. Subhashini
Department of Computer Science & Engineering (Data Science)
J.B. Institute of Engineering and Technology (UGC Autonomous), Hyderabad, Telangana, India

ABSTRACT
The project titled **"Online Fraud Detection Using Machine Learning and Deep Learning Algorithms"** focuses on developing an intelligent and automated framework for identifying fraudulent financial transactions in digital payment systems. With the rapid growth of online banking, e-commerce platforms, and digital wallets, fraudulent activities such as unauthorized transactions, phishing attacks, and payment fraud have become major challenges in the financial sector. The proposed system aims to improve fraud detection accuracy by integrating balanced Machine Learning and Deep Learning techniques.
The framework utilizes advanced preprocessing and balancing strategies, particularly the Synthetic Minority Oversampling Technique (SMOTE), to address the severe class imbalance present in financial datasets. The system combines Machine Learning models such as Random Forest and Naïve Bayes with Deep Learning architectures including Long Short-Term Memory (LSTM), TabNet, and AutoInt. Random Forest provides fast and reliable classification, while LSTM captures sequential transaction behavior. TabNet improves feature selection through attentive learning, and AutoInt identifies complex feature interactions using self-attention mechanisms.
The implementation follows a structured pipeline consisting of data collection, preprocessing, feature engineering, balancing, model training, evaluation, prediction, and visualization. The models were evaluated using performance metrics such as Accuracy, Precision, Recall, F1-Score, and ROC-AUC. Experimental analysis demonstrated that the Random Forest model with SMOTE achieved high fraud detection accuracy, while Deep Learning models showed improved capability in identifying hidden transaction patterns and reducing false positives.
Overall, the project demonstrates how Artificial Intelligence can enhance financial cybersecurity by automating fraud analysis and prediction. The developed system provides a scalable and intelligent solution that supports secure digital payment ecosystems and contributes to the advancement of AI-driven financial security systems.

Keywords:
AI, Fraud Detection, Machine Learning, Deep Learning, SMOTE, Random Forest, LSTM, TabNet, AutoInt, Financial Security, ROC-AUC, Classification

INTRODUCTION
The rapid growth of digital payment systems and online financial services has transformed the global economy by enabling faster, easier, and more convenient transactions. However, this transformation has also increased the risk of financial fraud, cybercrime, and unauthorized transactions. Fraudulent activities such as credit card theft, identity fraud, phishing attacks, and account takeover incidents have become major concerns for financial institutions and e-commerce organizations.
Traditional fraud detection systems mainly rely on static rule-based mechanisms and manual verification processes. Although these approaches can detect known fraud patterns, they often fail to identify new and evolving threats. Furthermore, manual analysis becomes inefficient when dealing with millions of daily transactions. Another critical challenge is the class imbalance problem, where fraudulent transactions represent only a very small portion of the total dataset.
To overcome these limitations, the project "Online Fraud Detection Using Machine Learning and Deep Learning Algorithms" proposes an intelligent AI-based framework that automates fraud analysis using balanced Machine Learning and Deep Learning models. The system incorporates SMOTE balancing techniques to improve minority

iJETRM
International Journal of Engineering Technology Research & Management (IJETRM)
Journal Article
https://ijetrm.com/issue/

class representation and combines algorithms such as Random Forest, Naïve Bayes, LSTM, TabNet, and AutoInt for accurate fraud prediction.
The framework follows a structured workflow that includes data preprocessing, feature engineering, balancing, model training, evaluation, and prediction. By integrating AI-driven analytics and automated learning techniques, the system improves fraud detection accuracy while minimizing false positives and operational losses.
Overall, this project highlights the importance of Artificial Intelligence in modern financial security systems and demonstrates how intelligent predictive models can enhance fraud prevention in digital payment ecosystems.

OBJECTIVES

The primary objectives of the Online Fraud Detection using Machine Learning and Deep Learning Algorithms project are:

1. To develop an intelligent AI-based system for detecting fraudulent financial transactions.
2. To collect and preprocess large-scale transaction datasets for effective analysis.
3. To apply SMOTE balancing techniques to handle class imbalance in fraud datasets.
4. To implement Machine Learning models such as Random Forest and Naïve Bayes for fraud classification.
5. To implement Deep Learning models such as LSTM for sequential transaction analysis.
6. To integrate advanced architectures such as TabNet and AutoInt for feature learning and interaction modeling.
7. To evaluate model performance using metrics such as Accuracy, Precision, Recall, F1-Score, and ROC-AUC.
8. To reduce false positives and improve fraud detection reliability.
9. To generate visual reports and dashboards for fraud analysis and prediction monitoring.
10. To support financial institutions and researchers in improving digital payment security..

METHODOLOGY

The methodology of the proposed Online Fraud Detection system follows a structured workflow for improving fraud identification accuracy and financial security.

1. **Data Collection:** Transaction datasets containing financial records, transaction details, and fraud labels were collected from publicly available sources and financial datasets.
2. **Data Preprocessing :** The collected data was cleaned and transformed by handling missing values, removing inconsistencies, scaling numerical features, and encoding categorical attributes.
3. **SMOTE Balancing:** Since fraudulent transactions are rare, SMOTE (Synthetic Minority Oversampling Technique) was applied to balance the dataset by generating synthetic fraud samples.**Data Splitting:** Data was divided into training and testing sets.
4. **Feature Engineering:** Important transaction features such as transaction amount, time patterns, frequency, and behavioral attributes were extracted for effective fraud analysis.
5. **Model Selection:** The system integrates multiple Machine Learning and Deep Learning models including Random Forest, Naïve Bayes, LSTM, TabNet, and AutoInt.
6. **Model Training:** The selected models were trained using balanced datasets to learn fraud patterns and transaction behavior.
7. **Model Evaluation:** The performance of the models was assessed using Accuracy, Precision, Recall, F1-Score, and ROC-AUC.
8. This methodology ensures efficient fraud analysis, balanced learning, accurate classification, and improved financial security.

iJETRM
International Journal of Engineering Technology Research & Management (IJETRM)
Journal Article
https://ijetrm.com/issue/

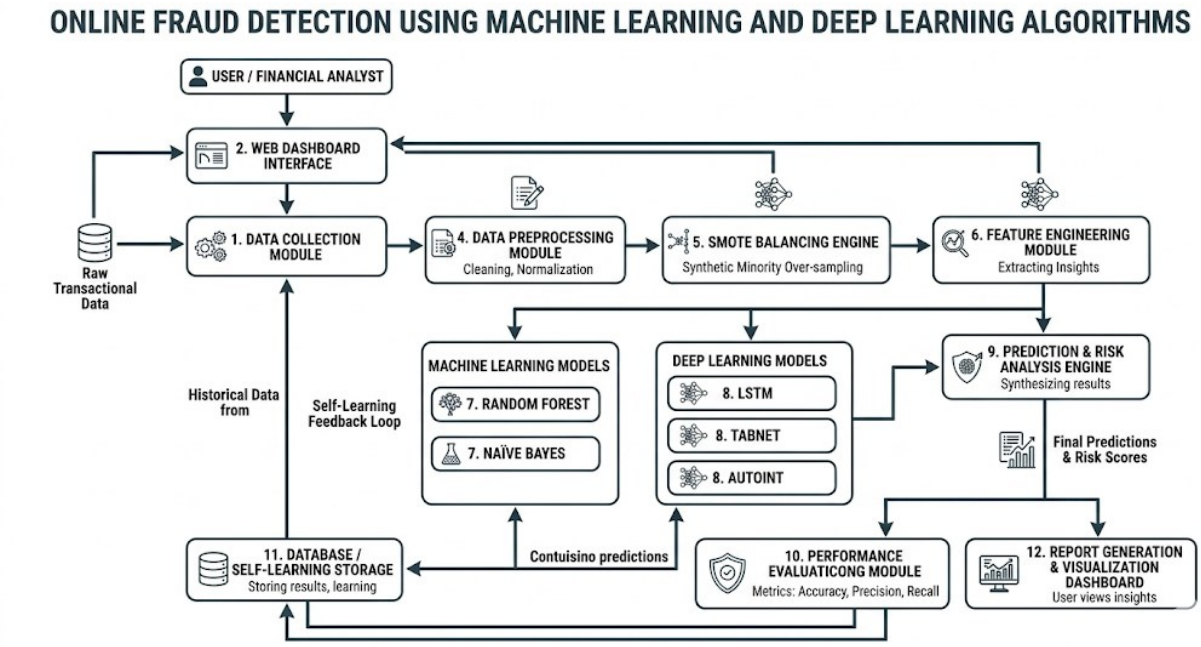

Figure 1: Proposed System Architecture of online fraud detection

RESULTS AND DISCUSSION

This section presents the comprehensive results and analysis of the developed Online Fraud Detection models. It includes a detailed evaluation of various Machine Learning and Deep Learning algorithms, analysis of fraud classification performance, and an overview of the complete fraud detection pipeline. The objective is to identify the most effective model and transaction features for accurate fraud prediction while minimizing false positives and false negatives. The system performance is evaluated using metrics such as Accuracy, Precision, Recall, F1-Score, and ROC-AUC. Comparative analysis demonstrates the effectiveness of models such as Random Forest, Naïve Bayes, LSTM, TabNet, and AutoInt in detecting fraudulent financial transactions. Additionally, visualization dashboards, confusion matrices, and risk analysis graphs are used to demonstrate the practical implementation and real-world applicability of the proposed fraud detection framework.

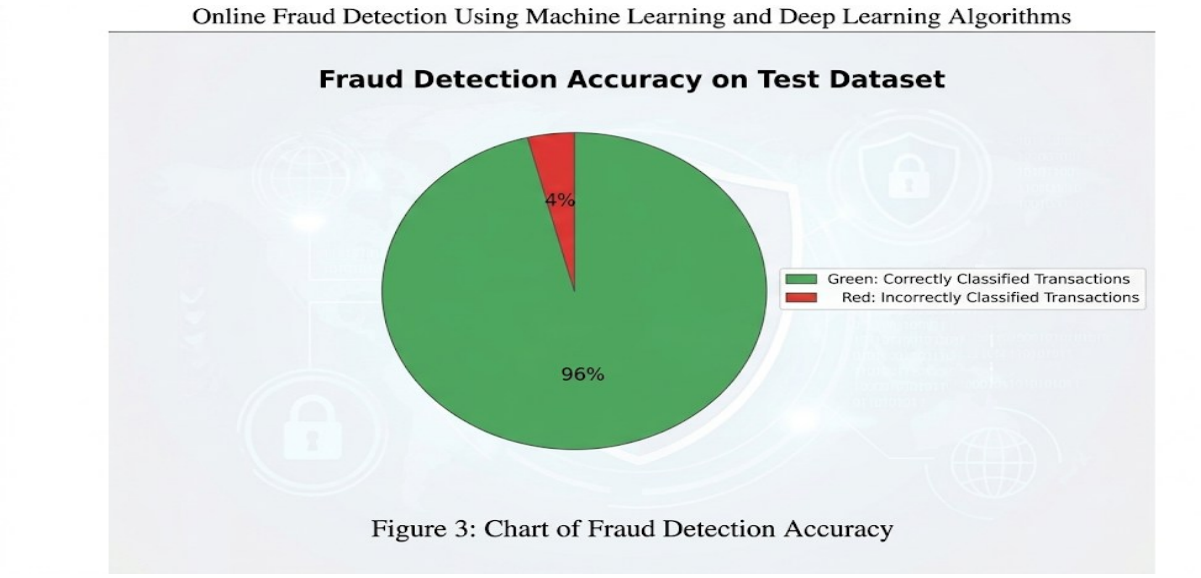

Figure 3: Chart of Fraud Detection Accuracy

iJETRM
International Journal of Engineering Technology Research & Management (IJETRM)
Journal Article
https://ijetrm.com/issue/

ACKNOWLEDGEMENT

Gratitude goes to Dr. Kavuri Roshan - leading the Department of Artificial Intelligence and Data Science at J.B. Institute of Engineering and Technology, Hyderabad - for steady direction during the project. His role as head and guide shaped much of what took place. Appreciation also reaches Principal Dr. P.C Krishnamachary., whose support mattered just as quietly. Gratitude goes to Dr. P.C Krishnamachary for shaping a space where research can grow. The team behind the scenes at the AIDS Department - those guiding classrooms and those keeping things running - deserve recognition too. Among them, students stepped forward during trials, offering thoughts that sharpened how well the system works. Their time shaped better results in ways that matter.

CONCLUSION

The Online Fraud Detection using Machine Learning and Deep Learning Algorithms project successfully demonstrates how Artificial Intelligence can be utilized to identify fraudulent financial transactions with improved efficiency, accuracy, and reliability. The system combines transaction analysis, data preprocessing, SMOTE balancing techniques, Machine Learning models, and advanced Deep Learning architectures to understand fraud patterns and predict suspicious activities in digital payment systems. By using intelligent models such as Random Forest, LSTM, TabNet, and AutoInt, the framework is capable of learning complex transaction behavior, identifying hidden fraud patterns, and detecting anomalies that are difficult to recognize using traditional rule-based systems.

The proposed system provides a modern and reliable alternative to manual fraud auditing and conventional fraud detection approaches. It automates the complete workflow including data collection, preprocessing, feature extraction, dataset balancing, model training, fraud prediction, and performance visualization. This reduces manual effort, saves processing time, and improves consistency in fraud analysis and financial security monitoring. The inclusion of SMOTE balancing techniques and advanced feature learning models further improves prediction quality by addressing class imbalance and enhancing fraud classification performance.

The evaluation results using metrics such as Accuracy, Precision, Recall, F1-Score, and ROC-AUC indicate that the developed framework performs effectively in detecting fraudulent financial activities. The system can assist banks, financial institutions, e-commerce platforms, and cybersecurity analysts in making faster and more accurate fraud-related decisions based on AI-driven insights. It also helps in minimizing false positives, reducing financial losses, and improving digital payment security.

Overall, this project highlights the growing importance of Artificial Intelligence in financial cybersecurity and proves that intelligent fraud detection systems can transform large-scale transaction data into meaningful security intelligence. The developed framework serves as a strong foundation for future AI-driven fraud prevention systems, real-time transaction monitoring platforms, and next-generation financial security applications.

REFERENCES

[1] Goodfellow, I., Bengio, Y., & Courville, A., *Deep Learning*, MIT Press, accessed February 20, 2026.
[2] Chollet, F., *Deep Learning with Python*, Manning Publications, accessed February 20, 2026.
[3] Brownlee, J., *Machine Learning Mastery for Fraud Detection Systems*, Machine Learning Mastery, accessed February 20, 2026.
[4] TensorFlow Documentation, Google Developers, accessed February 20, 2026, https://www.tensorflow.org/
[5] Scikit-learn Documentation, Machine Learning in Python, accessed February 20, 2026, https://scikit-learn.org/
[6] Pandas Documentation, Data Analysis and Manipulation Tool, accessed February 20, 2026, https://pandas.pydata.org/
[7] NumPy Documentation, Scientific Computing with Python, accessed February 20, 2026, https://numpy.org/
[8] Keras Documentation, Deep Learning API for Python, accessed February 20, 2026, https://keras.io/
[9] Imbalanced-learn Documentation, SMOTE and Imbalanced Dataset Handling, accessed February 20, 2026,
https://imbalanced-learn.org/
[10] Streamlit Documentation, Python Dashboard Framework, accessed February 20, 2026, https://streamlit.io/

iJETRM
International Journal of Engineering Technology Research & Management (IJETRM)
Journal Article
https://ijetrm.com/issue/

[11] Matplotlib Documentation, Visualization Library for Python, accessed February 20, 2026, https://matplotlib.org/
[12] Seaborn Documentation, Statistical Data Visualization Tool, accessed February 20, 2026, https://seaborn.pydata.org/
[13] Research Papers on Credit Card Fraud Detection using Machine Learning and Deep Learning Models, accessed February 20, 2026.
[14] Kaggle Financial Fraud Detection Dataset Repository, accessed February 20, 2026, https://www.kaggle.com/
[15] Research Articles on LSTM, TabNet, and AutoInt Architectures for Financial Fraud Detection, accessed February 20, 2026.