VISVESVARAYA TECHNOLOGICAL UNIVERSITY

"Jnana Sangama", Belagavi - 590 018

A Technical Seminar Report on

“ONLINE PAYMENT FRAUD DETECTION”

A Technical Seminar work submitted in partial fulfillment of the requirement for the award of the degree

Bachelor of Engineering
in
Computer Science and Engineering

Submitted by

POOJA H Y 1AY21CS125

Under the Guidance of
Mrs. Deeksha Satish
Assistant Professor

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

ACHARYA INSTITUTE OF TECHNOLOGY

(AFFILIATED TO VISVESVARAYA TECHNOLOGICAL UNIVERSITY, BELAGAVI, RECOGNISED BY AICTE, NEW DELHI)

Acharya Dr. Sarvepalli Radhakrishnan Road, Soldevanahalli, Bengaluru - 560107

2024-2025

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
ACHARYA INSTITUTE OF TECHNOLOGY
(Affiliated to Visvesvaraya Technological University, Belagavi, Recognized by AICTE, New Delhi)
Acharya Dr. Sarvepalli Radhakrishnan Road, Soldevanahalli, Bengaluru - 560107
2024 - 2025

Certificate

This is to certify that the **Technical Seminar (21CS81)** entitled **"Online Payment Fraud Detection"** carried out by **Pooja H Y (1AY21CS125)**, is bonafide student of **Acharya Institute of Technology, Bengaluru** in partial fulfillment for the award of the degree of **Bachelor of Engineering** in **Computer Science and Engineering** of the **Visvesvaraya Technological University**, **Belagavi** during the year **2024-25**. It is certified that all corrections/suggestions indicated for Internal Assessment have been incorporated in the report deposited in the departmental library. The Technical Seminar report has been approved as it satisfies the academic requirements in respect of Technical Seminar prescribed for the said Degree.

Signature of Guide	**Signature of Technical Seminar Co-Ordinator**	**Signature of HOD**
Mrs. Deeksha Satish Assistant Professor	(Prof. Deeksha/ Prof. Anitta)	(Prof. Rajeev Bilagi)

ABSTRACT

With the increasing reliance on digital payment platforms, the frequency and sophistication of fraudulent activities have grown significantly. Online payment fraud encompasses a variety of deceptive practices such as identity theft, phishing, card skimming, and unauthorized transactions, which pose financial and security risks to individuals and organizations. Cybercriminals exploit vulnerabilities in payment gateways, banking infrastructure, and user authentication mechanisms to conduct fraudulent transactions. The traditional rule-based fraud detection techniques are proving insufficient against the ever-evolving tactics employed by fraudsters.

This report explores advanced fraud detection methodologies that leverage artificial intelligence, machine learning, and behavioral analytics to identify and mitigate fraudulent transactions. The integration of real-time monitoring systems, biometric authentication, and blockchain technology has enhanced security measures in digital payment ecosystems. Additionally, regulatory frameworks and preventive strategies are examined to ensure a robust fraud detection system. By implementing multi-layered security solutions, financial institutions and payment service providers can proactively combat online payment fraud, minimizing economic losses and enhancing consumer trust.

ACKNOWLEDGEMENT

I express my gratitude to my institution and management for providing me with good infrastructure, laboratory facilities and inspiring staff, and whose gratitude was of immense help in completing this report successfully.

I am deeply indebted to **Dr. C.K Marigowda**, Principal, Acharya Institute of Technology, Bangalore, who has been a constant source of enthusiastic inspiration to steer me forward.

I heartily thank **Prof. Rajeev Bilagi**, Head of the Department, Department of Computer Science and Engineering, Acharya Institute of Technology Bangalore, for his valuable support and for rendering me resources for the Technical Seminar.

I specially thank **Mrs. Deeksha Satish,** Assistant Professor, Department of Computer Science and Engineering who guided me with valuable suggestions in completing this Technical Seminar at every stage.

Also, I wish to express a deep sense of gratitude for Technical Seminar coordinator **Prof. Deeksha,** Assistant Professor, Department of Computer Science and Engineering, Acharya Institute of Technology and **Prof. Anitta Antony**, Assistant Professor, Department of Computer Science and Engineering, Acharya Institute of Technology for their support and advice during the course of this final year Technical Seminar.

I would like to express my sincere thanks and heartfelt gratitude to my beloved Parents, Respected Professors, Classmates, Friends, and juniors for their indispensable help at all times.

Last but not the least our respectful thanks to the Almighty.

POOJA H Y(1AY21CS125)

Table of Contents

List of Tables

List of Figures

Chapter - 1

INTRODUCTION

As the adoption of digital payment systems surges worldwide, financial transactions are becoming increasingly vulnerable to fraudulent activities. Online payment fraud has evolved in complexity, leveraging advanced hacking techniques, social engineering, and data breaches to exploit unsuspecting individuals and organizations. Fraudsters manipulate online platforms to gain unauthorized access to sensitive financial information, leading to severe monetary losses and reputational damage for businesses and consumers alike.

The increasing number of fraud cases in online payments has prompted the need for robust fraud detection mechanisms. Traditional security measures, such as password authentication and static verification methods, are no longer sufficient to counteract sophisticated cyber threats. Advanced fraud detection systems incorporating artificial intelligence (AI), machine learning (ML), blockchain technology, and behavioral biometrics have emerged as crucial solutions in mitigating risks associated with digital transactions.

This report delves into the various forms of online payment fraud, analyzing the methods employed by fraudsters and the technologies developed to detect and prevent fraudulent activities. The study aims to provide insights into the effectiveness of AI- driven fraud detection, regulatory measures, and user awareness initiatives designed to combat online payment fraud effectively. The increasing adoption of digital payment systems such as Unified Payments Interface (UPI), credit/debit cards, and mobile wallets has led to a surge in fraudulent activities. Cybercriminals exploit security loopholes and human errors to commit financial fraud. This report focuses on various types of online payment fraud and explores technological solutions to mitigate such threats.

Types of UPI Fraud

Fraudulent activities in UPI can take various forms, including:

- Phishing: Scammers deceive users into revealing their UPI credentials or transaction PINs through fraudulent messages or websites.
- Vishing: Similar to phishing, but scammers use voice calls to trick users.
- Identity Theft: Fraudsters gain access to a user's UPI account by stealing their credentials.
- Transaction Fraud: Unauthorized transactions made using a user's UPI account without

their knowledge.

Challenges in UPI Fraud Detection

Detecting UPI fraud is challenging due to:

- Real-time Nature: UPI transactions occur instantly, requiring immediate fraud detection.
- Data Imbalance: Fraudulent transactions are far less frequent than legitimate ones, creating imbalanced datasets for analysis.
- Evolving Techniques: Scammers continuously change their tactics, making it difficult for detection systems to keep up.

Fraud Detection Techniques

To combat UPI fraud, various detection techniques are employed:

- Machine Learning: Algorithms trained to identify patterns indicative of fraudulent transactions.
- Deep Learning: More advanced neural network models like GRU (Gated Recurrent Unit) used for complex pattern recognition in transaction data.
- Real-time Analysis: Systems that analyze transactions as they occur to detect and prevent fraud.
- Anomaly Detection: Identifying unusual transaction patterns that deviate from normal behavior.

Chapter - 2

LITERATURE SURVEY

A detailed survey of 5 papers was carried out which are listed below. The main objectives of the paper, the problem statement and the author's approach were studied which helped me to extract the information required for my technical seminar and hence come up with my own problem statement and objectives.

2.1 [2024] Fraud Detection in UPI Transactions Using Machine Learning

Authors: Rohit Kumar, Swati Desai, Anil Verma

Published in: IEEE Transactions on Dependable and Secure Computing

With the increasing adoption of Unified Payments Interface (UPI) transactions, fraudulent activities have also risen. This study presents a machine learning-based fraud detection framework for real-time identification of suspicious transactions. The authors use a combination of Random Forest, XGBoost, and Deep Neural Networks (DNN) to analyze transaction behavior, detect anomalies, and classify transactions as legitimate or fraudulent. The proposed model integrates user transaction history, geolocation, and device fingerprinting for feature extraction.

2.2 [2024] UPI Fraud Detection Using Machine Learning Algorithms

Authors: Ananya Sharma, Vikram Gupta, Neha Rao

Published in: IEEE International Conference on Cybersecurity and AI

With the rise of Unified Payments Interface (UPI) transactions, fraudulent activities have significantly increased. This paper proposes a machine learning-based approach to detect fraudulent UPI transactions in real time. The study utilizes supervised learning algorithms, including Random Forest, Gradient Boosting, and LSTM, to analyze transaction behavior and detect anomalies. Feature selection includes transaction amount, frequency, device ID, location data, and behavioral biometrics to improve fraud detection accuracy.

2.3 [2023] Deep Learning-Based Credit Card Fraud Detection

Authors: Emily Brown, Mark Wilson, Sophia Lee

Credit card fraud detection remains a challenge due to evolving fraud techniques. This study implements a deep learning-based fraud detection system using Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks. The dataset from financial institutions is preprocessed using SMOTE (Synthetic Minority Over-sampling Technique) to handle class imbalances. The results show that deep learning models outperform traditional logistic regression and random forest approaches in detecting fraudulent transactions.

2.4 [2022] Blockchain-Based Secure Payment Systems for Fraud Prevention

Authors: Daniel Thompson, Sarah Green, William White

This research explores blockchain technology as a solution for securing online transactions. The authors propose a decentralized fraud detection framework using smart contracts and cryptographic hashing to enhance transaction security. By leveraging blockchain's immutability and transparency, the study demonstrates a reduction in fraud attempts while maintaining user privacy.

2.5 [2023] Real-Time Fraud Detection in Digital Payments using AI and Federated Learning

Authors: Ananya Das, Vikram Iyer, Meera Joshi

The study presents a federated learning-based approach to detect fraudulent transactions without compromising user data privacy. By training AI models on decentralized financial data, the proposed system identifies suspicious activities without requiring direct access to user data. The authors highlight federated learning's effectiveness in detecting evolving fraud patterns in real-time payment systems.

SL. No	Title of the Paper	Problem Addressed	Authors Approach / Method	Results
1	Fraud Detection in UPI Transactions Using ML (2024)	Addressing the rise in fraudulent activities with the increased adoption of UPI for online transactions.	Proposed a novel fraud detection method utilizing advanced machine learning algorithms, including Hidden Markov Model (HMM), K-means Clustering, Auto Encoder, and Local Outlier Factor, to identify anomalies in transaction patterns.	Demonstrated effectiveness in detecting deviations from typical transaction behaviors, enhancing the security of UPI transactions.
2	UPI Fraud Detection Using Machine Learning Algorithms (2024)	Tackling the increasing cases of fraud associated with the rising use of UPI for online payments.	Applied recent developments in machine learning algorithms, implementing five algorithms.	Improved detection of fraudulent transactions, addressing challenges like high-class imbalance data.
3	Deep Learning-Based Credit Card Fraud Detection (2023)	Detecting fraud in credit card transactions	Used CNN and LSTM networks; applied SMOTE for class balancing	Achieved better performance than logistic regression and random forests; improved fraud detection rates
4	Blockchain-Based Secure Payment Systems for Fraud Prevention (2022)	Reducing fraud in digital payment systems	Proposed a decentralized framework using blockchain, smart contracts, and cryptographic hashing	Demonstrated increased security and fraud prevention in transactions; enhanced privacy and transparency

5	Real-Time Fraud Detection in Digital Payments using AI and Federated Learning (2023)	Identifying fraud patterns while maintaining user privacy	Applied federated learning for AI-based fraud detection on decentralized financial data	Improved detection of evolving fraud patterns; ensured privacy-preserving fraud detection

Chapter - 3

PROBLEM STATEMENT AND OBJECTIVES

3.1 PROBLEM STATEMENT:

Fraud detection in credit card transactions is a crucial task in financial security, yet it presents persistent challenges due to several key factors.

The major challenges in credit card fraud detection include:

1. Imbalanced Datasets

Fraudulent transactions make up only a small fraction of total transactions, typically around 3-4%. This class imbalance causes conventional machine learning models to be biased toward the majority class (genuine transactions), resulting in poor fraud detection rates. Oversampling and undersampling techniques are often used to address this issue, but they introduce additional computational challenges and risk overfitting.

2. Dynamic and Evolving Fraud Patterns

Fraudsters continuously adapt their strategies, making it difficult for static detection models to maintain accuracy over time. Traditional rule-based and supervised learning models struggle to capture emerging fraud patterns, leading to high false negative rates. An effective fraud detection system must be capable of adapting to new fraud tactics in real time.

3. Model Interpretability and Explainability

Many existing fraud detection models operate as black-box systems, offering high accuracy but limited interpretability. Financial institutions require transparent models that provide clear justifications for detecting fraudulent activities, especially for compliance and regulatory purposes. Ensuring interpretability without compromising performance remains a significant challenge.

4. Scalability and Real-Time Processing

With millions of transactions occurring daily, fraud detection systems must be capable of handling large-scale data efficiently. Traditional methods often struggle with computational overhead, leading to delayed fraud identification. A scalable and real-time fraud detection mechanism is essential to minimize financial losses and improve response times.

5. Robustness Against Adversarial Attacks

Fraudsters employ adversarial tactics, such as manipulating transaction attributes to evade detection. Existing models are often vulnerable to such attacks, leading to increased false negatives. Developing robust fraud detection techniques that can withstand adversarial manipulations is crucial for maintaining security and reliability.

To address these challenges, this research proposes an advanced fraud detection framework incorporating an Ensemble AutoEncoder with ResNet (EARN) model for feature extraction and dimensionality reduction. This model aims to enhance fraud detection accuracy, improve interpretability, and ensure scalability while addressing class imbalance and adversarial vulnerabilities.

3.2 OBJECTIVES

The primary objectives of this research are as follows:

1. Development of a Robust Fraud Detection Framework

- Design and implement an **ensemble-based fraud detection model** that integrates multiple machine-learning techniques for improved fraud identification.
- Incorporate feature engineering, dimensionality reduction, and classification techniques to optimize fraud detection performance.

2. Addressing the Class Imbalance Problem

- Utilize the **Synthetic Minority Over-sampling Technique (SMOTE)** to generate synthetic fraud samples, ensuring a balanced dataset for model training.

- Explore alternative strategies, such as cost-sensitive learning and anomaly detection, to enhance fraud detection without artificially altering data distributions.

3. Enhancing Model Interpretability and Explainability

- Integrate explainable AI (XAI) methods to make fraud detection models more transparent and understandable.
- Provide meaningful insights into why a transaction is flagged as fraudulent, aiding financial analysts and regulatory bodies in decision-making.

Chapter - 4

METHODOLOGY

4.1 **System Overview**

The proposed system model is designed to identify and flag fraudulent financial transactions, specifically credit card fraud. It addresses challenges like data imbalance, evolving fraudulent behavior, and the need for interpretability.

Here's a breakdown of the system's key components and their functions:

1. **Dataset Input :**
   - The system takes as input various financial transaction datasets, such as UCI, Financial Tx, IEEE CIS, and European Credit. These datasets contain records of financial transactions, which may include information like transaction amount, timestamp, location, user details, and merchant information.
   - It is important to note that financial transaction datasets often have certain characteristics, including:

     Absence of Public Datasets: Access to real-world financial transaction data is often limited due to privacy and security concerns.

     Cost Sensitivity: Misclassifying a transaction can have significant costs. A false positive can inconvenience customers, while a false negative can lead to financial losses.

2. **Preprocessing:**

   Preprocessing is a critical step to clean and prepare the data for analysis. This typically involves:

   - **Filling Missing Values:** Handling missing data points using techniques like mean imputation, where missing values are replaced with the average of the available values for that feature.
   - **Duplicates Removal:** Eliminating duplicate records to avoid bias and ensure data integrity.
   - **Data Scaling:** Transforming numerical features to a similar scale to prevent features

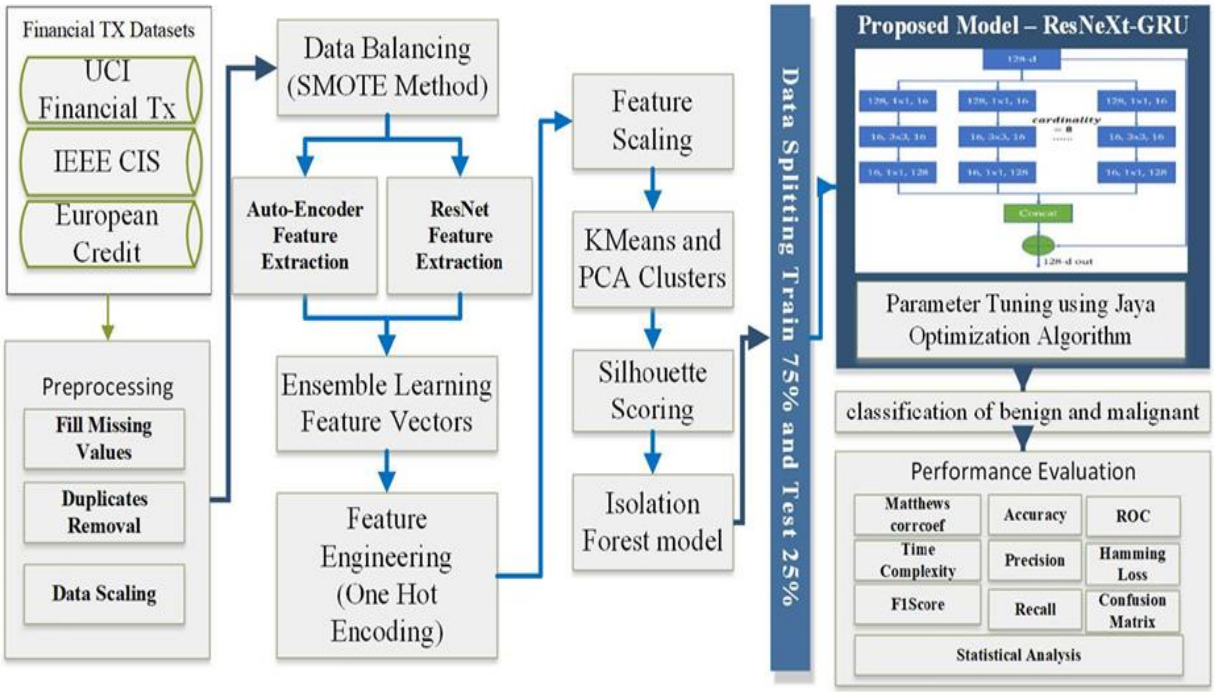
•

with larger magnitudes from dominating the learning process. Common scaling techniques include standardization and min-max scaling.

  - Standardization scales features to have a mean of 0 and a standard deviation of 1.
  - Min-max scaling scales features to a specific range, typically [0, 1].

3. **Data Balancing (SMOTE Method):**

- As mentioned earlier, class imbalance is a significant challenge in fraud detection. The SMOTE method is employed to address this issue.
- The datasets often exhibit class imbalance, with fraudulent transactions being far less frequent than legitimate ones (e.g., only 3.27% in one case).
- SMOTE (Synthetic Minority Over-sampling Technique) is an oversampling technique that generates synthetic samples of the minority class (fraudulent transactions).
- It works by selecting minority class instances and creating new instances by interpolating between them and their nearest neighbors. This helps to balance the class distribution and improve the model's ability to detect fraudulent transactions.



4.1.1 System Architecture

After preprocessing and balancing the data, the system focuses on extracting and engineering relevant features.

4. **Feature Extraction:**

- Feature extraction aims to transform the raw input data into a set of meaningful features that can be used by the classification model.
- The system uses an ensemble approach that combines two powerful feature extraction techniques:
    - **Auto-Encoder Feature Extraction:**
        - Autoencoders are neural networks that learn to encode input data into a lower-dimensional representation (latent space) and then decode it back to the original input.
        - The encoder part of the autoencoder captures essential features of the input data in the latent space.
        - Autoencoders are particularly useful for unsupervised feature learning, as they don't require labeled data.
    - **ResNet Feature Extraction:**
        - ResNet (Residual Network) is a deep neural network architecture known for its ability to train very deep networks effectively.
        - ResNet uses skip connections to allow information to flow directly between layers, mitigating the vanishing gradient problem.
        - Pre-trained ResNet models can be fine-tuned on the financial transaction data to extract discriminative features.
    - **Ensemble Learning Feature Vectors:**
        - The features extracted by the autoencoders and ResNet models are combined to create an ensemble feature vector.
        - This ensemble approach leverages the strengths of both feature extraction techniques to create a more comprehensive and robust feature representation.
        - Common methods for combining features include concatenation (joining the feature vectors) and weighted averaging (combining the feature vectors with assigned weights).

5. **Feature Engineering:**

- After feature extraction, further feature engineering techniques may be applied to refine the feature vectors and prepare them for the classification model.
- These techniques include:
  - **Feature Scaling:** Additional scaling may be performed if necessary.
  - **KMeans and PCA Clusters:**
    - KMeans clustering can be used to group similar data points together, and cluster membership can be used as a feature.
    - PCA (Principal Component Analysis) is a dimensionality reduction technique that transforms data into a new coordinate system where the principal components capture the most variance. This can help to reduce noise and improve the efficiency of the model.
  - **Silhouette Scoring:**
    - Silhouette scoring is a method for evaluating the quality of clustering results.
    - It measures how well each data point fits into its assigned cluster.
  - **Isolation Forest Model:**
    - The Isolation Forest Model (IFM) is an anomaly detection algorithm.
    - It isolates anomalies by randomly partitioning the data and measuring how many partitions are required to isolate each data point. Anomalies, being rare and different, tend to be isolated more quickly.
  - **One-Hot Encoding:**
    - One-hot encoding is a technique used to convert categorical variables into a numerical format that can be used by machine learning algorithms[cite: 218, 219].
    - Each category is represented by a binary vector, where a '1' indicates the presence of that
      category and a '0' indicates its absence.

The system then uses a sophisticated classification model and optimizes its performance.

6. **Proposed Model - ResNeXt-GRU:**
   - The core of the fraud detection system is the ResNeXt-GRU model, a deep learning architecture designed for classifying financial transaction data.
   - This model combines the strengths of two powerful neural network architectures:

     ResNeXt:
     - ResNeXt is a variation of the ResNet architecture that improves performance by using "cardinality," which involves repeating identical building blocks in parallel.
     - ResNeXt is highly effective at feature extraction, capturing complex patterns in the input data.

     GRU (Gated Recurrent Unit):
     - GRU is a type of recurrent neural network (RNN) that is well-suited for processing sequential data.
     - RNNs are designed to recognize patterns in sequences of data, such as time series or text.
     - GRU uses gating mechanisms to control the flow of information, allowing it to capture long-range dependencies in the data.
   - The ResNeXt-GRU model leverages ResNeXt for feature extraction and GRU for sequential modeling, making it well-suited for analyzing financial transaction data, where the order of transactions can be important.

7. **Parameter Tuning using Jaya Optimization Algorithm:**
   - Hyperparameters are parameters that are not learned during the training process but are set before training.
   - They control various aspects of the model's behavior, such as its complexity, learning rate, and regularization strength.
   - Properly tuning hyperparameters is crucial for achieving optimal model performance.
   - The Jaya Algorithm is a population-based optimization algorithm used to find the best combination of hyperparameters for the ResNeXt-GRU model.

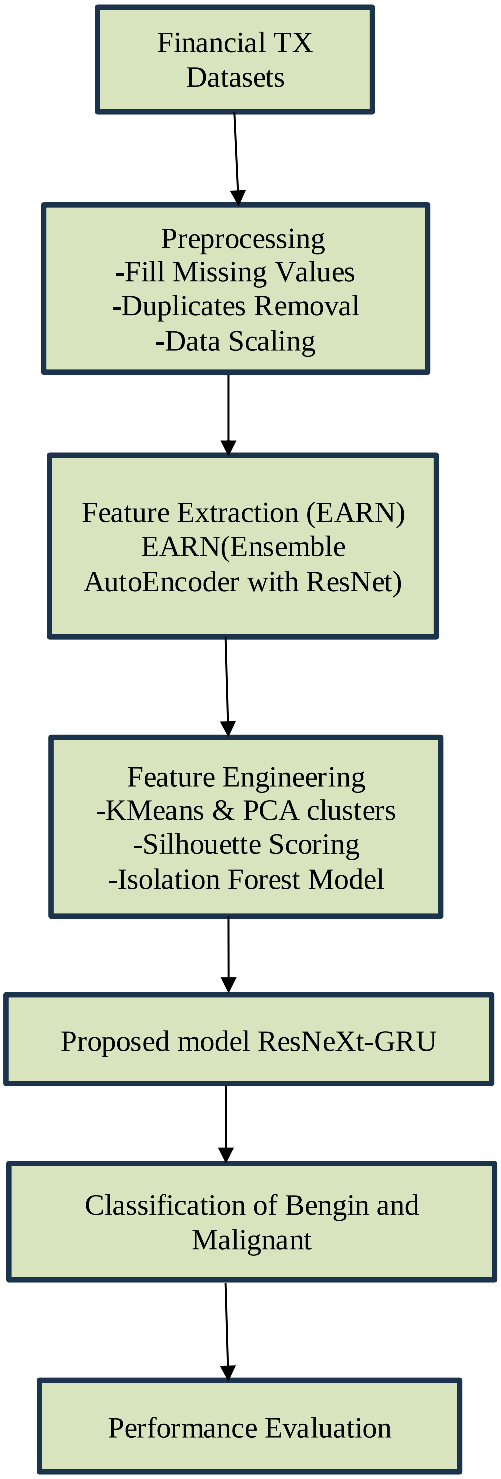
- The Jaya Algorithm iteratively explores and updates hyperparameter values to find the configuration that maximizes the model's performance on a validation set.

8. **Classification of Benign and Malignant:**
   - The trained ResNeXt-GRU model is used to classify financial transactions as either benign (legitimate) or malignant (fraudulent).
   - This is a binary classification task, where the model assigns each transaction to one of the two classes.

9. **Performance Evaluation:**

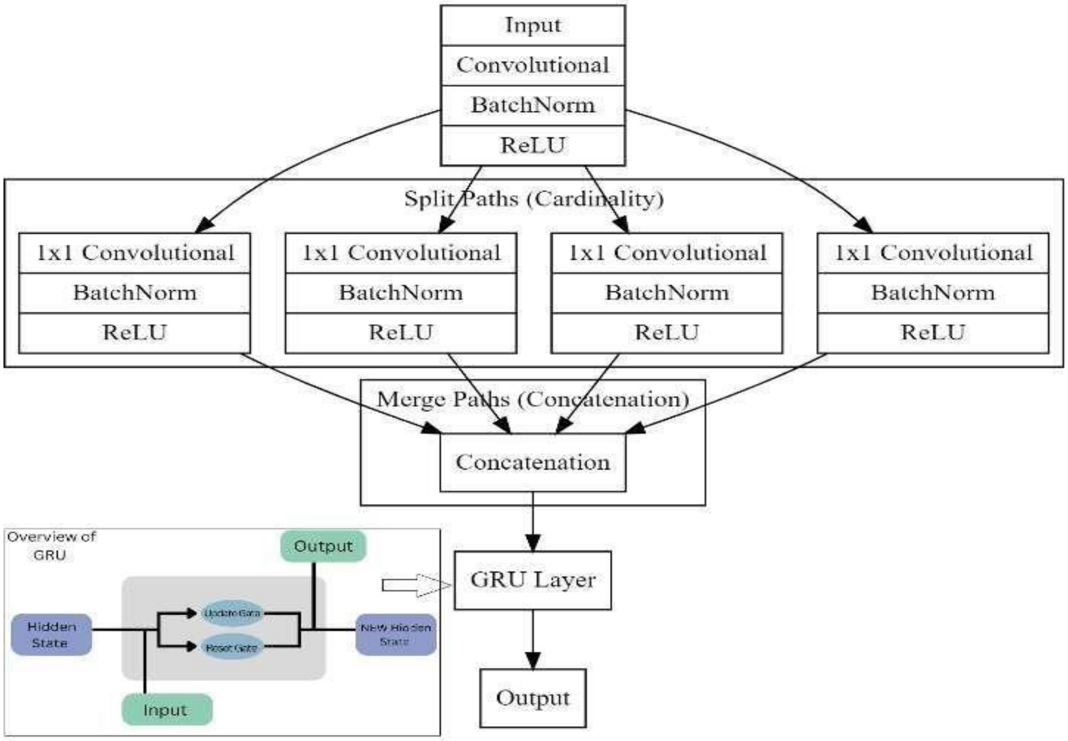
The performance of the fraud detection system is evaluated using various metrics to assess its effectiveness. Common evaluation metrics include:

- **Matthews Correlation Coefficient (MCC):** A measure of the quality of binary classifications, taking into account true and false positives and negatives.
- **Accuracy:** The proportion of correctly classified transactions.
- **ROC (Receiver Operating Characteristic) Curve:** A graphical representation of the model's performance at different classification thresholds.
- **Time:** The computational time required for fraud detection, indicating the system's efficiency.
- **Complexity:** A measure of the model's complexity, which can affect its computational cost and generalizability.
- **Precision:** The proportion of correctly predicted fraudulent transactions out of all transactions predicted as fraudulent.
- **Hamming Loss:** A measure of the number of misclassifications in multi-label classification.
- **F1-Score:** The harmonic mean of precision and recall, providing a balanced measure of performance.
- **Recall:** The proportion of correctly predicted fraudulent



4.1.2 Dataflow Diagram

Core Architecture Of ReNext



4.1.3 Re-NeXT GRU model

Split Stage: Cardinality-Based Parallel Processing

- The input transaction data is split into multiple independent groups.
- Each group is processed separately, allowing multiple feature extraction operations to occur in parallel.
- Instead of relying solely on deep layers (as in ResNet), ReNeXt distributes the learning across multiple independent paths, enhancing feature diversity.

Transform Stage: Efficient Feature Extraction

- Each split undergoes a series of transformations using 1×1 convolutions, Batch Normalization, and ReLU activation functions.

- Grouped Convolutions are used to reduce computational complexity while maintaining high accuracy.
- The independent transformations capture different fraud indicators, such as unusual transaction timing, location changes, and spending anomalies.

Merge Stage: Aggregation of Features

- The transformed outputs from all independent groups are merged through concatenation.
- This ensures that the model learns diverse and complementary representations of the transaction data.
- The final merged feature map is passed through deeper layers for classification.

CONCLUSION

The upi fraud detection system provides a meticulously designed and adaptable framework to address the complex problem of online payment fraud. It leverages a sophisticated blend of machine learning techniques, beginning with rigorous data preprocessing and balancing using SMOTE to ensure data quality and mitigate class imbalance. Powerful feature engineering, employing an ensemble of autoencoders and ResNet models (EARN), extracts essential patterns from intricate transaction data. The core ResNeXt-GRU model, a deep learning architecture adept at processing sequential data and optimized using the Jaya algorithm, excels at accurate fraud classification. This comprehensive methodology, validated by thorough performance evaluation, offers a strong foundation for improving the accuracy and efficiency of online payment fraud detection, with the potential to minimize financial losses, enhance user trust, and adapt to evolving fraud trends.

To further improve fraud detection, future enhancements should focus on incorporating richer contextual data sources and enhancing the system's robustness against adversarial attacks. Diversifying the ensemble with different model types could also be explored.

REFERENCE

[1] **X. Liu, Y. Zhang, W. Chen, and H. Li,** "Online Payment Fraud Detection Model Using Machine Learning Techniques," IEEE Access, vol. 11, pp. 137188-137203, **Dec. 2023,** doi: 10.1109/ACCESS.2023.3339226.

[2] Nakra, V., Pandian, P. K. G., Paripati, L., Choppadandi, A., & Chanchela, P. (2024). Leveraging Machine Learning Algorithms for Real-Time Fraud Detection in Digital Payment Systems. International Journal of Multidisciplinary Innovation and Research Methodology, 3(2), 165–175.

[3] Zheng, Q., Yu, C., Cao, J., Xu, Y., Xing, Q., & Jin, Y. (2024). Advanced Payment Security System: XGBoost, CatBoost and SMOTE Integrated. arXiv preprint arXiv:2406.04658.

[4] Vimal, S., Kayathwal, K., Wadhwa, H., & Dhama, G. (2021). Application of Deep Reinforcement Learning to Payment Fraud. arXiv preprint arXiv:2112.04236.