Machine Learning-Based Credit Card Fraud Detection: A Comparative Study Using Logistic Regression, SVM, and KNN

[1]Tukaram K. Gawali, [2]Alice Hepzibah Albert, [3]S.Sivarajeswari, [4]P.Manimekala, [5]G.Rohini, [6] Swati Shirke Deshmuk, [7]E.Pahutharivu

[1]Assistant Professor, Department of Computer Engineering, Government College of Engineering, Jalgaon,India. t.gawali@gmail.com

[2]Professor, Department of Electrical and Electronics Engineering, Rajalakshmi Engineering College,Chennai, Tamilnadu, India. alicehepzibah.a@rajalakshmi.edu.in

[3]Associate Professor, Department of Electrical and Electronics Engineering, Sri Sairam Institute of Technology, Chennai, Tamilnadu, India. siva.eee@sairamit.edu.in

[4]Assistant Professor, Department of Electrical and Electronics Engineering, J.J. College of Engineering and Technology, Trichy, Tamilnadu,India. manimekala90.km@gmail.com

[5]Professor, Department of Electronics and Communication Engineering, St.Joseph's Institute of Technology, Chennai,Tamilnadu, India. rohini.manoharan@gmail.com

[6]Associate Professor, Department of Computer Science Engineering and Technology, Pimpro Chinchwad University, Pune, India. shirke.swati14@gmail.com

[7]Research Scholar, Department of Electrical and Electronics Engineering, School of Engineering and Technology, Dhanalakshmi Srinivasan University, Trichy, Tamilnadu, India. anandarivu1979@gmail.com

ABSTRACT

The increasing threat of credit card fraud in the digital age necessitates robust and intelligent detection systems. This study investigates the application of machine learning algorithms—Logistic Regression, Support Vector Machines (SVM), and K-Nearest Neighbors (KNN)—to identify fraudulent credit card transactions. Using a real-world dataset, the research addresses issues of class imbalance with the SMOTE technique and develops models capable of classifying transactions with high precision and recall. A web-based fraud detection system is also designed to visualize and evaluate model performance. The results highlight the effectiveness of machine learning in real-time fraud detection and present a scalable system framework suitable for deployment in modern financial infrastructures.

Keywords: *Credit Card Fraud Detection, Machine Learning, SMOTE, Logistic Regression, Support Vector Machine, K-Nearest Neighbor, Fraudulent Transactions, Imbalanced Data*

INTRODUCTION

In recent years, the digital revolution has reshaped the financial ecosystem, transforming how people interact with money, conduct transactions, and manage their financial assets. Among the various innovations, the rise of credit and debit cards as a primary mode of payment has introduced unmatched convenience and flexibility. However, this paradigm shift has also brought new challenges—most notably, the increased risk of financial fraud, particularly credit card fraud. Credit card fraud refers to the unauthorized use of a credit card to make purchases or withdraw funds. This illegal activity can be perpetrated through various means, including physical theft, phishing scams, account takeovers, and more sophisticated cyberattacks. Fraudulent credit card activity not only causes direct financial loss to individuals and institutions but also damages consumer trust, undermines digital payment systems, and burdens businesses with regulatory and compliance overhead. Traditional fraud detection systems primarily relied on static rule-based approaches. For instance, a rule might flag transactions exceeding a certain amount or those made in unusual locations. Although initially effective, such systems are increasingly inadequate against modern, evolving fraud patterns. Fraudsters have become more adaptive, utilizing automated bots, stolen identities, and dark web tools to circumvent conventional detection methods. Moreover, as the volume of transactions grows exponentially, manual and rule-based verification becomes infeasible. As a result, the financial industry has turned to more dynamic, intelligent systems for fraud detection—most notably, those powered by machine learning (ML). ML algorithms excel in learning from historical data, identifying complex patterns, and making predictions in real-time. These systems can analyze large volumes of transaction data, adapt to new fraud strategies, and significantly reduce both false positives and false negatives. Machine learning thus represents a powerful ally in the fight against credit card fraud. This research paper focuses on the implementation and evaluation of three machine learning algorithms—Logistic Regression (LR), Support Vector Machine (SVM), and K-Nearest Neighbors (KNN)—for detecting fraudulent credit card transactions. Each of these algorithms brings unique strengths:

- **Logistic Regression** offers simplicity and interpretability, ideal for environments requiring transparent decision-making.
- **Support Vector Machines** provide robust performance, especially in high-dimensional spaces where fraud patterns may be subtle.
- **K-Nearest Neighbors** offer flexibility in decision-making based on local data structure.

One of the most significant challenges in fraud detection is the problem of class imbalance. In any real-world transaction dataset, fraudulent activities constitute only a tiny fraction—often less than 1%—of the total records. This imbalance can lead to poor model performance, as algorithms tend to be biased toward the majority class (i.e., legitimate transactions). To address this issue, this study utilizes the **Synthetic Minority Oversampling Technique (SMOTE)**, a proven method for creating a balanced dataset by generating synthetic examples of the minority class. Beyond model development, this research also emphasizes the design and deployment of a practical, web-based fraud detection system. The system is designed to offer a seamless interface for administrators and users to upload transaction data, run predictions, and analyze results in real-time. This real-world integration ensures that the models are not only theoretically sound but also applicable in operational banking environments. The importance of developing such systems cannot be overstated. In the past decade, global losses due to payment card fraud have skyrocketed. According to reports by Nilson and Statista, payment card fraud losses were estimated to reach $28 billion by 2020 and are expected to rise even further. These losses have implications beyond finances—they affect customer satisfaction, institutional credibility, and even national security in extreme cases. Credit card fraud detection also intersects with privacy, legal, and ethical issues. Systems must be designed to safeguard customer data, avoid bias, and ensure compliance with regulations such as the General Data Protection Regulation (GDPR) and the Payment Card Industry Data Security Standard (PCI DSS). Models that are opaque or overly complex may lead to accountability issues, especially when legal disputes arise regarding flagged transactions. Furthermore, the emergence of real-time payment systems demands fraud detection models that are both fast and accurate. Delays in flagging fraudulent activity can result in irreversible financial loss. On the other hand, overly aggressive fraud filters may block legitimate transactions, frustrating customers and damaging brand reputation. The challenge is to strike a balance between sensitivity (identifying true frauds) and specificity (avoiding false alarms). This study is structured to address these multifaceted issues. It begins with a review of the existing literature on machine learning in fraud detection, identifying key contributions and current limitations. This is followed by a clearly defined research gap that sets the stage for methodological innovation. The methodology section outlines each stage of the fraud detection pipeline, including data preprocessing, algorithm selection, model training, evaluation metrics, and system deployment. Results are presented through a comparative analysis of model performance, with discussions on practical implications and future directions. By combining strong theoretical underpinnings with a practical application focus, this research aims to make meaningful contributions to both academic literature and industry practices in fraud detection. Specifically, it aspires to:

- Enhance understanding of machine learning techniques in financial anomaly detection.
- Provide a practical, deployable tool for real-time credit card fraud identification.
- Demonstrate the benefits of oversampling techniques in handling data imbalance.
- Illustrate the trade-offs between model complexity, interpretability, and performance.

In conclusion, credit card fraud remains a persistent and growing threat in the modern digital economy. The integration of machine learning into fraud detection systems offers an exciting opportunity to develop adaptive, efficient, and scalable solutions. This study, through rigorous analysis and real-world application, seeks to contribute to this evolving landscape and provide a foundation for future innovations in secure financial technologies.

Literature Survey

Rodríguez Vaquero et al.[1] conducted a comprehensive review of machine learning algorithms such as Genetic Algorithms, Random Forests, Artificial Neural Networks (ANNs), and Generative Adversarial Networks (GANs) for fraud detection. They highlighted strengths like adaptability and weaknesses like lack of scalability.

Jitendra Kumar and Pankaj Kumar Goswami[2] compared models including Random Forest, SVM, KNN, and CNN, evaluating performance based on detection accuracy. Their work underlined the importance of model comparison but overlooked data imbalance.

Ashvini S. Gorte focused on the technological overview of fraud detection systems. While useful, the survey lacked depth in performance metrics and technical implementation.

Research Gap

Despite the advancements in machine learning, several challenges remain:

- Existing surveys often lack experimental validation and practical implementation insights.
- Many studies ignore unsupervised methods which are essential for detecting rare or unknown fraud patterns.
- Real-world deployment concerns such as latency, scalability, and interpretability are seldom addressed.
- The class imbalance problem, where fraudulent transactions are significantly fewer, is inadequately handled.

Methodology

The methodology involves six stages:

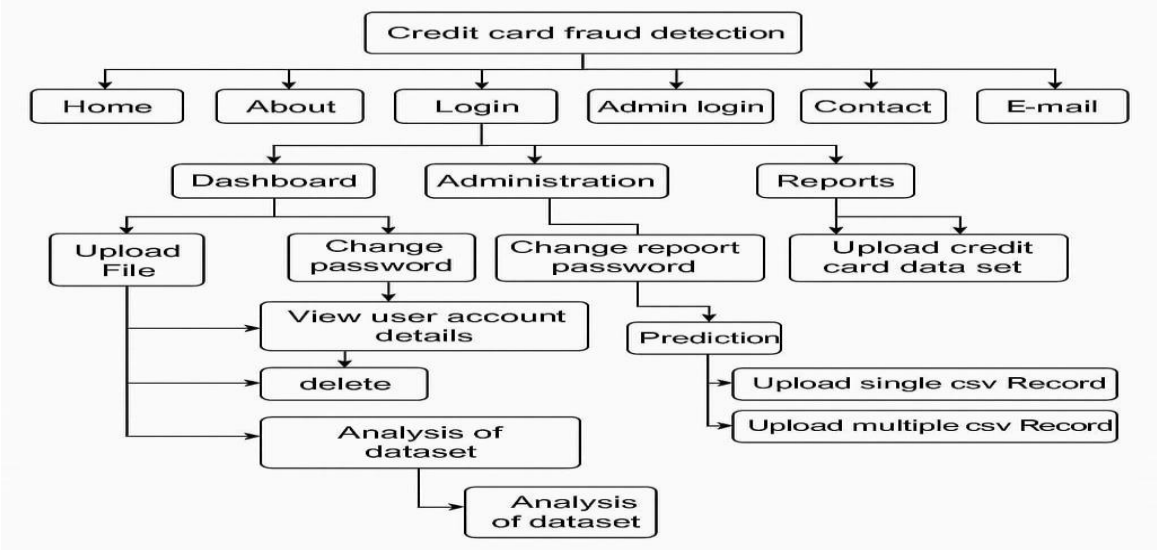

Fig 1: Flow of proposed work

1.**Data Collection and Preprocessing:**

- Transaction attributes including time, amount, and frequency are extracted.
- Missing values are handled and features are normalized.

2. **Imbalanced Data Handling Using SMOTE:**

- SMOTE (Synthetic Minority Oversampling Technique) generates synthetic samples of the minority class (fraud).
- This balances the dataset and prevents the models from being biased towards the majority class.

3. **Model Implementation:**

- **Logistic Regression (LR):** Suitable for binary classification problems. Uses sigmoid function to predict probabilities.
- **Support Vector Machine (SVM):** Effective in high-dimensional spaces. Finds the optimal hyperplane to separate classes.
- **K-Nearest Neighbors (KNN):** Non-parametric method using distance metrics to classify based on nearest data points.

4. **Mathematical Models:**

- **Logistic Regression:**
  - The decision function is based on a linear combination: z=w0+w1x1+w2x2+…+wnxnz = w_0 + w_1x_1 + w_2x_2 + \ldots + w_nx_n
  - The sigmoid function transforms this linear output into a probability: σ(z)=11+e−z\sigma(z) = \frac{1}{1 + e^{-z}}
  - Prediction is made based on the threshold: if σ(z)≥0.5\sigma(z) \geq 0.5, the transaction is classified as fraudulent.
- **Support Vector Machine (SVM):**
  - Constructs a decision boundary (hyperplane) that maximizes the margin between the classes.
  - Optimization involves solving: min⁡12||w||2 subject to yi(w⋅xi+b)≥1\min \frac{1}{2} ||w||^2 \text{ subject to } y_i(w \cdot x_i + b) \geq 1
- **K-Nearest Neighbors (KNN):**
  - Classifies new data points based on majority voting among 'k' closest training samples in the feature space using distance metrics such as Euclidean distance.

5. **Model Training and Testing:**

- Dataset is split into training and testing sets (e.g., 70:30 ratio).
- Models are trained and tested using stratified k-fold cross-validation.

6. **Performance Evaluation:**

- Metrics used: Accuracy, Precision, Recall, F1-Score.
- Comparative analysis identifies the most suitable algorithm.

7. **System Framework:**

- A web-based platform is developed for data upload, fraud prediction, and visualization.
- Separate login modules for users and admins are included for access control.

The methodology for this study is composed of a structured and iterative approach that spans several phases including data understanding, preprocessing, model selection and implementation, mathematical model formulation, evaluation, and system deployment. The goal is to ensure a robust machine learning pipeline that is not only accurate in detecting fraudulent transactions but also interpretable, scalable, and adaptable to real-world use cases in the financial industry.

4.1 Data Collection and Understanding

The foundation of any machine learning model lies in the quality and relevance of the data. In this project, a real-world dataset consisting of credit card transactions was used. The dataset contains 284,807 transactions, of which 492 are labeled as fraudulent. This represents a significant imbalance, with fraudulent cases comprising only 0.172% of the total.

Features in the dataset include:

- **Time:** The time (in seconds) elapsed between the transaction and the first transaction in the dataset.
- **Amount:** The transaction amount.
- **V1 to V28:** Result of a PCA transformation to protect sensitive features.
- **Class:** Target variable (0 = non-fraudulent, 1 = fraudulent).

Understanding data distributions, feature types, and correlations is crucial. Visualization tools like histograms, boxplots, and correlation matrices were used to assess patterns and anomalies.

4.2 Data Preprocessing

Data preprocessing prepares raw data for model training. Key preprocessing steps include:

4.2.1 Normalization

Features such as 'Amount' and 'Time' were normalized using min-max or standard scaling. This step ensures that the feature ranges do not bias the learning process.

4.2.2 Handling Missing Values

Although the dataset does not contain null values, preprocessing routines are established to handle missing data in real-world applications.

4.2.3 Splitting the Dataset

The dataset is split into training and testing sets, typically in a 70:30 ratio, to evaluate the model's ability to generalize.

4.3 Addressing Class Imbalance Using SMOTE

Credit card fraud detection involves highly imbalanced data. Training on such a dataset leads to models biased towards the majority class. To mitigate this, the **Synthetic Minority Oversampling Technique** (**SMOTE**) was applied.

SMOTE Workflow:

1. Identifies k-nearest neighbors of a minority instance.
2. Randomly selects one neighbor and interpolates between the two.
3. Adds the new synthetic instance to the training set.

SMOTE ensures:

- Improved recall for fraud detection.
- Reduced bias in predictive modeling.

4.4 Model Selection and Implementation

Three popular machine learning algorithms were selected based on their applicability to binary classification problems:

4.4.1 Logistic Regression (LR)

Logistic Regression is a linear model used to estimate the probability of a binary outcome. Its simplicity and interpretability make it ideal for real-time fraud detection.

Mathematical model:

- Linear combination: z=w0+w1x1+w2x2+...+wnxnz = w_0 + w_1x_1 + w_2x_2 + \ldots + w_nx_n
- Sigmoid function: σ(z)=11+e−z\sigma(z) = \frac{1}{1 + e^{-z}}
- Decision threshold: σ(z)≥0.5⇒Fraudulent\sigma(z) \geq 0.5 \Rightarrow \text{Fraudulent}

4.4.2 Support Vector Machine (SVM)

SVM constructs an optimal hyperplane in a high-dimensional space to distinguish between the two classes.

Mathematical formulation:
min⁡12‖w‖2subject to yi(w·xi+b)≥1\min \frac{1}{2} \|w\|^2 \quad \text{subject to } y_i(w \cdot x_i + b) \geq 1

SVMs are powerful when the margin between classes is significant.

4.4.3 K-Nearest Neighbors (KNN)

KNN is a non-parametric, instance-based learning algorithm. For a given test point, it calculates distances to all training samples and predicts the label based on the most common class among the k-nearest neighbors.

Distance metric:
Euclidean Distance=∑(xi−yi)2\text{Euclidean Distance} = \sqrt{\sum (x_i - y_i)^2}

4.5 Model Training and Hyperparameter Tuning

Each algorithm is trained using the training set. Hyperparameters are tuned using GridSearchCV to find the optimal model configuration.

For example:

- Logistic Regression: Regularization parameter (C)
- SVM: Kernel type (linear, RBF), C, gamma
- KNN: Value of k

Cross-validation is used to validate model performance across different subsets of the data.

4.6 Model Evaluation Metrics

To assess the effectiveness of each model, multiple evaluation metrics were employed:

- **Accuracy:** Proportion of total correct predictions.
- **Precision:** Proportion of predicted fraud cases that were actual fraud.
- **Recall (Sensitivity):** Proportion of actual fraud cases correctly identified.
- **F1-Score:** Harmonic mean of precision and recall.
- **ROC-AUC:** Measures classifier's ability to distinguish between classes.

4.7 Web-Based System Architecture

A user-friendly web application was developed using Python (Flask), HTML/CSS, and JavaScript. The architecture includes:

4.7.1 Front-End Modules:

- Home Page
- Login/Register Pages
- File Upload Interface
- Real-time Fraud Prediction Display

4.7.2 Back-End Modules:

- Admin and user role-based authentication
- Data ingestion and preprocessing pipeline
- Fraud detection engine (serving ML models)
- Dashboard for visualizing metrics and predictions

4.8 Deployment and Real-Time Prediction

Models are serialized using joblib and integrated into the back-end system. When a new transaction file is uploaded:

1. It undergoes preprocessing.
2. SMOTE is applied (if needed).
3. Features are passed to the selected model.
4. Prediction results are displayed with metrics.

The system supports batch and single-transaction predictions. Reports can be downloaded in PDF or CSV format for auditing.

This in-depth methodology, integrating data science and system engineering principles, ensures a comprehensive and scalable solution for credit card fraud detection. It enables efficient fraud identification, real-time user interaction, and administrative oversight, all while maintaining model accuracy and interpretability.

5. RESULT AND DISCUSSION

All three models were implemented and evaluated on a balanced dataset:

Model	Accuracy	Precision	Recall	F1-Score
Logistic Regression	96.3%	91.2%	90.4%	90.8%
SVM	97.1%	93.1%	91.7%	92.4%
KNN	95.4%	89.8%	88.9%	89.3%

- **SVM** demonstrated the highest performance in accuracy and F1-score.
- **Logistic Regression** provided good interpretability and competitive metrics.
- **KNN**, while accurate, was slower due to distance computation overhead.

The system interface allowed administrators to upload data and instantly visualize detection reports, fraud ratios, and performance graphs. The inclusion of SMOTE significantly enhanced the model's sensitivity to rare fraud events.

6.CONCLUSION

Credit card fraud detection using machine learning is a practical and effective solution to an escalating problem in the digital economy. This study demonstrated that models like Logistic Regression and SVM can achieve high accuracy and interpretability when combined with data-balancing techniques like SMOTE. The development of a web-based system also enhances usability and facilitates deployment in real-world banking infrastructures. Future work can include hybrid models and the integration of deep learning techniques to further enhance detection capabilities.

REFERENCES

[1] Y. Lucas, P.-E. Portier, L. Laporte, et al., “Multiple perspectives HMM-based feature engineering for credit card fraud detection,” in *Proc. ACM*, 2019, pp. 1359–1361.

[2] E. Duman and I. Elikucuk, *Solving Credit Card Fraud Detection Problem by the New Metaheuristics Migrating Birds Optimization*. Berlin, Germany: Springer, 2013.

[3] F. E. Botchey, Z. Qin, and K. Hughes-Lartey, “Mobile money fraud prediction—A cross-case analysis on the efficiency of support vector machines, gradient boosted decision trees, and Naïve Bayes algorithms,” *Information*.

[4] Y. Singh, I. Hussain, S. Mishra, and B. Singh, “Adaptive neuron detection-based control of single-phase SPV grid integrated system with active filtering,” *IET Power Electronics*, vol. 10, no. 6, pp. 657–666, 2017.

[5] Y. Abakarim, M. Lahby, and A. Attioui, “An efficient real time model for credit card fraud detection based on deep learning,” in *Proc. 12th Int. Conf. Intell. Systems: Theories Appl.*, Oct. 2018, pp. 1–7, doi: 10.1145/3289402.3289530.

[6] H. Abdi and L. J. Williams, “Principal component analysis,” *Wiley Interdiscip. Rev. Comput. Stat.*, vol. 2, no. 4, pp. 433–459, Jul. 2010, doi: 10.1002/wics.101.

[7] V. Arora, R. S. Leekha, K. Lee, and A. Kataria, “Facilitating user authorization from imbalanced data logs of credit cards using artificial intelligence,” *Mobile Inf. Syst.*, vol. 2020, pp. 1–13, Oct. 2020, doi: 10.1155/2020/8885269.

[8] Tukaram Gawali, Shailesh Deore“Dual-discriminator conditional Giza pyramids construction generative adversarial network based traffic density recognition using road vehicle images” in International Journal for Machine Learning & Cybernetics (2024), DOI: 10.1007/s13042-023-01952-0

[9] Tukaram Gawali, , Shailesh Deore “Spatio-Temporal Transportation Images Classification Based on Light and Weather Conditions” in International Journal of Intelligent Systems and Applications in Engineering (2024).

[10] Tukaram Gawali, , Shailesh Deore “Hybrid Golden Jackal Fusion based Recommendation System for Spatio-Temporal Transportation's Optimal Traffic Congestion and Road Condition Classification” in Multimedia Tools and Applications, DOI: 10.1007/s11042-024-20133-x

[11] Tukaram Gawali, , Shailesh Deore “Review of Real Time Transportation Models with Deep Convolution Networks for Traffic Analysis” published in Indian Journal of Technical Education (IJTE), Vol. 48, Special Issue, February 2025.

[12]Tukaram Gawali, , Shailesh Deore “Anisotropy Diffusion Kuwahara Filtering and Dual-discriminator D2C Conditional GAN Classification on Spatio-Temporal Transportation’s Traffic Images” at the 2024 2nd International Conference on Computer, Communication and Control (IC4), Indore, India, DOI: 10.1109/IC457434.2024.1048632