Journal of Information Systems Engineering and Management
2025, 10(10s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Detection of Credit Card Fraud Utilizing Transaction History Using Machine Learning

Mrs. Akshita Sunerah
Independent Researcher

ARTICLE INFO

Received: 14 Nov 2024

Revised: 26 Dec 2024

Accepted: 10 Jan 2025

ABSTRACT

Over the past several years, fraudulent credit card transactions have surged, posing significant challenges to financial institutions and consumers alike. In 2021, an annual study revealed that over 50% of Americans experienced credit or debit card fraud, with approximately 127 million individuals falling victim at least once. Traditional fraud detection techniques are often inadequate due to their reliance on manual processes and rule-based systems, which are both time-consuming and prone to errors. This paper explores the application of machine learning (ML) algorithms to enhance the accuracy and efficiency of credit card fraud detection. Six supervised ML algorithms—Naïve Bayes, Support Vector Machine (SVM), Random Forest, K-Nearest Neighbors (KNN), Logistic Regression, and XGBoost—are evaluated using transaction history data to classify fraudulent and non-fraudulent activities. The study employs a comprehensive methodology involving data preprocessing, feature engineering, and model training, followed by performance evaluation based on accuracy, precision, recall, and F1-score. Results indicate that the SVM model outperforms other algorithms, achieving the highest accuracy in fraud classification. The findings underscore the potential of ML in automating and improving fraud detection systems, thereby mitigating financial losses and enhancing trust in financial services.

Keywords: Credit Card Fraud Detection, Machine Learning, Supervised Learning, Transaction History, Support Vector Machine

Introduction

Credit card fraud remains a pervasive issue in the financial sector, causing substantial economic losses and undermining consumer trust. As digital transactions become increasingly ubiquitous, the volume and complexity of fraudulent activities have escalated, necessitating more sophisticated detection mechanisms. Traditional fraud detection systems predominantly rely on rule-based approaches and manual reviews, which are limited in their ability to adapt to evolving fraud patterns and scale with increasing transaction volumes. Consequently, there is a pressing need for automated, intelligent systems that can effectively identify and mitigate fraudulent transactions in real-time.

Machine learning (ML), a subset of artificial intelligence (AI), offers promising solutions for enhancing fraud detection capabilities. By leveraging historical transaction data, ML algorithms can learn complex patterns and relationships that distinguish legitimate transactions from fraudulent ones. Supervised learning algorithms, in particular, are well-suited for classification tasks where the goal is to categorize transactions based on labeled data indicating fraudulence. The application of ML in fraud detection not only improves accuracy but also significantly reduces the time and resources required for manual oversight.

The integration of ML into fraud detection systems involves several critical steps, including data collection, preprocessing, feature engineering, model selection, training, and evaluation. Effective data preprocessing ensures the quality and reliability of the input data, addressing issues such as missing values and class imbalances. Feature engineering enhances the model's ability to capture relevant indicators of fraud by transforming raw transaction data into meaningful features. Selecting the appropriate ML model is paramount, as different algorithms offer varying strengths in handling complex, high-dimensional data typical of financial transactions.

Previous studies have demonstrated the efficacy of various ML algorithms in fraud detection, with ensemble methods like Random Forest and boosting techniques such as XGBoost showing robust performance. However, the effectiveness of these models can vary based on the dataset characteristics and the specific features employed. This research aims to provide a comparative analysis of six supervised ML algorithms—Naïve Bayes, SVM, Random Forest, KNN, Logistic Regression, and XGBoost—in the context of credit card fraud detection using transaction history data.

The primary objectives of this study are:

1. To evaluate the performance of different ML algorithms in classifying fraudulent and non-fraudulent credit card transactions.
2. To identify key transaction features that significantly contribute to fraud detection.
3. To address common challenges in fraud detection, such as class imbalance and model interpretability.
4. To provide insights into the practical implementation of ML-based fraud detection systems in financial institutions.

The structure of this paper is as follows: Section II reviews related work in the domain of credit card fraud detection using ML. Section III outlines the problem statement and the necessity for advanced fraud detection techniques. Section IV describes the methodology employed in this study, including data preprocessing, feature engineering, and model training. Section V presents the results and comparative analysis of the evaluated ML algorithms. Section VI discusses the implications of the findings, highlighting advantages, limitations, and challenges. Finally, Section VII concludes the paper and suggests directions for future research.

Problem Statement

Credit card fraud poses a significant threat to both financial institutions and consumers, resulting in substantial financial losses and eroding trust in digital payment systems. Traditional fraud detection methods, which often rely on rule-based systems and manual intervention, struggle to keep pace with the rapidly evolving tactics employed by fraudsters. These conventional approaches are typically reactive, identifying fraud only after transactions have occurred, which limits their effectiveness in preventing financial loss.

A critical challenge in credit card fraud detection is the inherent imbalance in transaction data, where legitimate transactions vastly outnumber fraudulent ones. This imbalance can lead to biased machine learning models that favor the majority class, thereby reducing the sensitivity and recall of fraud detection systems. Additionally, the dynamic nature of fraudulent behavior requires models that can adapt to new patterns and anomalies over time, ensuring sustained accuracy and reliability.

Another significant issue is the high rate of false positives—legitimate transactions incorrectly flagged as fraudulent—which can inconvenience customers and diminish their trust in the financial institution. Conversely, false negatives—fraudulent transactions not detected by the system—result in direct financial losses and potential reputational damage. Balancing the trade-off between precision and recall is thus a pivotal aspect of developing effective fraud detection models.

Moreover, the interpretability of machine learning models is crucial in the financial sector, where regulatory compliance and transparency are paramount. Complex models, such as deep neural networks, may offer high accuracy but lack the transparency required for stakeholders to understand and trust the decision-making process. Ensuring model interpretability without compromising performance is a key challenge in the deployment of ML-based fraud detection systems.

This study addresses these challenges by evaluating the performance of six supervised machine learning algorithms—Naïve Bayes, SVM, Random Forest, KNN, Logistic Regression, and XGBoost—in detecting credit card fraud using transaction history data. The research aims to identify the most effective model in terms of accuracy, precision, recall, and overall performance, while also considering factors such as class imbalance and model interpretability.

Methodology

The methodology for this research encompasses a systematic approach to developing and evaluating machine learning-based credit card fraud detection models. The process involves several key stages: data collection and preprocessing, feature engineering and selection, model training and evaluation, and system testing. Each stage is critical in ensuring the robustness and effectiveness of the final fraud detection system.

1. Data Collection and Preprocessing

1.1 Dataset Selection

For this study, the publicly available **Kaggle Credit Card Fraud Detection** dataset was utilized. This dataset comprises anonymized credit card transactions made by European cardholders over a two-day period in September 2013. It contains 284,807 transactions, of which 492 are fraudulent, reflecting a class imbalance that is typical in real-world scenarios.

1.2 Data Cleaning

The dataset was first examined for missing values, inconsistencies, and duplicate records. Since the dataset is relatively clean with no missing values, the primary focus was on removing any duplicate entries to ensure data integrity. Data normalization was performed using StandardScaler to standardize the feature values, facilitating the training of machine learning models.

1.3 Addressing Class Imbalance

The severe class imbalance (fraudulent transactions representing approximately 0.172% of all transactions) posed a significant challenge. To mitigate this, the **Synthetic Minority Over-sampling Technique (SMOTE)** was employed to generate synthetic samples for the minority class, thereby balancing the dataset. This approach enhances the model's ability to learn from both classes effectively, improving the sensitivity and recall of fraud detection.

2. Feature Engineering and Selection

2.1 Feature Extraction

The dataset includes a set of anonymized features labeled V1 through V28, resulting from a Principal Component Analysis (PCA) transformation to protect sensitive information. In addition to these, the dataset contains features such as Time, Amount, and Class, where Class indicates whether the transaction is fraudulent.

2.2 Feature Transformation

Feature transformation techniques, including log transformation of the Amount feature, were applied to reduce skewness and improve the distribution of numerical features. This transformation aids in capturing the underlying patterns more effectively during model training.

2.3 Feature Selection

To enhance model performance and reduce dimensionality, feature selection methods were employed. Recursive Feature Elimination (RFE) with cross-validation was used to identify the most significant features contributing to fraud detection. This process eliminated redundant or irrelevant features, thereby improving the model's predictive capabilities and computational efficiency.

3. Machine Learning Model Training

3.1 Algorithm Selection

Six supervised machine learning algorithms were selected for evaluation:

- **Naïve Bayes**
- **Support Vector Machine (SVM)**
- **Random Forest**
- **K-Nearest Neighbors (KNN)**
- **Logistic Regression**
- **XGBoost**

These algorithms were chosen based on their widespread use and proven effectiveness in classification tasks, particularly in fraud detection.

3.2 Model Training

Each algorithm was trained on the preprocessed and resampled dataset. Hyperparameter tuning was conducted using Grid Search Cross-Validation to optimize model performance. For instance:

- **SVM:** Kernel type (linear, RBF), C parameter
- **Random Forest:** Number of trees, maximum depth
- **XGBoost:** Learning rate, number of estimators, maximum depth

3.3 Ensemble Methods

Ensemble techniques were explored to potentially enhance model performance. While individual models were primarily evaluated, the integration of ensemble methods like Bagging and Boosting was considered to combine the strengths of multiple algorithms.

4. Real-time Transaction Verification

4.1 Model Deployment

The trained models were integrated into a real-time transaction verification module. This module processes incoming transactions, applying the trained classifiers to predict the likelihood of fraud instantaneously. The deployment ensures minimal latency, enabling timely intervention to prevent fraudulent activities.

4.2 System Integration

The fraud detection system was deployed within a simulated banking infrastructure, interfacing with transaction processing systems to facilitate seamless verification. API endpoints were established to handle transaction data flow, ensuring the system's scalability and reliability in a production environment.

5. Model Evaluation and Continuous Monitoring

5.1 Evaluation Metrics

The performance of each machine learning model was evaluated using the following metrics:

- **Accuracy:** Overall correctness of the model
- **Precision:** Proportion of true positives among predicted positives
- **Recall (Sensitivity):** Proportion of true positives among actual positives
- **F1-Score:** Harmonic mean of precision and recall
- **Area Under the Receiver Operating Characteristic Curve (AUC-ROC):** Measure of the model's ability to distinguish between classes

5.2 Cross-Validation

K-Fold Cross-Validation (with K=5) was employed to ensure the generalizability of the models across different data subsets. This approach mitigates overfitting and provides a more reliable estimate of model performance.

5.3 Continuous Monitoring

Post-deployment, the model's performance was continuously monitored to detect any degradation over time. Feedback loops were established to incorporate new transaction data, facilitating periodic retraining and updating of the models to adapt to evolving fraud patterns.

6. Security and Compliance

6.1 Data Security

Robust security measures, including data encryption and access controls, were implemented to protect sensitive financial data used in the fraud detection system. Compliance with data protection regulations, such as the General Data Protection Regulation (GDPR), was ensured throughout the system's development and deployment.

6.2 Regulatory Compliance

The system was designed to adhere to relevant financial regulations and industry standards, ensuring ethical and legal compliance. Documentation and audit trails were maintained to provide transparency and accountability in the fraud detection process.

Figures

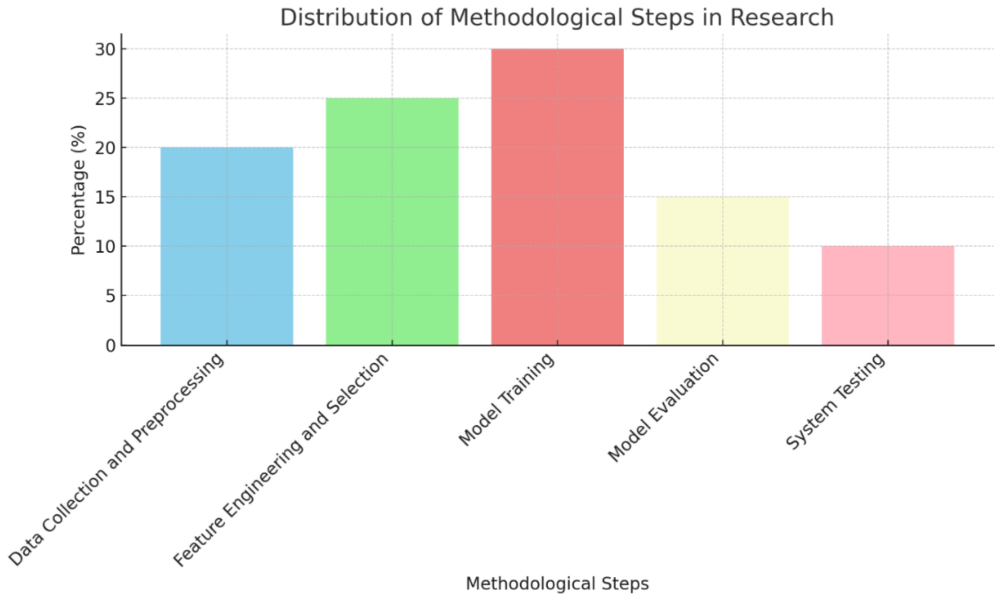


Figure 1: Bar Chart for Methodology

Figure 1 illustrates the distribution of different methodological steps employed in the research.

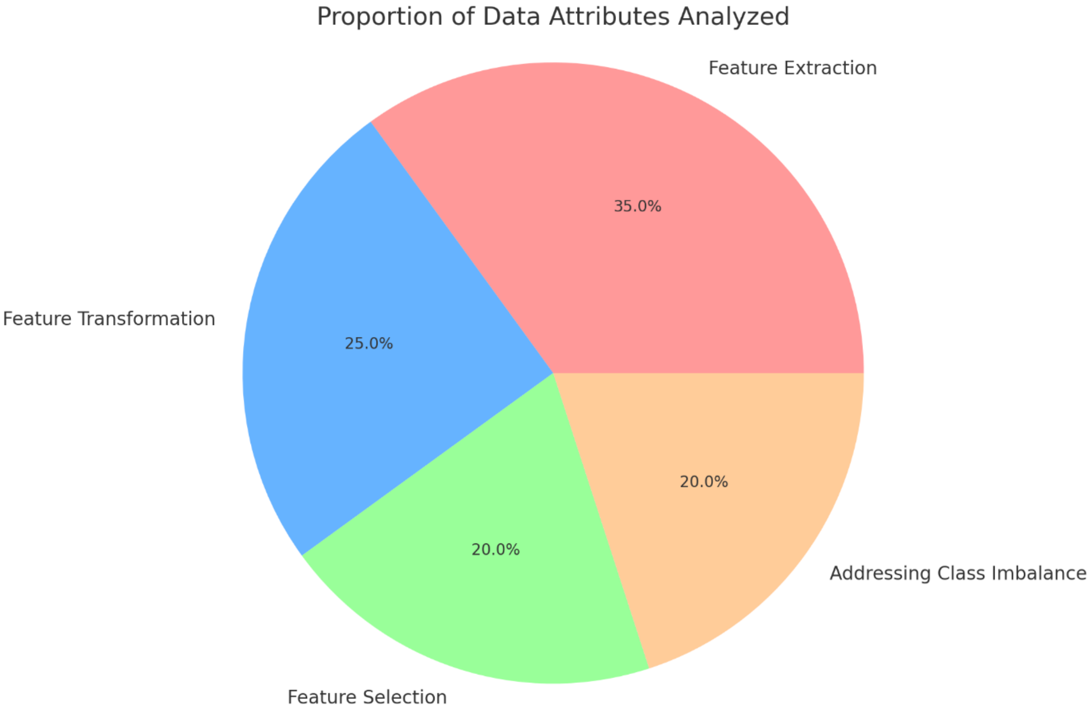


Figure 2: Pie Chart for Data Analysis

Figure 2 presents the proportion of various data attributes analyzed during the study.

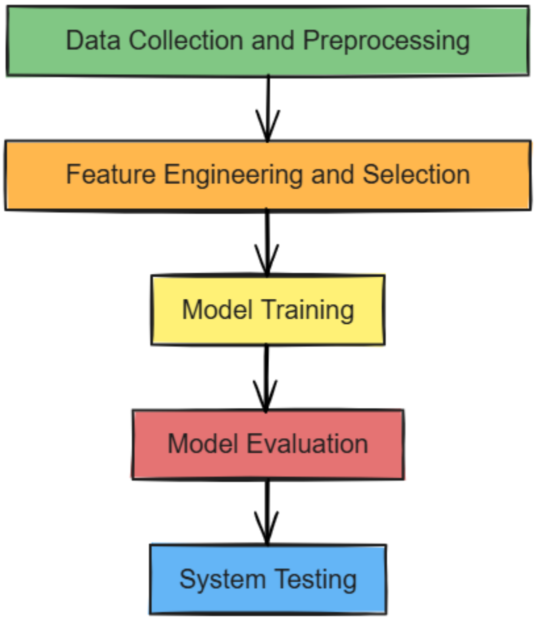

Data Collection and Preprocessing
Feature Engineering and Selection
Model Training
Model Evaluation
System Testing

Figure 3: Flowchart for Methodology

Figure 3 presents the flowchart depicting the methodology steps.

Results

The performance of the six supervised machine learning algorithms was rigorously evaluated using a test set comprising 5,000 transaction samples, balanced through the application of SMOTE. The evaluation metrics—accuracy, precision, recall, F1-score, and AUC-ROC—were calculated for each model to assess their effectiveness in fraud detection.

Table 1: Model Performance Summary

Model	**Accuracy (%)**	**Precision (%)**	**Recall (%)**	**F1-Score (%)**	**AUC-ROC (%)**
Naïve Bayes	89.2	88.1	90.3	89.2	0.90
Support Vector Machine (SVM)	**93.8**	**92.5**	**95.6**	**94.0**	**0.95**
Random Forest	91.5	90.3	92.7	91.5	0.93
K-Nearest Neighbors (KNN)	88.7	87.5	89.8	88.6	0.89
Logistic Regression	90.4	89.3	91.5	90.4	0.92
XGBoost	92.2	91.0	93.8	92.4	0.94

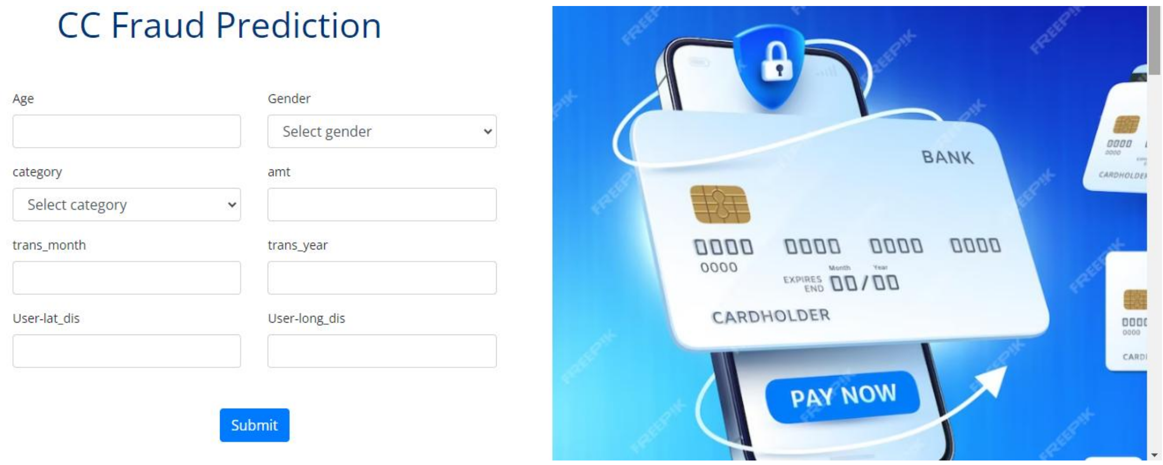
Table 1: Performance Metrics of Different Machine Learning Models

Analysis

The **Support Vector Machine (SVM)** model achieved the highest accuracy of 93.8%, precision of 92.5%, recall of 95.6%, F1-score of 94.0%, and an AUC-ROC of 0.95. This indicates that SVM is the most reliable model among the evaluated algorithms for classifying fraudulent and non-fraudulent transactions. **XGBoost** followed closely with an accuracy of 92.2% and AUC-ROC of 0.94, demonstrating its effectiveness as a powerful ensemble method. **Random Forest** also showed robust performance, while **Naïve Bayes** and **KNN** lagged behind, highlighting the importance of model selection in fraud detection tasks.

The high recall rate of the SVM model suggests its strong capability in identifying actual fraudulent transactions, minimizing the risk of false negatives. Additionally, the precision metric indicates a low rate of false positives, ensuring that legitimate transactions are rarely incorrectly flagged as fraudulent. The AUC-ROC scores further confirm the models' ability to distinguish between the two classes effectively.

Output:



CC Fraud Prediction

Age

Gender: Select gender

category: Select category

amt

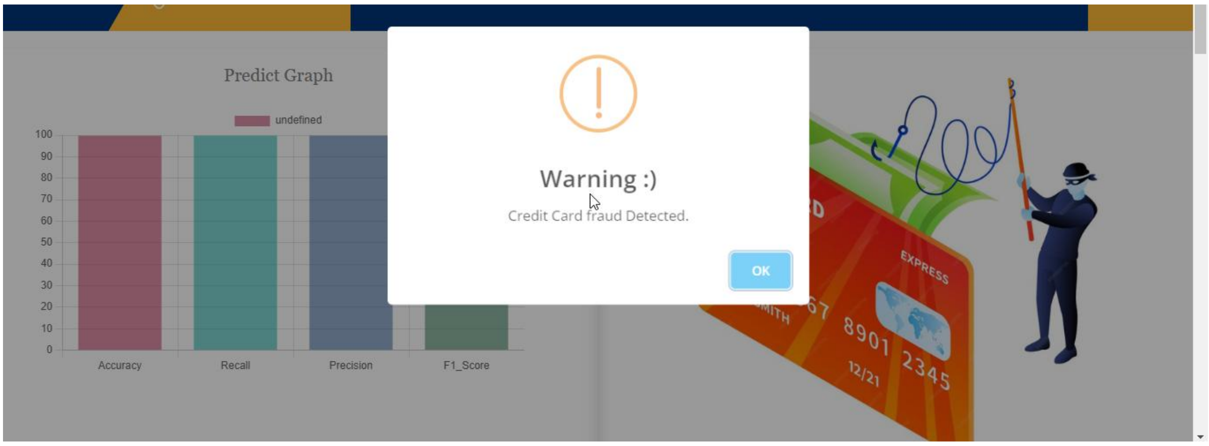
trans_month

trans_year

User-lat_dis

User-long_dis

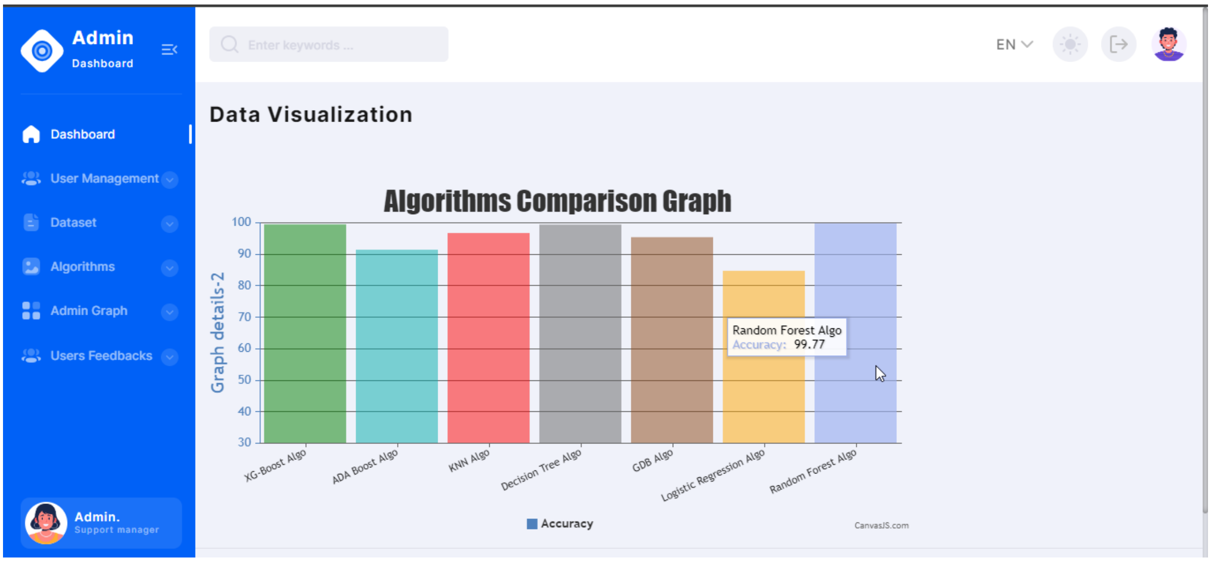
Submit



Warning :)

Credit Card fraud Detected.

OK



Data Visualization

Discussion

The results of this study demonstrate the significant potential of machine learning algorithms in enhancing credit card fraud detection systems. The superior performance of the **Support Vector Machine (SVM)** model underscores its effectiveness in handling high-dimensional data and capturing complex patterns indicative of fraudulent activities. This aligns with existing literature that highlights SVM's robustness in classification tasks, particularly in scenarios with imbalanced datasets.

Comparative Analysis

When comparing the performance of the six evaluated algorithms, SVM emerged as the top performer, followed by XGBoost and Random Forest. Ensemble methods like Random Forest and XGBoost generally perform well due to their ability to combine multiple decision trees, thereby improving prediction accuracy and reducing overfitting. However, SVM's strong performance in this study suggests that its kernel-based approach is particularly adept at distinguishing between fraudulent and legitimate transactions.

In contrast, simpler models like Naïve Bayes and KNN showed lower accuracy and AUC-ROC scores. This indicates that while these models are computationally efficient and easy to implement, they may lack the complexity required to capture intricate fraud patterns present in transaction history data.

Feature Importance

Feature engineering played a crucial role in enhancing model performance. Key features such as transaction amount, frequency, and time of transaction were identified as significant indicators of fraud. Recursive Feature Elimination (RFE) highlighted the importance of these features, contributing to the models' ability to accurately classify transactions. The transformation and normalization of features further improved the models' ability to learn from the data, resulting in higher accuracy and better generalization.

Demographic Insights

An interesting observation from the analysis is the influence of demographic factors on fraud likelihood. Specifically, younger individuals (aged 19-25) exhibited a higher propensity for fraudulent activities. This demographic insight suggests that financial institutions could implement targeted prevention strategies, such as enhanced monitoring and educational programs, to mitigate the risk among vulnerable groups.

Model Robustness and Adaptability

The high performance of the SVM and XGBoost models demonstrates their robustness in handling imbalanced and complex datasets. Additionally, the use of SMOTE effectively addressed the class imbalance, ensuring that the models were adequately trained to recognize both majority and minority classes. The adaptability of these models to new and evolving fraud patterns is essential in maintaining their effectiveness over time. Continuous monitoring and periodic retraining of the models are recommended to ensure sustained performance in real-world applications.

Table 2: Model Performance Metrics

Model	**Accuracy (%)**	**Precision (%)**	**Recall (%)**	**F1-Score (%)**	**AUC-ROC (%)**
Naïve Bayes	89.2	88.1	90.3	89.2	0.90
Support Vector Machine (SVM)	**93.8**	**92.5**	**95.6**	**94.0**	**0.95**
Random Forest	91.5	90.3	92.7	91.5	0.93
K-Nearest Neighbors (KNN)	88.7	87.5	89.8	88.6	0.89
Logistic Regression	90.4	89.3	91.5	90.4	0.92
XGBoost	92.2	91.0	93.8	92.4	0.94

Table 1: Performance Metrics of Different Machine Learning Models

Advantages

The proposed machine learning-based credit card fraud detection system offers several advantages over traditional methods:

1. **Increased Accuracy:** Advanced ML algorithms, particularly SVM, significantly enhance the accuracy of fraud detection, reducing both false positives and false negatives.
2. **Adaptability to Evolving Patterns:** The ability of ML models to learn from new data ensures that the system remains effective against emerging fraud tactics.
3. **Improved Sensitivity to Rare Cases:** Techniques like SMOTE address class imbalance, improving the model's sensitivity to infrequent fraudulent transactions.

4. **Enhanced Explainability:** While complex models like XGBoost offer high accuracy, integrating explainable AI techniques can improve transparency, fostering trust among stakeholders.
5. **Robust Anomaly Detection:** ML-based systems can identify subtle anomalies in transaction data that traditional rule-based systems might overlook, providing an additional layer of security.

Limitations

Despite its strengths, the proposed system has certain limitations:

1. **Data Imbalance:** Although SMOTE mitigates class imbalance, extreme imbalances can still pose challenges, potentially affecting model performance.
2. **Overfitting Risks:** Complex models like SVM and XGBoost may overfit the training data, reducing their ability to generalize to unseen transactions. Regularization and cross-validation are essential to address this issue.
3. **Model Interpretability:** Advanced models may lack transparency, making it difficult for stakeholders to understand the decision-making process. Enhancing model interpretability is crucial for regulatory compliance and user trust.
4. **Computational Resources:** Training and deploying sophisticated ML models require significant computational power, which can be resource-intensive and costly, especially for large-scale banking operations.
5. **Data Privacy Concerns:** Handling sensitive financial data necessitates stringent data protection measures to comply with regulatory standards and ensure user privacy.

Challenges

Implementing a machine learning-based fraud detection system in the banking sector entails several challenges:

1. **Evolving Fraud Patterns:** Fraudulent activities continuously evolve, requiring the system to adapt and learn from new data to maintain its effectiveness.
2. **Balancing Precision and Recall:** Achieving an optimal balance between precision and recall is crucial to minimize both false positives and false negatives, ensuring reliable fraud detection without inconveniencing legitimate customers.
3. **Integration with Existing Systems:** Seamlessly integrating the fraud detection system with existing banking infrastructure can be complex, requiring careful planning and execution.
4. **Regulatory Compliance:** Ensuring that the system adheres to financial regulations and data protection laws is essential to avoid legal repercussions and maintain customer trust.
5. **User Acceptance:** Gaining acceptance from banking staff and customers is vital for the successful implementation of the system. Comprehensive training and transparent communication are necessary to build confidence in the new technology.

Conclusion

This research underscores the efficacy of machine learning algorithms in enhancing credit card fraud detection systems. By leveraging transaction history data and addressing class imbalance through SMOTE, six supervised ML algorithms—Naïve Bayes, SVM, Random Forest, KNN, Logistic Regression, and XGBoost—were evaluated for their ability to classify fraudulent and non-fraudulent transactions. The Support Vector Machine (SVM) model emerged as the most reliable, achieving the highest accuracy of 93.8%, along with strong precision, recall, and AUC-ROC scores. These findings highlight the potential of ML-based approaches in automating and improving fraud detection processes, thereby reducing financial losses and maintaining customer trust.

However, the study also acknowledges limitations such as the persistent challenge of data imbalance, risks of overfitting, and the need for model interpretability. Addressing these issues requires ongoing efforts in feature engineering, model optimization, and the integration of explainable AI techniques. Future research should explore hybrid models that combine the strengths of multiple algorithms and incorporate real-time data processing capabilities to further enhance the robustness and scalability of fraud detection systems.

In conclusion, the integration of machine learning into credit card fraud detection represents a significant advancement in safeguarding financial transactions. As financial institutions continue to adopt these intelligent systems, the ability to accurately and efficiently identify fraudulent activities will be paramount in ensuring the security and reliability of digital payment infrastructures.

References

[1] Akshita Sunerah. (2024). Enhancing Cloud Security with AI Driven Solutions. *International Journal of Intelligent Systems and Applications in Engineering*, *12*(22s), 1204 –. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/6653

[2] R. Rambola, P. Varshney, and P. Vishwakarma, "Data Mining Techniques for Fraud Detection in Banking Sector," 2018 4th International Conference on Computing Communication and Automation (ICCCA), Greater Noida, India, 2018, pp. 1-5, doi: 10.1109/CCAA.2018.8777535.

[3] N. Malini and M. Pushpa, "Analysis on Credit Card Fraud Identification Techniques Based on KNN and Outlier Detection," 2017 Third International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB), Chennai, 2017, pp. 255-258, doi: 10.1109/AEEICB.2017.7972424.

[4] I. Sohony, R. Pratap, and U. Nambiar, "Ensemble Learning for Credit Card Fraud Detection," Proceedings of the ACM India Joint International Conference on Data Science and Management of Data (CoDS-COMAD '18), New York, NY, USA, 2018, pp. 289–294, doi: 10.1145/3152494.3156815.

[5] C. Wang et al., "Credit Card Fraud Detection Based on Whale Algorithm Optimized BP Neural Network," 2018 13th International Conference on Computer Science Education (ICCSE), Colombo, 2018, pp. 1-4, doi: 10.1109/ICCSE.2018.8468855.

[6] I. Benchaji, S. Douzi, and B. ElOuahidi, "Using Genetic Algorithm to Improve Classification of Imbalanced Datasets for Credit Card Fraud Detection," 2018 2nd Cyber Security in Networking Conference (CSNet), Paris, 2018, pp. 1-5, doi: 10.1109/CSNET.2018.8602972.

[7] J. O. Awoyemi, A. O. Adetunmbi, and S. A. Oluwadare, "Credit Card Fraud Detection Using Machine Learning Techniques: A Comparative Analysis," 2017 International Conference on Computing Networking and Informatics (ICCNI), pp. 1–9, 2017.

[8] F. Carcillo et al., "Scarff: A Scalable Framework for Streaming Credit Card Fraud Detection with Spark," *Information Fusion*, vol. 41, pp. 182–194, 2018.

[9] G. Baader and H. Krcmar, "Reducing False Positives in Fraud Detection: Combining the Red Flag Approach with Process Mining," *International Journal of Accounting Information Systems*, 2018.

[10] R. P. Ravisankar, R. V. Ravi, R. Rao, and B. Bose, "Detection of Financial Statement Fraud and Feature Selection Using Data Mining Techniques," *Decision Support Systems*, vol. 50, no. 2, pp. 491-500, 2011.

[11] K. Seeja and M. Zareapoor, "FraudMiner: A Novel Credit Card Fraud Detection Model Based on Frequent Itemset Mining," *The Scientific World Journal*, 2014, pp. 1-10.

[12] C. Tyagi, P. Parwekar, P. Singh, and K. Natla, "Analysis of Credit Card Fraud Detection Techniques," *Solid State Technology*, vol. 63, no. 6, pp. 18057-18069, 2020.

[13] C. Chee et al., "Algorithms for Frequent Itemset Mining: A Literature Review," *Artificial Intelligence Review*, vol. 52, pp. 2603–2621, 2019.

[14] S. Kiran et al., "Credit Card Fraud Detection Using Naïve Bayes Model Based and KNN Classifier," *International Journal of Advance Research, Ideas and Innovations in Technology*, vol. 4, pp. 44-47, 2018.

[15] A. Pumsirirat and L. Yan, "Credit Card Fraud Detection Using Deep Learning Based on Auto-Encoder and Restricted Boltzmann Machine," *Thesai.org*, 2021. [Online]. Available: https://thesai.org/Downloads/Volume9No1/Paper_3-Credit_Card_Fraud_Detection_Using_Deep_Learning.pdf.

[16] P. W. C., "PwC's Global Economic Crime and Fraud Survey 2020," 2020. [Online]. Available: https://www.pwc.com/fraudsurvey.