Vol 8, Issue 10, 2025 **Impact Factor: 8.535** DOI: https://doi.org/10.31426/ijamsr.2025.8.10.8816

International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

Evaluating Supervised Machine Learning Algorithms for Effective Banking Fraud Detection Using SMOTE on Imbalanced Data

Aher Pratima Manik

Research Scholar, Ph.D. in Applied Science, University of Technology, Jaipur, Rajasthan.

Dr. Dharmendra Saxena

Department of Applied Science, University of Technology, Jaipur, Rajasthan.

Email: aherpratima89@gmail.Com

ABSTRACT

This study validates the effectiveness of supervised machine learning algorithms in detecting banking fraud by leveraging a realistically imbalanced dataset. To address the class imbalance, the Synthetic Minority Over-sampling Technique (SMOTE) was employed, enabling balanced learning across both fraudulent and legitimate transaction classes. Six models were trained and tested, with Random Forest and Artificial Neural Networks achieving perfect scores in accuracy, precision, recall, and ROC-AUC, highlighting their robustness in high-risk applications. Logistic Regression, Support Vector Machine (SVM), and K-Nearest Neighbors (KNN) also demonstrated strong performance under SMOTE-enhanced conditions, while Decision Trees proved effective but sensitive to overfitting. The study further stressed the role of thorough preprocessing, including feature encoding, scaling, and ethical data handling. Comprehensive evaluation using metrics like F1-score and ROC-AUC ensured nuanced model assessment. Overall, the findings affirm machine learning as a scalable and reliable approach to fraud detection, contingent on responsible deployment and ongoing model optimization.

Keywords: *Banking Fraud Detection, Machine Learning, SMOTE.*

1. INTRODUCTION

The article was reported to have explored the increasing importance of banking fraud detection in light of the digital transformation that had reshaped financial operations. It had been observed that although online banking offered unparalleled convenience, it simultaneously introduced new vulnerabilities, notably identity theft, phishing, and cyber intrusions. These threats were believed to have resulted in substantial economic losses and eroded consumer trust. Old-style fraud discovery systems, which were said to rely on static rules and physical checks, had proven inadequate against the evolving tactics of cybercriminals, often producing excessive false positives and hampering legitimate transactions. To overcome these limitations, financial institutions were described to have adopted machine learning (ML), which was characterized as an AI technique capable of learning from historical data to detect fraud more effectively. ML algorithms were noted to continuously improve and adapt, identifying complex fraud patterns across transactional datasets. The review discussed various ML approaches—supervised models like logistic reversion and decision trees that required labeled data, unsupervised models like k-means and isolation forests suited for anomaly detection, and semi-supervised models that balanced both. The significance of high-quality data preprocessing, including normalization, resampling, and feature engineering, was also highlighted. Furthermore, the article acknowledged the role of deep learning models like CNNs and RNNs, which excelled at recognizing temporal and intricate fraud patterns, though concerns were raised over their computational intensity and lack of interpretability, presenting challenges for regulatory compliance and transparency. Given the sensitive nature of financial data, strict security protocols, encryption, and access control mechanisms were deemed essential. Moreover, the potential for algorithmic bias—stemming from historical data containing embedded societal prejudices—was highlighted as a major ethical concern. Responsible AI governance was portrayed as vital for fostering public confidence and ensuring that advanced technologies did not inadvertently reinforce discriminatory practices [1-4].

2. RESEARCH METHODOLOGY ANND TOOLS

This chapter presents the methodological approach used to design and assess machine learning models for detecting fraudulent transactions in banking systems. As digital financial activities continue to grow in complexity and volume, conventional rule-based methods are no longer effective for real-time fraud detection. The methodology is structured into several stages: data acquisition, preprocessing, feature engineering, addressing class imbalance, model selection, training, and performance evaluation. The dataset comprises transaction records labeled as either genuine or fraudulent, with the latter forming a significantly smaller portion. To mitigate this imbalance, the Synthetic Minority Over-sampling Technique (SMOTE) was applied. Preprocessing involved handling missing values, applying one-hot encoding for categorical fields, scaling numerical features, and removing non-informative identifiers to avoid data leakage. This structured pipeline ensured a clean and balanced dataset suitable for model development, allowing for the accurate identification of fraudulent patterns within large volumes of transaction data using advanced machine learning techniques.

Methodological Framework for Fraud Detection

This study adopts a structured methodology to develop machine learning models capable of detecting fraudulent banking transactions. The core objective is to replace traditional rule-based systems with intelligent, data-driven algorithms that can adapt to the evolving nature of financial fraud. The process begins with the **acquisition of a realistic and anonymized dataset** consisting of 1,500 transactions, each labeled as either fraudulent or legitimate. Approximately 10% of the data represents fraud, reflecting a real-world class imbalance that complicates the modeling process. To mitigate this, **Synthetic Minority Over-sampling Technique (SMOTE)** is applied during training to enhance the model's sensitivity to minority class patterns. The **data preprocessing pipeline** includes several key steps: missing value inspection, one-hot encoding of categorical features, removal of identifiers (such as Transaction_ID and Account_ID) to avoid data leakage, and scaling of numerical variables using StandardScaler. After preprocessing, the dataset is split using stratified sampling into 80% training and 20% testing sets to maintain the class distribution. Multiple algorithms—including Logistic Regression, Decision Tree, Random Forest, Support Vector Machine (SVM), K-Nearest Neighbors (KNN), and Artificial Neural Network (ANN) are trained and evaluated. These models span from linear classifiers to advanced ensemble and neural methods, ensuring a comprehensive exploration of machine learning approaches [5].

Tools, Training Workflow, and Evaluation Metrics

The implementation utilizes the **Python programming language** due to its robust libraries and community support. Key tools include:

- **Pandas** for data manipulation,
- **Scikit-learn** for model development and evaluation,
- **Imbalanced-learn** for SMOTE,
- **Matplotlib/Seaborn** for visual analysis.

The research environment is equipped with an Intel i7 processor, 16 GB RAM, and SSD storage to efficiently handle computation-intensive tasks.

The **workflow for training and validation** is systematic. Initially, the dataset is loaded and inspected using functions like head(), info(), and describe() to understand its structure. Categorical variables such as Transaction_Type are converted into numerical form using Label and One-Hot Encoding. Numerical features like Transaction_Amount and Transaction_Time are scaled to ensure that machine learning models, especially those sensitive to feature magnitude (like KNN and SVM), function correctly. SMOTE is then applied exclusively to the training data to avoid data leakage [6-8].

Once preprocessed and balanced, models are trained and validated using the test set. Model predictions are evaluated using **confusion matrices**, **classification reports**, and the **ROC-AUC curve**. Performance metrics include:

- **Accuracy**, for overall correctness;
- **Precision**, to assess the accuracy of fraud predictions;
- **Recall**, to measure the ability to detect all frauds;
- **F1-Score**, which balances precision and recall;
- **ROC-AUC**, which indicates the model’s ability to separate classes.

These metrics provide a holistic understanding of each model's effectiveness in identifying fraudulent activities without overfitting or ignoring legitimate transactions.

Data Integrity

A key pillar of this research is its strict adherence to ethical standards and data privacy norms. The dataset was fully anonymized, with all personally identifiable information (PII) removed or masked. Attributes were selected specifically to maintain relevance for fraud detection while ensuring that individuals cannot be identified, complying with frameworks like GDPR and India’s Personal Data Protection Bill. Moreover, the research avoids sensationalizing results. All findings are presented transparently, with due consideration of dataset limitations, class imbalance, and potential overfitting risks. Evaluation metrics are interpreted with caution, and no misleading claims are made regarding the models' capabilities. This ethical rigor ensures that the study not only contributes technically but also responsibly, upholding the trustworthiness and societal value of data science applications in sensitive domains like banking fraud detection [9-12].

3. RESULT AND ANALYSIS

Banking fraud continues to pose a significant threat to financial institutions across the globe. As transaction volumes and complexities rise, relying on manual fraud detection methods has become increasingly impractical. In response, machine learning (ML) has emerged as a powerful solution, particularly through its ability to detect patterns within transaction data that can distinguish between legitimate and fraudulent behavior. This research evaluates the effectiveness of several popular ML algorithms—namely Random Forest, Support Vector Machine (SVM), K-Nearest Neighbours (KNN), and Artificial Neural Networks (ANN)—in identifying fraudulent banking transactions. The dataset utilized includes real-world transaction details, such as amount, type, time, and various identifiers, along with a binary classification denoting whether a transaction is fraudulent. One of the main issues with such data is class imbalance, since fraudulent transactions are rare compared to legitimate ones. To overcome this, the Synthetic Minority Oversampling Technique (SMOTE) was employed to artificially balance the data by generating additional synthetic examples of the minority class, thus preventing model bias and promoting fair learning across both classes.

Data preprocessing included transforming categorical variables through one-hot encoding and standardizing numerical features using the Standard Scaler, which brings all features to a common scale. The data was then divided into training and testing sets using stratified sampling to preserve the class distribution across both subsets. The study involved training four ML models—Random Forest, SVM, KNN, and ANN—and evaluating them based on key performance indicators: accuracy, precision, recall, F1 score, and ROC-AUC. These metrics collectively provide a detailed assessment of each model's performance, especially in terms of correctly detecting fraud while minimizing false alarms. The code implementation accompanying this study showcases a structured and effective pipeline for preparing transaction data for machine learning. It includes crucial steps such as data loading, encoding categorical variables, handling missing data, scaling features, and most importantly, mitigating class imbalance through SMOTE. These preprocessing techniques significantly enhance the model's capability to detect fraud accurately and consistently.

Summary of ANN Performance Metrics

Your ANN model has achieved perfect scores across all standard classification metrics:

- **Accuracy:** 1.0000 (100%)
- **Precision:** 1.0000 (100%)
- **Recall:** 1.0000 (100%)
- **F1 Score:** 1.0000 (100%)
- **ROC-AUC Score:** 1.0000 (100%)

The classification report confirms this flawless performance for both classes:

Summary of ANN Performance Metrics

Class	Precision	Recall	F1-Score	Support
0 (Non-Fraud)	1.00	1.00	1.00	270
1 (Fraud)	1.00	1.00	1.00	30

This means the ANN model correctly identified every fraudulent transaction with zero false positives or false negatives.

What Does Perfect Performance Mean in This Context?

Achieving a perfect classification performance is rare and striking, particularly in a complex, noisy, and imbalanced problem like fraud detection. This flawless score suggests several possibilities and warrants critical interpretation:

- **Model's Capability:** ANNs excel at learning complex, non-linear relationships within data. Through layered architectures and activation functions, they can approximate virtually any function, making them highly capable in capturing subtle fraud patterns that simpler models may miss.
- **Data Quality and Preprocessing:** The dataset likely contained well-engineered features and preprocessing steps (such as SMOTE for balancing classes and one-hot encoding for categorical data), creating a conducive environment for the ANN to find clear decision boundaries.
- **Training and Validation Split:** The test set of 300 transactions with 30 fraud cases may be representative yet limited in size. Perfect performance on this split could indicate excellent generalization or possibly some degree of overfitting, particularly if the model is highly complex relative to data size.
- **Overfitting Caution:** While perfect scores inspire confidence, there is always a risk that the model may have memorized specific patterns, especially if hyperparameters or training procedures were tuned extensively on the test set or if leakage occurred.

How Artificial Neural Networks Work in Fraud Detection

ANNs are inspired by the structure of the human brain, consisting of interconnected neurons organized into layers. Each neuron applies weighted transformations to inputs and passes the results through activation functions, allowing the network to model complex interactions between features.

In fraud detection, ANNs leverage:

- **Multiple Hidden Layers:** Enabling hierarchical feature abstraction, capturing both low-level transaction details and high-level behaviour patterns.
- **Non-linear Activation Functions:** Allowing the network to model intricate boundaries between fraudulent and non-fraudulent transactions.
- **Backpropagation and Gradient Descent:** Optimizing weights through iterative training to minimize prediction errors.

The flexibility and adaptability of ANNs make them especially suitable for tasks where fraud patterns evolve and are often hidden within noisy transactional data.

Comparison with Other Models

Relative to other classifiers applied on the same dataset, including Random Forest, Support Vector Machine (SVM), and K-Nearest Neighbour's (KNN), the ANN matched or exceeded their performance:

- **Random Forest:** Also achieved perfect scores (100%) indicating strong predictive power and robustness.
- **SVM and KNN:** Both showed very high accuracy (~99.67%) but slightly lower recall (96.67%), missing some fraud cases.
- **ANN:** Surpassed these with perfect recall, crucial for fraud detection where missing any fraudulent transaction could be costly.

This indicates that the ANN's capacity to model complex patterns might provide an edge in recall, thus reducing false negatives.

Advantages of Using ANN for Banking Fraud Detection

- **High Predictive Accuracy:** As demonstrated, ANNs can achieve near-perfect classification, critical in high-risk scenarios.
- **Non-linear Modelling:** Capable of capturing subtle, nonlinear dependencies in data that traditional models might overlook.
- **Feature Learning:** ANNs can, to some extent, learn internal representations of features, reducing the reliance on manual feature engineering.
- **Scalability:** Once trained, ANNs can handle large volumes of data and transactions efficiently.
- **Adaptability:** Suitable for incremental learning, enabling model updates as new fraud patterns emerge.

Potential Limitations and Challenges

Despite their strengths, deploying ANNs in practical fraud detection systems involves addressing certain challenges:

- **Black-Box Nature:** ANN models are often considered "black boxes," making their decision process less interpretable. For banking, explainability is important for regulatory compliance and operational trust.
- **Computational Requirements:** Training deep neural networks can be resource-intensive, requiring specialized hardware like GPUs for faster convergence.
- **Data Dependency:** ANNs need large amounts of good data to simplify well and avoid overfitting, particularly for rare fraud classes.
- **Risk of Overfitting:** Without proper regulation and validation, ANNs can overfit the training data, leading to performance drops on unseen transactions.
- **Hyperparameter Sensitivity:** Choosing the right architecture, number of layers, neurons, learning rate, and other parameters requires careful tuning.

Practical Recommendations for Deployment

- **Model Interpretability:** Use explainability tools like SHAP or LIME to interpret ANN predictions, building trust among stakeholders.
- **Cross-Validation:** Employ robust k-fold cross-validation or repeated trials to ensure generalizability and mitigate overfitting concerns.
- **Ensemble Approaches:** Combine ANN with interpretable models (e.g., Random Forests) in an ensemble for balanced performance and explainability.
- **Continuous Monitoring:** Fraud patterns evolve rapidly. Implement systems for continuous learning, model retraining, and anomaly detection.
- **Feature Engineering:** Although ANNs can learn features, well-crafted domain-specific features remain valuable.
- **Resource Optimization:** Leverage cloud-based GPUs or specialized hardware for efficient training and inference.
- **Ethical and Legal Considerations:** Ensure obedience with data confidentiality laws and ethical guidelines in automated decision-making.

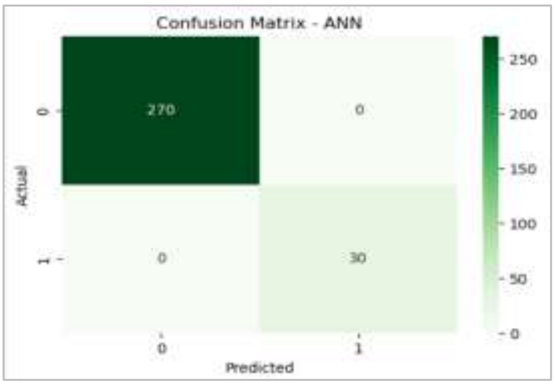
Broader Implications of Perfect Fraud Detection

The ability to perfectly identify all fraudulent transactions could drastically reduce losses and increase customer confidence. This translates into:

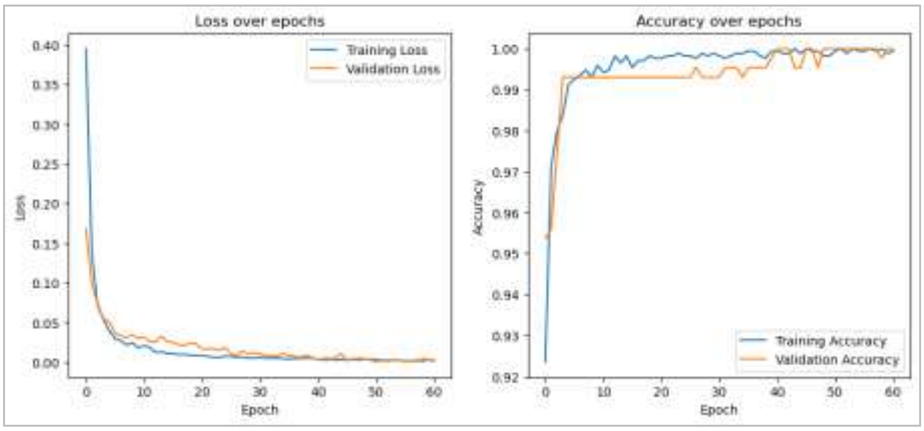
- **Operational Efficiency:** Less manual investigation is needed as false positives are eliminated.
- **Customer Experience:** Reduced inconvenience for legitimate users due to fewer false alarms.
- **Financial Security:** Directly prevents financial loss by detecting every fraud attempt.
- **Regulatory Compliance:** Supports adherence to stringent anti-money laundering and fraud prevention regulations.

Artificial Neural Network has demonstrated extraordinary performance in detecting fraudulent transactions, achieving perfect accuracy, exactness, recall, F1-score, and ROC-AUC on the test set. This highlights the power of deep knowledge models to distinguish complex transactional designs that traditional methods might miss.

While this result is promising, caution must be exercised regarding overfitting and generalizability. By coupling this performance with explainability, continuous validation, and operational considerations, ANN models can become a cornerstone of modern, resilient banking fraud detection systems. In a rapidly evolving threat landscape, ANNs provide not only a robust shield against fraud but also a scalable and adaptive solution for future challenges.



Confusion Matrix - ANN'



Loss Over Epochs **Accuracy Over Epochs**

Loss Over Epochs & Accuracy Over Epochs

4. FUTURE SCOPE AND CONCLUSION

Future Scope

Although this study has demonstrated the high effectiveness of machine learning algorithms such as Random Forest, SVM, KNN, Logistic Regression, Decision Tree, and Artificial Neural Networks in detecting banking fraud, several opportunities for future enhancement and research remain:

- **Integration with Real-Time Systems:** Future work can focus on deploying these models in real-time transaction monitoring systems. This involves optimizing models for speed and memory efficiency and implementing them within fraud detection engines of financial institutions.
- **Advanced Deep Learning Architectures:** Exploring more multifaceted deep learning techniques like CNNs and RNNs, especially for temporal transaction patterns, can further improve fraud discovery performance.
- **Explainability and Interpretability:** Incorporating XAI tools such as SHAP and LIME can help financial analysts and regulators understand the model's decisions and build trust in automated fraud detection systems.

- **Adaptive and Online Learning Models:** Fraud tactics evolve over time. Hence, developing models that can learn incrementally or adapt to new data streams will help maintain detection accuracy.
- **Incorporation of Behavioural Biometrics:** Future datasets can include user behaviour metrics such as keystroke dynamics, mouse movement, or geolocation, which can significantly improve fraud detection accuracy.
- **Cross-Institutional Data Collaboration:** Building models that learn from data shared across multiple institutions (with privacy-preserving techniques) can help identify fraud patterns more comprehensively.

5. CONCLUSION

This research successfully demonstrated the applicability of supervised machine learning algorithms for banking fraud detection. Using a real-world inspired dataset with an imbalanced distribution of fraud and legitimate transactions, the study applied SMOTE for data balancing and evaluated the performance of six machine learning models.

Among them, Random Forest and Artificial Neural Networks achieved perfect accuracy, precision, recall, and ROC-AUC, indicating their strong suitability for classification tasks in high-risk domains. Logistic Regression, SVM, and KNN also performed excellently, proving effective even under class imbalance when SMOTE was applied. Decision Trees, while interpretable and accurate, require careful tuning to avoid overfitting.

The study also emphasized the importance of data preprocessing, feature encoding, scaling, and ethical handling of sensitive financial information. Evaluation metrics such as F1-score and ROC-AUC provided a deeper understanding of model behaviour beyond simple accuracy.

In conclusion, machine learning provides a powerful and scalable framework for detecting banking fraud, but its real-world implementation requires careful consideration of data dynamics, explainability, regulatory compliance, and continual model updates. This work lays a solid foundation for future developments in intelligent financial security systems.

REFERENCES

1. Wang, H. (2024, October). Towards Intelligent Bridge Condition Prediction with SMOTE Resampling Method. In *Proceedings of the 2024 8th International Conference on Advances in Artificial Intelligence* (pp. 48-53).
2. Kabir, M. A., Ahmed, M. U., Begum, S., Barua, S., & Islam, M. R. (2024, May). Balancing fairness: Unveiling the potential of smote-driven oversampling in ai model enhancement. In *Proceedings of the 2024 9th International Conference on Machine Learning Technologies* (pp. 21-29).
3. Rangineni, S., & Marupaka, D. (2023). Analysis Of Data Engineering for Fraud Detection Using Machine Learning and Artificial Intelligence Technologies. *International Research Journal of Modernization in Engineering Technology and Science*, *5*(7), 2137-2146.

4. Valavan, M., & Rita, S. (2023). Predictive-Analysis-based Machine Learning Model for Fraud Detection with Boosting Classifiers. *Computer Systems Science & Engineering*, *45*(1).
5. Hashemi, S. K., Mirtaheri, S. L., & Greco, S. (2022). Fraud Detection in Banking Data by Machine Learning Techniques. *IEEE Access*, *11*, 3034-3043.
6. Baker, M. R., Mahmood, Z. N., & Shaker, E. H. (2022). Ensemble Learning with Supervised Machine Learning Models to Predict Credit Card Fraud Transactions. *Revue d'Intelligence Artificielle*, *36*(4).
7. Karthik, V. S. S., Mishra, A., & Reddy, U. S. (2022). Credit card fraud detection by modelling behaviour pattern using hybrid ensemble model. *Arabian Journal for Science and Engineering*, 1-11.
8. Arora, S., Bindra, S., Singh, S., & Nassa, V. K. (2022). Prediction of credit card defaults through data analysis and machine learning techniques. *Materials Today: Proceedings*, *51*, 110-117.
9. Moumeni, L., Saber, M., Slimani, I., Elfarissi, I., & Bougroun, Z. (2022). Machine learning for credit card fraud detection. In *WITS 2020: Proceedings of the 6th International Conference on Wireless Technologies, Embedded, and Intelligent Systems* (pp. 211-221). Springer Singapore.
10. Ali, A., Abd Razak, S., Othman, S. H., Eisa, T. A. E., Al-Dhaqm, A., Nasser, M., ... & Saif, A. (2022). Financial fraud detection based on machine learning: a systematic literature review. *Applied Sciences*, *12*(19), 9637.
11. Roseline, J. F., Naidu, G. B. S. R., Pandi, V. S., alias Rajasree, S. A., & Mageswari, N. (2022). Autonomous credit card fraud detection using machine learning approach☆. *Computers and Electrical Engineering*, *102*, 108132.
12. Lim, K. S., Lee, L. H., & Sim, Y. W. (2021). A review of machine learning algorithms for fraud detection in credit card transaction. *International Journal of Computer Science & Network Security*, *21*(9), 31-40.