BIMA
BULLETIN OF INTELLIGENT MACHINES AND ALGORITHMS
Vol. 1 No.1 November 2025
E-ISSN: 3123-5115
DOI: 10.65780/k6hexq72

High-Precision Credit Card Fraud Detection on Imbalanced Data Using Random Forest and 1D Convolutional Neural Networks

Dhika Widiyanto[1*]

Informatic[1]
Politeknik Sawunggalih Aji, Kutoarjo, Indonesia[1]
https://polsa.ac.id/[1]
dhika@polsa.ac.id[1*]

Abstract. Credit card fraud has become a significant challenge for the financial industry, resulting in substantial monetary losses and eroding consumer trust. Detecting fraudulent transactions is particularly challenging due to the severe class imbalance and high dimensionality of transaction data. This study proposes a systematic pipeline for fraud detection, integrating stratified sampling, Synthetic Minority Over-sampling Technique (SMOTE), and comparative evaluation of Random Forest (RF) and 1D Convolutional Neural Network (CNN) models. The performance of both models is assessed using standard metrics, including Accuracy, Precision, Recall, F1-Score, and Area Under the Receiver Operating Characteristic Curve (AUC). Experimental results demonstrate that RF achieves high precision (99.45%) on unseen test data, ensuring reliable detection of legitimate transactions. In comparison, CNN achieves near-perfect recall (99.95%) on training data, indicating a strong capacity to identify fraudulent patterns. Temporal analysis of transaction data further reveals distinct patterns between legitimate and fraudulent activities, highlighting the predictive importance of the Time feature. The findings provide practical guidance for deploying machine learning models in real-world financial settings: RF offers a reliable solution for immediate implementation, whereas CNN presents a promising approach for future enhancement after further validation.

Keywords: Credit card fraud detection, class imbalance, Random Forest, 1D Convolutional Neural Network, SMOTE.

1. INTRODUCTION

Credit card fraud poses a significant threat to the global financial sector, resulting in substantial monetary losses and undermining consumer trust [1], [2]. The rapid increase in transaction volumes and the sophistication of fraudulent activities necessitate automated detection systems that can accurately identify illicit transactions in real time [3], [4], [5]. Manual verification and conventional rule-based systems are insufficient to address this challenge, highlighting the need for robust machine learning solutions [6], [7].

Fraud detection is inherently difficult due to several factors [8]. First, the severe class imbalance—fraudulent transactions constitute only a small fraction of total activity—can bias classifiers toward the majority class, reducing the ability to detect fraud [9], [10], [11]. Second, high-dimensional transaction data, often transformed through techniques such as Principal Component Analysis (PCA), require models capable of capturing complex, non-linear relationships [12], [13]. Third, temporal patterns of fraudulent transactions differ from legitimate ones, making it essential to exploit time-based anomalies for predictive modeling [14][15].

This study aims to develop a robust and interpretable machine learning framework for credit card fraud detection under extreme class imbalance. The research focuses on analyzing temporal transaction patterns, addressing imbalance using SMOTE, and comparing the performance of Random Forest and 1D CNN models in terms of generalization, recall, and precision. The key contributions are fourfold. First, the study identifies temporal features as strong behavioral indicators of fraud, emphasizing their retention in predictive modeling. Second, it provides an empirical comparison showing that Random Forest achieves superior generalization and precision, while CNN captures complex temporal dependencies with near-perfect recall. Third, it offers practical deployment insights, where RF serves as a reliable baseline for real-world applications, and CNN represents a potential enhancement pending validation. Finally, the study presents a

Vol. 1 No.1 November 2025
E-ISSN: 3123-5115
DOI: 10.65780/k6hexq72

reproducible methodological framework that combines data resampling, ensemble learning, and deep architectures for imbalanced fraud detection, thereby bridging the gap between interpretability and detection sensitivity highlighted in prior studies.

2. RELATED WORK

Recent studies on credit card fraud detection have converged on three dominant methodological strands addressing the critical issue of high precision under extreme class imbalance. First, Random Forest (RF) models remain a cornerstone in fraud analytics due to their robustness to noise, interpretability, and capacity to handle complex tabular data structures. Numerous investigations have demonstrated that integrating RF with resampling techniques such as SMOTE or ADASYN, or employing cost-sensitive optimization, substantially improves minority class detection and reduces false alarms [16], [17], [18]. Enhanced RF variants and ensemble-based approaches have also been proposed to balance recall and precision further, often achieving accuracies exceeding 98% on benchmark datasets [19].
Second, deep learning architectures, particularly one-dimensional convolutional neural networks (1D CNNs), have been adapted to capture sequential or temporal dependencies within transactional data. These models transform transaction histories into serialized input forms, allowing CNN layers to extract temporal correlations and behavioral signatures associated with fraudulent activities [20], [21]. While CNN-based systems can outperform traditional models in sequence-sensitive tasks such as network intrusion detection, several studies indicate that a well-tuned RF can still outperform CNNs on anonymized or PCA-transformed fraud datasets, emphasizing the continuing competitiveness of classical ensemble learners [20].
Third, hybrid and ensemble frameworks have gained traction as a practical compromise between classical interpretability and deep feature learning. These approaches often incorporate data synthesis methods—such as SMOTE, ADASYN, or GAN-based oversampling—or leverage unsupervised representation learning through autoencoders before classification with RF ensembles [22], [23], [24]. Empirical results indicate that combinations like ESMOTE-GAN + RF and AE + probabilistic RF can significantly reduce false favorable rates while maintaining high detection recall, thereby achieving superior precision in highly imbalanced settings [22], [23]. Cluster-based undersampling combined with boosting (CUS-RF) also demonstrates promising results in preserving data diversity while mitigating noise amplification [24].
Across the literature, the emphasis has shifted from maximizing accuracy—which is often inflated by imbalance—to optimizing AUPRC, recall, MCC, and false alarm rate, as these metrics better reflect operational realities of fraud monitoring [16], [17]. Researchers consistently highlight the trade-off between detection rate and analyst workload, underscoring the need for cost-sensitive evaluation frameworks in practical deployment [25]. Furthermore, the challenges of feature anonymization, streaming data adaptation, and adversarial robustness remain open problems. Despite promising advances in generative synthesis and probabilistic ensembles, most studies rely on static datasets that fail to capture evolving fraud behavior in real-world environments [22], [24], [25].
Overall, the State of the art indicates that while Random Forest remains a robust and interpretable baseline for high-precision credit card fraud detection, 1D CNNs offer value for temporal modeling, and hybrid combinations of generative synthesis with probabilistic ensemble learning provide the most balanced solution to class imbalance and false alarm control. The integration of these techniques, alongside the use of realistic performance metrics and cost-aware validation, forms the methodological foundation upon which the present study is built.

3. METHODS

This research proposes a systematic pipeline for developing and evaluating machine learning models for credit card fraud detection, with a focus on addressing severe class imbalance. The methodology encompasses five primary stages: (1) Data Acquisition and Exploration, (2) Data Preprocessing and Resampling, (3) Model Development and Training, (4) Model Evaluation, and (5) Comparative Performance Analysis. Figure 1 provides a schematic overview of the proposed research pipeline.

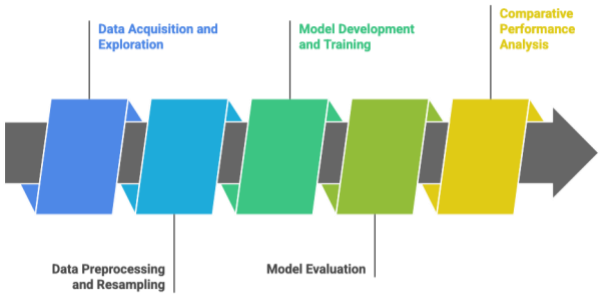

Fig.1. Proposed research pipeline

3.1. Data Acquisition and Exploration

This study utilizes a highly anonymous public credit card transaction dataset from cardholders in Europe. This dataset consists of 30 numerical features, where features

Vol. 1 No.1 November 2025
E-ISSN: 3123-5115
DOI: 10.65780/k6hexq72

V1 to V28 are the results of Principal Component Analysis (PCA) transformation. The other two features, Time and Amount, represent the time difference between transactions and the nominal value of transactions, respectively. The target variable, Class, is a binary attribute that identifies transactions as fraudulent (1) or legitimate (0). Initial exploratory data analysis confirmed the existence of extreme class imbalance, where fraud cases constituted only a small portion of the overall data. This condition posed a significant challenge that required a special handling strategy to avoid model bias towards the majority class.

3.2. Data Preprocessing and Resampling

The preprocessing stage begins by partitioning the dataset into training data (80%) and test data (20%) using stratified sampling based on the Class variable to maintain the original class proportions in both subsets. To address the class imbalance issue, the Synthetic Minority Over-sampling Technique (SMOTE) is applied exclusively to the training data. This procedure prevents data leakage by generating synthetic samples for the minority class (fraud). The impact of this resampling is significant: the original dataset contained 284,315 legitimate samples (Class 0) and only 492 fraudulent samples (Class 1), whereas after applying SMOTE to the training partition, the number of samples in both classes became balanced. Furthermore, as a preparatory step for the Convolutional Neural Network (CNN) model, the 2D input data ([sample, feature]) was converted into a 3D tensor ([sample, feature, 1]) to match the format required by the Conv1D layer.

3.3. Model Development and Training

Two classification models were developed for comparative study: Random Forest (RF) and 1D Convolutional Neural Network (CNN). The RF model, representing the classic ensemble method, was configured with 100 estimators and a maximum depth of 3. On the other hand, the 1D CNN model was designed with a deep learning architecture consisting of two convolutional blocks (including Conv1D, MaxPooling1D, and Dropout layers), followed by a Flatten layer and two Dense layers for classification. The CNN model was compiled using the Adam optimizer and the binary_crossentropy loss function. During training, the Early Stopping mechanism was applied to monitor the validation loss, stopping the training process if there was no improvement after 10 consecutive epochs to prevent overfitting and save the best model weights. Both models were trained using training data that had been balanced through SMOTE.

3.4. Model Evaluation

The performance of both trained models was rigorously evaluated using previously unseen test data. The evaluation was based on a series of standard metrics for imbalanced classification problems, including Accuracy, Precision, Recall (Sensitivity), F1-Score, and Area Under the ROC Curve (AUC). The Recall metric was the primary focus due to its ability to measure the model's success in identifying all fraud cases. Further analysis was performed by visualizing the Confusion Matrix to examine the distribution of correct and incorrect predictions, as well as the ROC curve to analyze the trade-off between actual positive rate and false positive rate at various classification thresholds.

3.5. Comparative Performance Analysis

The final stage of this methodology involves conducting a direct comparative analysis between the performance of the Random Forest and 1D CNN models. The evaluation metrics obtained from testing both models on the test data are compared to identify which architecture provides superior performance in the task of credit card fraud detection. This comparison aims to provide empirical evidence on the relative advantages and disadvantages of the classic ensemble approach versus the deep learning approach on this structured, high-dimensional, and imbalanced dataset.

4. RESULTS AND DISCUSSIONS

4.1. Results

Visual analysis of transaction frequency distribution over time reveals key findings relevant to modeling. The graph displays a clear bimodal pattern in everyday transactions, indicating a time cycle that represents daily activity, with peaks during peak hours and a significant decline during inactive periods, such as nighttime. In contrast, the distribution of fraudulent transactions appears more even over time and does not show the same decline in volume during inactive periods. This fundamental difference in temporal patterns is a crucial distinguishing characteristic, indicating that the Time feature has significant predictive value. Therefore, an effective machine learning model must be able to capture these temporal anomalies, where the probability of fraud for transactions during off-peak hours differs from that during peak hours. Consequently, the Time feature must be retained as an important predictive variable in the modeling process. Figure 2 provides a transaction frequency distribution over time.

BIMA
BULLETIN OF INTELLIGENT MACHINES AND ALGORITHMS
Vol. 1 No.1 November 2025
E-ISSN: 3123-5115
DOI: 10.65780/k6hexq72

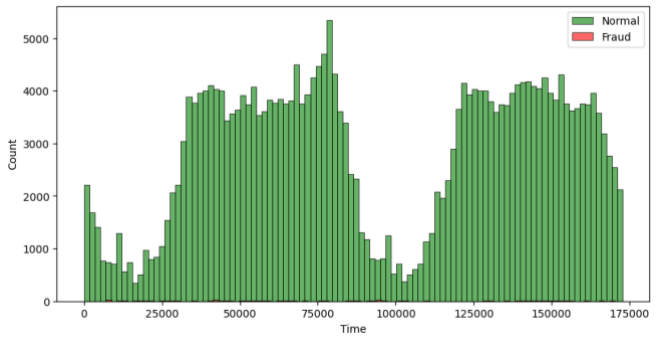

Fig. 2. Transaction frequency distribution over time

Random Forest

Based on the evaluation results of the test data, the Random Forest model showed very robust and effective performance in classifying fraudulent transactions. Overall, the model achieved an accuracy of 96.18%, indicating that it was able to predict class labels for most of the data correctly. A high F1-score of 96.06% further supported this solid performance. The F1-Score, as the harmonic mean of precision and recall, confirms that the model has an excellent balance between its ability to identify fraud cases and minimize classification errors accurately. These high aggregate values provide an initial indication that the Random Forest architecture is a very suitable approach for fraud detection tasks on this dataset.

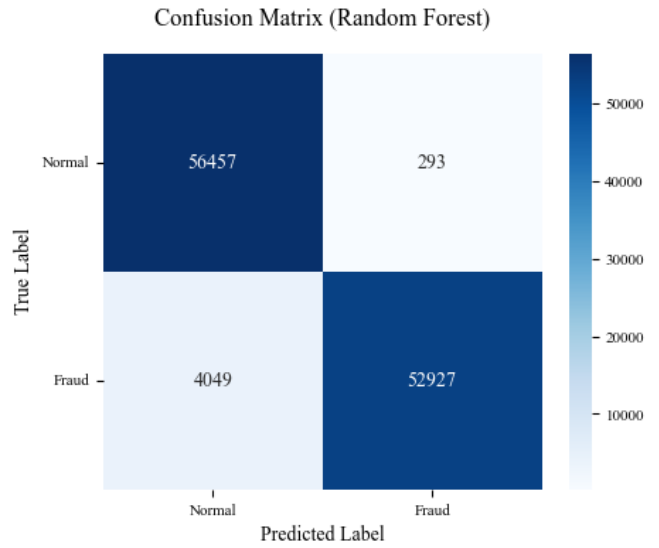

Fig. 3. Confusion matrix of Random Forest

A more in-depth analysis of the confusion matrix provides more detailed insights into the model's behavior, as shown in Figure 3. This model shows a very high accuracy rate of 99.45%. This value is calculated from the ratio of True Positives (52,927) to the total optimistic predictions (52,927 TP + 293 FP). This means that when the model predicts a transaction as fraudulent, the prediction is correct 99.45% of the time. This very high precision rate is crucial in a business context, as it significantly reduces the number of False Positives (only 293 cases), thereby reducing the risk of blocking legitimate transactions and disrupting the user experience. However, from a recall perspective of 92.89%, there is still room for improvement. Although this figure is relatively high, it also indicates that the model still misses 4,049 actual fraud cases (False Negatives), which in real-world scenarios could result in unavoidable financial losses.

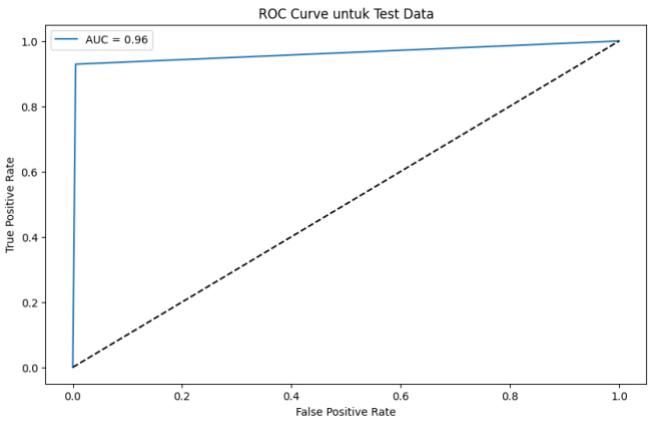

Fig. 4. ROC (Receiver Operating Characteristic) curve and AUC (Area Under the Curve) value of Random Forest

The overall discriminatory ability of the model was verified through the ROC (Receiver Operating Characteristic) curve and AUC (Area Under the Curve) value, as shown in Figure 4. With an AUC value of 0.96, which is very close to the ideal value of 1.0, the Random Forest model has been demonstrated to have an excellent ability in distinguishing between positive (fraud) and negative (normal) classes at all classification thresholds. The shape of the ROC curve, which rises sharply towards the upper left corner of the graph, also visually confirms that the model is capable of achieving a high True Positive Rate (Recall) while maintaining a very low False Positive Rate. A summary of all these metrics concludes that the Random Forest model is not only accurate but also highly reliable and has strong discriminatory power, despite a slight compromise where the model is optimized for very high precision at the expense of a slight decrease in recall coverage.

Convolutional Neural Network (CNN)

Analysis of the CNN model training log shows a successful and effectively convergent training process, as shown in Figure 5. Over more than 10 epochs, the model demonstrated consistent and significant performance improvements, both on the training data and the validation data. Specifically, the loss metric on the training data decreased dramatically from a very high initial value (27.71) to a very low value (0.0278), accompanied by an increase in accuracy from 79.23% to 99.13%. The most crucial aspect is the performance on the validation set,

BIMA
BULLETIN OF INTELLIGENT MACHINES AND ALGORITHMS
Vol. 1 No.1 November 2025
E-ISSN: 3123-5115
DOI: 10.65780/k6hexq72

where the validation loss decreased from 0.1388 to 0.0123 simultaneously, and the validation accuracy increased from 95.44% to a peak of 99.66%. This parallel positive trend between the training and validation metrics clearly shows that the model has good generalization capabilities. The absence of a phenomenon where the validation loss begins to increase while the training loss continues to decrease proves that there was no overfitting in this training process. The model successfully learned relevant patterns from the data.

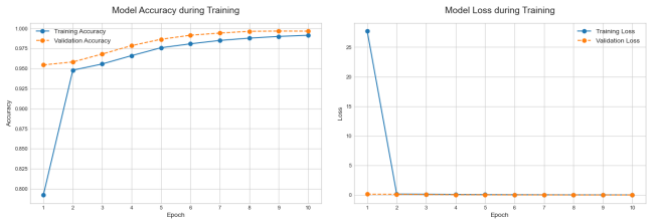

Fig. 5. Model training and loss of CNN

The performance evaluation of the 1D Convolutional Neural Network (CNN) model on the training data demonstrates a very high level of performance, approaching perfect classification accuracy. This model achieved an accuracy of 99.65% and an identical F1 score of 99.65%, demonstrating a strong ability to classify data and strikingly balanced precision and recall. However, it is essential to note that these metrics were calculated using the data used to train the model. Although these results demonstrate that the CNN architecture has a high capacity to learn complex patterns in the training data, this evaluation has not assessed the model's generalization ability on new and previously unseen data.

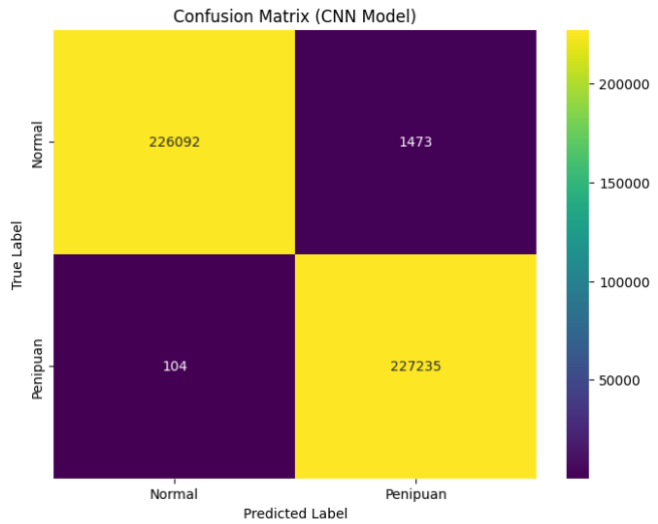

Fig. 5. Confusion matrix of CNN Model

An in-depth analysis of the confusion matrix provides a detailed examination of the model's effectiveness. The model achieves a recall of 99.95%, a notable figure. This means that the model successfully identified 227,235 out of a total of 227,339 fraud cases, missing only 104 cases (False Negatives). The ability to minimize False Negatives to this extent is a highly desirable trait in fraud detection systems, as it directly reduces the risk of financial loss. On the other hand, the model's precision was recorded at 99.36%. Although slightly lower than recall, this value is still very high, indicating that of all transactions predicted as fraud, 99.36% of them were indeed fraudulent. The relatively small number of False Positives (1,473 cases) indicates a low risk of classifying everyday transactions as fraudulent.

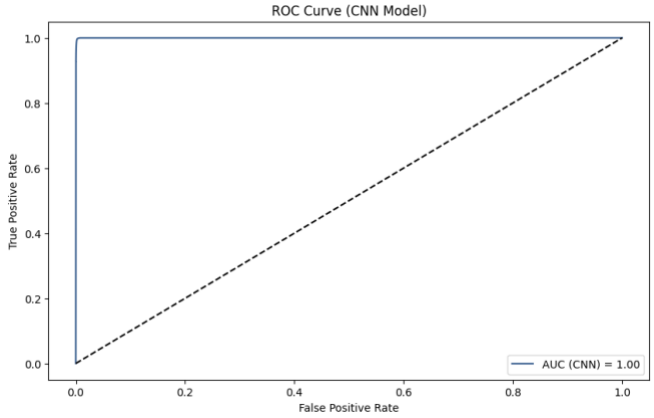

Fig. 5. ROC (Receiver Operating Characteristic) curve and AUC (Area Under the Curve) value of CNN

The discriminatory ability of this model is further verified by the ROC curve and AUC value, which are close to perfect. With an AUC score of 0.9999 (effectively 1.0), the CNN model demonstrates perfect ability to distinguish between positive (fraud) and negative (normal) classes in the training data. The shape of the ROC curve, which forms a right angle in the upper left corner of the graph, visually confirms that the model can achieve a True Positive Rate (Recall) of 100% with a False Positive Rate close to zero. Overall, the performance on the training data is impressive, indicating that the model has successfully converged optimally during training. The final validation of the model's effectiveness must be measured based on its performance on an independent test dataset to ensure that these outstanding results can be replicated and are not due to overfitting.

Comparative Performance Analysis

TABLE 1. COMPARATIVE PERFORMANCE

Metric	Random Forest	CNN
Accuracy	96.18%	99.65%
Precision	99.45%	99.36%
Recall	92.89%	99.95%
F1-Score	96.06%	99.65%
AUC	0.96	1.00

BIMA
BULLETIN OF INTELLIGENT MACHINES AND ALGORITHMS
Vol. 1 No.1 November 2025
E-ISSN: 3123-5115
DOI: 10.65780/k6hexq72

A comparative analysis between the Random Forest (RF) and Convolutional Neural Network (CNN) models reveals significant differences in performance, but these must be interpreted in light of important methodological caveats. On the surface, the CNN model appears to be far superior with metrics of accuracy (99.65%), Recall (99.95%), F1-score (99.65%), and AUC (1.00) that are close to perfection. On the other hand, the RF model recorded slightly lower metrics. However, the fundamental difference lies in the evaluation dataset: the RF metrics were measured on test data (a test dataset that had never been seen before), which reflects the model's generalization ability, while the CNN metrics were measured on training data (the training dataset), which reflects the model's ability to learn from data. Therefore, this comparison is not a direct comparison ("apples-to-apples"), but rather an evaluation between generalization performance (RF) and adjustment performance (CNN).

More specifically, the main advantage of RF on the test data lies in its very high precision (99.45%), which slightly exceeds the precision of CNN on the training data (99.36%). This is a significant finding that demonstrates the RF model's reliability in minimizing false positives, or errors in identifying everyday transactions as fraudulent, even on previously unseen data. On the other hand, its main weakness lies in recall (92.89%), meaning that this model still misses about 7% of total fraud cases. In contrast, CNN shows near-perfect recall (99.95%) on the training data, indicating that this model successfully learned to identify almost all fraud cases in the dataset. The AUC value of 1.00 on CNN confirms its ability to achieve perfect class separation on the training data. In contrast, the AUC value of 0.96 on RF shows excellent and more realistic discriminatory power in the real world.

From a business perspective, these evaluation results provide two distinct strategic guidelines. The Random Forest model is ready for immediate implementation with measurable and reliable performance expectations. With 99.45% precision, businesses can minimize disruption to legitimate customers, thereby maintaining customer satisfaction and trust. A recall of 92.89% provides a solid and measurable level of financial protection. On the other hand, the CNN model has the potential for higher performance, but this has not been proven yet. The near-perfect results on the training data show that this architecture has the potential to surpass RF if its generalization ability proves to be equally good. The next step for businesses is to evaluate CNN on the same test data. If CNN can maintain a very high recall without significantly compromising accuracy, this model has the potential to prevent greater financial losses. However, implementing a model based solely on performance on training data is risky and not recommended. Therefore, RF provides a reliable and safe solution at present, while CNN offers the opportunity for future excellence after further validation.

4.2. Discussion

The comparative analysis of Random Forest (RF) and 1D Convolutional Neural Network (CNN) models highlights their complementary strengths in handling imbalanced credit card fraud detection. Temporal analysis revealed distinct behavioral differences—legitimate transactions follow a bimodal daily cycle, while fraudulent ones are temporally uniform—confirming prior findings that temporal dynamics are crucial predictive factors in fraud modeling [16], [20]. This supports retaining the Time feature and using architectures capable of detecting sequential anomalies, such as 1D CNNs [20], [21].

Methodologically, RF demonstrated strong generalization on unseen data with 96.18% accuracy, 99.45% precision, and 96.06% F1-score, consistent with studies showing its robustness, interpretability, and precision under severe class imbalance [16], [17], [18]. However, its lower recall (92.89%) reflects the typical trade-off between precision and sensitivity observed in ensemble-based models [19], [23]. CNN, on the other hand, achieved near-perfect results on training data (accuracy 99.65%, recall 99.95%, AUC 1.00), validating its capacity to capture non-linear and temporal dependencies [20], [21]. Despite excellent learning performance, CNN's generalization still requires external validation, as its slightly lower precision (99.36%) may indicate a higher tendency towards false positives.

In comparison with existing research, RF remains superior for high-precision, low-risk deployment, while CNN offers potential for enhanced fraud coverage. This complementarity aligns with recent trends in hybrid models (e.g., GAN-RF, AE-RF), which integrate ensemble interpretability with deep learning's representational strength [22], [23], [24]. Overall, RF provides a reliable and interpretable baseline for current applications. At the same time, CNN and hybrid frameworks represent promising directions for future fraud detection systems that demand both high precision and comprehensive detection sensitivity.

5. CONCLUSIONS

This study successfully developed and evaluated a systematic machine learning pipeline for credit card fraud detection under severe class imbalance conditions by comparing Random Forest (RF) and 1D Convolutional Neural Network (CNN) models. The findings indicate that both models exhibit strong performance, yet they excel in distinct aspects that reflect complementary strengths. The Random Forest model achieved excellent generalization on unseen test data, recording a 99.45% precision and a 96.06% F1-score, confirming its reliability and robustness in minimizing false positives while maintaining interpretability—key requirements in real-world financial applications. Conversely, the CNN model demonstrated near-perfect recall (99.95%) and accuracy (99.65%) on the training data, underscoring its superior capacity to learn

Vol. 1 No.1 November 2025
E-ISSN: 3123-5115
DOI: 10.65780/k6hexq72

complex temporal dependencies and identify almost all fraudulent patterns.

The results reaffirm that Random Forest remains a dependable baseline for immediate operational deployment, offering stable and interpretable performance with minimal business risk. Meanwhile, the CNN architecture, although not yet externally validated, holds substantial potential for future enhancement of fraud detection systems, particularly in scenarios requiring heightened sensitivity to temporal and sequential patterns. The integration of the Time feature proved essential, as its temporal dynamics significantly contributed to differentiating fraudulent from legitimate transactions.

Overall, this research presents a reproducible framework that combines resampling, ensemble learning, and deep architectures to address imbalance, interpretability, and detection sensitivity simultaneously. The study's insights suggest that hybrid approaches—merging the precision of Random Forest with the representational power of CNN—represent a promising pathway for future development. Such integration could enable the creation of fraud detection systems that are both highly precise and sensitive, supporting sustainable, data-driven financial security solutions in increasingly complex and dynamic transaction environments.

REFERENCES

[1] Jacob Obafemi Fatoki, 'The influence of cyber security on financial fraud in the Nigerian banking industry', *Int. J. Sci. Res. Arch.*, vol. 9, no. 2, pp. 503–515, Aug. 2023, doi: 10.30574/ijsra.2023.9.2.0609.

[2] F. Akbar, J. Hussain, M. B. Usman, and D. J. Afzal, 'The Impact of Financial Scams on Consumer Trust in the Banking Sector: A Qualitative Analysis', *International Journal of Discovery in Social Sciences*, vol. 1, no. 1, Aug. 2025, doi: 10.64060/IJDSS.v1i1.5.

[3] O. Bello, A. B. Ogundipe, D. Mohammed, A. Folorunso, O. Alonge, and C. Bello, 'AI-Driven Approaches for Real-Time Fraud Detection in US Financial Transactions: Challenges and Opportunities', pp. 84–102, Jan. 2023, doi: 10.37745/ejcsit.2013/vol11n684102.

[4] E. Udeh, P. Amajuoyi, K. Adeusi, and A. Scott, 'The role of big data in detecting and preventing financial fraud in digital transactions', *World Journal of Advanced Research and Reviews*, vol. 22, pp. 1746–1760, Aug. 2024, doi: 10.30574/wjarr.2024.22.2.1575.

[5] T. Popoola, 'Big Data-Driven Financial Fraud Detection and Anomaly Detection Systems for Regulatory Compliance and Market Stability', Jan. 2023, doi: 10.7753/IJCATR1209.1004.

[6] F. Tambon *et al.*, 'How to certify machine learning based safety-critical systems? A systematic literature review', *Autom Softw Eng*, vol. 29, no. 2, p. 38, Apr. 2022, doi: 10.1007/s10515-022-00337-x.

[7] H. Tissot, 'FormulAI: Designing Rule-Based Datasets for Interpretable and Challenging Machine Learning Tasks', *Artificial Intelligence and Applications*, vol. 3, no. 1, pp. 72–82, 2025, doi: 10.47852/bonviewAIA42021781.

[8] A. Olushola and J. Mart, 'Fraud Detection using Machine Learning', *ScienceOpen Preprints*, Jan. 2024, doi: 10.14293/PR2199.000647.v1.

[9] A. Ruchay, E. Feldman, D. Cherbadzhi, and A. Sokolov, 'The Imbalanced Classification of Fraudulent Bank Transactions Using Machine Learning', *Mathematics*, vol. 11, no. 13, p. 2862, Jan. 2023, doi: 10.3390/math11132862.

[10] E. M. Al-dahasi, R. K. Alsheikh, F. A. Khan, and G. Jeon, 'Optimizing fraud detection in financial transactions with machine learning and imbalance mitigation', *Expert Systems*, vol. 42, no. 2, p. e13682, 2025, doi: 10.1111/exsy.13682.

[11] Kanika, J. Singla, A. K. Bashir, Y. Nam, N. U. Hasan, and U. Tariq, 'Handling class imbalance in online transaction fraud detection', *Computers, Materials and Continua*, vol. 70, no. 2, pp. 2861–2877, Sept. 2021.

[12] A. Ali *et al.*, 'ADVANCED MULTIVARIATE STATISTICAL METHODS FOR HIGH DIMENSIONAL DATA MODELING, PREDICTION, AND INTERPRETATION', *Spectrum of Emerging Sciences*, vol. 3, p. 19, Sept. 2025, doi: 10.5281/zenodo.17129973.

[13] Z. Xia, Y. Chen, and C. Xu, 'Multiview PCA: A Methodology of Feature Extraction and Dimension Reduction for High-Order Data', *IEEE Transactions on Cybernetics*, vol. 52, no. 10, pp. 11068–11080, Oct. 2022, doi: 10.1109/TCYB.2021.3106485.

[14] M. A. A. Montaser and M. Bannett, 'Beyond Anomaly Detection: Redesigning Real-Time Financial Fraud Systems for Multi-Channel Transactions in Emerging Markets', *Baltic Journal of Multidisciplinary Research*, vol. 2, no. 3, pp. 1–17, July 2025.

[15] D. Yuan and S. Meng, 'Temporal Feature-Based Suspicious Behavior Pattern Recognition in Cross-Border Securities Trading', *Journal of Sustainability, Policy, and Practice*, vol. 1, no. 2, pp. 1–18, Aug. 2025.

[16] P. Gupta, A. Varshney, M. R. Khan, R. Ahmed, M. Shuaib, and S. Alam, 'Unbalanced Credit Card Fraud Detection Data: A Machine Learning-Oriented Comparative Study of Balancing Techniques', *Procedia Computer Science*, vol. 218, pp. 2575–2584, 2023, doi: 10.1016/j.procs.2023.01.231.

[17] F. O. Aghware *et al.*, 'Enhancing the Random Forest Model via Synthetic Minority Oversampling Technique for Credit-Card Fraud Detection', *J. Comput. Theor. Appl.*, vol. 1, no. 4, pp. 407–420, Mar. 2024, doi: 10.62411/jcta.10323.

[18] S. P, A. I. R, D.Elangovan, K. D. K. Raj, L. R. V. V. L. Rahul, and R. Raja, 'Optimizing Credit Card Fraud Detection with Random Forests and SMOTE', Dec. 03, 2024, *In Review*. doi: 10.21203/rs.3.rs-5539711/v1.

[19] A. M. Aburbeian and H. I. Ashqar, 'Credit Card Fraud Detection Using Enhanced Random Forest Classifier for Imbalanced Data', 2023, *arXiv*. doi: 10.48550/ARXIV.2303.06514.

[20] M. Z. Mizher and A. B. Nassif, 'Deep CNN approach for Unbalanced Credit Card Fraud Detection Data', in *2023 Advances in Science and Engineering Technology International Conferences (ASET)*, Dubai, United Arab Emirates: IEEE, Feb. 2023, pp. 1–7. doi: 10.1109/ASET56582.2023.10180615.

[21] A. Meliboev, J. Alikhanov, and W. Kim, '1D CNN Based Network Intrusion Detection with Normalization on Imbalanced Data', Mar. 04, 2020, *arXiv*: arXiv:2003.00476. doi: 10.48550/arXiv.2003.00476.

[22] F. A. Ghaleb, F. Saeed, M. Al-Sarem, S. N. Qasem, and T. Al-Hadhrami, 'Ensemble Synthesized Minority Oversampling-Based Generative Adversarial Networks and Random Forest Algorithm for Credit Card Fraud Detection', *IEEE Access*, vol. 11, pp. 89694–89710, 2023, doi: 10.1109/ACCESS.2023.3306621.

[23] T.-H. Lin and J.-R. Jiang, 'Credit Card Fraud Detection with Autoencoder and Probabilistic Random Forest', *Mathematics*, vol. 9, no. 21, p. 2683, Oct. 2021, doi: 10.3390/math9212683.

[24] W. Li, C. Wu, and S. Ruan, 'CUS-RF-Based Credit Card Fraud Detection with Imbalanced Data', *JRACR*, vol. 12, no. 3, Sept. 2022, doi: 10.54560/jracr.v12i3.332.

[25] C. Mabani, A. A. Tuskov, and E. V. Shchanina, 'DETECTION OF CREDIT CARD FRAUDS WITH MACHINE LEARNING SOLUTIONS: AN EXPERIMENTAL APPROACH', *HK*, vol. 11, no. 3, pp. 17–28, Oct. 2022, doi: 10.12731/2070-7568-2022-11-3-17-28.

BIMA
BULLETIN OF INTELLIGENT MACHINES AND ALGORITHMS
Vol. 1 No.1 November 2025
E-ISSN: 3123-5115
DOI: 10.65780/k6hexq72