International Journal of Emerging Research in Engineering and Technology
Pearl Blue Research Group | Volume 7 Issue 1 PP 163-170, 2026
ISSN: 3050-922X | https://doi.org/10.63282/3050-922X.IJERET-V7I1P122

Original Article

Real-Time Detection of Credit Card Fraud in Online Payment Practices: A Deep Learning Methods

Moinul Islam
Algonquin College of Applied Arts and Technology, Ottawa, Ontario, Canada.

Received On: 04/01/2025 ***Revised On: 06/02/2026*** ***Accepted On: 11/02/2026*** ***Published On: 15/02/2026***

Abstract *- The detection of fraudulent credit card transactions has become more challenging due to the growing reliance on digital payment systems. This is especially true in situations with huge financial data dimensions and major class imbalances. A Convolutional Neural Network (CNN) based efficient credit card fraud (CCF) management system is proposed in this paper as a solution to this problem. The CNN can identify intricate and non-linear transaction patterns from transaction data. Experimentation was performed on the European cardholder credit card fraud data retrieved on Kaggle, which is highly imbalanced, and it mirrors the real-life behavior of transactions. Data cleanup, minmax normalization, feature selection using Principal Component Analysis (PCA), and class balance using the Synthetic Minority Oversampling Technique (SMOTE) were all steps in a lengthy data pretreatment pipeline. The data used for training and testing were divided 70:30. Used F1-score (F1), recall (REC), accuracy (ACC), and precision (PRE) to measure the suggested CNN model as well. Based on the experimental data, the CNN model outperforms some of the existing ML and DL models with 94.8% ACC, 93.9% PRE, 95.6% REC, and 94.7% F1. The results back up claims that a CNN-based system can detect CCF in online payment systems in real-time and is reasonable, reliable, and scalable.*

Keywords *- Credit card fraud, Fraud-detection system (FDS), Electronic transactions, Machine Learning, Deep Learning.*

1. Introduction

The increasing digitalization of financial services has significantly improved transaction accessibility and efficiency, but has also resulted in an outbreak of fraudulent activities. As online banking, e-commerce, and mobile payments increase, financial institutions continue to be threatened by advanced online fraudsters who take advantage of transaction systems' loopholes[1]. A new level of convenience for buyers and sellers has resulted from the meteoric rise of online shopping and payment processing. The growth, however, has brought with it the problem of online payment fraud, which seriously undermines the trustworthiness and safety of these systems. Large sums of money, damage to one's reputation, and a decline in customer confidence are all possible outcomes of fraud [2]. This has made it essential that businesses should develop effective fraud detection systems in order to protect their business activities and clientele[3][4]. The prevalent issue of credit card fraud (CCF) impacts both consumers and financial organizations. Online shopping and electronic payment systems are growing in popularity, giving fraudsters more chances to take advantage of security holes and commit fraud.

Credit card fraud (CCF) detection, as defined by US law, is the unlawful duplicate and unauthorized use of another person's bank account information[5]. Payments made by non-cardholders result in illegal transactions involving credit cards or account information. Increased amounts of fraudulent conduct, especially CCF, have resulted from the growing popularity of major digital payment networks and internet banking. The yearly financial losses incurred by criminals surpass billions of dollars[6][7]. Digital payments in today's financial institutions require CCF detection to protect data. The trend away from physical money is already visible, as all business owners can attest. A common payment option is eliminated from upcoming transaction methods[8]. As a result, today's payment systems cannot support future business expansion. Business operations routinely interfere with cash flow. Payments made with debit and credit cards are the most popular methods. Businesses must thus update their environment to accommodate new payment methods. According to current expectations, things have gotten far worse than anticipated[9]. A variety of pertinent real-time issues are involved in the problem of CCF, which includes class imbalance, idea drift, and verification delays. Nevertheless, the great majority of existing systems are based on presumptions that rarely address all of the critical issues of a fraud-detection system (FDS), such as data mining, genetic algorithms, AI, fuzzy logic, DL, ML, and so forth[10][11]. In order to differentiate between legitimate and fraudulent transactions, CCFD usually use DL and ML approaches to develop classification models[12][13]. DL algorithms are discovered to have excellent performance. These algorithms can handle a variety of tasks when used to address issues with the help of big data.

1.1. Motivation and Contribution

The motivation for this study stems from the increasing complexity and frequency of CCF in online payment systems, which pose serious security and financial threats to both financial institutions and customers. Conventional fraud detectors are usually ill-suited to handle highly lopsided data and are slow to adjust to changing fraud trends. To overcome this challenge, it is important to come up with smart models that are data-driven and can detect the rare fraudulent activities effectively without affecting the performance of the normal transactions. The study uses sophisticated ML and DL methodologies, excellent feature selection, and data balancing strategies to increase the ACC and dependability of fraud detection systems, eventually making digital financial transactions safer. This study has a number of contributions to the study of CCFD on Online Payment:

- Using the SMOTE oversampling method, the Kaggle CCFD dataset was utilised to tackle the severe class imbalance issue.
- Used a full-fledged data pre-processing pipeline such as outlier removal, normalization and missing value processing to guarantee data quality.
- Used PCA to efficiently reduce model dimensionality and select features, leading to more ACC and efficient results.
- Proposed and evaluated an innovative CNN model that outperformed conventional models in terms of performance metrics.
- Assessed model performance comprehensively using several assessment indicators, such as REC, ACC, PRE, and F1.

1.2. Justification and Novelty

The justification behind this work is based on the fact that there is a need to get proper and dependable fraud-detection models that can process high-dimensional and highly imbalanced online transaction data. The traditional methods of machine learning can typically be based on hand-defined feature engineering and demonstrate weak capabilities to learn sophisticated, non-linear fraud trends. The suggested CNN-based model is capable of detecting transactions by automatically learning hierarchical representations of transaction data. A combination of PCA and SMOTE also improves model efficiency and class balance. The innovation is in the successful adaptation of a convolutional DL structure to structured credit card data, with the simultaneous balance of improvement in all major performance indicators.

2. Literature Review

A wide range of significant research studies on CCFD in online payment systems have been reviewed and analyzed to inform and strengthen the foundation of this work.

Prajapati, (2025) details a method for detecting financial fraud using recurrent neural networks on the Kaggle CCFD dataset, which takes into account the imbalance between classes and the dimensionality of features. Effective training and enhanced model performance were ensured by pre-processing the dataset using methods such as PCA for feature reduction and SMOTE for data balancing. The proposed RNN model demonstrated exceptional predictive capability, achieving an ACC of 99.78%, PRE of 99.73%, REC of 99.79%, and an F1 of 99.76%[14]. Dharma and Latha (2025) present a hybrid ML method for identifying CCF. The analysis's dataset was gathered from 284,807 European cardholder transactions in September 2013. The results of Hybrid ML methods depend on ACC, PRE, REC, and F1. Results state that, described model achieves high performance parameters, ACC, PRE, REC and F1 of 97%,96%,97%,970/0 respectively than other models[15]. Emangusi et al., (2024) creation of a model capable of reliably detecting CCF is key. Synthetic minority oversampling has helped with the issue of class inequality. To assess how well the suggested model works, compared its f-measure, detection rate, and ACC to previous research in the field. The results show that the proposed model is better than the state-of-the-art relevant models that are already available. It has an F-measure of 0.75976 and an ACC of 0.99924 [16].

Gajakosh et al. (2024) aim to create an SVM model that can distinguish abnormalities from regular patterns produced by CSO based on data. The CSO-SVM method, which is based on unsupervised learning, is employed to efficiently detect CCF. In comparison to other methods such as DCNN, and coarse KNN, the applied CSO-SVM strategy delivers great performance with an accuracy rate of 99.88% [17]. Khanom et al., (2024) propose an optimized RNN for detecting fraudulent transactions. The RNN model obtained over 100% ACC, as shown by testing on two public benchmark datasets. The macro average ACC, REC, and F1 for the first dataset were 0.83, 0.93, and 0.87, respectively. With an ACC of 99%, macro average PRE of 0.70, REC of 0.89, and F1 of 0.76 for the second dataset, it fared better than traditional ML models[18]. Mizher and Nassif (2023) provide two machine learning techniques and a CNN method to tackle the issue of CCFD. The results indicate that the RF classifier outperformed other models with an accuracy of 99.7% [19].

Arun and Rajesh (2022) focus on creating the BEPO-OGRU methodology, which is a feature selection method based on BEPO and OGRU for detecting CCF. Additionally, the OGRU-based credit card categorization model demonstrates the work's uniqueness, which is generated by using the Harris Hawks optimization (HHO) method to best choose the GRU's hyperparameters. The BEPO-OGRU approach was enhanced through a variety of simulations, resulting in increased accuracy of 94.78% and 94.16% on the German Credit dataset and CCFD dataset, respectively[20]. Karthika and Senthilselvi, (2022) The research project's goal is to apply ensemble-based machine learning algorithms for CCFD. Two authentic datasets of credit card transactions in the public domain—both legitimate and fraudulent—were used to execute standard tests on the suggested model. The additional tree classifier has outperformed previous machine learning techniques and attained excellent efficiency, including 96% ACC and 57.95% F1-measure[21].

The Table I summarizes recent deep learning studies on CCFD for online payments, highlighting innovative models, datasets used, key outcomes, and the challenges faced.

Table 1: Overview of Recent Studies on Credit Card Fraud Detection for Online Payment using deep learning

Author	Proposed Work	Dataset	Key Findings	Challenges/recommendation
Prajapati (2025)	RNN-based fraud detection with PCA and SMOTE	Kaggle CCFD	F1-score: 99.76%, Accuracy: 99.78%, Precision: 99.73%, Recall: 99.79%	Class imbalance handled with SMOTE; deep learning outperforms traditional ML
Dharma & Latha (2025)	Hybrid ML model using SVM and Logistic Regression	284,807 transactions (Sept 2013, Europe)	F1-score: 97%, recall: 97%, accuracy: 97%, and precision: 96%	Emphasizes hybrid modeling for better results
Elmangoush et al. (2024)	Sequential DL with SMOTE	Real-world CCFD	Accuracy: 99.924%, F1-score: 0.75976	Improved feature extraction; addresses class imbalance
Gajakosh et al. (2024)	CSO-SVM anomaly detection	Credit card transaction data	Accuracy: 99.88%	CSO-SVM outperforms CNN, DCNN, and KNN
Khanom et al. (2024)	Optimized RNN model	Two public datasets	Dataset 1: Accuracy ≈ 100%, F1: 0.87; Dataset 2: Accuracy: 99%, F1: 0.76	RNN outperforms traditional models; emphasizes transaction security
Mizher & Nassif (2023)	CNN with ML for fraud and attack detection	Real-world imbalanced dataset	RF Accuracy: 99.7%	Need for better handling of unfamiliar patterns and large-scale data
Arun & Rajesh (2022)	BEPO-based feature selection with OGRU (GRU tuned with HHO)	German Credit & Kaggle CCFD	Accuracy: 94.78% (German), 94.16% (Kaggle)	Novel optimization enhances GRU performance
Karthika & Senthilselvi (2022)	Ensemble ML with RFE and SMOTE	Two public CCFD datasets	Accuracy: 96%, F1-score: 57.95%	Emphasis on ensemble classifiers and RFE for feature importance

3. Research Methodology

The proposed Convolutional Neural Networks (CNN) model was implemented for CCFD using a structured methodology. Initially, the dataset from Kaggle was cleaned by removing missing values and outliers. Data normalization, SMOTE, and PCA were utilized for feature selection and dimensionality reduction. After that, a portion of the data was split into 30% testing and 70% training. The CNN model is a linked neural layer DL architecture, designed to enhance feature learning and pattern recognition. The model's performance was assessed using common metrics such as F1, ACC, PRE, and REC in order to confirm how well it predicted and classified CCF in online payments. Figure 1 shows the entire procedure.

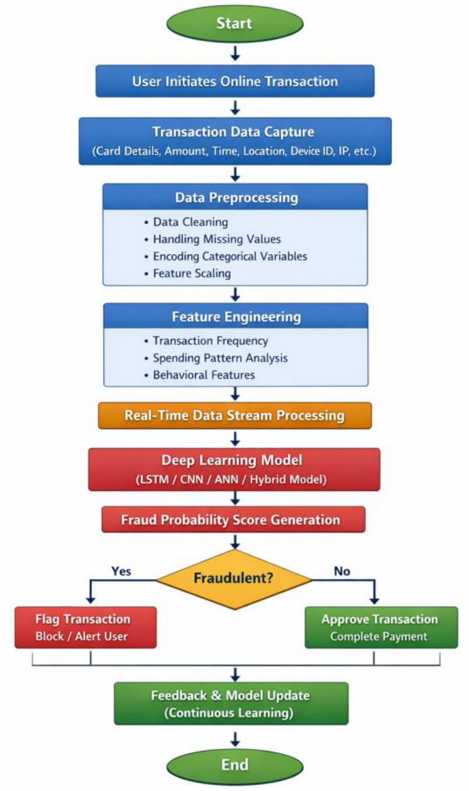

Fig 1: Proposed flowchart for Credit Card Fraud Detection

The following provides a comprehensive explanation of each step described in the suggested flowchart for predictive modeling of CCFD in online payment systems.

3.1. Data collection

Data from 284,807 transactions spanning two days was collected from Kaggle and pertains to credit card transactions made by European cardholders. With 284,315 regular transactions and just 492 fraudulent transactions, the sample is wildly unbalanced. It has 31 characteristics, such is the quantity of transactions and the moment at which a transaction occurred, and 28 other characteristics labelled V1 through V28. As an added bonus, it features the target label "Class," which uses a binary value of "1" or "0" to assess if a transaction is fraudulent. Attack distribution, feature correlations, and other data were examined using data visualizations, including bar plots and heatmaps, which are shown below:

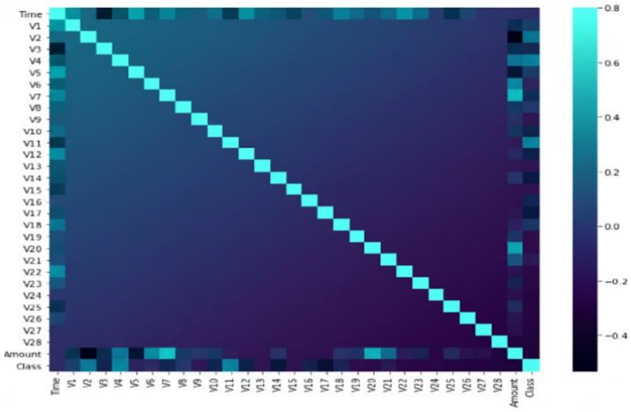

Fig 2: Correlation Plot of Feature Variables

Figure. 2 presents the heatmap of the relationship between the dataset's feature variables for CCFD. The diagonal elements show perfect self-correlation with the value of 1.0, with the majority of the off-diagonal correlations near zero, indicating weak linear relationships among features. The correlation coefficients are mostly within the range of about -0.5 to 0.8, with a few features having mild positive and negative correlations.

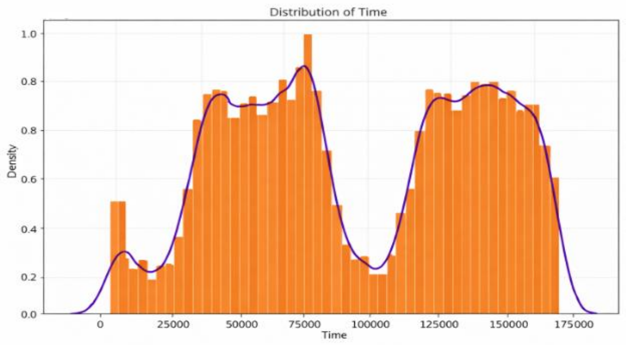

Fig 3: Transaction Time of European Cardholder Dataset

In the credit card records of European cardholders, Figure. 3 shows how the transaction times are spread out. The histogram (as well as the smooth density curve) demonstrates that transactions are not distributed across time evenly but are of different activity patterns with several peaks. It is also found that higher transaction densities are experienced at certain time intervals, meaning the time when the card is used more frequently and the densities are lower and show the time when the card is not used significantly.

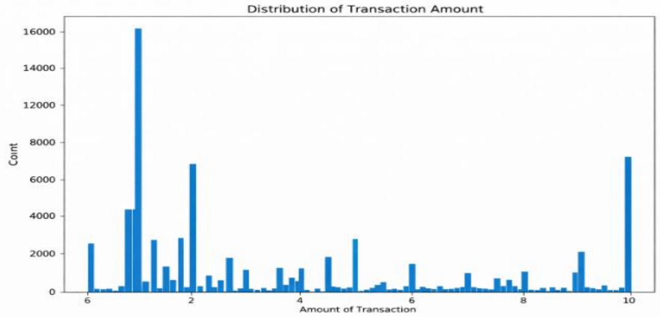

Fig 4: Transaction Amount of European Cardholder Dataset

Figure. 4 illustrates the distribution of transactions in the European Cardholder credit card data is distributed. In the histogram, the distribution is very skewed, with most of the transactions on the lower amount values and a few on the higher amount values. This extended behavior suggests that high-value transactions are quite infrequent in number, but noteworthy, which is characteristic of real-world financial data. This variability in the transaction amounts underscores the significance of amount-related characteristics in differentiating normal and fraudulent transactions in the CNN model to allow it to learn meaningful patterns related to abnormal behavior in transactions.

3.2. Data pre-processing

The data preparation process began with the acquisition of the Kaggle CCFD dataset, which was cleaned and concatenated to preserve consistency. Relevant features were determined and any missing values and outliers were eliminated. This dataset was then pre-processed with the transformation and normalization of the data. Pre-processing details are presented below:

- Remove missing value: Removing missing values from a dataset is a common task in data pre-processing. The method used would depend on the kind and extent of the missing data[22].
- Remove Outliers: The practice of identifying and removing outliers from a dataset is known as data cleaning, which are items that are not similar to the rest of the data.

3.3. Data Normalization

Normalization of records was performed with the min-max method, and limited the values to a range between 0 and 1[23]. This was done to optimize the performance of the used classifiers and to counter the influence of outliers. Normalization was done based on the mathematical Equation (1) as follows:

$$X' = \frac{X - X_{min}}{X_{max} - X_{min}}$$

the feature's initial value X, its normalised score X', its minimum value X_{min}, and its maximum value X_{max}.

3.4. Feature selection using PCA

The goal of feature selection in ML is to enhance the model's performance and readability by selecting the most relevant subset of features (input variables) from a bigger collection [24]. A feature selection can be used to reduce overfitting, decrease the computational cost and also enhance the accuracy and generalization of a model by eliminating the features. The feature selection can be performed with the help of PCA, which identifies and selects the most significant features according to their contribution to the principal components. The original characteristics are transformed by PCA into a set of principal components, a new collection of uncorrelated variables, which show the directions with the greatest variation in the data.

3.5. Data balancing with SMOTE

The acronym SMOTE stands for Synthetic Minority Oversampling Technique. Similarly, the problem of uneven class representation in datasets has been addressed by SMOTE, specifically in the creation of models that forecast CCF. To overcome the lack of minority-class instances, it generates synthetic data points without recreating them.

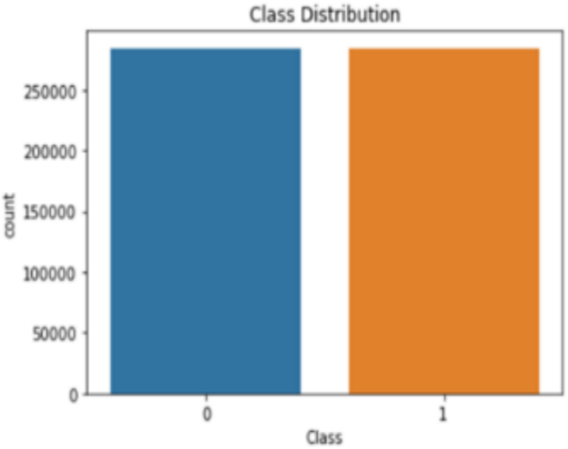

Fig 5: Balancing Graph of Applying SMOTE

The distribution of classes produced after using SMOTE, with an equal quantity of legitimate and fraudulent transactions, is shown in Figure. 5. By minimizing class imbalance, this equilibrium enables the model to acquire the two classes in equal measure, which enhances its capacity to detect fraud.

3.6. Data Splitting

The model's efficacy was assessed by dividing the datasets into testing and training subsets; the former were utilised for 70% of the evaluation, while the latter were reserved for 30% of the testing and performance evaluation.

3.7. Proposed Convolutional Neural Networks (CNN) Model

A number of CCFD models have recently made use of the CNN, a well-liked DL architecture. The results it produces for picture recognition are state-of-the-art. The structure's neurones can acquire biases and weights through learning. The CNN's completely associated coatings transform the final output after the pooling and convolutional layers have down-sampled and recovered features, respectively[25]. This conversion provides a probability estimate in a classification issue such as CCFD for each category (fraud or non-fraud).

The CNN mimics the information processing in organic brain systems by adaptively modifying these connections, allowing the network's capacity to independently extract sample attributes without previous information[26]. The result of the last iteration, y_{ccnn} , is acquired once the iterations are finished. Following y_{cnn}'s passage into the fully linked layer, Equation (2) yields the network's ultimate output:

$$y_{out} = A_2.\left(ReLU(A_1 \cdot y_{cnn} + C_1)\right) + c_2$$

The activation function is ReLU, the weight matrix and bias of the second fully connected layer utilised for classification are A_2 and C_2, the activation function of the first fully connected layer is A_1 and C_1, and the output vector followed by the second fully connected layer utilised for classification is y_{out}. The following equation (3) represents it:

$$ReLU(X) = max(x, 0)$$

Use the cross-entropy loss function to tell the network what changes to make based on the difference between what the model said would happen and what actually happened.

4. Results and Discussion

This part describes the setup of the experiment and evaluates the suggested model's performance in both the training and testing phases. The convolutional neural network (CNN) model was built using a Windows 10 PC with a 2.30 GHz processor, 8 GB of RAM, and Excel 2013 as the coding language.

4.1. Evaluation Metrics

The dataset's high-class imbalance renders accuracy an inappropriate criterion for evaluating the model. The purpose of CCFD systems is to identify all fraudulent activity and minimize false alarms, which are legitimate transactions that are incorrectly labeled as fraudulent. The choice of the measure for assessment is contingent upon the nature of the solution[27]. In this work, employ a confusion matrix to categorize circumstances that are fraudulent as positive and non-fraudulent (legal) as negative. FN are fraud cases that are expected to be nonfraud, FP are nonfraud instances that are anticipated to be fraud, and TN are instances of nonfraud that are correctly expected to be fraudulent. The following equations can help understand the assessment measures: Accuracy, Precision, Recall, and F1 Score, which are derived from Equations (4-7):

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{FP} + \text{FN} + \text{TN}}$$

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}}$$

$$\text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}}$$

$$\text{F1} - \text{score} = 2 * \frac{(\text{precision} * \text{recall})}{(\text{precision} + \text{recall})}$$

It is evident that positive anticipated values are linked to accuracy. Because precision rises as the frequency of FP falls, it is a helpful indication when the cost of having FP is high. Recall is linked to TP, according to Eq. (6). Recall is improved by lowering the number of FN, and problems with the high expense of FN usually lead to strong recall[28]. To identify CCF, a balance between FP and FN must be maintained. The REC is high, but the ACC, PRE, and F1 are low if all samples are projected to be fraudulent, if all samples are anticipated to be nonfraudulent, the REC is nil, the PRE is undefined, and the F1 is high. To enable fair comparison and trustworthy performance evaluation, these measures were used uniformly across all models.

4.2. Results

In Table II findings on the CCFD dataset reveal that with an average of 94.8% ACC, 93.9% PRE, 95.6% REC, and a 94.7% F1, the proposed CNN model is highly effective in identifying CCF, which means that it can reliably and well-balanced identify fraud transactions on the internet payment systems.

Table 2: Experiment Results of Proposed Models for of Credit Card Fraud Detection for Online Payment on CCFD dataset

Performance matrix	Convolutional Neural Networks (CNN) Model
Accuracy	94.8
Precision	93.9
Recall	95.6
F1-score	94.7

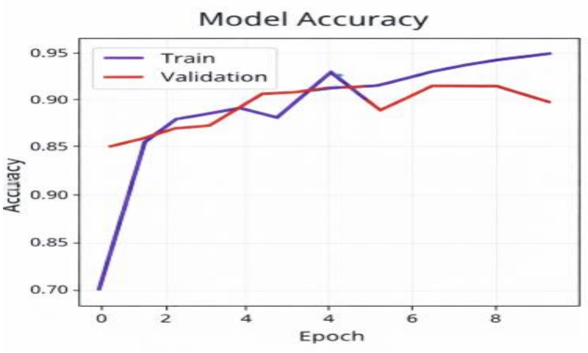

Fig 6: Accuracy Curves for the CNN Model

The training and validation accuracy curves for the CNN model with epochs are shown in Figure. 6. The ACC of the training is in a straight increasing pattern, which means the model is being learned successfully and has converged. The validation accuracy shows that there are slight fluctuations compared to the training curve, indicating good generalization and a little at that point, overfitting.

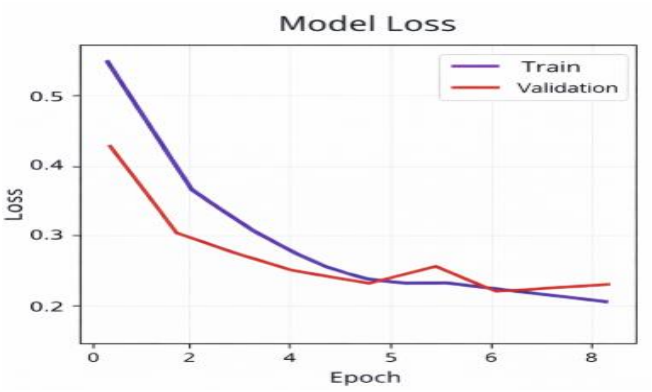

Fig 7: Loss Curves for the CNN Model

The CNN model's training and validation loss curves as a function of subsequent epochs are displayed in Figure 7. The training loss continues to decrease, suggesting that it is optimised and that model learning is progressing. Likewise, the validation loss is a decreasing trend with random variations that are relatively close to the training loss, indicating a good generalization and a small amount of overfitting. The two curves coming together is an indication of the stability of CNN model and its effectiveness in utilising the CCFD dataset to precisely identify CCF.

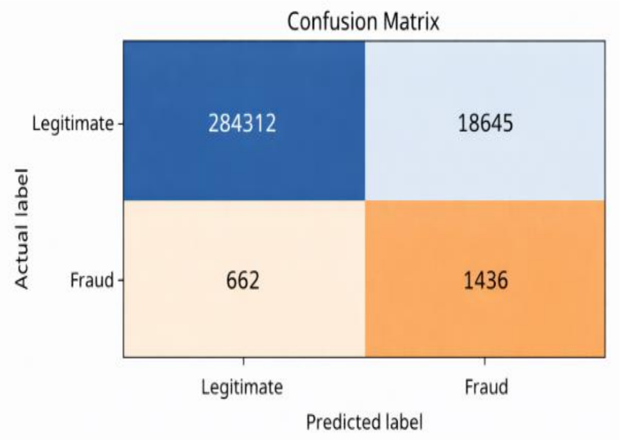

Fig 8: Confusion Matrix for CNN

Figure 8 displays the confusion matrix of the CNN model used to identify CCF using the CCFD dataset. The model properly differentiates 284,312 legitimate and 1,436 fraudulent transactions, which can be said to have a good discrimination capacity. A relatively large part of legitimate transactions (18,645) is misclassified as fraud, whereas very few fraudulent transactions (662) are misclassified as legitimate.

4.3. Comparative Analysis

A comparison accuracy analysis was carried out against other current models to verify the efficacy of the suggested CNN model, as shown in Table III. With the best ACC (94.8%), PRE (93.9%), REC (95.6%), and F1 (94.7%) of all the tested approaches, the suggested CNN model is better and more balanced. Conversely, the DT model achieves moderate accuracy 92% with low levels of reporting of precision, whereas DenseNet121 and SVM models have lower ACC and F1, which reflect poor generalization and fraud detection.

Table 3: Accuracy Comparison of different Predictive models of Credit Card Fraud Detection for Online Payment

Models	Accuracy	Precision	Recall	F1-score
DT[29]	92	-	93	92
DenseNet121[30]	89.1	84.9	89.4	89.8
SVM[31]	89.6	85.6	90.3	87.9
CNN	94.8	93.9	95.6	94.7

The suggested model for detecting CCF, which was developed using a CNN, is aimed at learning complex and non-linear patterns of online payment system transaction data that are high-dimensional in nature. The model is able to learn subtle patterns in behavioral distinctions between fraudulent and legal transactions without having to manually engineer a large number of features by using automatic feature extraction and learning hierarchical representations. The primary advantage of the suggested model is its high detection, as seen by higher REC, ACC, PRE, and F1. These lowers missed fraud instances and false positives.

5. Conclusion and future study

The number of financial transactions carried out online has dramatically expanded since the advent of digital commerce, and banks and payment service providers are now concerned about CCF. The demand is high to have clever models capable of discriminating between clearly legitimate and malicious transactions as fraud cases have become increasingly sophisticated. This study evaluates a highly skewed dataset of European cardholders to offer a workable model for identifying CCF using a CNN. Through thorough data preparation, including normalization, PCA feature selection, and SMOTE class balancing, the model demonstrated the ability to learn intricate and non-linear transaction patterns. The experiment's results show that the proposed CNN model may offer a comprehensive assessment of the ability to detect fraud and lower false alarms, with 94.8% ACC, 93.9% PRE, 95.6% REC, and 94.7% F1. The CNN model's power and superiority are further demonstrated by comparison with existing ML and DL techniques.

Further research will be carried out to prove the model on several large-scale and real-time datasets, implement the online and incremental learning methods to address the dynamic behavior of fraud and investigate new and advanced architectures, including hybrid CNNLSTM or attention-based architectures. Moreover, Transparency may be increased by employing explainable AI (XAI) approaches and trust of the model, and make the system more realistic to be implemented in real-field financial context.

References

[1] V. Verma, “Deep Learning-Based Fraud Detection in Financial Transactions : A Case Study Using Real-Time Data Streams,” vol. 3, no. 4, pp. 149–157, 2023, doi: 10.56472/25832646/JETA-V3I8P117.

[2] S. K. Tiwari, “Quality Assurance Strategies in Developing High-Performance Financial Technology Solutions,” *Int. J. data Sci. Mach. Learn.*, vol. 05, no. 01, pp. 323–335, Jun. 2025, doi: 10.55640/ijdsml-05-01-26.

[3] P. Bernard, N. El Mekkaoui De Freitas, and B. B. Maillet, “A financial fraud detection indicator for investors: an IDeA,” *Ann. Oper. Res.*, vol. 313, no. 2, pp. 809–832, Jun. 2022, doi: 10.1007/s10479-019-03360-6.

[4] S. B. Shah, “Advancing Financial Security with Scalable AI: Explainable Machine Learning Models for Transaction Fraud Detection,” in *2025 4th International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE)*, IEEE, Apr. 2025, pp. 1–7. doi: 10.1109/ICDCECE65353.2025.11034838.

[5] D. Patel, “Enhancing Banking Security: A Blockchain and Machine Learning- Based Fraud Prevention Model,” *Int. J. Curr. Eng. Technol.*, vol. 13, no. 06, pp. 576–583, 2023, doi: 10.14741/ijcet/v.13.6.10.

[6] F. Z. El Hlouli, J. Riffi, M. A. Mahraz, A. Yahyaouy, K. El Fazazy, and H. Tairi, “Credit Card Fraud Detection: Addressing Imbalanced Datasets with a Multi-phase Approach,” *SN Comput. Sci.*, vol. 5, no. 1, p. 173, Jan. 2024, doi: 10.1007/s42979-023-02559-6.

[7] A. Nerella *et al.*, “AI-Driven Risk Assessment Models for Personalized Credit Scoring in Emerging FinTech Ecosystems,” in *in The 16th International IEEE Conference On Computing, Communication And Networking Technologies (ICCCNT)*, 2025.

[8] A. Parupalli, “Business Intelligence in ERP ML-Based Comparative Study for Financial Forecasting,” *ESP Int. J. Commun. Eng. Electron. Technol.*, vol. 2, no. 4, pp. 17–26, 2024, doi: 10.56472/25839217/IJCEET-V2I4P103.

[9] E. Ileberi, Y. Sun, and Z. Wang, “Performance Evaluation of Machine Learning Methods for Credit Card Fraud Detection Using SMOTE and AdaBoost,” *IEEE Access*, vol. 9, pp. 165286–165294, 2021, doi: 10.1109/ACCESS.2021.3134330.

[10] A. Dal Pozzolo, G. Boracchi, O. Caelen, C. Alippi, and G. Bontempi, “Credit Card Fraud Detection: A Realistic Modeling and a Novel Learning Strategy,” *IEEE Trans. Neural Networks Learn. Syst.*, vol. 29, no. 8, pp. 3784–3797, Aug. 2018, doi: 10.1109/TNNLS.2017.2736643.

[11] T. Shah, “The Role of Customer Data Platforms (CDPs) in Driving Hyper-Personalization in FinTech,” *Int. Res. J. Eng. Technol.*, vol. 12, no. 04, p. 10, 2025.

[12] R. R. Popat and J. Chaudhary, “A Survey on Credit Card Fraud Detection Using Machine Learning,” in *Proceedings of the 2nd International Conference on Trends in Electronics and Informatics, ICOEI 2018*, 2018. doi: 10.1109/ICOEI.2018.8553963.

[13] R. Q. Majumder, “A Review of Anomaly Identification in Finance Frauds Using Machine Learning Systems,” *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 5, no. 10, pp. 101–110, Apr. 2025, doi: 10.48175/IJARSCT-25619.

[14] V. Prajapati, “Exploring Machine Learning Models for

Fraud Identification Through Credit Cards in Financial Market," in *2025 Global Conference in Emerging Technology (GINOTECH)*, IEEE, May 2025, pp. 1–6. doi: 10.1109/GINOTECH63460.2025.11076669.

[15] B. Dharma and D. Latha, "Fraud Detection in Credit Card Transactional Data Using Hybrid Machine Learning Algorithm," in *2025 6th International Conference on Mobile Computing and Sustainable Informatics (ICMCSI)*, 2025, pp. 213–218. doi: 10.1109/ICMCSI64620.2025.10883549.

[16] A. M. Elmangoush, H. O. Hassan, A. A. Fadhl, and M. A. Alshrif, "Credit Card Fraud Detection Using Synthetic Minority Oversampling Technique and Deep Learning Technique," in *2024 IEEE 7th International Conference on Advanced Technologies, Signal and Image Processing (ATSIP)*, 2024, pp. 455–458. doi: 10.1109/ATSIP62566.2024.10638849.

[17] A. Gajakosh, R. A. Reddy, M. Mundher adnan, G. Rajalaxmi, and P. R, "Fraud Detection in Credit Card Using Competitive Swarm Optimization with Support Vector Machine," in *2024 International Conference on Distributed Computing and Optimization Techniques (ICDCOT)*, 2024, pp. 1–4. doi: 10.1109/ICDCOT61034.2024.10515953.

[18] K. Khanom, M. Jannat, A. K. M. Masum, R. Connolly, and M. A. K. Azad, "A Novel Approach to Credit Card Fraud Detection: Optimizing Recurrent Neural Networks," in *2024 4th International Conference on Ubiquitous Computing and Intelligent Information Systems (ICUIS)*, 2024, pp. 49–56. doi: 10.1109/ICUIS64676.2024.10867025.

[19] 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 2023*, 2023. doi: 10.1109/ASET56582.2023.10180615.

[20] G. K. Arun and P. Rajesh, "Design of Metaheuristic Feature Selection with Deep Learning Based Credit Card Fraud Detection Model," in *Proceedings of the 2nd International Conference on Artificial Intelligence and Smart Energy, ICAIS 2022*, 2022. doi: 10.1109/ICAIS53314.2022.9742937.

[21] J. Karthika and A. Senthilselvi, "Credit Card Fraud Detection based on Ensemble Machine Learning Classifiers," in *3rd International Conference on Electronics and Sustainable Communication Systems, ICESC 2022 - Proceedings*, 2022. doi: 10.1109/ICESC54411.2022.9885649.

[22] Y. Macha and S. K. Pulichikkunnu, "An Explainable AI System for Fraud Identification in Insurance Claims via Machine-Learning Methods," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 3, no. 3, pp. 1391–1400, Jul. 2023, doi: 10.48175/IJARSCT-11978X.

[23] S. B. Karri, S. Gawali, S. Rayankula, and P. Vankadara, "AI Chatbots in Banking: Transforming Customer Service and Operational Efficiency," in *Advancements in Smart Innovations, Intelligent Systems, and Technologies*, 2025, pp. 61–81. doi: 10.3233/FAIA251498.

[24] S. R. Kurakula, "Architectural Challenges in Modernizing Legacy Financial Systems with Microservices and AI," *World J. Adv. Eng. Technol. Sci.*, vol. 15, no. 02, pp. 1328–1337, 2025.

[25] S. J. Wawge, "A Survey on the Identification of Credit Card Fraud Using Machine Learning with Precision, Performance, and Challenges," *Int. J. Innov. Sci. Res. Technol.*, vol. 10, no. 4, pp. 3345–3352, May 2025, doi: 10.38124/ijisrt/25apr1813.

[26] B. R. Ande, "Federated Learning and Explainable AI for Decentralized Fraud Detection in Financial Systems," *J. Inf. Syst. Eng. Manag.*, vol. 10, no. 35s, pp. 48–56, 2025, doi: 10.52783/jisem.v10i35s.5921.

[27] Y. Wu, L. Wang, H. Li, and J. Liu, "A Deep Learning Method of Credit Card Fraud Detection Based on Continuous-Coupled Neural Networks," *Mathematics*, vol. 13, no. 5, pp. 1–18, 2025, doi: 10.3390/math13050819.

[28] V. Verma, "Security Compliance and Risk Management in AI-Driven Financial Transactions," *Int. J. Eng. Sci. Math.*, vol. 12, no. 7, pp. 107–121, 2023.

[29] J. K. Afriyie *et al.*, "A supervised machine learning algorithm for detecting and predicting fraud in credit card transactions," *Decis. Anal. J.*, vol. 6, Mar. 2023, doi: 10.1016/j.dajour.2023.100163.

[30] A. A. Almazroi and N. Ayub, "Online Payment Fraud Detection Model Using Machine Learning Techniques," *IEEE Access*, vol. 11, pp. 137188–137203, 2023, doi: 10.1109/ACCESS.2023.3339226.

[31] P. Jeyachandran, A. S. V. V. Akisetty, P. Subramani, O. Goel, S. P. Singh, and E. A. Shrivastav, "Leveraging Machine Learning for Real-Time Fraud Detection in Digital Payments," *Integr. J. Res. Arts Humanit.*, vol. 4, no. 6, pp. 70–94, Nov. 2024, doi: 10.55544/ijrah.4.6.10.