Journal of Global Research in Electronics and Communication
Volume 1, No. 8, August 2025
Available Online at: www.jgrec.info

RESEARCH PAPER

Development in Machine Learning (ML) Algorithms for Fraudulent Identification in Banking Sector Via Credit Cards

Dr. Bal Krishna Sharma
Professor
Department of Computer Sciences and Applications
Mandsaur University
Mandsaur
bksharma7426@gmail.com

***Abstract*—The banking industry is seeing an alarming rise in credit fraud, highlighting the critical need for advanced and flexible fraud detection systems. Using state-of-the-art machine learning algorithms, this study systematically reduces the amount of false positives and increases accuracy in identifying credit card fraud. The CCFD dataset will be meticulously prepared to remove any instances of duplicate or missing data. The subsequent stage is to reduce the dimensionality using PCA. To fix the class disparity, the SMOTE method, which stands for Synthetic Minority Oversampling Technique. LR, NB, and XGBoost are three popular older models that are put side by side with the state-of-the-art CCNN. In trials, the CCNN achieved better results than the benchmark models in terms of F1-score (99.97), accuracy (99.96), precision (99.97), and recall (99.97). When compared to XGBoost (97.22%), NB (91.22%), and LR (94.44%), LR produces an exceptional outcome. The model can identify fraudulent transactions, which makes financial transaction systems more secure and dependable. at this exact moment. The XGBoost, CCNN, LR, NB, machine learning, financial sector, credit card fraud detection dataset, and overall financial industry are subjects that are linked to this topic.**

Keywords—Credit Card Fraud Detection, Machine Learning Algorithms, Convolutional Neural Networks (CCNN), SMOTE (Synthetic Minority Oversampling Technique), Principal Component Analysis (PCA), Financial Transaction Security.

I. INTRODUCTION

Revolutionary advancements in digital technology have caused a sea change in the financial sector during the previous several decades [1]. Among the greatest repercussions of this digital transition is the popularity of credit cards that has become a common place as a mode of payment not only in this world. The convenience and flexibility that comes with using the credit cards are unmatched and through this; people are able to undertake smooth transactions as they make their daily purchase, pay bills as well as online shopping [2][3][4][5]. In addition to the debit card functionality, credit cards also offer additional compensation to customers in the event of purchase of damaged, lost and stolen items.

This increase in use of credit cards can however be traced with the increased fraud that has accompanied the use of credit cards making credit card fraud an imminent problem in the eyes of financial institutions [6]. The online and offline fraudulent transactions have risen to greater levels and fraudsters have come up with advanced tactics in taking advantage of loopholes in the systems. Fraud with credit card usually implies that the information of the card could be used for making transactions with the card without even possessing the card as such [7][8][9][10][11][12].

There is an immediate need to create more intelligent fraud detection systems because the dangers have elevated due to the addictive nature of online transactions [13][14][15][16]. To combat modern deception techniques, traditional approaches are losing ground. See references [17][18][19][20]. The outcome of this is machines and methods to progress credit card fraud detection systems in the banking sector by utilizing AI and ML. By utilizing real-time anomaly and unauthorized activity detection, these technologies enable financial institutions to react to evolving forms of fraud [21][22][23][24]. Incorporating top-tier ML models into business processes can help cut down on losses and win back customers' confidence with lightning-fast, secure transactions [25][26][27][28][29]. Since the methods of fraud are constantly developing, it is crucial to implement efficient AI- and ML-based systems of fabric detection to ensure security and safety in the financial environment.

A. Motivation and Contribution of the Study

The worldwide increase in online financial transactions has made credit card fraud a big concern for banking institutions. Because of factors such as the high dimensionality and anonymization of characteristics, the ever-changing complexity of fraud descriptions, and the incredibly imbalanced nature of transaction data sets, real-time fraud prediction is challenging. The design of traditional machine learning models fails to capture them adequately and as a result the accuracy of detection suffers and false positives are high. Based on this need to overcome these challenges, this paper suggests the use of brain-inspired DL based on architecture of Continuous-Coupled Neural Network (CCNN) that can be utilized in feature learning, class imbalance handling and oriented towards the changes over time in fraudulent transaction in the financial system that can then provide a more versatile and consistent way of fraud detection in financial system. The most important contributions of this study are the following:

- Trains a powerful Utilization of dataset Credit Card Fraud Detection (CCFD) dataset.
- A systematic pre-processing procedure: treating missing values and duplicates, transforming features using Principal Component Analysis (PCA) and

oversampling minority classes with SMOTE helped to enhance the quality of the data and learning of models efficiently.

- To prove its effectiveness, the proposed model will be systematically contrasted with such well-known decision classification algorithms as LR, NB and XG Boost.
- The models are evaluated using the following metrics: F1-score, recall, accuracy, and precision. That way, it can test how well the models detect and generalize.

B. *Justification and Novelty*

The study presented here says that traditional ways of thinking about credit card fraud detection are not good enough because they have problems with class imbalance, higher-dimensional data, and finding complex fraud patterns. The number of false negatives in practical financial systems is going down because models like LR and NB aren't as good at finding small amounts of fraud. In hopes of overcoming such complexities, this paper presents a new methodology using the CCNN which is a brain-inspired deep learning framework that can learn complex spatial and temporal features using dynamic interactions between the neurons and continuous activation functions. The originality of this study is the implementation of CCNN to detect fraud on a credit card, not tested earlier and a strong data pre-processing pipeline represented by feature transformation through PCA and unbalancing of the groups through SMOTE. The proposed method improves traditional models in a number of respects, including accuracy, precision, recall, and F1-score, rendering it a more reliable answer to the problem of financial fraud.

C. *Structure of the Paper*

The paper structure is as follows: Section II reviews the Previous research on identifying fraudulent charges on credit cards. Section III explains the proposed methodology that should be followed, pre-processing and CCNN model. In Section IV, experimental results and analysis are carried out. The paper ends with section V which gives an indication of further work.

II. Literature Review

In this section of the study of the literature on the subject of using ML for credit card fraud detection in financial institutions. Almost all of the studies looked at used some sort of classification method.

Reddy et al. (2025) fraud of credit cards being an issue of paramount importance in the contemporary financial arena, the existing solutions must be potent and effective to reduce the realized losses and protect consumer security. Some of the ML methods evaluated in this study were ML, DL, and BN, and among them were LR, SVM, RF, DT and XGBoost as the ML techniques as well as MLP and DNN as the DL systems. Further, BN was used in causal analysis of relations between features. This characterized a probabilistic framework that can be interpreted efficiently. Despite the remarkable accuracy, precision, and recall demonstrated by ML and DL approaches, Bayesian Networks emerged as the top method for delivering an additional requirement of interpretability and reliability [30].

Beri, Gill and Sharma (2024) popular ML algorithms for detecting fraudulent charges on credit cards include XGBoost and ANN. Credit card transaction data that is publicly available was used to assess the algorithms' recall, accuracy, precision, and F1-score. They investigated the relative computing costs and scalability of ANNs and XGBoost to see which one would be better used in real-time fraud detection systems. In some regions, ANNs outperformed XGBoost, with an accuracy of 92.7%. Financial institutions can use the results to better understand the benefits and drawbacks of each method when trying to implement or upgrade their fraud detection system. This study supports the continuous endeavors to combat credit card fraud and improve monetary safety by utilizing advanced ML techniques [31].

Mosa et al. (2024) FD is a complex topic that alters fraudsters' tactics and the relative rarity of fraudulent versus genuine enterprises. To keep money out of the wrong hands and transactions safe, fraud detection needs to be top-notch. Improved FD mechanism performance and reliability are outcomes of this study's work on a framework for moving from unbalanced to balanced data. data used from the Kaggle CCF benchmark datasets, which comprised information about European credit cardholders, to determine the traits that were most suggestive of fraudulent behaviour. In order to determine how the provided parameters affect the prediction accuracy, two ML classifiers, RF and SVM are employed. They can see that the model is much more efficient now; they achieved a classification accuracy of 97% or higher [32].

Chauhan et al. (2024) ML system that could detect fraudulent and lawful credit card transactions would save $24 billion per year. The system could use methods like Logistic Regression, DT, and KNN. In fraud detection, the cross-validation score, ROC AUC score, and F1 score show the accuracy rates of various systems. using ANOVA for feature selection. They need balanced datasets if they want to improve fraud detection and compare algorithm results appropriately. The logistic regression model had a 92.35% ROC AUC, a 98.01% cross-validation accuracy rate, and a 91% F1 score in regards to fraud detection. Alternatively, the cross-validation score for fraud detection using a decision tree classifier was 96.67% [33].

Afriyie et al. (2023) credit card fraud is at an all-time high, according to Singhal. Several algorithms can now determine, thanks to developments in ML, whether a financial transaction is fake. evaluating the performance of three machine learning models, DT, LR, and RF in predicting, categorizing, and identifying instances of fraudulent credit card purchases. RF outperformed all other examined models with an accuracy rate of 96%. RF is the best ML algorithm for detecting and predicting credit card fraud [6].

Gambo, Zainal and Kassim (2022) ever-changing world of CCF is a staggering yearly loss for both customers and financial institutions. The ability to quickly and accurately detect fraudulent transactions initiated by criminals is, hence, crucial among the several authorized operations. The ADASYN sampling technique is proposed as a CNN model for credit card fraud detection in this research. A more balanced dataset is the target. They generated a 0.99 using their model [34].

Table I summarizes the datasets, techniques, important findings, difficulties, and suggested future research areas of the examined studies on credit card fraud detection, as well as their comparative comparison.

TABLE I. REVIEW SUMMARY OF MACHINE LEARNING APPROACH IN CREDIT CARD FRAUD DETECTION

Author(s)	Dataset	Methodology	Findings / Challenges	Future Work
Reddy et al. (2025)	Not specified	LR, SVM, RF, DT, XGBoost, MLP, DNN, Bayesian Network	ML and DL achieved high accuracy; Bayesian Network offered superior interpretability and reliability.	Explore hybrid models combining interpretability with high-performance classifiers.
Beri, Gill and Sharma (2024)	Public credit card transaction dataset	ANN, XGBoost	XGBoost performed best with 92.7% accuracy. Evaluated on precision, recall, F1-score, and computational efficiency.	Improve scalability and optimize ANN for real-time processing.
Mosa et al. (2024)	Kaggle (European cardholders CCF dataset)	Random Forest, SVM; Feature selection & data balancing	Improved accuracy (up to 97%) using selected features and balanced data; highlighted the challenge of imbalanced datasets.	Apply ensemble models and extend feature engineering strategies.
Chauhan et al. (2024)	Not specified	Logistic Regression, DT, KNN; ANOVA for feature selection	Logistic Regression: 98.01% cross-validation accuracy, 91% F1 score. DT: 96.67% CV accuracy. Emphasized importance of balanced datasets.	Apply the system on larger, real-time datasets to enhance robustness.
Afriyie et al. (2023)	Not specified	LR, RF, DT	Random Forest achieved highest accuracy of 96%. Recommended as best performer.	Explore ensemble learning and deep learning for further improvement.
Gambo, Zainal and Kassim (2022)	Not specified; used ADASYN for balancing	CNN with ADASYN sampling	CNN model handled imbalanced data well and achieved 0.99 performance score (likely AUC or F1).	Expand CNN architecture and integrate temporal patterns in transaction sequences.

III. METHODOLOGY

The suggested approach for finding credit card fraud uses a step-by-step process shown in Figure 1. It starts with pre-processing the CCFD to get rid of missing values and duplicate entries. Next, features are changed using PCA, and data is balanced using SMOTE to fix problems with class imbalance. It is common practice to use the bulk of the processed dataset for training and put aside a smaller subset for testing. After that, these groups are used to build and test the CCNN classification model, among others like LR, NB, and XG Boost. The process concludes with an exhaustive evaluation of performance using F1-score metrics, accuracy, precision, and recall to find the best model setup for identifying financial transaction systems that process credit card fraud.

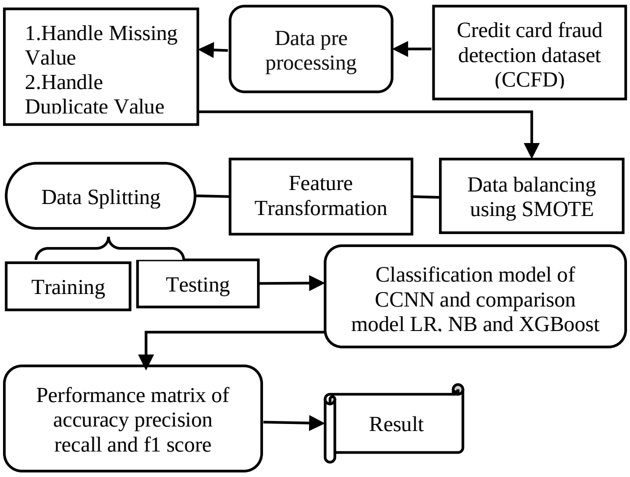
1.Handle Missing Value
2.Handle Duplicate Value
Data pre processing
Credit card fraud detection dataset (CCFD)
Data Splitting
Feature Transformation
Data balancing using SMOTE
Training
Testing
Classification model of CCNN and comparison model LR. NB and XGBoost
Performance matrix of accuracy precision recall and f1 score
Result

Fig. 1. Flowchart for Credit Card Fraud Detection

Credit card fraud detection in the banking industry flow diagram is presented in this section.

A. Data Collection

The dataset used was the Kaggle CCFD one, which is two days' worth of data containing 284,807 transactions. With only 492 fraudulent transactions out of 284,315 normal ones, the dataset is severely skewed. It can get this dataset on Kaggle; it's a popular choice for studies on credit card fraud detection. Following is a description of a few methods for data visualization and analysis:

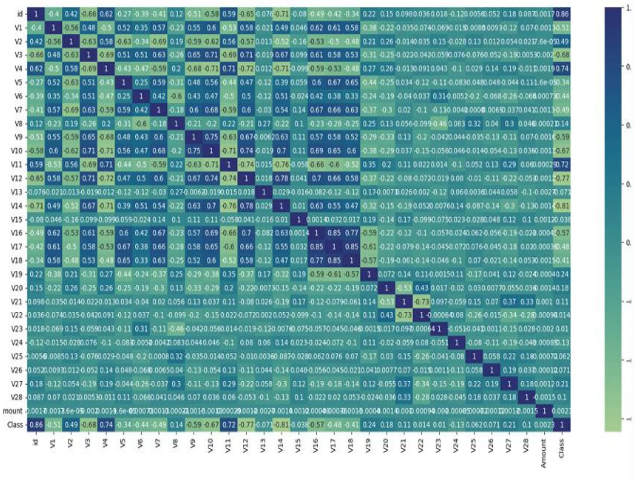

Fig. 2. Correlation heatmap of dataset features

Figure 2 show the relationship matrix heatmap visualizing the relationships between multiple dataset features. The heatmap uses a color-coded scheme ranging from blue (indicating negative correlation) to yellow-green (indicating positive correlation), with numerical correlation coefficients displayed within each cell. This correlation analysis is essential for feature selection and understanding inter-variable relationships in credit card fraud detection models, helping to identify redundant features and optimize model performance in financial transaction analysis.

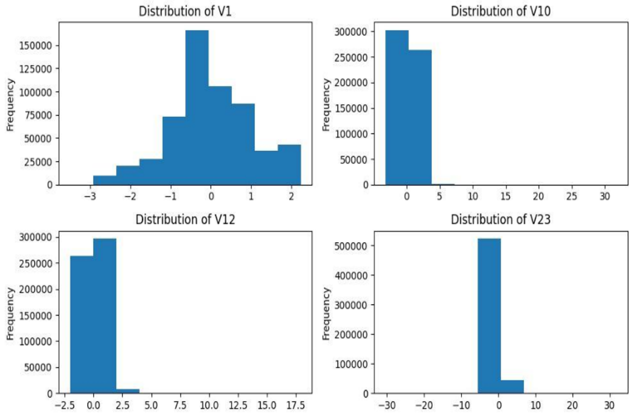

Fig. 3. Distribution plots of CCFD dataset features

Figure 3 shows the four histogram subplots showing the frequency distributions of features V1, V10, V12, and V23 from the dataset. Each feature exhibits distinct distribution patterns, with V1 showing a right-skewed distribution, V10 and V23 displaying highly concentrated distributions around zero with peak frequencies exceeding 300,000 and 500,000, respectively and V12 demonstrating an extremely left-skewed pattern.

B. *Data Preprocessing*

Data pre-processing is crucial for building effective models. Missing transaction values are carefully imputed to maintain data accuracy, and duplicate entries are removed to avoid misleading patterns. Using SMOTE, it may create fictitious instances of fraudulent transactions to tackle the common problem of imbalanced datasets. Normalization helps ensure all the aspects of a transaction are scaled the same, and feature transformation using PCA helps reduce dimensionality, which is great for model training and accuracy. Separating the information into training and testing sets is the last stage in assessing the model's capacity to identify banking-related credit card fraud.

What follows is a rundown of the pre-processing steps:

- **Handle missing value:** Datasets with missing values might hinder model training and lead to less accurate predictions. When it comes to preventing card fraud [35], it's important to first check for missing data. missing values can be filled using techniques like mean, median.
- **Handle duplicate value:** Duplicate records can cause model bias and overfitting, especially with repeated transactions. Detecting and removing them ensures unique data, improving model accuracy and fraud detection reliability.

C. *Data Balancing Using SMOTE*

Specifically, SMOTE creates synthetic samples from under-represented classes in order to level the playing field in the dataset and improve the model's minority class detection capabilities [36]. Two days of data collection by the SMOTE yielded 284,807 transactions, which reduced overfitting, improved the model's generalizability, and solved the class imbalance issue. A total of 492 fraudulent transactions (0.1 percent of the samples) and 284,315 normal transactions (99.83 percent of the samples) create a massive imbalance in the dataset.

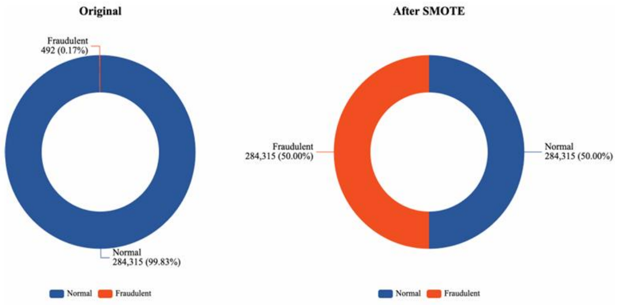

Fig. 4. Comparison before and after using smote

The number of incorrect samples in the Kaggle CCFD dataset increased dramatically from 492 to 284,315 after using the SMOTE strategy to attain class balance (Figure 4). A total of 284,315 samples were found to be free of fraud, which remained constant from the previous year.

D. *Feature Transformation with PCA*

PCA is a method for lowering a dataset's dimensionality that keeps all of the original data intact by reducing the dataset's variables to a smaller set [25]. The first step is to standardize the data so that all of the attributes in the dataset for credit card fraud detection are the same size.

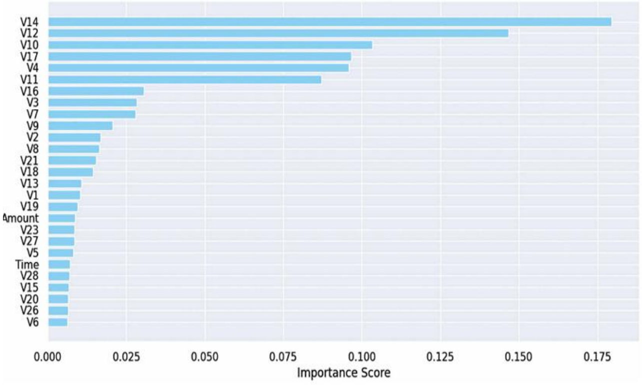

Fig. 5. Feature selection with PCA

Using PCA, the original characteristics are anonymized and compressed into 28 principal components (V1 to V28). This process, seen in Figure 5, helps to minimize redundancy and enhance model performance by focusing on the most informative elements of the data.

E. *Data Normalization*

Data normalization is essential for improving the model's accuracy by utilizing a normalization strategy to scale each feature to a defined range. To show how standardization works, one example is as Equation (1).

$$\mathrm{x} = \frac{(X - x_{min})}{(x_{max} - x_{min})} \quad (1)$$

The feature's maximum and minimum values are represented by x_{max} and x_{min} , respectively, while the modified value is denoted by x' [37].

F. *Data Splitting*

There is a 70% training and 30% testing set. For efficient model training and evaluation, this yields around 85,000 samples for testing and about 199,000 samples for each class in the training set, guaranteeing a balanced representation of legitimate and fraudulent transactions.

G. *Proposed CCNN (Continuous-Coupled Neural Network) Model*

A new model of neural network that evolved from the CNN is the CCNN. One of its primary design goals is to mimic the behavior of actual neurons as precisely as possible in dynamic [38]. The CCNN differs from the CNN in that it produces continuous values as output.

The foundation of the CCNN is a set of well-organized equations. Each CCNN neuron's state is determined by five primary components: feeding input, couple linkage, modulation product, dynamic activity, and continuous outputs (Equation (2) below).

$$\begin{cases} f_{ij}(n) = e^{-\alpha f} F_{ij}(n-1) + v_F M_{ijkl} * y_{kl}(n-1) + s_{ij} \\ L_{ij}(n) = e^{-\alpha f} L_{ij}(n-1) + v_L W_{ijkl} * y_{kl}(n-1) \\ u_{ij}(n) = F_{ij}(n)(1+\beta L_{ij}(n)) \\ Y_{ij}(n) = sigmoid(u_{ij}(n) - E_{ij}(n)) \\ E_{ij}(n) = e^{-\alpha e} E_{ij}(n-1) + v_E y_{ij}(n-1) \end{cases} \quad (2)$$

Figure 6 shows the training approach of the CCNN model to detect credit card fraud. Each time step, the CCNN neuron updates its feeding input f_{ij} by considering an external stimulus, the weighted sum of outputs from neighboring neurones, and the exponentially decaying preceding input. In a similar vein, the computation of the coupling link L_{ij} captures neuronal interactions. In the modulation stage, f_{ij} and L_{ij} are combined, and the signal is either amplified or suppressed using a scaling factor 1 + βLij. The modulated signal is subjected to a sigmoid activation function, with the adjustment made by the dynamic activity E_{ij}, in order to generate the output Yij.

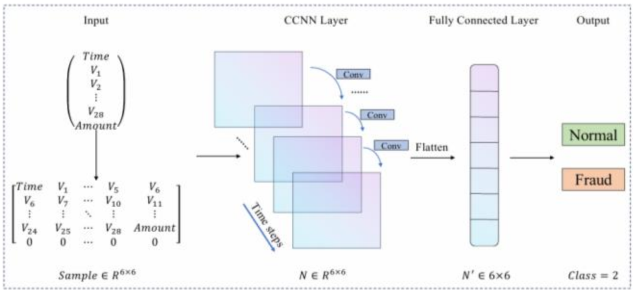

Fig. 6. CCNN model for credit card fraud detection

Figure 6 shows the CCNN model that can identify cases of credit card theft. Its design aims to provide classification functionality with minimal network structure. Using a CCNN layer with an array of neuron that scales with the input samples, once y_{ccnn} reaches the completely linked layer, the network's final output is shown in Equation (3).

$$y_{out} = A_2.Relu(A_1.y_{ccnn} + c_1)) + c_2 \tag{3}$$

therefore, y_{out} is the classification-related output vector following the second fully-connected layer; The first completely connected layer's weight matrix (A1) and bias (c1) are; The second fully connected layer used for classification has a weight matrix and bias denoted as A2 and c2, respectively, while the activation function is represented by ReLU.

H. Performance Metrics

Using a battery of performance metrics, they determine how well supervised learners do on categorization jobs. Included in this category are metrics like F-measure, accuracy, precision, and recall. The effectiveness of the classifiers to differentiate between valid and fraudulent transactions may be fully assessed using these indicators when combined. Binary classification tasks, like fraud detection, often use a confusion matrix to summarize their results [39]. See Figure 7 for an illustration of the confusion matrix, which is made up of TPs, FPs, FNs, and TNs.

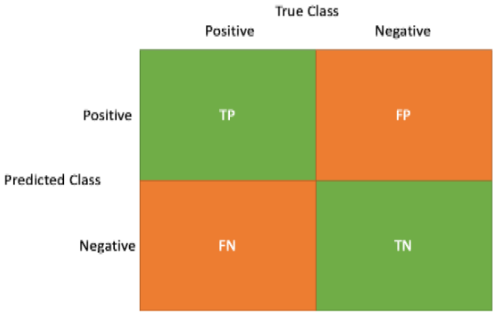

Fig. 7. Confusion Matrix

- **True positive (TP):** True positive estimates are denoted by TP.
- **True negative (TN):** TN stands for genuine negative estimates.
- **False positive(FP):** FP denotes estimations that are falsely positive.
- **False negative (FN):** False negative estimates are denoted by FN.

1) *Accuracy*

This statistic measures the overall accuracy of the model by comparing the total number of cases to the proportion of cases where predictions were correct, including both positive and negative outcomes. The answer is provided in Equation (4):

$$Accuracy = \frac{TN + TP}{TP + TN + FP + FN} \tag{4}$$

2) *Precision*

Divide the total number of transactions by the predicted number of fraudulent transactions to get the measure Equation (5):

$$Precision = \frac{TP}{TP+FP} \tag{5}$$

3) *Recall*

The accuracy with which the model can detect real affirmative cases is gauged by this parameter. It is shown in Equation (6):

$$Recall = \frac{TP}{TP+FN} \tag{6}$$

4) *F1-score*

The F1 score is another name for it. By summing memory and accuracy, the F-measure provides a harmonic average. By putting the two measures together into one, it finds a good middle ground in Equation (7):

$$F1 = \frac{2*(precision*recall)}{precision+recall} \tag{7}$$

5) *Loss*

A model's loss is the numerical value that stands for the disparity between the goal value and the model's expected output. It quantifies how well or poorly the model is performing during training. Model performance comparisons also make use of these matrices

IV. Result and Discussion

Efficient memory and processing were guaranteed by the 12.0 GB RAM and Intel(R) Core (TM) i7-2520M CPU utilized in the experimental arrangement. Its processing speed is 2.50 GHz. A combination of the local machine's large storage capacity and the available 900 GB of cloud storage made for an appropriate host for the dataset and project files. The results of different classification systems are summarized in this article. Results from testing the CCNN model on the dataset for detecting credit card fraud are displayed in Table II. Memory, accuracy, precision, and F1 score are some of the factors that go into determining an individual's rating. Excellent results are consistently achieved by it because of its consistently high levels of accuracy, precision, memory, and F1-score, which reach 99.97%. In this study, it was found that the CCNN model effectively identify instances of credit card fraud.

TABLE II. IMPROVING THE CCNN MODEL FOR DETECTING CREDIT CARD FRAUD USING A DATASET

Evaluation Matrix	**CCNN**
Accuracy	99.97
precision	99.96
Recall	99.97
F1-score	99.97

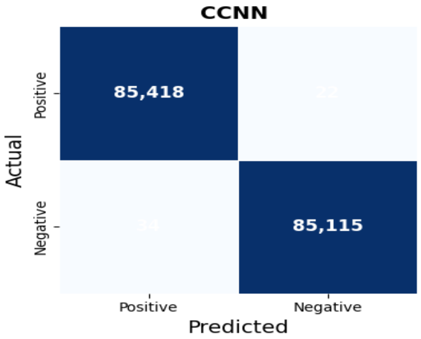

Fig. 8. Confusion Matrix of CCNN Model

Figure 8 shows the confusion matrix for the CCNN model, displaying classification performance with 85,418 true positive and 85,115 true negative predictions. The matrix depicts good classification accuracy featuring equal performance of both positive and negative classes, which means that the model works well causing minimal errors to occur during classification. Such an outstanding performance demonstrates the efficacy of the CCNN model to applications of credit card fraud detection in the financial sector.

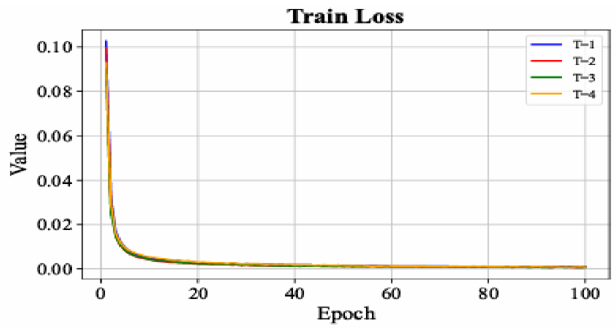

Fig. 9. Loss graph of CCNN model

Figure 9 illustrates the training loss over 100 epochs of training of CCNN model when the model is trained with various configurations (T-1, T-2, T-3 and T-4). The graph proves quick convergence with all the variations reaching almost zero loss values during the first 20 epochs and it shows efficient training and optimization of a model. This trend of steadily decreasing losses proves that the CCNN model is highly effective in detecting credit card fraud in the banking industry.

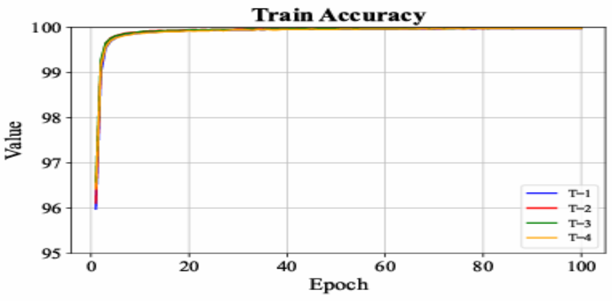

Fig. 10. Accuracy graph of CCNN model

Figure 10 shows the accuracy curves of CCNN model with cos-sine training for different sets of configurations on training across 100 epochs. It can be seen in the graph that the accuracy is increasing very fast, and all variants were converging to around 99.8 at the end of the first 10 epochs and kept the accuracy stable till the end of the 200th epoch. This high level of convergence of the accuracy signifies the robustness and high learning efficiency of the CCNN model when deployed in the financial sector to detect credit card frauds.

A. *Comparative Analysis*

This section gives the comparison between the proposed CCNN model with performance of the base model including LR, XG Boost and NB. The previously mentioned CCNN model outperforms all others with a 99.97% accuracy, 99.96% precision, 99.97% recall, and 99.97% F1-score. On the other hand, LR achieves CC, PP, RR, and F1-scores of 94.44%, 94.60%, 94.44%, and 94.43%, respectively. XG Boost has the performance of 97 percentages in all measures, and the NB model has the lowest score of 91.22 accuracy, 97.22 precision, 84.87 recall, and 90.63 F1-score. Table III shows the comparative analysis for credit card fraud detection between base and propose model.

TABLE III. COMPARATIVE ANALYSIS FOR CREDIT CARD FRAUD DETECTION BETWEEN BASE AND PROPOSE MODEL

Performance Matrix	**CCNN**	**LR**[40]	**XG Boost** [41]	**NB** [42]
Accuracy	99.97	94.44	97%	91.22
precision	99.96	94.60	97%	97.22
Recall	99.97	94.44	97%	84.87
F1-score	99.97	94.43	97%	90.63

The proposed CCNN-based credit card fraud detection model offers significant advantages, including high accuracy, robustness in handling complex and imbalanced transactional data, and effective performance on large-scale datasets. Its deep learning structure and powerful predictive ability make its models more reliable in picking the least number of false positive and false negative. The CCNN performs better in classification rates than traditional models, which guarantees enhanced precision, recall, and detection rates as compared to the traditional models. These strengths ensure that it can be effectively used to detect frauds with precision in the financial sectors that will aid in the safe and sound decision-making process in credit card transaction monitoring systems.

V. CONCLUSION AND FUTURE WORK

Credit cards are one of the means of cashless transactions in the financial sector which provide comfort, availability and purchasing capacity to the consumers. It is also an important source of revenue to financial institutions in the form of interest, fees etc. and processing fees given to credit card companies. By extensively pre-processing the data such as managing missing and duplicate data, transformation of features through PCA, and class balancing the original dataset with the help of SMOTE allowed the data to be made suitable in terms of training powerful models. Out of the tested models, the suggested Continued Coupled Neural Network (CCNN) was the model with the greatest accuracy of 99.97%. This shows a much better performance of the CCNN model in identifying fraudulent purchases and a good prospect to fixing the financial systems by increasing their security and reliability. The model is on the one hand extremely accurate, but on the other has limitations, such as possible overfitting, so future research can be used to perform along several areas to make it even stronger. To begin with, real-time streaming data and online learning environment will help enhance the responsiveness of the model to changing patterns of frauds. Second, utilization of explainable AI (XAI) methods will enhance financial decision-making trustworthiness and transparency of the models. Finally, adding multi-source data items to the framework, like user behavior analytics and device fingerprints, may also increase the detection rates and increase resiliency to sophisticated techniques of frauds.

References

[1] G. Li, X. Wang, D. Bi, and J. Hou, "Risk Measurement of the Financial Credit Industry Driven by Data," *J. Glob. Inf. Manag.*, vol. 30, no. 11, pp. 1–20, Aug. 2022, doi: 10.4018/JGIM.308806.

[2] R. Bin Sulaiman, V. Schetinin, and P. Sant, "Review of Machine Learning Approach on Credit Card Fraud Detection," *Human-Centric Intell. Syst.*, vol. 2, no. 1–2, pp. 55–68, Jun. 2022, doi: 10.1007/s44230-022-00004-0.

[3] B. Chaudhari and S. C. G. Verma, "Synergizing Generative AI and Machine Learning for Financial Credit Risk Forecasting and Code Auditing," *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.*, vol. 11, no. 2, 2025.

[4] V. Pillai, "Anomaly Detection for Innovators: Transforming Data into Breakthroughs," *Lib. Media Priv. Ltd.*, 2022.

[5] S. B. Shah, "Machine Learning for Cyber Threat Detection and Prevention in Critical Infrastructure," *J. Glob. Res. Electron. Commun.*, vol. 2, no. 2, pp. 1–7, 2025, doi: 10.5281/zenodo.14955016.

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

[7] 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.

[8] R. Q. Majumder, "A Review of Anomaly Identification in Finance Frauds Using Machine Learning Systems," *Int. J. Adv. Res. Sci. Commun. Technol.*, pp. 101–110, Apr. 2025, doi: 10.48175/IJARSCT-25619.

[9] S. P. Kalava, "Revolutionizing Customer Experience: How CRM Digital Transformation Shapes Business," *Eur. J. Adv. Eng. Technol.*, vol. 11, no. 3, pp. 163–166, 2024.

[10] P. Chatterjee, "Smart Contracts and Machine Learning: Exploring Blockchain and AI in Fintech," *Indian J. Sci. Technol.*, vol. 18, no. 2, pp. 113–124, Jan. 2025, doi: 10.17485/IJST/v18i2.3838.

[11] V. Pillai, "System and Method for Intelligent Detection and Notification of Anomalies in Financial and Insurance Data using Machine Learning," 202421099024, 2025

[12] R. Tarafdar, "Detect Malware in Cyber Security by Using AI and ML," 2025

[13] N. Tressa *et al.*, "Credit Card Fraud Detection Using Machine Learning," *2023 3rd Asian Conf. Innov. Technol. ASIANCON 2023*, no. Iciccs, pp. 1264–1270, 2023, doi: 10.1109/ASIANCON58793.2023.10270805.

[14] N. K. Prajapati, "Federated Learning for Privacy-Preserving Cybersecurity: A Review on Secure Threat Detection," *Int. J. Adv. Res. Sci. Commun. Technol.*, pp. 520–528, Apr. 2025, doi: 10.48175/IJARSCT-25168.

[15] P. Chatterjee, "AI-Powered Payment Gateways : Accelerating Transactions and Fortifying Security in Real-Time Financial Systems," *Int. J. Sci. Res. Sci. Technol.*, 2023.

[16] N. Malali, "Artificial Intelligence in Life Insurance Underwriting: A Risk Assessment and Ethical Implications," *Int. J. Interdiscip. Res. Methods*, vol. 12, no. 1, pp. 36–49, Jan. 2025, doi: 10.37745/ijirm.14/vol12n13649.

[17] S. Fan, Y. Shen, and S. Peng, "Improved ML-Based Technique for Credit Card Scoring in Internet Financial Risk Control," *Complexity*, vol. 2020, no. 1, pp. 1–14, Nov. 2020, doi: 10.1155/2020/8706285.

[18] V. Thangaraju, "Enhancing Web Application Performance and Security Using AI-Driven Anomaly Detection and Optimization Techniques," *Int. Res. J. Innov. Eng. Technol.*, vol. 9, no. 3, 2025, doi: 10.47001/IRJIET/2025.903027.

[19] 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, 2025, doi: 10.38124/ijisrt/25apr1813.

[20] S. Tyagi, "Analyzing Machine Learning Models for Credit Scoring with Explainable AI and Optimizing Investment Decisions," *Am. Int. J. Bus. Manag.*, vol. 5, no. 01, pp. 5–19, 2022.

[21] F. K. Alarfaj, I. Malik, H. U. Khan, N. Almusallam, M. Ramzan, and M. Ahmed, "Credit Card Fraud Detection Using State-of-the-Art Machine Learning and Deep Learning Algorithms," *IEEE Access*, 2022, doi: 10.1109/ACCESS.2022.3166891.

[22] B. O. O., K. J. A., and A. A. A., "Credit Card Fraud Detection Using Machine Learning Algorithms," *Br. J. Comput. Netw. Inf. Technol.*, vol. 7, no. 3, pp. 1–35, Jul. 2024, doi: 10.52589/BJCNIT-YDIJNXG2.

[23] N. Malali, "Using Machine Learning to Optimize Life Insurance Claim Triage Processes Via Anomaly Detection in Databricks: Prioritizing High-Risk Claims for Human Review," *Int. J. Eng. Technol. Res. Manag.*, vol. 6, no. 6, 2022, doi: 10.5281/zenodo.15176507.

[24] J. K. Chaudhary, S. Tyagi, H. P. Sharma, S. V. Akram, D. R. Sisodia, and D. Kapila, "Machine Learning Model-Based Financial Market Sentiment Prediction and Application," in *2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)*, IEEE, May 2023, pp. 1456–1459. doi: 10.1109/ICACITE57410.2023.10183344.

[25] O. Ogundile, O. Babalola, A. Ogunbanwo, O. Ogundile, and V. Balyan, "Credit Card Fraud: Analysis of Feature Extraction Techniques for Ensemble Hidden Markov Model Prediction Approach," *Appl. Sci.*, vol. 14, no. 16, 2024, doi: 10.3390/app14167389.

[26] A. K. Polinati, "AI-Powered Anomaly Detection in Cybersecurity: Leveraging Deep Learning for Intrusion Prevention," *Int. J. Commun. Networks Inf. Secur.*, vol. 17, no. 3, 2025.

[27] S. Kabade and A. Sharma, "Intelligent Automation in Pension Service Purchases with AI and Cloud Integration for Operational Excellence," *Int. J. Adv. Res. Sci. Commun. Technol.*, pp. 725–735, Dec. 2024, doi: 10.48175/IJARSCT-14100J.

[28] B. Chaudhari and S. Chitraju, "Achieving High-Speed Data Consistency in Financial Microservices Platforms Using NoSQL Using Nosql (Mongodb, Redis) Technologies," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 4, no. 2, pp. 750–759, Jun. 2024, doi: 10.48175/IJARSCT-18890.

[29] D. D. Rao, S. Madasu, S. R. Gunturu, C. D'britto, and J. Lopes, "Cybersecurity Threat Detection Using Machine Learning in Cloud-Based Environments: A Comprehensive Study," *Int. J. Recent Innov. Trends Comput. Commun.*, vol. 12, no. 1, 2024.

[30] A. K. Reddy, H. V. Rapeti, D. A. Reddy, and M. Srinivas, "Credit Card Fraud Detection Utilizing Machine Learning, Deep Learning, and Bayesian Networks," in *2025 International Conference on Artificial Intelligence and Data Engineering (AIDE)*, 2025, pp. 398–402. doi: 10.1109/AIDE64228.2025.10987438.

[31] M. Beri, K. S. Gill, and N. Sharma, "Enhancing Credit Card Fraud Detection: A Comparative Analysis of Machine Learning Models," in *2024 4th International Conference on Sustainable Expert Systems (ICSES)*, IEEE, Oct. 2024, pp. 449–454. doi: 10.1109/ICSES63445.2024.10763059.

[32] D. T. Mosa, S. E. Sorour, A. A. Abohany, and F. A. Maghraby, "CCFD: Efficient Credit Card Fraud Detection Using Meta-Heuristic Techniques and Machine Learning Algorithms," *Mathematics*, vol. 12, no. 14, pp. 1–27, 2024, doi: 10.3390/math12142250.

[33] S. Chauhan, K. S. Gill, R. Chauhan, and H. S. Pokhariya, "Smart Solutions for Utilizing Advanced Machine Learning for Robust Credit Card Fraud Detection," in *2024 First International Conference on Electronics, Communication and Signal Processing (ICECSP)*, 2024, pp. 1–6. doi: 10.1109/ICECSP61809.2024.10698053.

[34] M. L. Gambo, A. Zainal, and M. N. Kassim, “A Convolutional Neural Network Model for Credit Card Fraud Detection,” in *2022 International Conference on Data Science and Its Applications (ICoDSA)*, 2022, pp. 198–202. doi: 10.1109/ICoDSA55874.2022.9862930.

[35] W. Bisen, H. Padwad, G. Keswani, Y. Agrawal, R. Tiwari, and V. Tiwari, “Autoencoder-Driven Insights into Credit Card Fraud : A Comprehensive Analysis,” *Int. J. Intell. Syst. Appl. Eng.*, vol. 12, no. 12, pp. 115–120, 2024.

[36] N. Mqadi, N. Naicker, and T. Adeliyi, “A SMOTe based Oversampling Data-Point Approach to Solving the Credit Card Data Imbalance Problem in Financial Fraud Detection,” *Int. J. Comput. Digit. Syst.*, vol. 10, no. 1, pp. 277–286, Feb. 2021, doi: 10.12785/ijcds/100128.

[37] A. Ruchay, E. Feldman, D. Cherbadzhi, and A. Sokolov, “The Imbalanced Classification of Fraudulent Bank Transactions Using Machine Learning,” *Mathematics*, 2023, doi: 10.3390/math11132862.

[38] H. Liu, M. Liu, D. Li, W. Zheng, L. Yin, and R. Wang, “Recent Advances in Pulse-Coupled Neural Networks with Applications in Image Processing,” *Electronics*, vol. 11, no. 20, 2022, doi: 10.3390/electronics11203264.

[39] M. Tayebi and S. El Kafhali, “Generative Modeling for Imbalanced Credit Card Fraud Transaction Detection,” *J. Cybersecurity Priv.*, vol. 5, no. 1, 2025, doi: 10.3390/jcp5010009.

[40] A. R. Khalid, N. Owoh, O. Uthmani, M. Ashawa, J. Osamor, and J. Adejoh, “Enhancing Credit Card Fraud Detection: An Ensemble Machine Learning Approach,” *Big Data Cogn. Comput.*, 2024, doi: 10.3390/bdcc8010006.

[41] L. Theodorakopoulos, A. Theodoropoulou, F. Zakka, and C. Halkiopoulos, “Credit Card Fraud Detection with Machine Learning and Big Data Analytics: A PySpark Framework Implementation,” *Preprints*, 2024, doi: 10.20944/preprints202407.0022.v1.

[42] B. Borketey, “Real-Time Fraud Detection Using Machine Learning,” *J. Data Anal. Inf. Process.*, vol. 12, no. 02, pp. 189–209, 2024, doi: 10.4236/jdaip.2024.122011.