Volume (1) No (10), 2025
Journal of Global Research in Multidisciplinary Studies (JGRMS)
Review Paper/Research Paper
Available online at https://saanvipublications.com/journals/index.php/jgrms/index

Comparative Study on Deep Learning Approaches for Fraudulent Transaction Detection

Dr. Manish Saraswat
Associate Professor (CSE) and Controller of Examinations
Faculty of Science and Technology
The ICFAI University,
Himachal Pradesh
manish.saraswat@iuhimachal.edu.in

***Abstract*—Credit card theft has become a major problem in the financial world because of the huge rise in online shopping and the complexity of fraud cases. A convolutional neural network (CNN) 1D could be useful in spotting fraudulent transactions, according to recent research. As part of the preparation, the data will be standardised and validated. The Synthetic Minority Over-Sampling Technique (SMOTE) will be used to balance the classes. Next, datasets are created for training, validation, and testing purposes. Impressive results in domains such as recall, accuracy, and precision (including a 99.7 F1-score) are achieved by the proposed CNN 1D model, surpassing more traditional ML models like Support Vector Machine, Naive Bayes, and K-Nearest Neighbour. Furthermore, the model's robustness and generalisability were demonstrated using learning rate optimization, ROC-AUC, and confusion matrices. The results indicate that CNN 1D model is a highly predictable and scalable credit card fraud detection model with significant better performance compared to the traditional methods in accuracy, sensitivity and scalability.**

***Keywords*—Fraud Detection, Credit card transaction, Machine learning, Deep Learning.**

I. INTRODUCTION

Financial services are rapidly becoming digitalized, making transactions faster, easier to access, and more convenient. However, this has also led to more complex scams. Financial institutions are under continual threat from fraud schemes that take advantage of weaknesses in transaction infrastructures due to the proliferation of internet banking, e-commerce, and mobile payment systems [1]. The main methods for detecting fraud in the past have been rule-based systems and manual audits; however, both procedures are slow, reactive, and often fail to capture changing fraud trends as they occur. On the other hand, knowing the ins and outs of fraud is crucial for effectively preventing it [2][3]. Credit card fraudsters employ a range of tactics to execute their crimes. When someone gets their hands on the physical card or when sensitive information about the account, like the account number, becomes accessible to anybody during a legitimate transaction, it's considered credit card fraud [4][5]. Numbers like the PAN and other card details are printed on the card at regular intervals and kept on a magnetic stripe on the reverse in a machine-readable format. [6][7]. Credit card theft can be reduced by implementing all of these strategies.

Various fraud detection technologies are constantly being developed to prevent criminals from modifying their illegal transactions [8]. Several forms of fraud can be broadly categorised as follows: Financial crimes such as identity theft, bankruptcies, fraudulent charges on credit cards, counterfeit goods, and application-based fraud [9][10]. To mitigate these challenges, financial institutions are increasingly adopting artificial intelligence (AI) and deep learning-based approaches, which offer proactive, scalable, and adaptable solutions for detecting fraudulent transactions[7][11][12]. Traditional supervised and unsupervised learning models, typically applied on structured attribute-value datasets derived from transactional records, can classify transactions as legitimate or fraudulent[13][14]. However, such models face limitations when dealing with complex fraud behaviors like money laundering, where transactions are interdependent rather than isolated events. Several fields are making use of the most recent deep learning (DL) techniques, including cybersecurity, malware detection, banking, insurance, and intrusion detection systems [15][16]. Credit card fraud detection using DNN, however, has received shockingly little attention.

A. *Significance and contribution*

Credit card fraud detection is crucial in preventing banks and other financial organizations from falling victim to more complex forms of theft. Even a tiny amount of fraud, out of the billions of digital transactions that happen every day, can cause huge losses in both money and trust from customers. Due to their ineffectiveness in keeping pace with evolving fraud trends, traditional rule-based systems must be replaced by DL approaches. Improving financial security, minimizing false positives, and boosting real-time decision-making are all outcomes of this research's demonstration of how predictive analytics can accurately identify fraudulent transactions. Important advancements include:

- Merged data from the credit card fraud detection dataset that is available to the public, including both real and fake purchases.
- Applied comprehensive preprocessing steps, including initial inspection, missing value analysis, standardization using StandardScaler, and class balancing with SMOTE, to address severe data imbalance.
- Trained and deployed a CNN 1D DL model, which is specifically trained to identify sequential trends in the transactional data, and it is more accurate in identifying fraudulent cases.

- The F1-score, recall, accuracy, precision, confusion matrix, and ROC-AUC are all comprehensive metrics of predictive performance. These were used to evaluate the model's performance.

B. Justification and Novelty

Credit card fraud is on the rise, which is worrisome for both customers and banks, so action is required. While traditional ML approaches do work to a certain degree, they aren't up to the task of capturing the complicated, non-linear patterns present in transaction data or dealing with the extremely skewed nature of fraud datasets. This work's distinctive features include a 1D convolutional neural network for fraud detection, feature scaling to handle class imbalance, and robust preprocessing methods like SMOTE. Our model outperforms the current state of the art in terms of accuracy, precision, recall, and F1-score by utilizing DL capability to automatically extract meaningful patterns from sequences of transactions. Using cutting-edge preprocessing and CNN 1D architecture, our system is built to identify fraudulent transactions. It finds several uses and can be changed. Here we provide a novel approach to financial fraud detection through deep learning.

C. Structure of the paper

The paper is structured as follows: Section II presents a survey of research on detecting fraudulent transactions. Section III details the suggested methodology, which encompasses the following: dataset description, preprocessing techniques, and the architecture of the 1D CNN model. What follows is a discussion of the experimental results detailed in Section IV. Section V concludes the study and lays out the directions for further research.

II. LITERATURE REVIEW

This section examines several review articles that discuss the application of deep learning and machine learning in identifying fraudulent transactions. The writers, methodologies, datasets, important results, limitations, and future work are summarized in Table I.

Pandiyan, Nagarajan and Sathya (2025), This study delves into the revolutionary impact of AI on pushing the envelope of next-gen information security by way of automated, real-time fraud detection. In this innovative hybrid method, Autoencoder and LNN work together to create a lower-dimensional data representation and detect fraudulent transactions. This data could potentially reveal more intricate patterns in time-series or sequential data. An F1-score of 90.48, a recall of 89.28, precision of 92.89, and accuracy of 99.65 are the performance measures by which this model is evaluated [17].

Shah (2025), uses ML methods to the Financial Fraud Detection Dataset that is accessible on Kaggle, including feature engineering, data preparation, and class balancing. Optimized and trained using GridSearchCV models include a Voting Classifier, RF, AdaBoost, and LGBM. Results Achieved: LGBM achieves the highest accuracy (90.20%), followed by the Voting Classifier (90.02%), while RF and AdaBoost record 89.26% and 88.37%, respectively. SHAP analysis provides insights into feature importance, enhancing model interpretability[18].

Elmangoush *et al.* (2024), the goal of creating a reliable model for detecting fraudulent charges on credit cards. The class imbalance problem has been addressed using a synthetic minority oversampling algorithm. The next step was to build a credit card identification model that would make use of the SMOTE data to enhance feature extraction and representation, hence solving the issue of inadequate features. This model would employ sequential deep learning techniques. Used f-measure, detection rate, and accuracy as metrics to evaluate the proposed model and compare it to similar studies. The outcomes clearly demonstrate that the proposed model outperforms the existing top-tier models in this domain. The accuracy is 0.99924 and the F-measure is 0.75976. [19].

Beri, Gill and Sharma (2024), investigates the detection of fraudulent charges on credit cards by contrasting two well-known ANN models, XGBoost. The study evaluated various algorithms utilizing precision, accuracy, recall, and F1 score, all of which were applied to a publicly available dataset consisting of credit card transactions. Aspects such as computing efficiency, scalability, and the potential use of ANNs to real-time fraud detection systems are also carefully examined. Product, XGBoost. ANN performs the best among the five recommended methods with an accuracy of 96.9%, XGBoost has best performance with an accuracy of 92.7% among the classifiers [20].

Prasad *et al*. (2023), Implementing a CNN is the next step towards making scam detection more effective. The use of layers in a CNN aids in accurate detection. A large-scale empirical analysis utilized the most recent CNN model's hidden layer count, epochs, and applications. Recall, precision, accuracy, and F1 score all influence the algorithm's output. The AUC has been adjusted to take advantage of 99.9%, 85.71%, 93%, and 98% values. A ROC curve is constructed using the confusion matrix. [21].

Ghosh *et al.* (2023), presents a new approach to improving the Bitcoin network's fraud detection capabilities using ensemble DL models. Training and evaluation of the suggested ensemble model—which includes MLP, FNN, and Attention LSTM—follows extensive data preparation and feature engineering. The results demonstrate that the ensemble model outperformed the competitors in terms of accuracy, precision, and recall. Recall values of 99% and outstanding precision are achieved by the ensemble, which is particularly noteworthy, along with an astounding 99.62% accuracy [22].

Credit card fraud prevention using DL and ML models has been extensively studied. However, problems still remain, such as how to deal with a big class imbalance and how to find complex sequential trends in transaction data. Autoencer-LNN and ensemble-based models like LGBM are examples of hybrid models that are more accurate than other models but are not as robust at recall, meaning they cannot be used in real-time to prevent fraud. The sequential methods based on SMOTE and ANN/XGBoost comparisons are very robust; however, they have scaling/generalizability problems. Both CNN and ensemble-based methods are highly accurate, however, they exhibit precision-recall trade-offs and expose false negatives of fraudulent cases. To achieve this goal, the current study proposes a CNN 1D coupled up with the StandardScaler and SMOTE to equalize the data representation. The above is because, the proposed model ensures quality extraction of features, improved balance of classes and improved detection, hence, providing an effective and scalable solution to the real world of fraud detection systems.

TABLE I. SUMMARY OF BACKGROUND STUDY FOR FRAUDULENT TRANSACTION DETECTION

Authors	Methods	Dataset	Key Findings	Limitations & Future Work
Pandiyan, Nagarajan & Sathya, 2025	AutoLiquid-FD (Hybrid: Autoencoder + Liquid Neural Network)	Pre-processed digital transaction dataset	Achieved 99.65% accuracy, precision 92.89, recall 89.28, F1-score 90.48; effectively captures sequential patterns	Needs validation on large-scale real-time transactions; robustness under adversarial attacks can be explored
Shah, 2025	RF, AdaBoost, LightGBM, Voting Classifier + SHAP Explainability	Kaggle Financial Fraud Detection dataset	LGBM highest accuracy 90.20%, Voting Classifier 90.02%; SHAP improves interpretability	Requires validation on diverse datasets; real-time adaptability not tested
Elmangoush et al., 2024	Sequential Deep Learning + SMOTE for imbalance handling	Credit card fraud dataset (oversampled with SMOTE)	Accuracy 0.99924, F-measure 0.75976; outperforms existing models	Overfitting risk due to SMOTE; further real-world validation needed
Beri, Gill & Sharma, 2024	ANN vs XGBoost (comparative study)	Public credit card dataset	ANN accuracy 96.9%; XGBoost accuracy 92.7%; ANN best for real-time fraud detection	Computational cost of ANN is high; XGBoost more scalable
Prasad et al., 2023	CNN with deep hidden layers + confusion matrix ROC evaluation	Credit card fraud dataset	Accuracy up to 99.9%, precision 93%, recall 98%; CNN reduces false negatives effectively	Generalization to unseen transaction types needs testing; high computational demand
Ghosh et al., 2023	Ensemble DL (MLP + FNN + Attention LSTM)	Bitcoin transaction dataset	Accuracy 99.62%, precision & recall >99%; ensemble outperforms individual models	Limited to cryptocurrency domain; cross-domain applicability requires study

III. METHODOLOGY

The methodology for detecting fraudulent transactions begins with the collection of the credit card fraud detection dataset. Subsequently, data processing databases play a crucial role, followed by the initial examination and detection of missing values. A standardization of the dataset is then done to ensure consistency among the numerical features. The SMOTE is implemented to address the issue of unequal course distribution. This cleaned dataset is used to build the testing, validation, and training sets. Using a DL model that is built on a CNN 1D for data classification is the next step. Common measures used to assess model performance include F1-score, recall, accuracy, and precision. Figure 1 outlines the entire methodology, with the final stage of the research examining the CNN 1D model's ability to recognize fraudulent transactions.

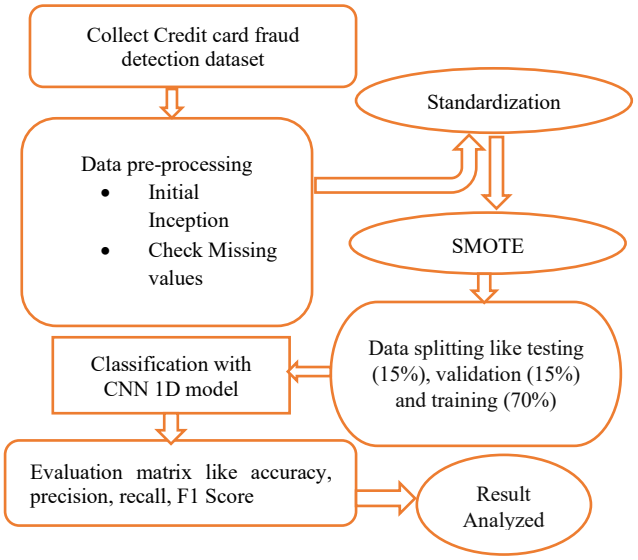

Fig. 1. Flowchart of the Proposed Deep Learning-Based Credit Card Fraud Detection Model

The following steps of proposed methodology are briefly discussing in below:

A. Data collection

The dataset used for this analysis is the Credit Card Fraud Detection database, which contains two days' worth of credit card transactions conducted by cardholders across Europe in September 2013. Out of a total of 28,4807 transactions in this dataset, 0.172% are fraudulent. Along with time and amount, the dataset contains thirty characteristics (V1,…., V28). The dataset only contains numerical attributes. Presented below are various visual representations of the data, including pie charts, heat maps, and boxplots.:

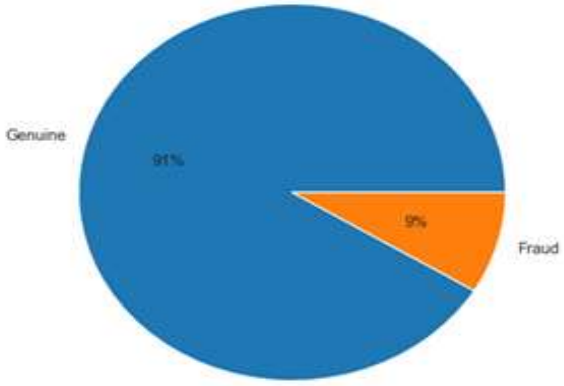

Fig. 2. Pie chart of the dataset classes distribution

In Figure 2, the distribution of transactions between genuine and fraudulent cases is illustrated using a pie chart. The chart shows that 91% of the transactions are genuine, while only 9% are fraudulent. In a dataset where legitimate transactions predominate, the fact that fraudulent ones constitute a tiny percentage stands out.

The correlation heatmap in figure 3 shows the correlations between the dataset variables, including aspects like Time, V1-V28, Amount, and Class. A heatmap displays correlation coefficients; numbers close to 0 signify weak or nonexistent correlations, while values near 1 or -1 indicate strong relationships. Features such as Amount and Class exhibit weak correlations with a few of the principal components; this information can be helpful for detecting trends during model training and fraud detection, as seen by the diagonal line of white squares, which indicates perfect self-correlation of each feature with itself.

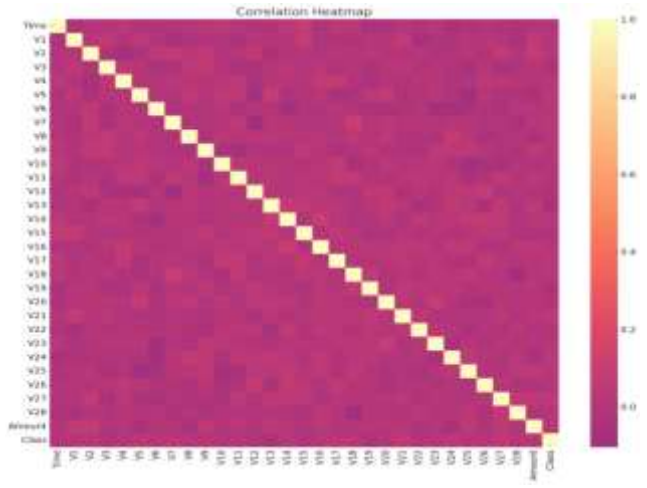

Fig. 3. Correlation heatmap of the dataset attributes

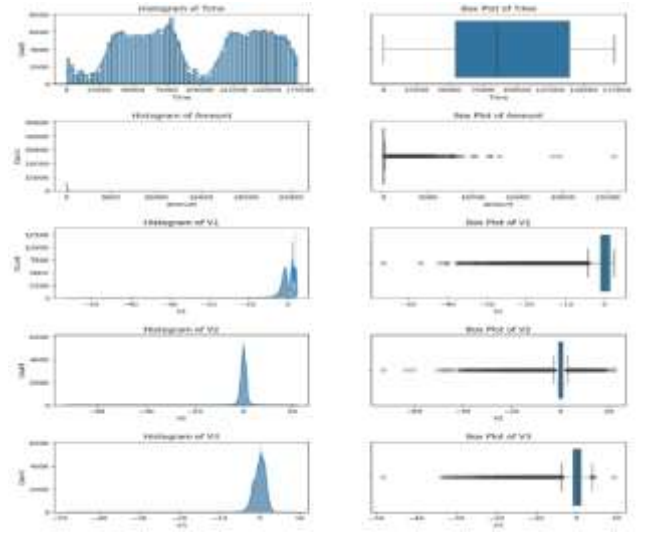

Fig. 4. Histograms and Box Plots of Transaction Time, Amount

Credit card fraud detection dataset distribution and dispersion are shown in Figure 4 by means of box plots and histograms. The histogram of Time shows transaction occurrences across the dataset, while its box plot indicates a relatively uniform spread with no significant outliers. The Amount histogram highlights that most transactions are concentrated at lower values, whereas the box plot reveals the presence of several high-value outliers.

B. *Data preprocessing*

The Credit Card Fraud Detection Dataset's preprocessing is highlighted due to its inherent inconsistencies and noise. The process began with an initial inspection that revealed a missing value. These steps align with standard practices reported in existing literature to improve model performance and generalizability:

- **Initial Inspection:** The initial analysis was conducted using the .head(),.tail(),.shape(),.info(), and.describe() functions to get insights into the structure, data types, and summary statistics of the dataset.
- **Checking missing values:** The initial step in data cleaning involved checking for missing values. The isnull(). sum() function was used to identify them, and no null entries were found in the dataset.

C. *Feature scaling with StandardScaler*

Machine learning frequently makes use of StandardScaler, a data preprocessing tool, to normalize numerical features. As a result of data normalization, all features have the same mean and standard deviation, which ensures that all variables, regardless of their starting scale, contribute equally to the model. It works particularly well for algorithms that care a lot about feature magnitude. It is mathematically stated that the transformation is as in equation 1:

$$x' = \frac{(x-\mu)}{\sigma} \quad (1)$$

x' stands for the value that has been standardised, μ for the standard deviation, σ for the mean of the feature, and x for the original value of the feature. This results in features with a mean of 0 and a variance of 1 for feature-sensitive models.

The original feature value is represented by x, the average feature value is x, the dispersion is x, and the standardization value is x. This produces features whose mean is zero and whose variance is one, which is especially useful in models whose results are sensitive to scaling of features.

D. *SMOTE*

SMOTE is a method for improving data that can be used to fix problems with class imbalance. Fig. 5 shows the results of applying SMOTE to the credit card fraud detection data. The two classes, 0 and 1, were evenly distributed since the sample sizes for both were almost equal. The dataset was skewed prior to using SMOTE, with the majority of samples (284,315) belonging to the class of 0 (non-fraud) and just 492 belonging to the class of 1 (fraud). The classes were resampled after SMOTE, both to 284,315 instances each, so that the distribution of classes was the same. This is because of the fact that SMOTE allows the model to be trained on a more representative dataset by artificially producing new instances of the minority class utilizing feature space similarities. This technique improves classifier performance by mitigating bias toward the majority class.

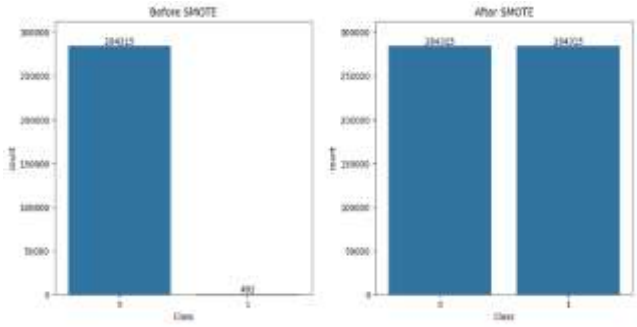

Fig. 5. Balancing with SMOTE

E. *Data splitting*

Training, validation, and testing comprise the three sections of the credit card fraud dataset. Training uses 70% of these, validation 15%, and testing 15%.

F. *Classification with 1D- CNN Model*

The area of computer vision did not begin to use one-dimensional convolutional neural networks (1D-CNNs), despite their existence since the late 80s, until the mid-2000s. Speech recognition tasks were the initial applications of 1D-CNNs, with audio signals serving as the input data. Data with a principal structure along a single axis, such as time-series

data, sequences (like text), or any other type of data, can be handled by 1D-CNNs. A 1D CNN just uses one dimension for the kernel (or filter) to move along. The kernel can be used to find patterns in a series by sliding over a vector [x1, x2,…,xn] that represents the data. Size, or dimension (k), is a way to characterize the kernel's shape as an array of dimensions (1D). The input vector's single axis allows the kernel to slide. To grasp patterns over time, the kernel, in a time-series application, for instance, travels along the x-axis. A 1D CNN kernel's receptive fields are adjacent bits in the input data. Hence, the kernel averages data from k consecutive elements as it moves across the input [23]. Equation (2) gives the convolution process for a 1D-CNN layer with an input sequence x and a kernel w:

$$(x * \omega)(t) = \sum_{i=0}^{k-1} x(t+i) \cdot \omega(i) \quad (2)$$

All of the following are represented numerically: x, for the input sequence, ω for the kernel or filter, $(x * \omega)(t)$ for the convolution of x and ω at position t, k for the kernel size, $x(t+i)$ for the input sequence element, and $\omega(i)$ for the kernel element.

G. Evaluation metrics

An evaluation of the Credit Card Fraud classification models is carried out using a confusion matrix, which records the results of real classifications compared to the anticipated ones. The matrix includes four key components. The confusion matrix is listed in below:

- TP is shorthand for the sum of all correctly predicted positive outcomes.
- The total of all incorrect predictions that are considered positive is called FP.
- FN refers to the total of all incorrect predictions that are tagged as negative.
- The sum of all correctly predicted negative outcomes is called the TN.

Following performance measures are as follows:

1) Accuracy

This statistic compares the total number of instances to the number of right predictions (including genuine negatives and positives), which is helpful for measuring the model's general accuracy. Here is the expected outcome derived from equation (3) [24]:

$$Accuracy = \frac{\text{TP+TN}}{\text{TP+Fp+TN+FN}} \quad (3)$$

2) Precision

Accuracy in positive prediction is reflected in precision, which is obtained in equation (4) as follows:

$$Precision = \frac{\text{TP}}{\text{TP+FP}} \quad (4)$$

3) Recall

The model's ability to identify real positive cases is assessed using this statistic. The formula for it is (5):

$$Recall = \frac{\text{TP}}{TP+FN} \quad (5)$$

4) F1-score

An F-measure, often known as an F1 score, is computed as a harmonic mean of recall and precision. It averages the two criteria' relative importance and produces a single score. Equation (6) provides the value:

$$F1 - Score = \frac{2(Precision * Recall)}{\text{Precision+Recall}} \quad (6)$$

5) ROC

A popular statistic for assessing classification methods is the area under the ROC curve. The ROC curve at different threshold levels shows the link between TPR and FPR. What follows is a curve representing the classifier's capacity to differentiate between classes, with FPR on the x-axis and TPR on the y-axis. A higher AUC, a scalar measure of the model's whole performance, indicates an enhanced discriminatory capacity.

6) Loss

The loss function is employed to quantify the extent to which the model deviates from its designated objectives throughout the training process. Throughout training, this loss is fine-tuned to minimize it as a performance metric for the model.

These matrices are utilized to determine the deep learning models.

IV. Result Analysis And Discussion

The project's testing was carried out using Python (Python 3). Scikit-Learn, pandas, NumPy, and matplotlib are some of the open-source tools that were utilised in this study. This experiment required a desktop computer with the following specifications: Windows 10 64-bit, an Intel Core i7 1.80 GHz processor, and 16 GB of RAM. Results from the Credit Card Fraud Detection dataset tests of the DL model's ability to detect fraudulent transactions are shown in Table II. Key performance indicators used to assess the model were F1-score, Accuracy, Precision, and Recall. The CNN 1D model achieved remarkable results in detecting fraudulent transactions on the credit card dataset, with an F1-score of 99.7%, recall of 99.7%, precision of 99.6%, and accuracy of 99.7%.

TABLE II. DL model on the Credit Card Fraud Detection dataset for fraudulent transaction identification.

Performance Measures	CNN 1D
Accuracy	99.7
Precision	99.6
Recall	99.7
F1-score	99.7

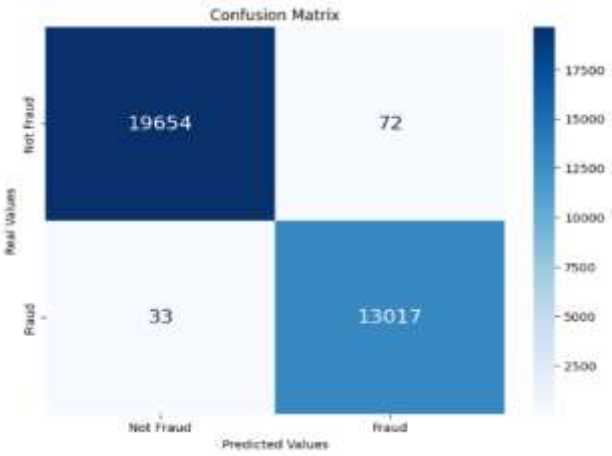

Fig. 6. Confusion matrix of CNN 1D model

This dataset is used to detect credit card fraud; the confusion matrix for the model trained using a convolutional

neural network (CNN) 1D model is shown in Figure 6. The model got 19,654 occurrences of the 'Not Fraud' category right, but it got 72 occurrences of fraud wrong. In the 'Fraud' category, the model accurately identified 13,017 instances, with only 33 instances misclassified as not fraud.

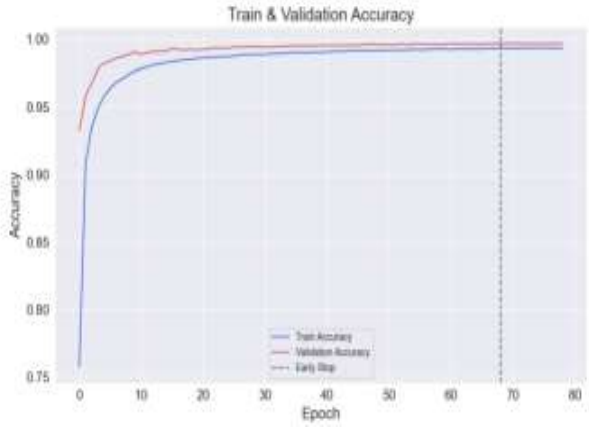

Fig. 7. Train and Validation Accuracy graph of CNN 1D model

Figure 7 displays the CNN 1D model's training and validation accuracy curves on the Credit Card Fraud Detection dataset. The model's accuracy increased sharply during the initial epochs and gradually converged toward near-perfect accuracy as training progressed. Both training and validation accuracies stabilized close to 100%, with the early stopping criterion marked around the 70th epoch.

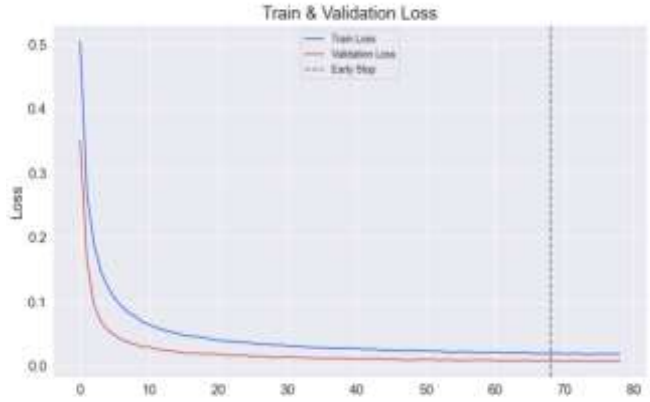

Fig. 8. Train and Validation Loss graph for CNN 1D Model

Figure 8 shows the CNN 1D model's training and validation loss curves applied to the dataset. You can see from the graph that training and validation losses both go down quickly in the beginning and then level out as training progresses. Additional training did not result in significant improvements since the early stopping rule is identified at the 70th epoch. An almost identical training and validation loss curve for the CNN 1D model lends credence to its robustness in detecting fraudulent transactions; this suggests that the model performed admirably on unknown data and that overfitting did not occur during training.

The ROC figure (Figure 9) shows the accuracy of the CNN 1D model in detecting fraudulent transactions in the Credit Card Fraud Detection dataset. When looking at the graph at different levels of categorization, it is clear that the TPR and the FPR are related. Accurately distinguishing between fraudulent and non-fraudulent transactions, the CNN 1D model proved its worth with an AUC of 0.997, all thanks to its outstanding discriminatory measure.

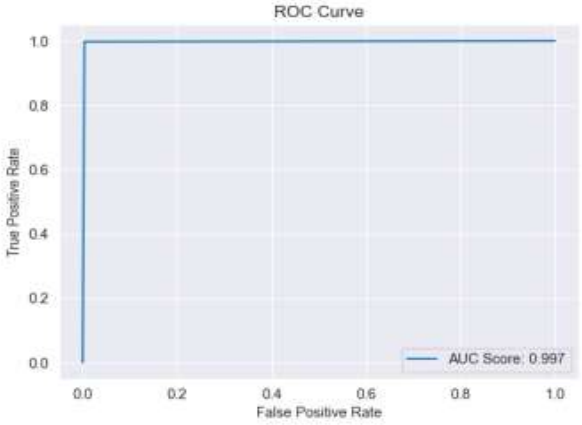

Fig. 9. ROC Curve of CNN 1D model

A. Comparative Analysis and Discussion

This section compares the approaches taken to detect fraudulent financial dealings. The capacity of the four models—CNN 1D, NB, SVM, and KNN—to identify fraudulent transactions is assessed in Table III using a number of performance indicators, including Accuracy, Precision, Recall, and F1-score. As far as F1-score, accuracy, and precision are concerned, the CNN 1D model stood head and shoulders above the competition with a score of 99.7. Following that, KNN is highly ranked with a 94.20 F1-score, 93.68 Accuracy, 94.50 Precision, and 94.50 Recall. The SVM model achieved a perfect score of 93.77 on Accuracy, 94.49 on Precision, 93.24 on Recall, and 93.60 on F1-score, with no noticeable difference in any of the measures. With a Recall of 85.48, an Accuracy of 91.48, and a Precision of 97.17, the NB boasts an F1-score of 90.95. The results show that deep learning methods, like CNN 1D, are superior for detecting fraudulent transactions.

TABLE III. ML AND DL MODELS COMPARISON FOR FRAUDULENT TRANSACTION IDENTIFICATION.

Performance Measures	CNN 1D	NB [25]	SVM [26]	KNN [27]
Accuracy	99.7	91.48	93.77	93.68
Precision	99.6	97.17	94.49	94.50
Recall	99.7	85.48	93.24	94.20
F1-score	99.7	90.95	93.60	94.20

Deep learning and ensemble-based systems, especially the CNN 1D, are better at finding credit card fraud than standard machine learning systems, according to the results. With an accuracy of 99.7, the CNN 1D model outperformed all other models, demonstrating its consistency and robustness across all metrics of evaluation. These results confirm the usefulness of deep learning-based solutions to address complex real-life fraud detection challenges.

V. CONCLUSION AND FUTURE WORK

One of the most serious issues facing the banking industry is credit card fraud. It is always changing and costs the world a lot of money. A major challenge in detecting fraudulent transactions is the extremely uneven nature of real-world data, as fraud incidents constitute a negligible percentage of actual transactions. In order to tackle these problems, this paper suggests a deep learning strategy that makes use of a CNN 1D.

A ROC AUC of 0.997, an F1-score of 99.7, a precision of 99.6 percent, a recall of 99.7 percent, and an accuracy of 99.7 percent were all attained by the model with the use of feature scaling and SMOTE for preprocessing and class balancing. Based on the results of the comparison, CNN 1D is an excellent choice for detecting financial transaction fraud because it outperforms conventional ML approaches.

For future work, the system can be enhanced through hybrid architectures combining CNN with LSTM or attention mechanisms, allowing more effective capture of both local and sequential transaction patterns. Additionally, real-time fraud detection frameworks should be implemented to handle large-scale financial streams. Finally, financial institutions and stakeholders will have more faith in the models thanks to explainable AI's (XAI) increased openness.

REFERENCES

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

[2] J. Mishra, B. B. Biswal, and N. Padhy, "Machine Learning for Fraud Detection in Banking Cyber security Performance Evaluation of Classifiers and Their Real-Time Scalability," in *2025 International Conference on Emerging Systems and Intelligent Computing (ESIC)*, IEEE, Feb. 2025, pp. 431–436. doi: 10.1109/ESIC64052.2025.10962752.

[3] B. Chaudhari, S. Verma, and S. Somu, "A Review of Secure API Gateways with Java Spring for Financial Lending Platforms," vol. 14, pp. 315–326, 2024, doi: 10.56975/ijcsp.v14i4.303090.

[4] H. Kali, "Optimizing Credit Card Fraud Transactions Identification And Classification In Banking Industry Using Machine Learning Algorithms," *Int. J. Recent Technol. Sci. Manag.*, vol. 9, no. 11, pp. 1–12, 2024.

[5] V. Prajapati, "Enhancing Threat Intelligence and Cyber Defense through Big Data Analytics: A Review Study," *J. Glob. Res. Math. Arch.*, vol. 12, no. 4, pp. 1–10, 2025.

[6] K. B. Thakkar and H. P. Kapadia, "The Roadmap to Digital Transformation in Banking: Advancing Credit Card Fraud Detection with Hybrid Deep Learning Model," in *2025 2nd International Conference on Trends in Engineering Systems and Technologies (ICTEST)*, IEEE, Apr. 2025, pp. 1–6. doi: 10.1109/ICTEST64710.2025.11042822.

[7] 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, 2025, doi: 10.48175/IJARSCT-25619.

[8] S. Gajula, "Leveraging Enterprise Architecture for Enhanced Risk Governance in Financial Institutions: Data Integration, Compliance, and Fraud Detection," *Int. J. Sci. Technol.*, vol. 16, no. 1, pp. 1–13, Mar. 2025, doi: 10.71097/IJSAT.v16.i1.2519.

[9] G. Mantha, "Transforming the Insurance Industry with Salesforce: Enhancing Customer Engagement and Operational Efficiency," *North Am. J. Eng. Res.*, vol. 5, no. 3, pp. 1–2, 2024.

[10] S. B. Shah, "Machine Learning for Cyber Threat Detection and Prevention in Critical Infrastructure," *Dep. Oper. Bus. Anal. Inf. Syst. (OBAIS*, vol. 2, no. 2, pp. 1–7, 2025, doi: 10.5281/zenodo.14955016.

[11] A. R. Bilipelli, "Forecasting the Evolution of Cyber Attacks in FinTech Using Transformer-Based Time Series Models," *Int. J. Res. Anal. Rev.*, vol. 12, no. 3, pp. 1–7, 2023.

[12] A. Sharma and S. Kabade, "Optimization Algorithms for Pension Asset Allocation Under Market Volatility," *TIJER – Int. Res. J.*, vol. 11, no. 9, pp. 1–8, 2024.

[13] S. 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. 1–8, 2025.

[14] H. Kali, "THE FUTURE OF HR CYBERSECURITY: AI-ENABLED ANOMALY DETECTION IN WORKDAY," *Int. J. Recent Technol. Sci. Manag.*, vol. 8, no. 6, 2023.

[15] H. Kapadia and K. C. Chittoor, "Quantum Computing Threats to Web Encryption in Banking," *Int. J. Nov. Trends Innov.*, vol. 2, no. 12, pp. a197–a204, 2024.

[16] S. Gajula, "A Review of Anomaly Identification in Finance Frauds using Machine Learning System," *Int. J. Curr. Eng. Technol.*, vol. 13, no. 06, Jun. 2023, doi: 10.14741/ijcet/v.13.6.9.

[17] M. Pandiyan, B. Nagarajan, and K. Sathya, "AutoLiquid-FD: Next-Gen Liquid Neural Network for Fraudulent Transaction Detection," in *2025 11th International Conference on Communication and Signal Processing (ICCSP)*, IEEE, Jun. 2025, pp. 1438–1443. doi: 10.1109/ICCSP64183.2025.11088594.

[18] 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)*, 2025, pp. 1–7. doi: 10.1109/ICDCECE65353.2025.11034838.

[19] 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.

[20] 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)*, 2024, pp. 449–454. doi: 10.1109/ICSES63445.2024.10763059.

[21] P. Y. Prasad, A. S. Chowdarv, C. Bavitha, E. Mounisha, and C. Reethika, "A Comparison Study of Fraud Detection in Usage of Credit Cards using Machine Learning," in *7th International Conference on Trends in Electronics and Informatics, ICOEI 2023 - Proceedings*, 2023. doi: 10.1109/ICOEI56765.2023.10125838.

[22] C. Ghosh, A. Chowdhury, N. Das, and B. Sadhukhan, "Enhancing Financial Fraud Detection in Bitcoin Networks Using Ensemble Deep Learning," in *2023 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS)*, IEEE, Oct. 2023, pp. 1–6. doi: 10.1109/ICBDS58040.2023.10346590.

[23] A. O. Ige and M. Sibiya, "State-of-the-Art in 1D Convolutional Neural Networks: A Survey," *IEEE Access*, vol. 12, pp. 144082–144105, 2024, doi: 10.1109/ACCESS.2024.3433513.

[24] 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.

[25] 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.

[26] X. Feng and S.-K. Kim, "Novel Machine Learning Based Credit Card Fraud Detection Systems," *Mathematics*, vol. 12, no. 12, p. 1869, Jun. 2024, doi: 10.3390/math12121869.

[27] 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.

