IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 6, June 2026
Impact Factor: 8.2

Enhancing Cybersecurity in FinTech Through Predictive Intelligence-based Machine Learning Algorithms

Mr. Sachin Manekar
Assistant Professor, Department of Computer Sciences and Applications
Mandsaur University, Mandsaur
Sachin.manekar@meu.edu.in

Abstract: *The rapid growth of financial technologies (FinTech) has facilitated more accelerated and intelligent digital transactions, but has also brought new challenges in cybersecurity especially in the detection of fraudulent activities. Traditional rule-based fraud detection methods can be susceptible to the constantly evolving, complex attack patterns, which drive the need for predictive intelligence enabled by machine learning. To overcome this issue, this paper presents two predictive models, a Convolutional Neural Network (CNN) and a K-Nearest Neighbors (KNN) model, to improve fraud detection in FinTech systems. Systematic preprocessing techniques are employed, including label encoding to convert categorical features to numerical values, min-max normalization to scale features, and the Synthetic Minority Oversampling Technique (SMOTE) to address class imbalance. CNNs are meant to learn high-level hierarchies with convolutional, pooling, and fully connected layers, whereas KNN classifies transactions using a distance measure in a multi-dimensional space. The models are ideally trained and assessed based on accuracy (Acc), precision (Prec), recall (Rec), F1-score and ROC. The experimental analysis indicates that CNN scores an impressive 99.96% on acc, prec, rec, and F1score and KNN obtains reasonable scores at 99.95% accuracy and balanced detection rate. A comparison with Support Vector Machine (SVM) and MLP indicates that the proposed models, especially the CNN, are superior at providing robust, reliable fraud detection for FinTech cybersecurity.*

Keywords: Fintech industry, cyber threats, credit card transaction dataset, CNN model, Machine learning

I. INTRODUCTION

FinTech has been experiencing exponential growth in recent years, changing the way financial services are delivered by leveraging technology to offer faster, more efficient, and more accessible solutions[1]. This rapid digital transformation has made FinTech platforms an excellent target of sophisticated cyber-attacks[2]. Cybersecurity hazards in the FinTech industry have evolved into a vast and complex issue, incorporating among others, ransomware and phishing attacks, insider threats, and zero-day vulnerabilities [3][4][5]. The protection of information pertaining to finance and the great role of FinTech in the world economy make cybersecurity very important, thus enhancing the effects of such attacks[6].

ML and big data have become necessities to combat cybersecurity worries[7]. Data analytics can handle huge amounts of data in both organized and unorganized forms, and at the same time find patterns that are not visible but may suggest the existence of security gaps[8]. Apparently, machine learning models assist in dynamic threat detection by utilizing both past and present data streams. These technologies together allow Fintech companies to predict and prevent cyber-attacks[9], moving from a reactive to a proactive approach.

One of the main areas where predictive analytics is employed is in the development of Cyber Threat Intelligence [CTI]

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 6, June 2026
Impact Factor: 8.2

consisting identifying and reducing possible cyber threats beforehand their realizing[10]. The FinTech sector can use predictive analytics to see when attacks will happen, to use their resources in the best way, and to reduce the amount of time their systems are not working by analyzing network traffic patterns, behaviors, and finding anomalies in user activity[11]. In addition to making threat detection more accurate, combining CTI with Big Data and ML speeds up response time, which is a crucial factor in limiting losses during a cyber crisis.

A. Motivation and Contribution of study

FinTech has resulted in a quick growth of the financial services sector, which is now easier to access and use but also more prone to security incidents. The old-fashioned safeguards simply don't work anymore with modern threats like ransomware, phishing, and zero-day attacks. To address such problems, Big Data and ML offer advanced capabilities for real-time anomaly detection and large-scale data analysis. Combined with Cyber Threat Intelligence (CTI), they enable proactive threat prediction and faster response times, underscoring the need for predictive intelligence systems to protect FinTech systems.

- Creation of a hybrid fraud detection system that utilizes CNN and KNN to make use of both deep feature extraction and distance-based classification to enhance accuracy.
- Complete preprocessing pipeline with min-max normalization, SMOTE-based class balancing and encoding mechanism to guarantee the quality of data and equitable model training.
- Substantial experimental assessments of acc, prec, rec, F1score, and ROC analysis derived evidence of better CNN and KNN behavior than SVM and MLP baselines.
- Applicability in practice to FinTech security, demonstrating that the offered models are reliable, scalable, and real-time detecting fraud that can be utilized in financial systems.

B. Justification and novelty

The novelty of this work consists of the combination of CNN and KNN to detect fraud and an effective preprocessing (SMOTE, normalization, and label encoding) to address imbalance and scale characteristics. The imbalanced nature of the environment worsens SVM and MLP, whereas the proposed models display near-perfect accuracy, prec, rec, and F1scores. The urgency behind this is explained by the ardent necessity to have a stable, real-time detection of fraud in financial systems, where CNN identifies intricate patterns and KNN provides a strong classification, which can result in a scalable and viable solution. The relative findings further confirm that the models are more effective compared to the traditional baselines hence their application in contemporary financial systems is very appropriate.

C. Structure of paper

The essay is organized as follows: Section II examines relevant studies on FinTech Security Intelligence. Section III details the suggested technique and KNN model implementation. Section IV presents the findings and analysis, while Section V concludes the study by outlining future predictions.

II. LITERATURE REVIEW

The section examines previous research on predictive intelligence in FinTech security by using machine learning, the main contributions and limitations are summarized in Table I. The synthesis presents research trends and provides a background to identify gaps for future work.

Shah (2025) applied the ML techniques to the Kaggle Financial Fraud Detection Dataset, including the preprocessing, feature engineering, and class balancing. Random Forest, AdaBoost, LightGBM, and a Voting Classifier were optimized with GridSearchCV with LightGBM having the maximum accuracy (90.20%). SHAP analysis also showed important features that ensured the effectiveness and interpretability of EnsembleLearning models in the detection of fraud in financial institutions[12]. Silvia *et al.* (2024) established that online banking fraud is outpacing traditional detection systems. They combined behavioral analytics and ML to increase the detection accuracy and decrease FP.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 6, June 2026 Impact Factor: 8.2

Convolutional Neural Networks performed better with a highest accuracy of 95 percent[13]. Sharma *et al.* (2024) compared ML and DL methods in identifying fraud in the online financial systems. CNNs and RNNs were applied to a transactional dataset. The RNN model performed better as compared to CNNwith 95.8% acc, 93.7% sens-itivity, 97.5% spec-ificity, and an AUC of 0.972[14]. Sultana *et al.* (2023) discovered that conventional fraud detection tools are weak at fighting advanced financial crimes. They suggested a hybrid system combining ML and blockchain to improve fraud detection and prevention in banking transactions. The experiment compared the performance of XGBoost, KNN, CatBoost and RF to identify real-time fraudulent behaviors [15]. Pranto *et al.* (2022) built a system of SmartContracts and blockchain technologies to boost ML algorithms in the event of e-commerce fraud. The architecture provides privacy for the data and automates network operations. It promotes cooperation by means of adaptive incentive structure and effective mining criterion. The framework had 98.93% testing accuracy[16].

Despite the use of ML, DL, and combination blockchain framework in fraud detection in FinTech, essential challenges have not been fully resolved. Existing models perform well in accuracy but are not scalable, adaptable to changing patterns of fraud, have a problem of class imbalance, false positives, and real-time applications. Also, numerous methods are tested on controlled data rather than on realistic financial systems, which limits their applicability. This lack of information requires predictive intelligence-based ML models that guarantee the accuracy, interpretability and strength of FinTech platform security.

TABLE 1: COMPARATIVE ANALYSIS OF MACHINE LEARNING TECHNIQUES FOR PREDICTIVE INTELLIGENCE FOR FINTECH SECURITY

Author	Methodology	Data	Key Findings	Limitation	Future Work
Shah (2025)	Random Forest, AdaBoost, LightGBM, Voting Classifier with GridSearchCV; SHAP for feature interpretability	Kaggle Financial Fraud Detection Dataset	LightGBM achieved highest accuracy (90.20%); SHAP highlighted key features for interpretability	Focused mainly on ensemble models; limited exploration of deep learning; tested only on Kaggle dataset	Extend to deep learning and hybrid models; validate on real-world financial datasets
Silvia et al. (2024)	Behavioral analytics + Machine Learning (CNN)	Online banking transactional data	CNN outperformed traditional methods with ~95% accuracy; reduced false positives	Limited generalization to other fraud types; interpretability issues with CNN	Explore explainable AI (XAI) and cross-domain fraud detection
Sharma et al. (2024)	Compared CNN and RNN for fraud detection	Transactional dataset (digital financial infrastructures)	RNN outperformed CNN with 95.8% acc, sens-itivity 93.7%, spec-ificity 97.5%, AUC 0.972	High computational cost; limited scalability for real-time applications	Optimize RNN for real-time fraud detection; apply on large-scale streaming data
Sultana et al. (2023)	Hybrid framework: ML + Blockchain; used XGBoost, KNN, CatBoost, RF	Banking transactions (fraudulent activities)	The hybrid approach improved fraud prevention; ensemble ML showed competitive accuracy	Blockchain integration may increase system overhead; limited interpretability	Develop lightweight blockchain–ML systems; focus on scalability
Pranto et al. (2022)	Blockchain + Smart Contracts integrated with ML	E-commerce fraud dataset	Achieved 98.93% testing accuracy; ensured privacy, automation, and incentive mechanism	Domain-specific (e-commerce); limited application to financial institutions	Generalize to FinTech fraud detection; test across diverse domains

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 6, June 2026
Impact Factor: 8.2

III. METHODOLOGY

The systematic pre-processing, model building, and evaluation approach is used to enable good fraud detection. Pre-processing involves normalization to minmax to bring features to a range from 0 to 1, SMOTE to ease class imbalance by creating synthetic fraud cases, missing values handling through either elimination or statistical replacement, and converting categorical variables into numeric through encoding of labels into numbers. The data is split into training, validation, and testing sets for a fair assessment of performance. Two predictive models are built one is CNN, which performs convolution, pooling, and fully connected layers to extract complex feature representations, and KNN classifier which classifies transactions using a distance measure in a multi-dimensional space. The two models are first optimized and afterward evaluated using the standard metrics acc, F1score, prec, rec, and ROC analysis which facilitates a comparative study with the baseline methods to verify their effectiveness in detecting fraud.

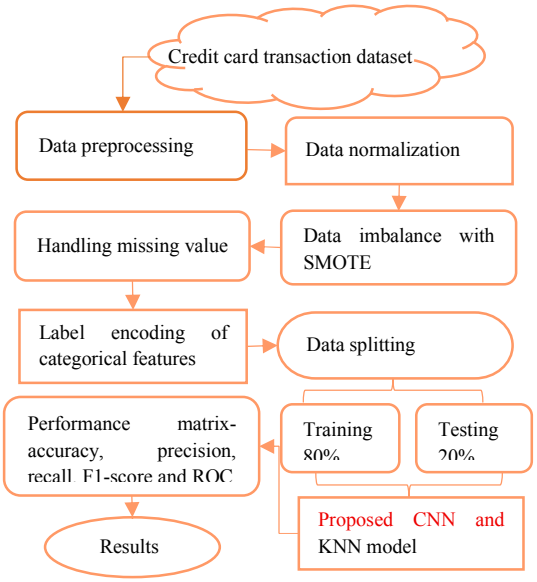

Fig. 1. Flowchart Depicting Predictive Intelligence Framework for FinTech Security

The subsequent sections outline each step in detail, consistent with the methodology and the proposed flowchart shown in Fig 1.

A. Data Collection and Visualization

The dataset used in the experimental analysis is a publicly available credit card transaction dataset, consisting of 284,807 cases collected over two days in September 2018, of which 492 (0.172) are fraudulent. In order to ensure confidentiality, the majority of attributes were anonymized using PCA to generate the anonymized features V1-V28, whereas the Time, Amount, and Class Features (0 legitimate, 1 fraud) were left in place. The dataset is a good reference point in fraud detection studies where visualization of the class imbalance and feature patterns offers a better understanding of the difficulties in model creation.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 6, June 2026
Impact Factor: 8.2

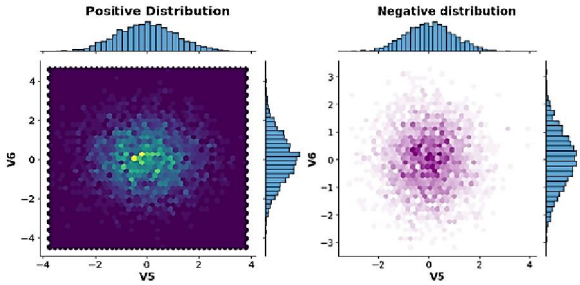

Fig. 2. Positive and Negative distribution of the data

Fig. 2 shows the hexbin density plots of features V5 and V6 with marginal histograms of the positive (left) and negative (right) transaction classes. The positive distribution has a greater clustering around the origin, as compared to the negative distribution which is more dispersed, featuring very clear interactions of features that can be used in fraud detection.

Fig. 3 demonstrates the extremely skewed balance of verified and fraudulent transactions, approximately 280,000 legitimate records versus under 500 cases of fraud. This imbalance causes problems with machine learning models, which is common in financial datasets and favors the majority class. Certain methods such as resampling, cost-sensitive learning, or anomaly detection are required to address this issue and make the detection of fraud more effective.

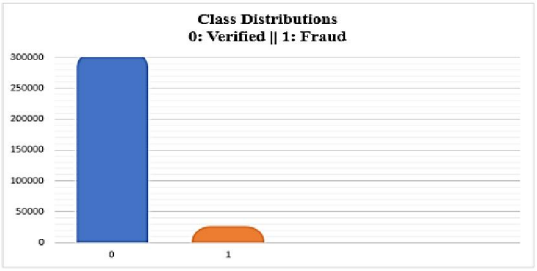

Fig. 3. Class distribution of fraudulent and nonfraud transactions.

B. Data Preprocessing

An important step in training the model is pre-processing to ensure it is prepared to be trained. These are min-max normalization to bring feature values to the range of 0 and 1, SMOTE to equalize classes by creating synthetic samples of fraud, missing values either removed or imputed, and Label Encoding to transform categorical features into numerical ones. The following steps are discussed below:

C. Data Normalization

Minimum maximum normalization is to allow the varying sizes of features and scale the values to 0 and 1. This avoids the dominance of the larger-magnitude features, strengthens the convergence, and the performance of the DL models. This study applies min-max normalization, which transforms the data based on the minimum and maximum values of every feature using the formula in equation (1):

$$\text{normalize}(X) = \frac{X - X_{\min}}{X_{\max} - X_{\min}} \quad (1)$$

By distributing the training workload evenly across all features, this step prevents features with larger numerical ranges from becoming the dominant learning variables. Also, it makes the model more accurate and faster to converge.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 6, June 2026
Impact Factor: 8.2

D. Data Imbalance with Smote

The dataset has a large imbalance in terms of classes but a small percentage of all transactions are fraudulent[17]. This can be reduced by applying the SMOTE, which interpolates between existing fraud samples and generates new ones. In doing so, the dataset is also balanced, the ability of the model to detect the presence of fraud is reinforced, and valuable metrics such as rec and F1score are enhanced at minimal computational cost.

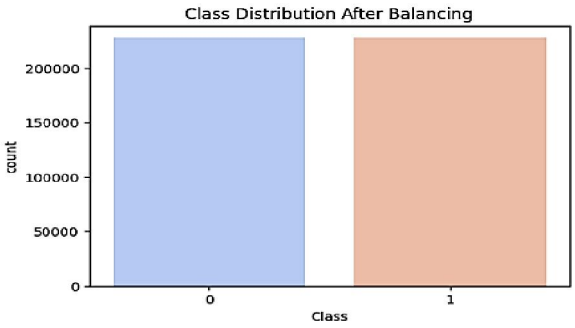

Fig. 4. Class distribution after balancing

Fig. 4 defines the distribution of the classes following the utilization of a balancing method on the unbalanced credit card data. Legitimate and illegal transactions are equally represented, with more than 220,000 cases of each. This balance makes the model less biased toward the majority category and it detects fraudulent cases better, increasing the model performance on important metrics like rec and F1score.

E. Handling Missing Values

Missing data can either be deleted (when the feature is not essential) or can be imputed with statistical techniques, e.g. mean or median. This ensures that the dimensions of input are also similar in all the samples and the model is represented through misinterpreting missing values.

F. Label Encoding of Categorical Features

Label encoding converts categorical variables in the dataset into a numerical format. ML algorithms require numerical input and therefore this step is crucial. Every type is assigned an integer number and maintains the integrity of the data and prepares it to be analyzed.

G. Data Splitting

Pre-processing is followed by the division of the dataset into training 80% and the testing 20%. The training set is used to come up with a validation set, which is utilized to tune the hyperparameters and avoid overfitting. This design guarantees that the model is tested on unknown data, allowing for a more realistic study of its performance.

H. Proposed CNN Model

One element of deep neural networks that processes and analyzes visual imagery input is known as a convolutional neural network (CNN). The picture will be saved in pixels as a 2D array if it is a colorful or grayscale image. Furthermore, CNNs are used to manage 2D arrays of audio spectrograms. Nonetheless, the CNN model has three different types of layers: convolution, pooling, and classification layers [18]. Fig. 5 shows an example of CNN.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 6, June 2026
Impact Factor: 8.2

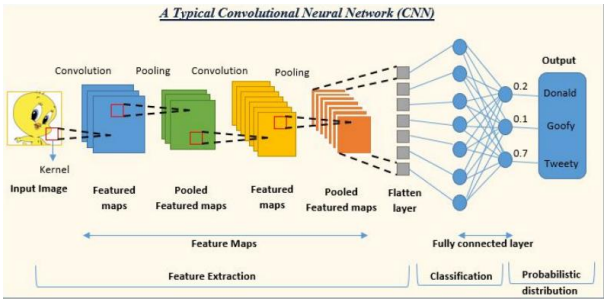

Fig. 5. Architecture of CNN Model

I. Proposed KNN Model

KNN is a comparatively straightforward classifier with no parameters or goal functions. The correlation between test and training samples is examined by this algorithm. The distances between the test sample and the k-nearest samples are calculated in order to classify the test sample. Equation (2) defines Makowski distance, which is the metric employed in this study to calculate distance:

$$dist = \left(\sum_{j=1}^{n} |x_j - z_j|^r\right)^{1/r} \quad \square\square\square$$

where the coordinates of the sample points in a multidimensional space are represented by xj and zj; dist denotes the Manhattan distance when r=1 and the Euclidean distance when r=2. To reduce the redundancy of the closest neighbor search and expedite the diagnosis process, a k-dimensional tree, also known as a ball tree, is developed as a diagnostic model.

J. Performance Matrix

Classic methods for estimating machine learning classifiers can apply confusion metrics which consider the difference between the ultimate truth of the dataset and the prediction made by the model; in this context, TP, TN, FP, and FN refer to true positive, true negative, false positive, and false negative, respectively.

Accuracy: Accuracy is used to gauge how well data processing and evidence domain recovery are going. Equation (3) may be used to describe the percentage of outcomes that are successfully categorized as follows:

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

Precision: Precision, a performance metric, measures the ratio of successfully recognized positives to the total number of positives. This is shown in equation (4) as follows.

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

Recall: Equation (5) shows that the recall, also called the sensitivity, is the ratio of linked instances recovered over the total number of retrieved instances.

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

F1_Score: The f-measure takes into account both recall and precision. Equation (6) illustrates how the average weight of all values can be considered the f-measure.

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

ROC: The ROCcurve compares the TPR to the FPR to assess model performance across different thresholds. In this study, five classifiers were tested without resampling, and their AUC-ROC scores were compared. The proposed model achieved the highest AUC, indicating the best ability to distinguish between churned and non-churned customers[19][20].

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 6, June 2026
Impact Factor: 8.2

IV. RESULTS AND DISCUSSION

The proposed models were implemented in Python 3.6.5 on a PC equipped with an i5-8600 K CPU, a GeForce 1050 Ti GPU, 16GB RAM, a 250GB SSD, and a 1 TB HDD. A learning rate of 0.01, a dropout of 0.5, a batch size of 5, 50 epochs, and ReLU activation were among the parameters. Table II summarizes the performance of KNN and CNN on the credit card transaction dataset. CNN achieves the highest acc (99.96%), prec (99.95%), rec and F1score (99.96), reflecting its superior detection capability. KNN also demonstrates strong performance, with 99.95% accuracy, 99.56% precision, 98.29% recall, and 99.54% F1-score, showing a reliable balance between minimizing false positives and detecting fraudulent cases. These results validate the robustness of both models, with CNN being singled out as the best at detecting credit card fraud.

TABLE 2: PERFORMANCE MATRIX OF PROPOSED KNN AND CNN MODELS ON AVAILABLE CREDIT CARD TRANSACTION DATASET

Measures	KNN	CNN
Accuracy	99.95	99.96
Precision	99.56	99.95
Recall	98.29	99.96
F1-score	99.54	99.96

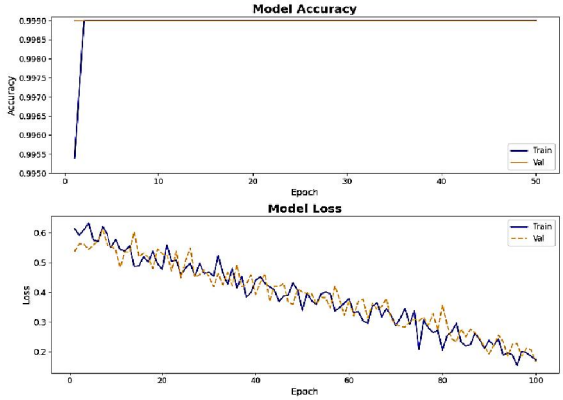

Fig. 6. Accuracy & Loss graph for the KNN Model

The training and validation accuracies of the proposed model after 50 epochs are illustrated in Fig. 6, where the training accuracy grows significantly in the initial iterations and then stabilizes at 0.999. The validation accuracy, which reveals strong generalization and almost perfect performance, remains high and stable, with only minor fluctuations.

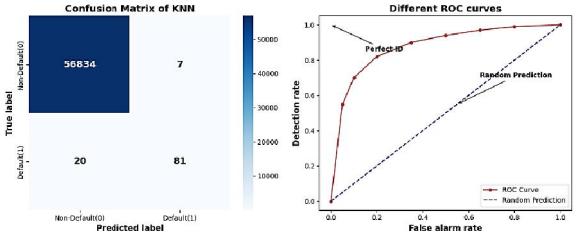

Fig. 7. Confusion matrix and ROC curve of KNN Model

Fig. 7 shows the KNN Classifier performance in a ROC curve and confusion matrix. The model accurately classified 36,834 non-defaults and 81 defaults, with minor misclassifications (7 defaults and 20 non-defaults). Despite high accuracy on non-defaults, class imbalance has slightly affected default detection. The ROC curve, located well above the diagonal, corroborates the model's high discriminative power and a good balance between detection rate and false

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 6, June 2026
Impact Factor: 8.2

alarms.

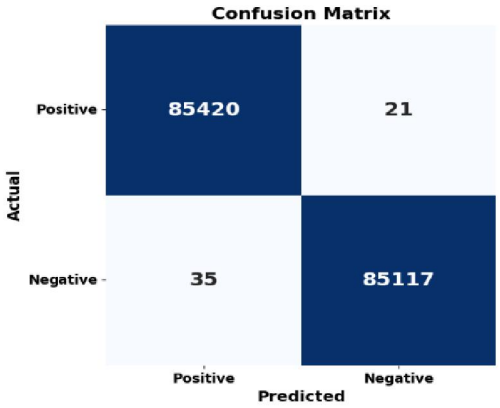

Fig. 8. Confusion matrix of CNN model.

The confusion matrix of a CNN (1-1) model is shown in Fig 8, which successfully classified 85,420 positives and 85,117 negatives, resulting in only 21 false negatives and 35 false positives, demonstrating high reliability and accuracy in fraud detection.

TABLE 3: COMPARISON BETWEEN BASE AND PROPOSED MODEL PERFORMANCE MATRIX FOR CREDIT CARD TRANSACTION DATASET

Matrix	**KNN**	**CNN**	**SVM**[21]	**MLP**[22]
Accuracy	99.95	99.96	98	95.8
Precision	99.56	99.95	54	97.6
Recall	98.29	99.96	93	93.9
F1-score	99.54	99.96	57	95.8

Table III compares the performance of KNN, CNN, SVM, and MLP on the credit card transaction dataset using Acc, Prec, Rec, and F1score as evaluation metrics. CNN has a total score of 99.96% across all metrics, making it highly trustworthy for fraud detection. KNN also performs satisfactorily with 99.95% accuracy, 99.56% precision, 98.29% recall, and 99.54% F1-score, indicating a good balance between detection and false alarms. On the other hand, SVM shows relatively low precision (54%) and F1-score (57%), indicating its limitations in imbalanced data. MLP is also a good performer with very high precision (97.6) but very low recall (93.9), so the F1-score is 95.8. These results show that CNNs and KNN outperform classic models for strong, efficient fraud detection.

V. CONCLUSION AND FUTURE SCOPE

The growth of FinTech ecosystems has led to an increase in complexity in protecting transactions, as internet crime has become more sophisticated than traditional fraud detection tools. To mitigate this, the current research will present two predictive machine learning approaches CNN and KNN in order to enhance fraud detection using predictive intelligence. An organized methodology was used, which involved min-max normalization, class balancing, treatment of missing values and coding of labels to guarantee effective preprocessing and equal distribution of data. Experimental findings reveal that CNN demonstrated better performance with 99.96% accuracy, prec, recall and F1score, whereas KNN returned 99.95% accuracy, which proves its usefulness as a viable alternative. Further comparisons with SVM and MLP confirmed the effectiveness of the proposed models, with CNN emerging as the most effective. In the future, adaptive learning methods, explainable AI, transparency, ensemble models to reduce false positives, and real-time deployment via cross-institutional and big-data platforms could be potential research areas to enable scalable cybersecurity for FinTechs.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 6, June 2026
Impact Factor: 8.2

REFERENCES

[1] S. Shivam, T. P. Patel, A. K. Padhy, C. Kulkarni, C. Medicherla, and V. Soni, "Anomaly Detection in Financial Payment Transactions Using Efficient Data-Driven Machine Learning Techniques," *2026 IEEE 5th Int. Conf. AI Cybersecurity*, pp. 1–6, Feb. 2026, doi: 10.1109/ICAIC67076.2026.11395758.

[2] T. Shah, "Cloud-Based Data Warehousing for Marketing Agility: Lessons from FinTech Migrations to Snowflake and AWS," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 4, no. 4, March, pp. 642–652, 2024, doi: 10.48175/IJARSCT-16000B.

[3] F. Ekundayo and E. O. Iyabode Atoyebi , Adesola Soyele, "Predictive Analytics for Cyber Threat Intelligence in Fintech Using Big Data and Machine Learning," *Int. J. Res. Publ. Rev.*, vol. 5, no. 11, pp. 5934–5948, 2024.

[4] A. R. Bilipelli, "AI-Driven Intrusion Detection Systems for Large-Scale Cybersecurity Networks Data Analysis: A Comparative Study," *TIJER – Int. Res. J.*, vol. 11, no. 12, December, pp. a922–a928, 2024.

[5] J. B. Mehta, "Autonomous Patch Validation For Zero-Day Exploits In Enterprise Clouds," *Int. J. Appl. Math.*, vol. 38, no. 4s, pp. 1270–1285, August, 2025, doi: 10.12732/ijam.v38i4s.685.

[6] J. W. Sajja and A. Nerella, "Enterprise Finance Reimagined: Harnessing ERP and Data Innovation for Next-Generation Value Creation," *Comput. Fraud Secur.*, vol. 2024, no. 4, p. 10, Apr. 2024, doi: 10.52710/cfs. 743.

[7] M. Parikh, A. A. Soni, S. M. Shah, and A. R. Jha, "Big Data Workload Profiling for Energy-Aware Cloud Resource Management," in *2026 International Conference on Data Analytics for Sustainability and Engineering Technology (DASET 2026)), Track: Big Data and Machine Learning Applications*, IEEE, Ed., arXiv preprint arXiv, 2026, pp. 01–07, January. doi: 10.48550/arXiv.2601.11935.

[8] R. Patel, "Automated Threat Detection and Risk Mitigation for ICS (Industrial Control Systems) Employing Deep Learning in Cybersecurity Defense," *Int. J. Curr. Eng. Technol.*, vol. 13, no. 06, pp. 584–591, 2023, doi: 10.14741/ijcet/v.13.6.11.

[9] D. R. S. Sathesh P Sivashanmugam, Shiva Kumara, Ashay Mohile, "Improving Detection Accuracy of Phishing Attacks with Feature Selection and Machine Learning Techniques in Cybersecurity," in *2026 1st International Conference on Emerging Trends in Advancements and Applications of Computational Intelligence Techniques (ETAACT)*, Bhubaneswar, India: IEEE, 2026, pp. 1–6, April. doi: 10.1109/ETAACT69135.2026.11542138.

[10] N. Rane, "Role and Challenges of ChatGPT and Similar Generative Artificial Intelligence in Finance and Accounting," *SSRN Electron. J.*, 2023, doi: 10.2139/ssrn.4603206.

[11] V. K. Bollu, "Threat Landscape in Artificial Intelligence Systems: Taxonomy, Attack Vectors and Security Implications," *World J. Adv. Res. Rev.*, vol. 29, no. 1, pp. 285–294, 2026, doi: 10.30574/wjarr. 2026.29.1.0007.

[12] 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.

[13] P. Silvia, Q. Aini, E. A. Nabila, Henderi, and H. Nusantoro, "The Role of User Behavior Patterns in Enhancing Fraud Detection in Online Banking: A Bibliometric Analysis," in *2024 2nd International Conference on Technology Innovation and Its Applications (ICTIIA)*, IEEE, Sep. 2024, pp. 1–6. doi: 10.1109/ICTIIA61827.2024.10761930.

[14] R. Sharma and A. Sharma, "Combatting Digital Financial Fraud through Strategic Deep Learning Approaches," in *2024 2nd International Conference on Sustainable Computing and Smart Systems (ICSCSS)*, 2024, pp. 824–828. doi: 10.1109/ICSCSS60660.2024.10625249.

[15] S. Sultana, M. S. Rahman, and M. Afroj, "An efficient fraud detection mechanism based on machine learning and blockchain technology," in *2023 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies, 3ICT 2023*, 2023. doi: 10.1109/3ICT60104.2023.10391306.

[16] T. H. Pranto, K. T. A. M. Hasib, T. Rahman, A. B. Haque, A. K. M. N. Islam, and R. M. Rahman, "Blockchain

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 6, June 2026
Impact Factor: 8.2

and Machine Learning for Fraud Detection: A Privacy-Preserving and Adaptive Incentive-Based Approach," *IEEE Access*, vol. 10, pp. 87115–87134, 2022, doi: 10.1109/ACCESS.2022.3198956.

[17] S. Shivam, V. Nutalapati, T. P. Patel, A. K. Padhy, M. Kumari, and R. Purushothaman, "Transformer-Based Framework for Imbalanced Transaction Fraud Detection in FinTech Systems," in *2026 14th International Symposium on Digital Forensics and Security (ISDFS)*, IEEE, Mar. 2026, pp. 1–6. doi: 10.1109/ISDFS69419.2026.11459102.

[18] S. V Hiremath and M. P. Yogananth, "COVID-19 Image Classification Using VGG-16 & CNN based on CT Scans," *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. 10, no. 5, pp. 1477–1483, 2022, doi: 10.22214/ijraset.2022.42565.

[19] S. Singh, S. A. Pahune, P. Chatterjee, and R. Sura, "Advanced Machine Learning Techniques for Prediction of Customer Churn in Telecommunication Sector," in *2025 IEEE 6th India Council International Subsections Conference (INDISCON)*, Rourkela, India: IEEE, 2025, pp. 1–6, August. doi: 10.1109/INDISCON66021.2025.11252233.

[20] H. Ravilla, "Predictive Analytics for Customer Churn in Salesforce Service Cloud," in *Learning and Analytics in Intelligent Systems*, 2026, pp. 14–24. doi: 10.1007/978-3-032-05377-0_2.

[21] M. Jabeen, S. Ramzan, A. Raza, N. L. Fitriyani, M. Syafrudin, and S. W. Lee, "Enhanced Credit Card Fraud Detection Using Deep Hybrid CLST Model," *Mathematics*, vol. 13, no. 12, p. 1950, Jun. 2025, doi: 10.3390/math13121950.

[22] K. Hayat and B. Magnier, "Data Leakage and Deceptive Performance: A Critical Examination of Credit Card Fraud Detection Methodologies," 2025.