A Survey On Machine Learning And Deep Learning Approaches For Credit Card Fraud Detection

A.Keerthi[1], P.Devalekka[2], M.Sahana[3], Dr R.Punithavathi[4]
[1, 2, 3]Dept of Artificial intelligence and Data Science
[4]AssistantProfessor, Dept of Computer Science and Engineering
[1, 2, 3, 4] ChettinadCollege of Engineering and Technology, Karur , India

Abstract- *Digital payment systems have become a vital part of daily life, with credit cards being widely used for both online and offline transctions.Banks, retailers, and clients have all experienced large financial losses because of the sharp increase in credit card fraud brought on by the growing use of credit cards. The highly unbalanced nature of transaction data, where fraudulent activities are rare and frequently concealed among legitimate transactions, makes it difficult to identify fraudulent transactions. Furthermore, fraud patterns are always changing, requiring quick and accurate detection techniques.Recent developments in deep learning and machine learning have shown tremendous potential in detecting complex and hidden trends in transaction data. This survey examines popular methods for detecting credit card fraud, such as machine learning, deep learning, and hybrid approaches. It focuses on techniques like multi-layer perceptrons, autoencoders, convolutional neural networks, attention mechanisms, and ensemble learning models.*

Keywords- Credit Card Fraud Detection, Class Imbalance, Focal Loss, CNN-BiLSTM, Attention Mechanism.

I. INTRODUCTION

The way people do banking and shopping has changed a lot because of mobile payment apps and online stores[1,2]. Credit cards are widely preferred due to their ease of use and broad acceptance across merchants[1]. Credit cards eliminate the need for carrying physical cash and make it easy to buy things fast [1,6]. The high usage of credit cards among peoplemade it much easier to commit fraudulent activities. [1,3]

Credit card fraud is when someone takes your credit card information and uses it without authorization [1,2]. This will lead tohuge financial losses. Banks have to deal with credit card fraud every day, and it is a lot of work for them to stop credit card fraud[4,8].

Finding fraud transactions is really tough because of how transaction data works. The fraudulent transactions are very few. This makes it hard to find fraud transactions[6,8]. Fraudsters are always coming up with ways to trick us so we have to be careful all the time[6,10]. A fraudulent transaction often becomes identifiable only when analyzed in the context of a user's past transaction history[8,10]. Fraud detection focuses on identifying fraudulent transactions and preventing financial losses [8].

Fraud detection systems used to be rule-based. They would check things like the amount of money being transferred. If something seemed off, they would flag it for review. These old systems were created by people. Were based on simple rules that made sense. They were easy to understand [7,9].

Fraud detection is changing and adapting to new situations. Fraud detection systems must be able to keep up with types of fraud, but these old systems cannot do that. The old ways of doing things are not working anymore because there are many transactions happening and fraud is getting more complicated. Fraud detection systems need to keep up with the fraud patterns. Fraud detection systems need to be able to keep up with fraud patterns and fraud techniques [3,11].

Machine learning and deep learning are really good at finding patterns. They can detect patterns and extract features.These studies show combining machine learning models in ways usually works better at finding credit card fraud. Machine learning and deep learning are used for finding credit card fraud.This survey brings together all these ways and compares. The survey looks at all the ways to detect credit cardfraud.

II. CREDIT CARD FRAUD DETECTION

A credit card fraud detection system begins by collecting information about credit card transactions.

Transaction data includes:
-Transaction amount
-Timestamp
-Merchant type

-Payment method
-Customer behavior patterns

There are hardly few data of fraudulent transactions in the data[1,4]. Fraudulent transactions are usually than one percent of all transactions [1].

This is a problem because,if our model says every single transaction is legitimate it can still seem like it is doing its job. The thing is, fraudulent transactions are what our model is really trying to find so if it does not see many of them it can be misleading. Our model is supposed to identify transactions so this is a big problem for the model. We have to see how well our model works [6,10]. To do this we use things like precision and recall and F1-score and AUC-ROC[8,10].
Recall is really important when we talk about transactions. This is because if our model does not find a fraud transaction we will lose money. Our model has to be very good at finding fraud transactions, so recall is very important for finding fraudulent transactions. We need to make sure our model is good, at finding transactions. [6,10]

III. LEARNING-BASED APPROACHES FOR FRAUD DETECTION

By implementing learning-based techniques, modern fraud detection systems have become more successful at spotting suspicious and fraudulent activity. These systems use a variety of models, each of which is aimed at recognizing particular trends in transaction data.Certain models are trained using past events to identify the traits of fraudulent behavior [3,7]. Others focus on examining transaction sequences over time in order to identify unusual trends or sudden changes in user behavior.

In addition, hybrid approaches combine multiple techniques to improve detection accuracy, while integrated systems bring these methods together into a single, robust framework.

By leveraging these learning-based approaches, fraud detection systems can adapt to evolving fraud patterns and respond more quickly to new threats [4,11]. As a result, they play a crucial role in preventing fraudulent activities and protecting both financial institutions and customers.

A. Autoencoder-Based Models

The primary objective of autoencoders is to learn the patterns of normal transactions and reconstruct them accurately [9,12]. Because they are familiar with typical transaction patterns, autoencoders are effective at detecting transactions [9,14]. This facilitates the detection of transactions that differ from the norm.

When it comes to handling transaction data, autoencoders are effective [6,9]. Autoencoders are able to eliminate redundant or irrelevant information from transaction data [12,14].

B. Temporal Sequence Models

Fraud typically takes the form of someone's spending behavior changing over time, not as a one-off purchase [7,9]. There are some machines like LSTM and BiLSTM which are really good at identifying patterns that occur over time [9,13]. These models can assist in discovering fraud by examining how the spending habits of individuals evolve[7].Such as, if someone starts purchasing things in a store or begins buying more frequently .They also observe when people begin spending a lot of money on the goods they buy [9,13].These models do a really good job at detecting or finding these patterns with the things that people purchase [7,9,13].

C. Attention Mechanism

By enabling them to selectively concentrate on the most informative portions of the input data, attention mechanisms improve deep learning models [7,10].When it comes to credit card fraud detection, attention aids the model in determining which transactions, time intervals, or characteristics have the most impact on the fraud prediction [10,11].

Long sequences of valid transactions frequently contain fraudulent activity, which makes it challenging for standard models to identify [7,9].

In order to overcome this difficulty, attention mechanisms give suspicious patterns—such as odd spending amounts, unusual transaction locations, or abrupt changes in transaction frequency—higher weights [10,11]. By minimizing the impact of unnecessary or redundant information, this selective focus increases detection accuracy [10,12].

D. Ensemble Learning Approaches

Instead of depending on a single classifier, ensemble learning techniques combine the predictions of several models to enhance fraud detection performance [5,12].Ensemble methods reduce variance, increase stability, and produce more accurate predictions by combining decisions from various models [5,9].

Random Forest and gradient boosting techniques are two frequently used ensemble techniques in credit card fraud detection [5,12].Gradient boosting builds models sequentially to fix mistakes made by earlier learners, whereas Random Forest creates multiple decision trees using various subsets of data and features [5].These techniques work especially well with high-dimensional, noisy transaction data [3,5].
Combining ensemble classifiers with deep learning-based feature extraction improves detection performance significantly [9,11].

In these configurations, raw transaction data is transformed into complex representations by deep learning models, which are subsequently fed into ensemble classifiers [7,11].

Because Multilayer Perceptrons can capture non-linear relationships, they are frequently used as baseline deep learning models [7,8].

However, MLPs may find it difficult to illustrate transaction sequences that change over time due to their lack of explicit temporal modeling capabilities [7,9].

IV. COMPARATIVE ANALYSIS

The best results usually come from models that combine a technique like CNNs and recurrent layers and attention mechanisms. These hybrid deep learning models are really good at figuring out patterns in transaction data. These models can detect things that happen over time. These models require high computational resources for traning and deployment. Autoencoder-based models are effective for anomaly detection and dimensionality reduction.

Table 1: Comparative Analysis of Credit Card Fraud Detection Approaches

Model Category	Core Techniques	Feature Learning	Temporal Modeling	Interpretability Basis	Computational Structure
Hybrid DL [8][13]	CNN + BiLSTM + Attention	Hierarchical & attention-based representation	Bidirectional sequence modeling	Architecture-driven	Multi-layer deep framework
Autoencoder-Based [8][13]	Autoencoder + Classifier	Latent space encoding	Reconstruction-oriented	Latent feature representation	Encoder–decoder structure
RNN-Based [5][8][13]	LSTM / BiLSTM	Sequential feature learning	Recurrent dependency modeling	Hidden-state representation	Recurrent neural framework
Ensemble Methods [4][5][11]	RF, XGBoost, Blending	Tree-based aggregation	Feature-engineered sequences	Feature-importance analysis	Parallel ensemble structure
MLP-Based [14]	Deep Feedforward NN	Non-linear transformation layers	Static input modeling	Weight-based representation	Feedforward architecture
Traditional ML [1][3][11]	LR, SVM, DT	Manual feature engineering	Static modeling	Coefficient / rule-based	Lightweight statistical models

V. CHALLENGES AND LIMITATIONS

Although fraud detection systems have significantly improved over time, several challenges remain unresolved.

One big problem is that the data they use to make decisions is not balanced. This means that the fraud detection models they create can be unfair and make mistakes. The fraud detection systems can be biased because of this imbalance in the data they use to make decisions, about fraud. This challenge is particularly significant for hybrid systems that integrate multiple modeling techniques.

VI. FUTURE SCOPE

Despite the progress achieved in machine learning and deep learning-based credit card fraud detection, several research opportunities remain. Future work should focus on developing adaptive models that can handle evolving fraud patterns through online learning and concept drift detection. Improving the interpretability of deep learning models is also essential to ensure transparency and trust in financial decision-making. Additionally, addressing class imbalance more effectively, optimizing models for real-time detection, and incorporating privacy-preserving techniques such as federated learning will be critical for practical deployment. Integrating

diverse data sources, including behavioral and contextual information, may further enhance detection accuracy in real-world financial systems.

VII. CONCLUSION

This survey reviewed and compared various machine learning and deep learning approaches for credit card fraud detection. The findings indicate that hybrid and ensemble-based models generally achieve superior performance by integrating feature learning, temporal modeling, model interpretability, and computational complexity remain critical research areas, Continued development of scalable, explainable, and adaptive fraud detection systems is essential to ensure secure digital financial ecosystems.

REFERENCES

[1] V. Kumar K. S. *et al.*, "Credit Card Fraud Detection Using Machine Learning Algorithms," *International Journal of Engineering Research & Technology*, 2021.[Online]. Available: https://www.ijert.org/credit-card-fraud-detection-using-machine-learning-algorithms

[2] M. A. Gill, M. Qureshi, A. Rasool, and M. M. Hassan, "Detection of Credit Card Fraud Through Machine Learning in Banking Industry," *Journal of Computing & Biomedical Informatics*, 2021.Online.Available: https://jcbi.org/index.php/Main/article/view/204

[3] E. Ileberi, Y. Sun, and Z. Wang, "A Machine Learning-Based Credit Card Fraud Detection Using Genetic Algorithm for Feature Selection," *Journal of Big Data*, vol. 9, no. 1, 2022. [Online]. Available: https://doi.org/10.1186/s40537-022-00573-8

[4] A. K. Verma *et al.*, "Review of Machine Learning Approach on Credit Card Fraud Detection," *Discover Artificial Intelligence*, Springer Nature, 2022.[Online]. Available: https://doi.org/10.1007/s44230-022-00004-0

[5] 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 and Cognitive Computing*, vol. 8, no. 1, 2024.[Online]. Available: https://doi.org/10.3390/bdcc8010006

[6] D. Rai and J. S. N., "Credit Card Fraud Detection Using Machine Learning and Data Mining Techniques — A Literature Survey,"Zenodo, 2023.[Online]. Available: https://doi.org/10.5281/zenodo.8190094

[7] S. R. Patel *et al.*, "Credit Card Fraud Detection Using Deep Learning: A Survey,"*DeepAI*, 2023.Online. Available: https://deepai.org/publication/credit-card-fraud-detection-using-machine-learning-a-survey

[8] R. Sharma and P. K. Singh, "Credit Card Fraud Detection: A Comparative Study of Machine Learning and Deep Learning Methods," *Engineering, Technology & Applied Science Research*, vol. 10, no. 5, 2023.[Online]. Available: https://doi.org/10.47191/etj/v10i05.45

[9] J. Wang *et al.*, "Enhancing Credit Card Fraud Detection Using DBSCAN-Augmented Disjunctive Voting Ensemble,"*Scientific Reports*, vol. 15, 2025. [Online]. Available: https://doi.org/10.1038/s41598-025-22960-w

[10] M. Al-Hassan *et al.*, "A Systematic Review of AI-Enhanced Techniques in Credit Card Fraud Detection," *Journal of Big Data*, vol. 12, no. 1, 2025. [Online]. Available: https://doi.org/10.1186/s40537-024-01048-8

[11] L. Zhang *et al.*, "Enhancing Fraud Detection in Credit Card Transactions: A Comparative Study of Machine Learning Models," *Computational Economics*, 2025.[Online]. Available: https://doi.org/10.1007/s10614-025-11071-3

[12] A. R. Khalid *et al.*, "Voting Ensemble-Based Credit Card Fraud Detection Using Machine Learning," *Big Data and Cognitive Computing*, 2024. [Online]. Available: https://www.mdpi.com/2504-2289/8/1/6

[13] R. K. Mishra *et al.*, "Autoencoder and LSTM-Based Credit Card Fraud Detection," *SN Computer Science*, vol. 4, no. 4, 2023. [Online]. Available: https://doi.org/10.1007/s42979-023-01977-w

[14] S. Mehta *et al.*, "A Comparative Study of Machine Learning and Deep Learning Models for Credit Card Fraud Detection," *Computational Economics*, 2025. [Online]. Available: https://doi.org/10.1007/s10614-025-11071-3