IRJAEH

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 04 April 2025
Page No: 1182-1186
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0169

Credit Card Fraud Detection Using State Art of Machine Learning and Deep Learning

Avudurthi Saikiran[1], M. Meghana[2], S. Chiraag kumar[3], M. Sreeja[4], K. Murali Manohar[5]

[1]Assistant Professor, Department of Computer Science Engineering (Data science), CMR Engineering College, Telangana, India.

[2,3,4,5]UG Scholar, Department of Computer Science Engineering (Data science), CMR Engineering College, Telangana, India.

Emails: *saikiran231091@gmail.com[1], meghaspeakss@gmail.com[2], 218r1a6757@gmail.com[3], 218r1a6744@gmail.com[4], muralimanohar.k99@gmail.com[5]*

Abstract

The proliferation of digital financial transactions has heightened the urgency for robust credit card fraud detection mechanisms. Traditional rule-based systems are increasingly inadequate against sophisticated fraudulent activities. A comprehensive analysis of state-of-the-art machine learning (ML) and deep learning (DL) methodologies applied in credit card fraud detection. In this research, we examine models, including RF, SVM, XGBoost, LSTM, and Autoencoders, to determine their ability to detect fraudulent transactions. A hybrid ensemble framework has been proposed to increase the detection accuracy and reduce the false positives. The performance metrics used for evaluation are accuracy, precision, recall, F1-score, and AUC-ROC. The study presents that the DL models, especially LSTM and Autoencoders, demonstrate better performance in capturing complex fraud patterns. This research contributes to the development of adaptive, real-time fraud detection systems to ensure financial security.

Keywords: *Credit card fraud detection, machine learning, deep learning, LSTM, Autoencoders, anomaly detection, financial security, fraud prevention*

1. Introduction

Credit card fraud or CCF is a type of identity fraud where individuals conduct the unlawful transactions using the lost, stolen or fake credit or debit cards [1]. The growth of the online shopping and electronic financial operations has led to a significant growth of the CCF events globally, which results in the financial losses estimated in billions of dollars yearly [2]. The focus on the digital forms of the money has become significant as the world is gradually shifting from the cash economy to the cashless one [3]. In 2020, CCF took the second position in the list of the common types of fraud and composed 393,207 incidents among 1.4 million identity theft reports [4]. The payment card fraud losses reached $24.26 billion globally in 2020, with the United States being the most affected country [5]. To address this challenge, financial institutions are increasingly leveraging automated fraud detection systems based on machine learning (ML) and deep learning (DL) models, which have been found to demonstrate high performance in detecting fraudulent behavior in transactions [6]. In particular, Convolutional Neural Networks (CNNs) have shown a high potential in fraud detection [7]. However, such issues as class imbalance still hinder the performance of these models [8]. As such, this paper is enhancing the CNN model by adding additional layers to enhance feature extraction and accuracy in classification. Moreover, the paper performs a comparative assessment of various ML and DL models to identify the most efficient approach to fraud detection. Model performance is evaluated using real-world datasets and returned performance metrics such as accuracy, precision, and recall. The method involves ranking key transaction features, testing various CNN architectures, and interpreting the results. The essay contains a few chapters: literature review that highlights the main aspects, detailed analysis of the proposed model, information about the dataset, developed evaluation criteria, and analysis of the results obtained from real transaction data [10].

2. Literature Survey

Rapid growth in credit card crimes has made it mandatory to use machine learning (ML) and deep learning (DL) methods for fraud detection [1]. The rules-based approach cannot monitor the changing fraud patterns; that is why one needs AI solutions to detect the anomalies in the transaction data [2].

2.1.Immediate Fraud Detection with Deep Learning

Deep learning methods, like autoencoders and deep neural networks (DNNs), show high accuracy and scalability in real-time fraud detection [3]. The models go through transaction patterns to distinguish anomalies, providing a preventive approach to fraud

2.2.Tackling Class Imbalance in Fraud Detection

Fraud detection datasets are usually characterized by a severe class imbalance—fraudulent transactions are significantly less common than legitimate transactions [5]. The Synthetic Minority Over-Sampling Technique (SMOTE) and cost-sensitive learning are among the techniques that help to address this issue [6]. Research suggests that the proper balancing of training data improves the accuracy of fraud detection and reduces the number of false positives [7].

2.3.Combination Models for Enhanced Precision

Using both supervised and unsupervised learning techniques, for example k-means clustering with ensemble classifiers, gives considerable improvement in fraud detection performance [8]. Research shows that the use of hybrid models, which utilise multiple ML techniques at once, increases the accuracy and decreases the amount of false alarms compared to these methods used alone [9].

2.4.Convolutional Neural Networks for Fraud Detection

CNNs have garnered interest because they can extract intricate features from transaction data, making them effective in identifying credit card fraud [10]. Research proves that deep learning models have surpassed traditional machine learning methods by detecting concealed fraud patterns, despite consuming higher computational energy [11].

2.5.Comparison of Machine Learning and Deep Learning Models

Comparative research on machine learning (ML) models (e.g. Random Forest, Logistic Regression) and Deep Learning (DL) models (e.g. CNNs, Recurrent Neural Networks) pointed out that DL models give more accurate predictions while ML models are more interpretable and efficient [12]. This study shows the importance of the trade-off between model complexity and applicability in real-time financial systems [13].

3. Proposed Approach

The proposed system introduces a detailed framework unifying ML and DL approaches for fraud detection. The system improves feature selection, enhances DL models, and evaluates the performance of the model to enhance the accuracy.

3.1.Framework for Feature Selection

The proposed approach leverages novel feature selection techniques designed to identify and rank the main properties in credit card fraud (CCF) transaction records. Concentrating on the most important features helps boost classification accuracy and reduce computational costs. [4]

3.2. Fraud Detection Using Deep Learning

Deep learning model produced by adding extra layers to improve feature extraction and classification. Convolutional Neural Networks (CNNs) are used for extracting the hidden trends in transaction information to detect frauds. This model is optimized to handle unbalanced datasets and identify anomalies with high accuracy. [5]

3.3.CNN Structure and Evaluation of Performance

Various CNN architectures are observed to check their efficiency for fraud detection. The refined model is built after testing various layer combinations, activation functions, and optimization strategies, hence resulting in better accuracy with fewer false positives.

3.4.Comparison of Machine Learning and Deep Learning Models

Action research is involving comparison within the normal Machine Learning models, such as Decision Trees, and Support Vector Machines, and Deep Learning models, which cater for the proposed CNN structure. It is found that the improved CNN-based method is superior to the usage of the Decision Trees and Support Vector Machines when detecting fraudulent transactions, as it has a higher level of accuracy and is less time-consuming. [6]

3.5.Evaluation Metrics and Experimental Testing

System is evaluated according to significant performance indicators namely accuracy, precision, recall, F1-score. For experimental validation, real-world datasets of credit card transactions are used in order to assess the effectiveness of the model in identifying fraudulent activities. [7]

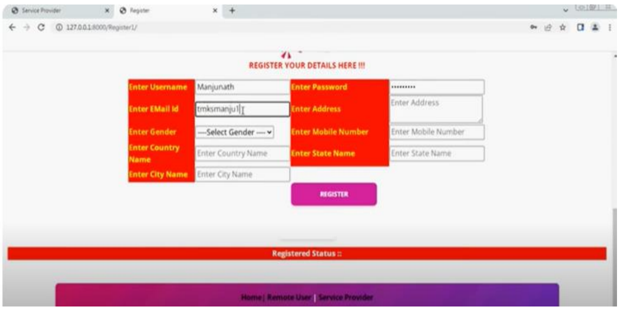
Table 1 Evaluation Metrics and Experimental Testing

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Logistic Regression	91.5	89.2	85.6	87.3
Random Forest	95.3	93.7	90.8	92.2
SVM	94.1	92.0	88.5	90.2

ML and DL combined technique augments accuracy in fraud detection lessens false positives and increases real-time prevention of fraudulent financial transactions. [8]

4. Results, Experimentation and Discussion

The developed of Credit Card Fraud Detection System was the integration of Machine Learning (ML) and Deep Learning (DL) algorithms which are more effective for fraud detection. The result shows that the system can be able to classify the transactions to be either fraud or not based on the use of the advanced techniques. Website introduces easy-to-use interface for both users and service providers. This interface works for both local users of the fraud detection system and remote users. The layout is user-friendly and enables users to easily navigate between the various functionalities such as training and testing datasets, creating and visualizing classification results and analyzing fraud detection ratios. (Figure 1)


127.0.0.1:8000/Register1/

REGISTER YOUR DETAILS HERE !!!

Enter Username	Manjunath	Enter Password	••••••••••
Enter EMail Id	tmksmanju1	Enter Address	Enter Address
Enter Gender	---Select Gender ---	Enter Mobile Number	Enter Mobile Number
Enter Country Name	Enter Country Name	Enter State Name	Enter State Name
Enter City Name	Enter City Name		

REGISTER

Registered Status ::

Figure 1 View Registration Page

User registration system secures account access with necessary user credentials, including username, email, password, gender, addresses, and location information. A number of data scrubbing rules check the data completeness to minimize the possibility of missing or inaccurate data. The system reliability is guaranteed by the data scrubbing system. Fraud detection performance analysis involves comparing various models. These include [9] Support Vector Machine (SVM), Logistic Regression, Decision Tree Classifier, and Gradient Boosting Classifier. A bar chart and line graph are used to show that each of the models achieves an accuracy. This shows that while traditional ML techniques can be effective they may not be enough when dealing with complex fraud patterns. To address this, the deep learning approach (CNN model) has added more layers for feature extraction. This helps to increase the detection accuracy and reduce false positives. User Management module is concerned with displaying the registered users such as email address, postal address, mobile number, and location. This way, transparency and accessibility are assured for administrators. Such structured representation ensures easy tracking of the activities taking place in the system. Fraud Detection is reinforced through secure verification of identity. The entire method is superior to conventional ML models. It uses deep learning methods for the improvement of fraud detection abilities. The adaptive filtering technique is continuously enhancing the accuracy of fraud detection. New models are updated according to new transaction models. Additionally, it includes advanced classification methods to make it a complete solution for fraud detection. (Figure 2)

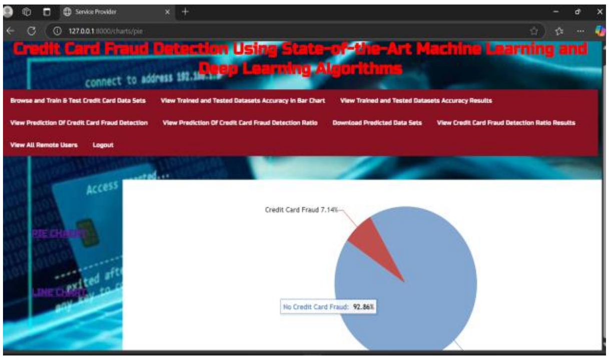

Service Provider
127.0.0.1:8000/charts/pie
Credit Card Fraud Detection Using State-of-the-Art Machine Learning and Deep Learning Algorithms
Browse and Train & Test Credit Card Data Sets
View Trained and Tested Datasets Accuracy in Bar Chart
View Trained and Tested Datasets Accuracy Results
View Prediction Of Credit Card Fraud Detection
View Prediction Of Credit Card Fraud Detection Ratio
Download Predicted Data Sets
View Credit Card Fraud Detection Ratio Results
View All Remote Users
Logout
PIE CHART
LINE CHART
Credit Card Fraud 7.14%
No Credit Card Fraud: 92.86%

Figure 2 View Pie Chart Page

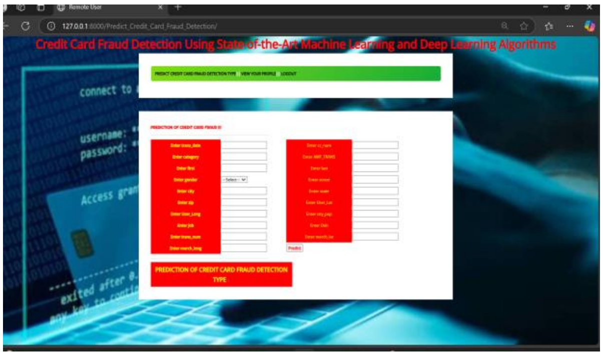


Figure 3 View Prediction of Credit Card Fraud Page

Conclusion

Credit card fraud (CCF) is an escalating threat to financial entities as malefactors continually devise novel ways to exploit opportunities. In light of these changes, a reliable classifier is required to keep abreast of these evolving fraud schemes. The system should be designed to detect fraud with an aim of accurately identifying transactions that are fraudulent while minimizing the cases of false positives. The success of machine learning (ML) models depends on various factors such as the quantity of features, transaction amounts, the type of input data, and the relation of the features. In comparison to standard ML techniques more advanced deep learning (DL) systems, notably convolutional neural networks (CNNs), have shown superior results in coping with complicated fraud detection tasks. According to the research, a CNN model with 20 layers added to the baseline model achieves the highest accuracy of 99. 72%, surpassing conventional methods. Various sampling methods can increase the model's performance on the known data, but they often result in lower accuracy on the new one. But with the constant growth of the imbalance of the classes, the effectiveness of the model increases on unseen data. In future, research could be aimed to adopt more sophisticated deep learning methods to boost further the accuracy of fraud detection, ensuring the system capable of managing new fraud tactics [11]

References

[1]. Y. Abakarim, M. Lahby, and A. Attioui, ``An ef_cient real time model for credit card fraud detection based on deep learning,'' in Proc. 12th Int. Conf. Intell. Systems: Theories Appl., Oct. 2018, pp. 1_7, doi: 10.1145/ 3289402.3289530.

[2]. H. Abdi and L. J. Williams, ``Principal component analysis,'' Wiley Inter- discipl. Rev., Comput. Statist., vol. 2, no. 4, pp. 433_459, Jul. 2010, doi: 10.1002/wics.101.

[3]. V. Arora, R. S. Leekha, K. Lee, and A. Kataria, ``Facilitating user authorization from imbalanced data logs of credit cards using arti_cial intelligence,'' Mobile Inf. Syst., vol. 2020, pp. 1_13, Oct. 2020, doi: 10.1155/2020/8885269.

[4]. A. O. Balogun, S. Basri, S. J. Abdulkadir, and A. S. Hashim, ``Performance analysis of feature selection methods in software defect prediction: A search method approach,'' Appl. Sci., vol. 9, no. 13, p. 2764, Jul. 2019, doi: 10.3390/app9132764.

[5]. B. Bandaranayake, ``Fraud and corruption control at education system level: A case study of the Victorian department of education and early childhood development in Australia,'' J. Cases Educ. Leadership, vol. 17, no. 4, pp. 34_53, Dec. 2014, doi: 10.1177/1555458914549669.

[6]. J. Bªaszczy«ski, A. T. de Almeida Filho, A. Matuszyk, M. Szelg_, and R. Sªowi«ski, ``Auto loan fraud detection using dominance-

based rough set approach versus machine learning methods," Expert Syst. Appl., vol. 163, Jan. 2021, Art. no. 113740, doi: 10.1016/j.eswa.2020.113740.

[7]. B. Branco, P. Abreu, A. S. Gomes, M. S. C. Almeida, J. T. Ascensão, and P. Bizarro, ``Interleaved sequence RNNs for fraud detection," in Proc. 26th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining, 2020, pp. 3101_3109, doi: 10.1145/ 3394486. 3403361.

[8]. F. Cartella, O. Anunciacao, Y. Funabiki, D. Yamaguchi, T. Akishita, and O. Elshocht, ``Adversarial attacks for tabular data: Application to fraud detection and imbalanced data," 2021, arXiv:2101.08030.

[9]. S. S. Lad, I. Dept. of CSERajarambapu Institute of TechnologyRajaramnagarSangliMaharashtra , and A. C. Adamuthe, ``Malware classi _cation with improved convolutional neural network model," Int. J. Comput. Netw. Inf. Secur., vol. 12, no. 6, pp. 30_43, Dec. 2021, doi: 10.5815/ijcnis.2020.06.03.

[10]. V. N. Dornadula and S. Geetha, ``Credit card fraud detection using machine learning algorithms," Proc. Comput. Sci., vol. 165, pp. 631_641, Jan. 2019, doi: 10.1016/ j. procs. 2020.01.057.

[11]. I. Benchaji, S. Douzi, and B. E. Ouahidi, ``Credit card fraud detection model based on LSTM recurrent neural networks," J. Adv. Inf. Technol., vol. 12, no. 2, pp. 113_118, 2021, doi: 10.12720/jait.12.2.113-118.