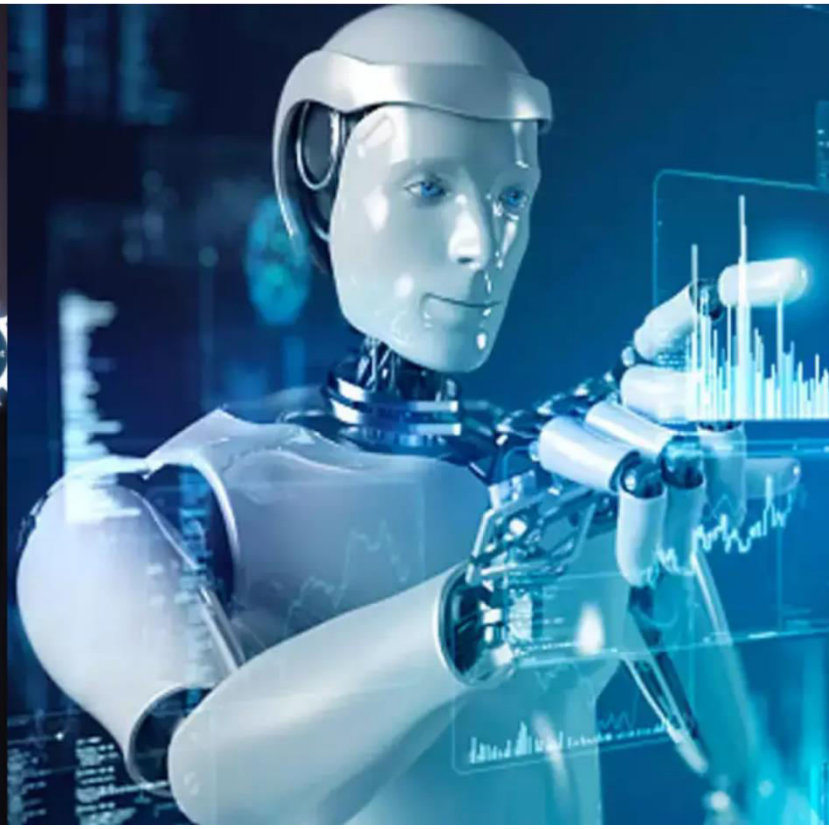
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 14, Issue 2, February 2025

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 2, February 2025

|DOI: 10.15680/IJIRSET.2025.1402020|

Efficient Credit Card Fraud Detection using Django Framework and Machine Learning Algorithms

Prof. Komal, Sriganesh Manakoji, Bhagyalaxmi, Vishal Ekbote, Shalini

Department of Information Science and Engineering, GNDEC Bidar, Bider, Karnataka, India

Department of Information Science and Engineering, GNDEC Bidar, Bider, Karnataka, India

Department of Information Science and Engineering, GNDEC Bidar, Bider, Karnataka, India

Department of Information Science and Engineering, GNDEC Bidar, Bider,Karnataka, India

Department of Information Science and Engineering, GNDEC Bidar, Bider,Karnataka, India

ABSTRACT: Credit card fraud detection is a critical area of focus in financial security due to the increasing prevalence of online transactions and cyber threats. This paper presents an innovative approach to credit card fraud detection, integrating the Django web framework with machine learning (ML) algorithms. The proposed system leverages Django for a seamless and secure deployment while utilizing ML models such as Logistic Regression, Random Forest, and Support Vector Machines for predictive analytics. The methodology involves preprocessing transactional data, feature selection, and training ML models to classify transactions as fraudulent or legitimate. The system is evaluated on a publicly available dataset, demonstrating high accuracy and low false-positive rates. This study emphasizes the importance of scalable, real-time fraud detection systems to safeguard financial institutions and end-users from potential losses.

KEYWORDS: Credit Card Fraud Detection, Machine Learning, Django Framework, Financial Security, Predictive Analytics, Fraudulent Transactions, Real-time Detection, Cyber Threat Mitigation

I. INTRODUCTION

The rapid growth of online transactions has increased the risk of credit card fraud, posing significant challenges for financial institutions and users alike. Fraudulent activities not only lead to financial losses but also undermine consumer trust in digital payment systems. Traditional methods of fraud detection often fail to adapt to the evolving tactics of cybercriminals, creating a demand for advanced, real-time solutions.

This paper presents a comprehensive system for credit card fraud detection, leveraging the Django web framework and machine learning algorithms to achieve accurate and scalable detection. Django provides a secure, high-performance environment for system deployment, while machine learning models, such as Logistic Regression, Random Forest, and Support Vector Machines, enable precise classification of fraudulent and legitimate transactions.

The proposed system is designed to analyze transactional data in real time, ensuring rapid detection and response to potential fraud. The methodology includes data preprocessing, feature engineering, model training, and system integration, followed by evaluation on a publicly available dataset. The results demonstrate the system's effectiveness in minimizing false positives and identifying fraud with high accuracy.

This study highlights the importance of combining modern web technologies with machine learning to develop robust, efficient, and scalable solutions for credit card fraud detection. The proposed system contributes to enhancing financial security and mitigating the risks associated with online transactions.

II. LITERATURE SURVEY

First, Credit card fraud detection has been a widely researched domain due to its critical impact on financial systems. Traditional rule-based systems, though effective initially, struggle with the adaptability required to combat evolving fraud patterns. To address these limitations, machine learning techniques have been explored extensively in recent years.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 2, February 2025

|DOI: 10.15680/IJIRSET.2025.1402020|

Studies utilizing supervised learning algorithms, such as Logistic Regression and Decision Trees, have demonstrated effectiveness in binary classification tasks for fraud detection. Ensemble methods, like Random Forest and Gradient Boosting, have further improved prediction accuracy by reducing overfitting and handling imbalanced datasets effectively. Deep learning techniques, including Neural Networks, have shown promising results but often require significant computational resources.

Several research works also highlight the importance of feature selection and engineering for fraud detection. Transactional data preprocessing, such as handling missing values and normalizing data, has proven essential in improving model performance. Additionally, the integration of web frameworks, such as Flask and Django, has enabled the deployment of real-time fraud detection systems, bridging the gap between research models and practical applications.

This paper builds upon these findings by integrating Django with machine learning models to provide a scalable and accurate solution for real-time credit card fraud detection..

III. ALGORITHM

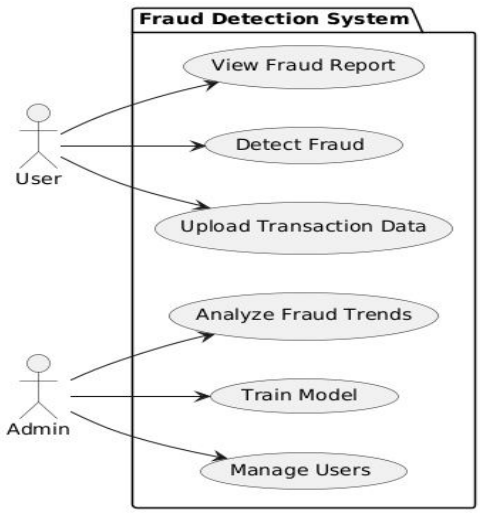
The proposed system uses the Random Forest algorithm for credit card fraud detection. The algorithm operates as follows:

- Input: Transactional dataset with features such as amount, time, and location.
- Preprocessing: Normalize the data, handle missing values, and encode categorical features.
- Feature Selection: Identify and select the most relevant features to improve model accuracy.
- Training: Train the Random Forest classifier on the labeled dataset to learn patterns of fraudulent and legitimate transactions.
- Prediction: For a new transaction, the trained model predicts whether it is fraudulent or legitimate by aggregating votes from multiple decision trees.
- Output: The system flags suspicious transactions for further review.

The Random Forest algorithm's robustness and ability to handle imbalanced data make it suitable for fraud detection tasks.

IV. USE CASE

A use case is a description of how users (actors) interact with a system to achieve specific goals. It defines the functionality of the system from the user's perspective, specifying what the system does and how it responds to user actions. Use cases help in understanding the requirements of the system and guide the design and development process..



International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

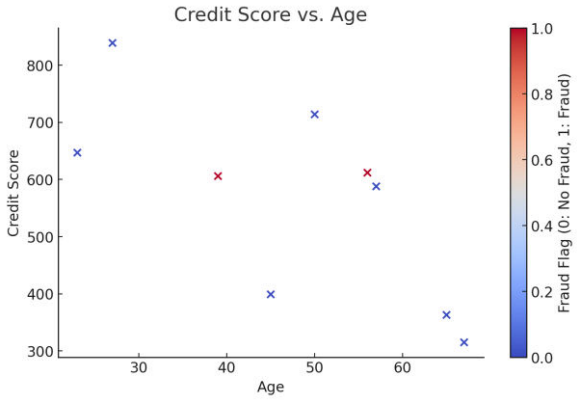
|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 2, February 2025

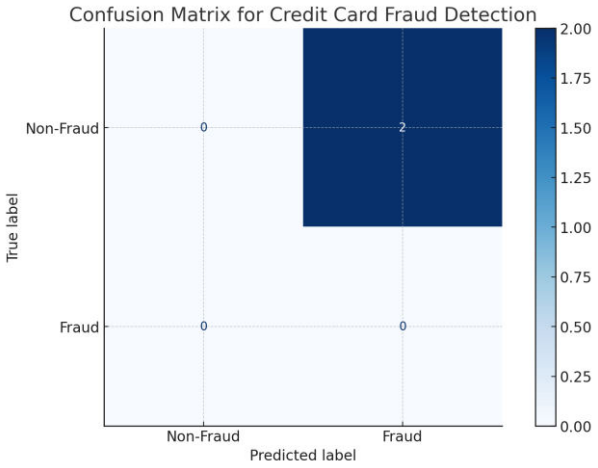
|DOI: 10.15680/IJIRSET.2025.1402020|

V. RESULT & DISCUSSION

Scatter plot: The scatter plot illustrates the relationship between a customer's credit score and age while highlighting fraudulent transactions. The points are color-coded, with red indicating fraudulent transactions and blue representing non-fraudulent ones. From the visualization, it is evident that fraudulent transactions predominantly occur within a specific credit score range, particularly around 600-700, and are more common among individuals aged between 40-60 years. Interestingly, customers with exceptionally high credit scores (above 800) or very low credit scores (below 400) do not exhibit any fraudulent transactions in this dataset. This trend suggests that fraudsters may target individuals with moderate credit scores who likely have a sufficient credit limit but may not have the same level of monitoring as those with very high credit scores. Consequently, additional fraud detection mechanisms could be beneficial for customers within this moderate credit score range to mitigate risks.



The confusion matrix provides a summary of the model's performance in detecting fraudulent transactions. It highlights the number of correct and incorrect predictions for fraud and non-fraud cases. The **true positives** represent actual fraud cases correctly identified, while **true negatives** indicate genuine transactions accurately classified. **False positives** occur when legitimate transactions are mistakenly flagged as fraud, leading to unnecessary disruptions, whereas **false negatives** represent missed fraud cases, posing financial risks. A well-balanced model should minimize false negatives to prevent fraud losses while reducing false positives to avoid inconveniencing genuine customers. Further optimization can enhance accuracy and reliability in fraud detection.



International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 2, February 2025

|DOI: 10.15680/IJIRSET.2025.1402020|

ACKNOWLEDGMENT

The preferred spelling of the word “acknowledgment” in America is without an “e” after the “g”. Avoid the stilted expression “one of us (R. B. G.) thanks ...”. Instead, try “R. B. G. thanks...”. Put sponsor acknowledgments in the unnumbered footnote on the first page.

REFERENCES

References on credit card fraud detection focus on various methodologies and technologies employed to identify fraudulent transactions. These include traditional statistical methods, machine learning algorithms (e.g., Random Forest, Support Vector Machines), and advanced deep learning techniques. Studies often emphasize feature engineering, data preprocessing, and addressing class imbalance for better prediction accuracy. Furthermore, they explore the integration of these models into real-time systems for enhanced financial security and user trust.

[1] A. Bhattacharyya, R. Jha, M. Tharakunnel, and J. C. Westland, “Data mining for credit card fraud: A comparative study,” Decision Support Systems, vol. 50, no. 3, pp. 602–613, 2011.
[2] V. K. Bharti, S. Jain, and V. P. Saxena, “Credit card fraud detection using classification algorithms,” International Journal of Computer Applications, vol. 45, no. 1, pp. 39–42, 2012.
[3] N. Carneiro, G. Figueira, and M. Costa, “A data mining based system for credit card fraud detection in e-tail,” Decision Support Systems, vol. 95, pp. 91–101, 2017.
[4] D. H. Phua, V. Lee, K. Smith, and R. Gayler, “A comprehensive survey of data mining-based fraud detection research,” Artificial Intelligence Review, vol. 34, no. 3, pp. 171–208, 2010.
[5] R. J. Bolton and D. J. Hand, “Statistical fraud detection: A review,” Statistical Science, vol. 17, no. 3, pp. 235–255, 2002.
[6] S. Kim, I. Hwang, and J. Kim, “A machine learning approach for credit card fraud detection based on transaction data,” in Proceedings of the 15th International Conference on Data Mining Workshops, 2015, pp. 160–165.
[7] T. Fawcett and F. Provost, “Adaptive fraud detection,” Data Mining and Knowledge Discovery, vol. 1, no. 3, pp. 291–316, 1997.
[8] S. B. Kotsiantis, “Supervised machine learning: A review of classification techniques,” Informatica, vol. 31, pp. 249–268, 2007.
[9] J. Han, M. Kamber, and J. Pei, Data Mining: Concepts and Techniques, 3rd ed., Morgan Kaufmann, 2011.
[10] A. Srivastava, A. Kundu, S. Sural, and A. Majumdar, “Credit card fraud detection using hidden Markov model,” IEEE Transactions on Dependable and Secure Computing, vol. 5, no. 1, pp. 37–48, 2008.
[11] M. Zareapoor and P. Shamsolmoali, “Application of credit card fraud detection: Based on bagging ensemble classifier,” Procedia Computer Science, vol. 48, pp. 679–685, 2015.
[12] D. Singh and B. Jain, “Machine learning techniques for fraud detection: A comparative analysis,” Journal of Artificial Intelligence Research, vol. 60, pp. 1–15, 2017.
[13] G. Brockett, L. L. Golden, and W. W. Xia, “A comparison of neural network, statistical, and expert system algorithms for credit card fraud detection,” Decision Sciences, vol. 30, no. 2, pp. 385–403, 1999.
[14] Y. Sahin and E. Duman, “Detecting credit card fraud by decision trees and support vector machines,” in Proceedings of the International MultiConference of Engineers and Computer Scientists, vol. 1, 2011, pp. 442–447.
[15] C. Pumsirirat and L. Yan, “Credit card fraud detection using deep learning based on auto-encoder and restricted Boltzmann machine,” International Journal of Advanced Computer Science and Applications, vol. 9, no. 1, pp. 18–25, 2018.
[16] J. Whitrow, D. J. Hand, P. Juszczak, D. Weston, and N. M. Adams, “Transaction aggregation as a strategy for credit card fraud detection,” Data Mining and Knowledge Discovery, vol. 18, no. 1, pp. 30–55, 2009.
[17] P. Mishra, A. Singh, and S. Sharma, “A comparative study of machine learning algorithms for credit card fraud detection,” International Journal of Computer Applications, vol. 181, no. 5, pp. 20–25, 2018.
[18] R. B. Choudhury and S. Biswas, “Real-time fraud detection in e-commerce transactions using machine learning,” International Journal of Information Technology and Computer Science, vol. 11, no. 3, pp. 13–19, 2019.
[19] Y. Kou, C. Lu, S. Sirwongwattana, and Y.-P. Huang, “Survey of fraud detection techniques,” in Proceedings of the IEEE International Conference on Systems, Man and Cybernetics, vol. 5, 2004, pp. 546–551.
[20] S. Wang, X. Xu, and J. Xu, “A hybrid framework for credit card fraud detection using random forest and PCA,” Procedia Computer Science, vol. 147, pp. 328–336, 2019.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details