www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 04, April 2025, pp : 866-869

e-ISSN : 2583-1062
Impact Factor : 7.001

CREDIT CARD FRAUD DETECTION

Shinde Vaishnavi Ramdas[1], Tambe Mayuri Subhash[2], Dhavale Akshada Ramdas[3], Agre Anjali Datattray[4], Auti S. S[5]

[1,2,3,4]Student, Department of Computer Engineering, Samarth polytechnic, Belhe, Pune, India

[5]Guide, Department of Computer Engineering, Samarth polytechnic, Belhe, Pune, India

ABSTRACT

With the increased prevalence of online transactions and digital payments, credit card fraud detection has become increasingly important. Machine learning has been a powerful and effective support for identifying and predicting fraudulent transactions based on patterns and anomalies in transactions data. This paper investigates the use of different machine learning methods for detecting credit card fraud, including supervised and unsupervised options. We preprocess transaction history datasets to deal with class imbalance, feature extraction, and normalization of the input. Multiple algorithms including logistic regression, decision trees, random forests, support vector machine, and neural networks classifiers were explored for identifying fraudulent transactions. Methods for improving fraud detection such as ensemble methods and anomaly-based detection including isolation forests and auto encoders were also evaluated. Overall results indicate that advanced machine learning models can improve fraud detection through real time analysis and minimizes false-positives and enhances financial security. This study demonstrates the need to continually evaluate the model to combat new fraud schemes, contributing to improve secure using a machine learning approach to prevent credit card fraud detection.

Keywords: Credit card fraud detection, Machine learning, fraudulent transactions, supervised learning, and unsupervised learning, Transaction data.

1. INTRODUCTION

The significance of machine learning in the detection of credit card fraud is that it can improve security in the digital payment system. As e-commerce and online transactions rise, so do the profound fraud techniques that threaten both financial institutions and consumers. Traditional approaches of fraud detection lack the flexibility necessary to detect new fraud patterns, resulting in higher rates of false positives and instreamed fraudulent transactions. Machine learning provides a flexible approach to fraud detection by leveraging real-time data to identify patterns, detect anomalies, and even self-update to accommodate new fraud schemes. The project is important because it addresses the critical need for an efficient, scalable fraud detection mechanism capable of keeping pace with the rapid development of fraud. By leveraging a number of machine learning techniques, this project is aimed at improving overall detection accuracy, reducing losses in loss revenue, and enhancing consumer confidence, thereby increasing payment security infrastructure resilience.

2. METHODOLOGY

A common approach to detecting credit card fraud with machine learning is as follows:

1. Collection of data- A dataset of transactions will be gathered, including information like transaction amount, location, date/time, and whether or not the transaction was fraudulent.
2. Preprocessing data:

- Use imputer techniques to address any missing or inconsistent data.
- Re-scale or normalize numerical features.
- Encode categorical variables.
- Address any class imbalance (fraudulent transactions are typically less frequent) using approaches like over-sampling (SMOTE) or under-sampling.

3. Feature Selection/Engineering:

- Identify the most informative features relative to fraud detection.
- Perform dimensionality reduction using methods such as PCA to improve performance.

4. Model Selection:

- Choose one or more ML algorithms such as Logistic Regression, Decision Trees, Random Forests, Gradient Boosting, or Neural Networks.
- Consider unsupervised models such as Auto encoders or Isolation Forests for anomaly detection.

5. Model Training:

- Train/test split of the dataset before model training.
- Train the model on the training data using labelled data if supervised learning is selected.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 04, April 2025, pp : 866-869
www.ijprems.com
editor@ijprems.com
e-ISSN : 2583-1062
Impact Factor : 7.001

6. Model Evaluation:
- Performance metrics to evaluate your model may include, but are not limited too, Precision, Recall, a F1-score, and area under the ROC (AUC).
- Verify the inherent balance of false positives and false negatives in the model.

7. Model Deployment:
- Once a model is properly trained, it is integrated into the transactional system.

3. USE CASE DIAGRAM

Fig.1 use case diagram

BLOCK DIAGRAM

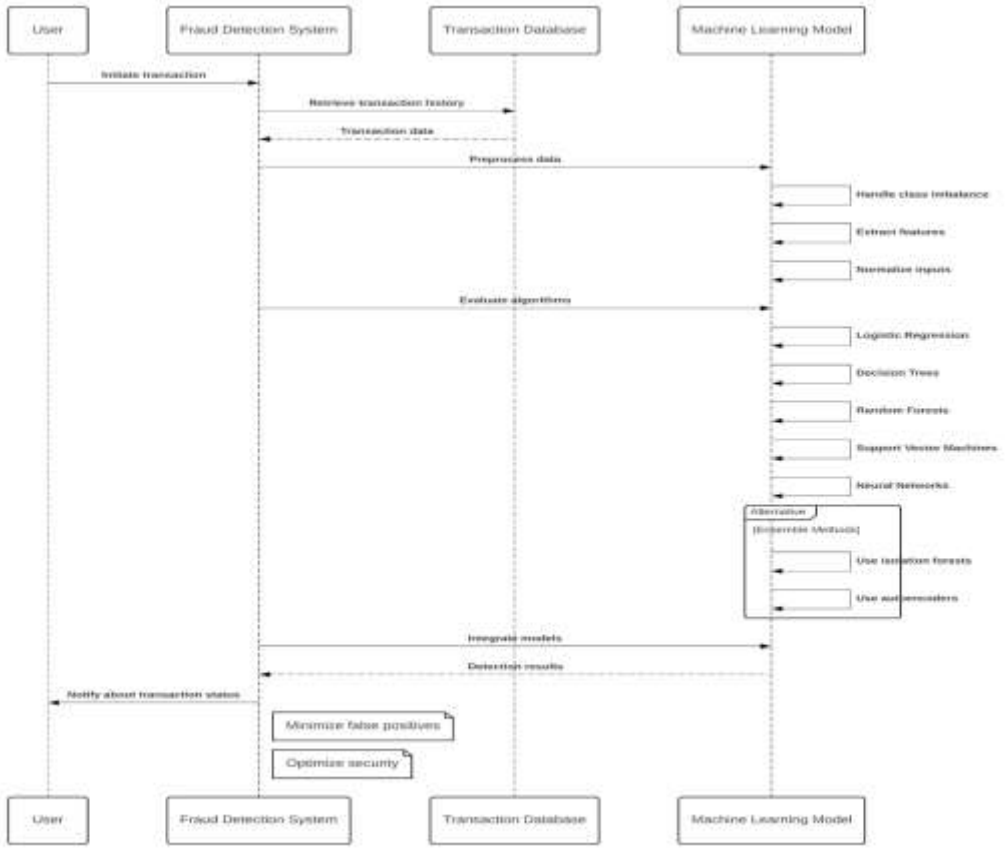

Fig.2 Block diagram

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 04, April 2025, pp : 866-869

e-ISSN : 2583-1062
Impact Factor : 7.001

FUTURE SCOPE

Technological improvements and novel methodologies will both shape the future of credit card fraud detection. Artificial intelligence and machine learning for immediate and precise anomaly identification.
Blockchain technology for a protected and irreproachable credit card transactions.
Behavioral biometrics for distinguishing users in accordance with their specific traits.
Predictive analytics for anticipating fraud through transaction trends.
Future information integration for optimizing accuracy with further transaction data.

LIMITATION

Credit card fraud detection systems encounter challenges such as false positives and false negatives, evolving fraud strategies, and data imbalance. Additionally, they face challenges such as privacy concerns, scalability, and interpreting complex models. All of these challenges highlight the need for continual improvements in technology.

4. RESULT DISCUSSION

When assessing results for credit card fraud detection systems, the focus is often on evaluating their accuracy and effectiveness. Here are some important things to consider:

1. Accuracy: How well the system is at catching fraudulent transactions while not catching legitimate ones.
2. Precision and Recall:-Precision: Two organizations agree on the precision, that is the ratio of correctly catching fraud out of all transactions flagged as fraud.-Recall: The ratio of correctly catching fraud out of total fraud incidents.
3. False Positives and False Negatives:-False positives are transactions that are flagged as fraudulent that are not actual fraud.-False negatives are transactions that are fraud but were not flagged as such.
4. Scalability: The ability of the system to scale with an increasing number of transactions, while maintaining performance.
5. Adaptive: The ability of the system to adapt to changes in fraud tactics.
6. Understand ability: The degree to which a user can understand why a transaction was flagged, especially in the severe instances where machine learning systems are used.

5. CONCLUSION

Systems that monitor and detect credit card fraud using machine learning approaches are an essential safeguard in a range of industries, including financial transaction processing, banking, e-commerce and digital payments. Sophisticated algorithms, real-time data processing, and evolving models are utilized to detect and identify non-conforming or suspicious accounts and transactions, thus mitigating financial losses and enhancing security.

The core principles and practices involved in this process include data pre-processing, feature engineering, model selection, and executing real-time simulations to create customized solutions that are robust and scalable in their application. The monitoring and testing of these systems is essential to endeavor effective performance against fraud patterns as they emerge and evolve. In addition to the mitigation of fraud, these systems reduce the cost associated with performance of manual detection, which benefits consumers to re-acquire lost trust. Sector-wide, machine learning based credit card fraud detection depersonalizes the risk which further allows regulatory standards to be met with quality financial standards that consumers can rely upon and expect from all institutions. Demand for continuing innovation in machine learning based credit card fraud detection will be accelerated through the increased growth and reliance on digital payment systems, which themselves are evolving and changing consumer payment behaviors. Machine learning based credit card fraud detection therefore will fundamentally underpin the future of availing safe well secure, reliable and efficient financial systems.

6. REFERENCES

[1] https://www.researchgate.net/publication/336800562_Credit_Card_Fraud_Detection_using_Machine_Learning_and_Data_Science
[2] https://www.sciencedirect.com/science/article/pii/S187705092030065X
[3] Ngai, E. W., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). "The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature." Decision Support Systems, 50(3), 559-569. doi:10.1016/j.dss.2010.08.006.
[4] Bhatla, T. P., Prabhu, V., & Dua, A. (2003). "Understanding credit card frauds." Monograph, Department of Electrical and Computer Engineering, Carnegie Mellon University.

[5] Yeh, I. C., & Lien, C. H. (2009). "The comparisons of data mining techniques for the predictive accuracy of probability of default of credit card clients." Expert Systems with Applications, 36(2), 2473-2480. doi:10.1016/j.eswa.2007.12.020.

[6] Carcillo, F., Dal Pozzolo, A., Le Borgne, Y. A., Caelen, O., Mazzer, Y., & Bontempi, G. (2018). "Scarff: a scalable framework for streaming credit card fraud detection with Spark." Information Fusion, 41, 182-194. doi:10.1016/j.inffus.2017.09.005.

[7] Chen, J., & Chen, Z. (2015). "Anomaly detection for credit card fraud with unsupervised learning." Proceedings of the International Conference on Computer Science and Applications.

[8] Kaggle. (n.d.). "Credit Card Fraud Detection Dataset." Available at: https://www.kaggle.com/datasets/mlg-ulb/creditcardfraud

[9] Vishwanathan, A., Bhattacharyya, S., Jha, S., & Westland, J. C. (2010). "Data mining techniques for credit card fraud detection." Computational Intelligence in Data Mining - Volume 1, 82-88.

[10] European Central Bank. (2020). "The Importance of Tackling Payment Fraud." Retrieved from https://www.ecb.europa.eu