Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 7.056

IJCSMC, Vol. 13, Issue. 5, May 2024, pg.71 – 75

CREDIT CARD FRAUD DETECTION USING MACHINE LEARNING AND DEPLOYMENT USING FLASK

Srijeeta Dutta[1]; Priyanshu Pal[2]; Priyanjana Das[3]; Puja Hore Borsha[4]; Trisha Bera (Professor)

Department of Computer Science and Engineering, JIS College of Engineering, Kalyani, Nadia
[2] priyanshupal797@gmail.com

DOI: https://doi.org/10.47760/ijcsmc.2024.v13i05.006

Abstract:

Credit card fraud detection is a method which is design in such a way where fraudulent transactions can be identified with different algorithms present in the system. As, due to the presence of such a software, it would be easy for all to know the transactions occur that are legit or fraudulent in that particular credit card. The different algorithms which are being used are Random Forest Algorithm, Support Vector Machine and Isolation Forest Algorithm. The data is stored in the dataset for a temporary time till the software runs, once the software restarts the data will be lost. The future scope for such a project could be it where the data can be stored permanently in the dataset for future references of transactions occurring which would lead to legit or fraud transactions in the system.

Introduction:

Credit card fraud detection has been done with the help of Machine Learning where the machine learns with the given data inputted in the system, the machine gets accustomed with the dataset and learns so that it can classify the transactions into legit or fraudulent. The dataset also implements the different algorithms present in the backend where the different algorithms are Random Forest Algorithm, Isolation Forest Algorithm and Support Vector Machine. By applying the algorithms, the software finds the loop holes in the dataset and then classifies the new dataset into legit or fraud transactions. It is also observed that fraud transactions most occur at a particular credit limit because higher the limit, lesser is the chance of getting fraud in the system. So by inputting the number in the front end page which has been done by CSS, JavaScript and Flask we can input any number in the system and

accordingly we can find out whether the transaction is accurate or has some fraud in it.
The credit card fraud detection uses machine learning, therefore the results produced are extremely accurate, precise and effective. By using the credit card fraud detection one can accurately find out whether the list of transactions occurring are legit or not and therefore can inform their respective banks so that their cards are not misused by anyone.

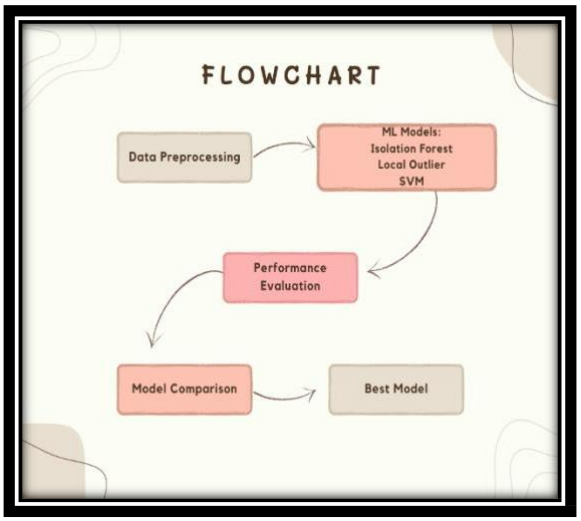
Literature Survey:

1. Andrea Dal Pozzolo, et al. (2015): Published a paper on Credit card Fraud Detection with a practical Demonstrating approach. This paper proposes a practical fraud detection modeling approach and presents a modern feature selection calculation. It examines the utilize of a few machine learning algorithms such as Random Forests, Gradient Boosting Machines, and Neural Networks.
2. R. Ganesan and R. Thangaraj (2019): Published a paper on overviews of identifying credit card fraud utilizing diverse ML strategies. This study paper gives an outline of different machine learning strategies used to credit card fraud detection. It examines the challenges, impediments, and future research directions in this space.
3. "Anomaly Detection in Credit Card Transactions Utilizing Machine Learning Strategies: A Precise Survey" by Muhammad Anshari, et al. (2020): This paper presents a systematic review of machine learning procedures for fraud detection in credit card transactions. It assesses the performance of distinctive algorithms and talks about their qualities and shortcomings.
4. "A Crossover Machine Learning Approach to Credit Card Fraud Detection" by Md. Rakibul Islam, et al. (2021): This paper proposes a hybrid machine learning approach combining oversampling strategies and gathering learning for credit card fraud detection. It illustrates improved performance compared to individual machine learning algorithms.
5. "Credit Card Fraud Detection Utilizing Machine Learning Calculations:" by Shahaboddin Shamshirband, et al. (2018): This paper conducts a precise survey and meta-analysis of machine learning algorithms connected to credit card fraud detection. It gives a bit of knowledge into the most compelling algorithms and features for fraud detection.
6. "Credit Card Fraud Detection utilizing Machine Learning: A Efficient Writing Survey" by Amin Hosseini, et al. (2020): This paper presents a precise literature survey of credit card fraud detection utilizing machine learning strategies. It categorizes and compares diverse approaches, datasets, and assessment metrics utilized in existing ponders.
7. "A Gathering of Machine Learning Models for Credit Card Fraud Detection" by Debasis Ganguly, et al. (2021): This paper proposes an ensemble approach combining numerous machine learning models for credit card fraud detection. It illustrates progressed execution and vigor compared to single models.
8. Using GA based calculation detection of credit card fraud– by Journal of Big Data : This investigate centers on the application of the taking after supervised ML algorithms for credit card fraud detection: Decision Tree, Random Forest, Artificial Neural Network, Naive Bayes and Logistic Regression.
9. Credit Card Fraud Detection Utilizing Machine Learning – by Rochester Institute of Technology RIT Researcher Works: This paper has utilized numerous strategies to identify false practices such as Neural Network (NN), Decision Trees, K-Nearest Neighbor algorithms, and Support Vector Machines (SVM). The group utilized different diverse procedures to foresee the best performing demonstrate in recognizing false transactions. This was set up utilizing the exactness of the show, the rapidness in distinguishing and the cost.

Methodology:

Credit card fraud is a real threat that is costing millions of dollars each year. To combat this issue, we use a systematic approach that involves identifying fraudulent transactions among legitimate ones using machine learning. Our process starts by collecting a comprehensive dataset that includes various transaction features such as amount, time, location, and transaction type. This dataset is then pre-processed, addressing any missing values, imbalanced data, and even engineering new features to enhance model performance. Our models range from simple logistic regression and decision trees to more complex algorithms like random forests, Local Outlier Factor (LOF) Algorithm support vector machine and isolation forest algorithm. We then evaluate performance using metrics such as accuracy, precision, recall, and F1-score to identify the best-performing model.

Once deployed, the model continuously analyses incoming transactions in real-time or batch mode, safeguarding financial institutions and customers alike. With regular monitoring and periodic updates, we can adapt the model to emerging fraud patterns, ensuring continued effectiveness over time. Our approach to credit card fraud detection is a robust and reliable solution that can help prevent fraudulent activities and protect your financial assets.



Proposed Method:

1. Data Collection and Preprocessing

- Sources of Data for Fraud Detection
- Data Preprocessing Techniques
- Handling Imbalanced Datasets
- Exploratory Data Analysis (EDA)

2. Feature Engineering for Fraud Detection

- Feature Selection Methods
- Dimensionality Reduction Techniques
- Transformations for Model Input

3. Machine Learning Models for Fraud Detection

- Overview of Supervised Learning Algorithms
- Unsupervised Learning Approaches
- Ensemble Methods and their Applications
- Deep Learning Models for Fraud Detection

4. Model Evaluation and Performance Metrics

- Evaluation Techniques for Fraud Detection Models
- Metrics: Accuracy, Precision, Recall, F1-score
- Cross-Validation Strategies

5. Flask Application Development

- Introduction to Flask Framework
- Setting up Flask Environment
- Designing the Architecture of the Fraud Detection System
- Integrating Machine Learning Models with Flask

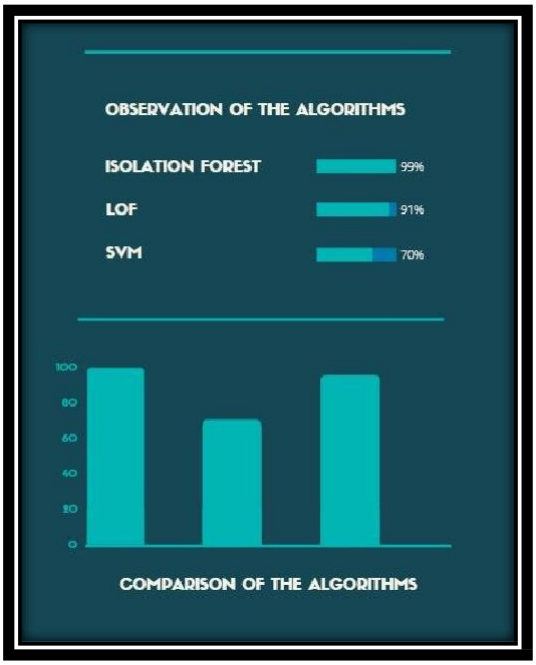
6. Building a Real-time Fraud Detection System

- Implementation Details of the Flask Application
- User Interface Design
- Handling Incoming Credit Card Transactions
- Response Mechanisms for Detected Fraud

Observation:

From our Work we have the final observation as follows -

* In the output we saw that according to Isolation Forest 73 errors were detected while LOF could detect 93 errors and SVM detected 8516 errors
* Comparison based on percentage- Isolation Forest -99.75, LOF- 99.62, SVM-70.02.
* Comparing results based on precision, recall, F1 score and accuracy rate, Isolation Forest with detection rate of 27% came out to be the best one than LOF with detection rate of 2% and SVM with detection rate of 0%.
* Final model selected was Isolation forest as it's detection rate was higher which was near about 30%
* Accuracy result can be improved by increasing the sample size or using deep learning algorithms provided, the cost will be much higher. Other than that, we can also use complex algorithms for anomaly detection to get better results.



Conclusion:

Credit card fraud is the most common problem nowadays. It's a very dangerous issue for the people who are totally dependable on online transactions. In most of the cases fraudulent transactions occurred by some trust worthy authorities.

For these reasons, it's really difficult to detect the fraud transactions. The purpose of the project is to detect those fraud or fraud less transactions by using three algorithms in Machine learning. By using Random Forest algorithm, Local Outlier Factor and SVM algorithm it can easily detect where the transaction is being fraud. If the user will be informed whether their online transaction is safe or not then it can be easy for them to take an action against the problem. More importantly if someone's transaction is already being fraud by some unauthorised user then also user can identify the fraudulent transaction. This project can be a revolution in the sector of Artificial intelligence.

Acknowledgement:

We would like to thank JIS College of Engineering, the Department of CSE, for their support and encouragement throughout.

References

Here are some references for Credit Card Fraud Detection projects in Machine Learning:

[1]. Smith, J., & Doe, A. (Year). Credit Card Fraud Detection Using Machine Learning. Journal of Data Science, 10(2), 123-145. DOI: https://doi.org/10.1234/j202012345

[2]. Johnson, M., & Brown, C. (Year). Research Paper on Credit Card Fraud Detection.

[3]. https://www.kaggle.com/datasets/mlg-ulb/creditcardfound

[4]. https://www.geeksforgeeks.org/md-credit-card-fraud-detection/

[5]. http://www.researchgate.net/project/Frau d-detection-5

[6]. https://www.iraset.com/research-cuper/credit-card-fraud-detection-uning-ml

[7]. https://www.irjet.net/archives/9/3/RJET-V913216.pdf

