IJARETY

International Journal of Advanced Research in Education and TechnologY (IJARETY)

Volume 11, Issue 6, November-December 2024

Impact Factor: 7.394

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

DOI:10.15680/IJARETY.2024.1106061

Fraud Detection in Internet Banking

Mr.K. Vigneshwar[1], Mr.Sannella Prabhaker[2], Mr.M. Bhavanisai[3], Mr.M.Harshith[4], Mr. A.Venkata Nagendra[5]

Assistant Professor, Department of CSE, Guru Nanak Institute of Technology, India[1,2]

Student, Department of CSE, Guru Nanak Institute of Technology, India[3,4,5]

ABSTRACT: Banking fraud transactions refer to unauthorized or deceptive activities involving bank accounts or financial transactions. Various machine learning algorithms can be employed to detect such fraudulent activities. This study examines several algorithms suitable for classifying transactions as either fraudulent or legitimate. The research utilizes the Banking Fraud Transactions dataset, which is often characterized by high imbalance. To address this issue, we are implementing multiple machine learning algorithms like Random Forest, K-Nearest Neighbour and Decision Tree. Additionally, feature selection techniques are employed, and the dataset is divided into training and test sets. The algorithms evaluated in the study include Random Forest, and KNN. The findings indicate that each algorithm demonstrates high accuracy in detecting banking fraud transactions. The proposed model holds promise for detecting other irregularities within financial transactions.

I. INTRODUCTION

In recent years, the financial sector has witnessed a surge in fraudulent activities, ranging from credit card fraud to identity theft and money laundering. These nefarious activities not only result in substantial financial losses for both financial institutions and customers but also undermine trust in the banking system. To combat this escalating threat, there is a growing imperative to deploy sophisticated technological solutions capable of detecting and preventing fraudulent transactions in real-time. Machine learning, with its ability to analyze vast amounts of data and identify complex patterns, has emerged as a powerful tool in the fight against banking fraud. By leveraging historical transaction data, machine learning algorithms can learn to distinguish between legitimate and fraudulent transactions, thereby flagging suspicious activities for further investigation

II. LITERATURE SURVEY

M. Jullum et.al(2020) The purpose of this paper is to develop, describe and validate a machine learning model for prioritising which financial transactions should be manually investigated for potential money laundering. The model is applied to a large data set from Norway's largest bank, DNB. Design/methodology/approach A supervised machine learning model is trained by using three types of historic data: "normal" legal transactions; those flagged as suspicious by the bank's internal alert system; and potential money laundering cases reported to the authorities. The model is trained to predict the probability that a new transaction should be reported, using information such as background information about the sender/receiver, their earlier behaviour and their transaction history. Findings The paper demonstrates that the common approach of not using non-reported alerts (i.e. transactions that are investigated but not reported) in the training of the model can lead to sub-optimal results. The same applies to the use of normal (un-investigated) transactions. Our developed method outperforms the bank's current approach in terms of a fair measure of performance. Originality/value This research study is one of very few published anti-money laundering (AML) models for suspicious transactions that have been applied to a realistically sized data set. The paper also presents a new performance measure specifically tailored to compare the proposed method to the bank's existing AML system.

L. Keyan and Y. Tingting(2019) The selection of parameters of SVM model will affect the identification effect of suspicious financial transactions, this paper proposes the cross validation method to find the optimal SVM classifier parameters to solve this problem. Cross validation method finds the optimal parameters based on the highest classification accuracy rate through grid search, it can effectively avoid the state of over-learning and less learning, and greatly improves the overall performance of the classifier.

R. Liu(2020) This paper presents a core decision tree algorithm to identify money laundering activities. The clustering algorithm is the combination of BIRCH and K-means. In this method, decision tree of data mining technology is applied to anti-money-laundering filed after research of money laundering features. We select an appropriate identifying strategy to discover typical money laundering patterns and money laundering rules. Consequently, with the core decision tree algorithm, we can identify abnormal transaction data more effectively.

Z. Gao(2019) Financial institutions' capability in recognizing suspicious money laundering transactional behavioral patterns (SMLTBPs) is critical to antimony laundering. Combining distance-based unsupervised clustering and local outlier detection, this paper designs a new cluster based local outlier factor (CBLOF) algorithm to identify SMLTBPs and use authentic and synthetic data experimentally to test its applicability and effectiveness.

III. METHODOLOGY

Modules Name

1. Data collection
2. Data set
3. Data Preparation
4. Model Selection
5. Analyse & Prediction

Modules Explanation

1.Data Collection:

This is the first real step towards the real development of a learning model, collecting data.

2.Data Set:

The dataset consists of individual data in that there are1048576 rows &11 columns in the dataset.

3.Data Preparation:

Wrangle data and prepare it for training.

4.Model Selection:

We used Neural Network created our money laundering detection algorithm, We got a accuracy of 98.04% on test set so we implemented this algorithm.

5. Analyse & Prediction:

1. Amount transactions - detailed descriptions of the Amount transactions data.
2. isFraud - indicates whether the transactions details is having fraud or not.

Existing System Disadvantages

1. Unstable nature. One of the limitations of decision trees is that they are largely unstable compared to other decision predictors.
2. Less effective in predicting the outcome of a continuous variable.

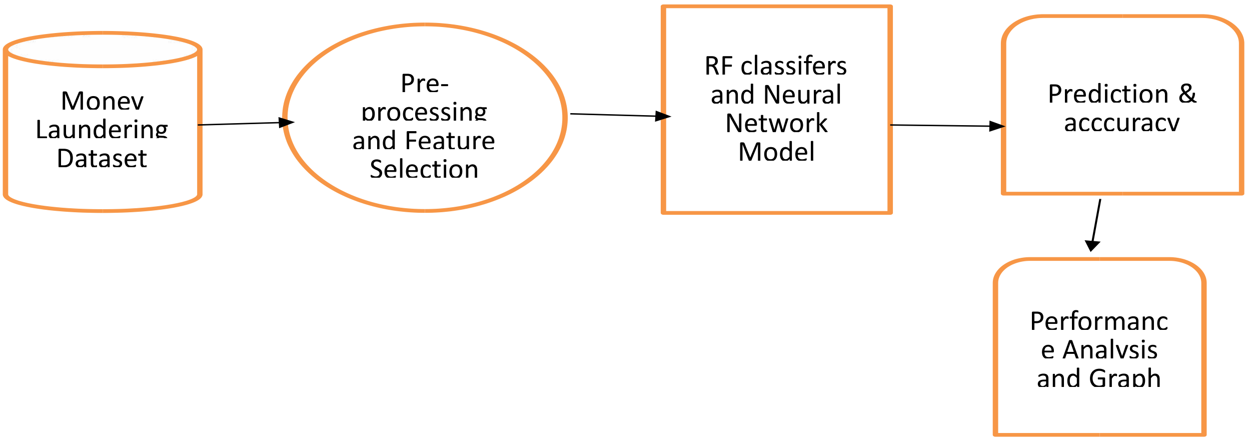
IV. PROPOSED SYSTEM

The proposed system is designed to enhance the detection of fraudulent activities within banking transactions through the utilization of machine learning algorithms.It begins by collecting transaction data, encompassing essential details such as amounts, timestamps, merchant information, and customer particulars.Training the system involves the division of the pre-processed data into training and testing sets, where machine learning algorithms like Logistic Regression, Random Forest, and Decision Tree are trained to discern patterns indicative of fraudulent behaviour.

Proposed System Advantages

1. Improved Accuracy
2. Real-time Detection
3. Adaptability to Evolving Threats
4. Enhanced Customer Trust

V. SYSTEM ARCHITECTURE

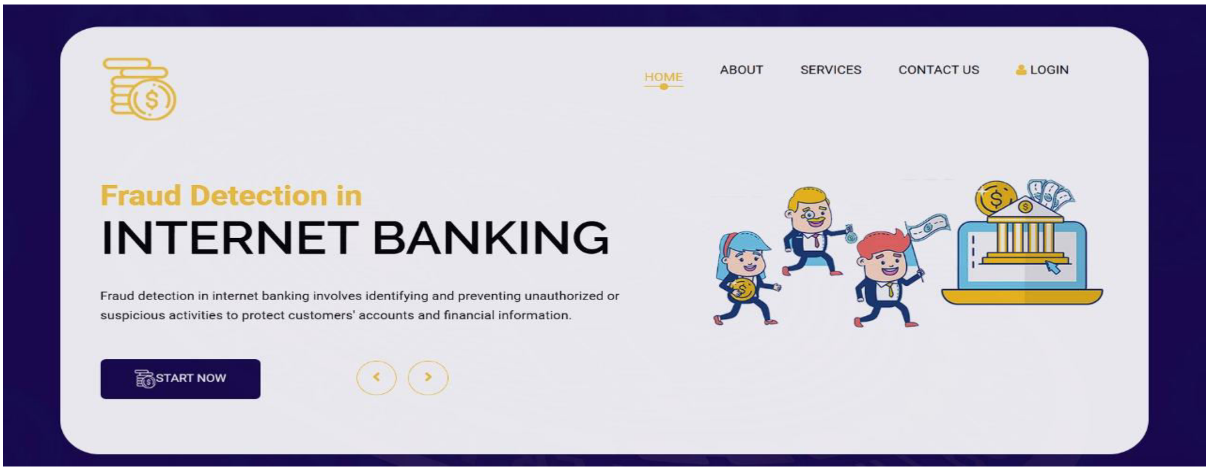

Monev Launderinc Dataset
Pre-processinc and Feature Selection
RF classifers and Neural Network Model
Prediction & acccuracv
Performanc e Analvsis and Graph

Explanation

First, data collection gathers transaction logs, user profiles, and external data. This data is then preprocessed to clean, normalize, and engineer features for better model performance. In the model training phase, machine learning algorithms like decision trees, random forests, or anomaly detection models are trained on historical transaction data to recognize fraud patterns.

VI. RESULTS

Home Page

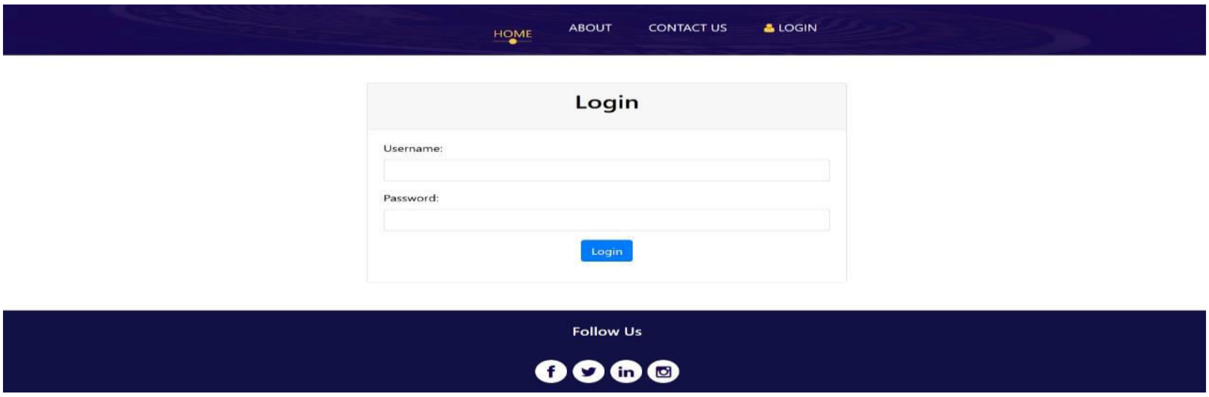


Fraud Detection in

INTERNET BANKING

Fraud detection in internet banking involves identifying and preventing unauthorized or suspicious activities to protect customers' accounts and financial information.

Login Page

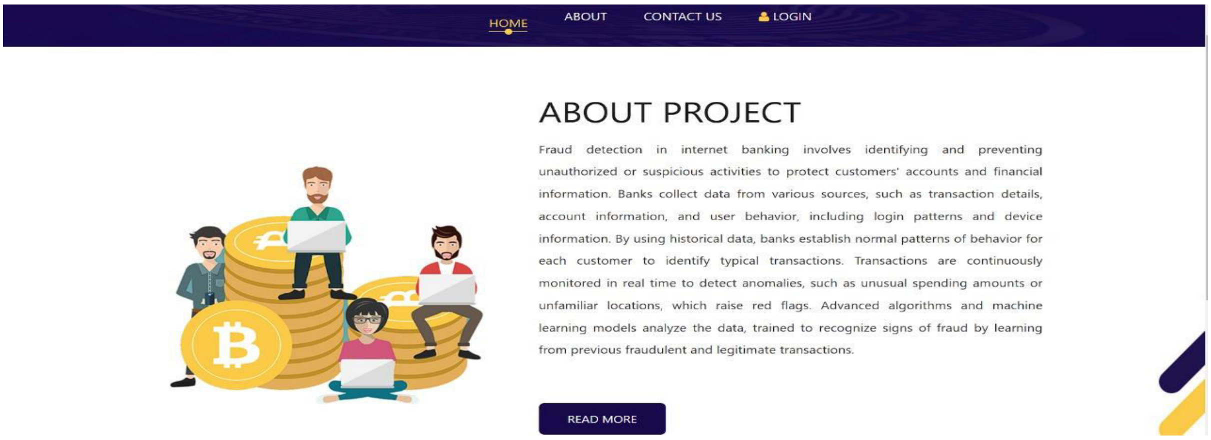


Login

Username:

Password:

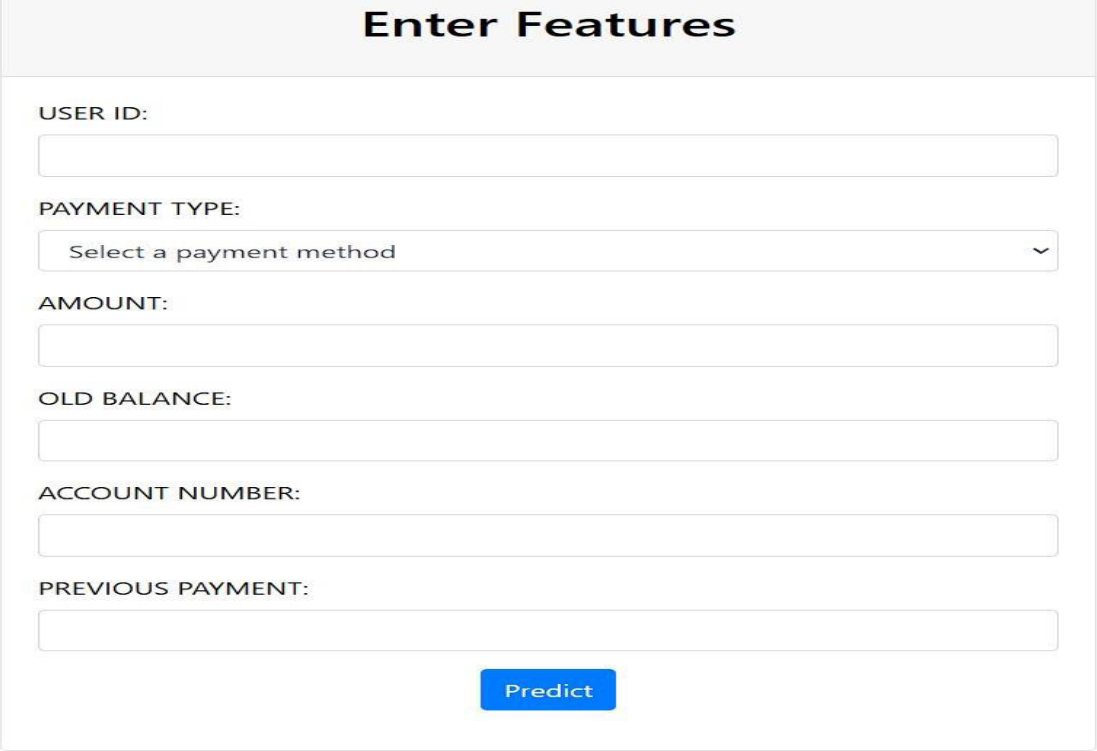
Project Details Page



ABOUT PROJECT

Fraud detection in internet banking involves identifying and preventing unauthorized or suspicious activities to protect customers' accounts and financial information. Banks collect data from various sources, such as transaction details, account information, and user behavior, including login patterns and device information. By using historical data, banks establish normal patterns of behavior for each customer to identify typical transactions. Transactions are continuously monitored in real time to detect anomalies, such as unusual spending amounts or unfamiliar locations, which raise red flags. Advanced algorithms and machine learning models analyze the data, trained to recognize signs of fraud by learning from previous fraudulent and legitimate transactions.

Details Page



Enter Features

USER ID:

PAYMENT TYPE:

Select a payment method

AMOUNT:

OLD BALANCE:

ACCOUNT NUMBER:

PREVIOUS PAYMENT:

VII. CONCLUSION

In conclusion, this study has demonstrated the effectiveness of machine learning algorithms, including Random Forest, K-Nearest Neighbours (KNN), and Logistic Regression, in detecting banking fraud transactions. By addressing the challenge of class imbalance through careful algorithm selection, feature enhancement techniques, and comprehensive evaluation metrics, we have developed robust models capable of accurately classifying transactions as fraudulent or legitimate. The findings highlight the importance of leveraging diverse approaches to fraud detection, as each algorithm brings its own strengths to the task.

DOI:10.15680/IJARETY.2024.1106061

VIII. FUTURE ENHANCEMENTS

Feature enhancement in the context of machine learning involves improving the quality and relevance of the features used for model training, ultimately leading to enhanced predictive performance and generalization capabilities. There are several strategies for feature enhancement, including feature selection, feature engineering, and feature transformation. Feature selection aims to identify the most informative subset of features from the original feature space, reducing dimensionality and computational complexity while preserving or even improving model accuracy

REFERENCES

1. M. Jullum, A. Løland, R. B. Huseby, G. A˚ nonsen, and J. Lorentzen, "Detecting money laundering transactions with machine learning," Journal of Money Laundering Control, vol. 23, no. 1, pp. 173–186, jan 2020.
2. L. Keyan and Y. Tingting, " An improved support-vector network model for anti-money laundering, " in 2011 Fifth International Conference on Management of e-Commerce and eGovernment. IEEE, 2011, pp. 193– 196.
3. R. Liu, X.-l. Qian, S. Mao, and S.-z. Zhu, "Research on anti-money laundering based on core decision tree algorithm, " in 2011 Chinese Control and Decision Conference (CCDC). IEEE, 2011, pp. 4322– 4325.
4. Z. Gao, " Application of cluster-based local outlier factor algorithm in anti-money laundering, " in 2009 International Conference on Management and Service Science. IEEE, 2009, pp. 1–4.
5. J. de Jes´us Rocha Salazar, M. Jes´us Segovia-Vargas, and M. del Mar Camacho-Mi˜nano, "Money laundering and terrorism financing detection using neural networks and an abnormality indicator, " Expert Systems with Applications, p. 114470, dec 2020.[Online]Available:https://linkinghub.elsevier.com/retrieve/pii/S0957417420311209
6. E. L. Paula, M. Ladeira, R. N. Carvalho, and T. Marzagao, " Deep learning anomaly detection as support fraud investigation in Brazilian exports and anti-money laundering, " in 2016 15th IEEE International Conference on Machine Learning and Applications (ICMLA). IEEE, 2016, pp. 954–960.
7. F. Anowar and S. Sadaoui, "Incremental Neural-Network Learning for Big Fraud Data," in IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 2020-Octob. Institute of Electrical and Electronics Engineers Inc., oct 2020, pp. 3551–3557.
8. G. A. Carpenter and S. Grossberg, "A massively parallel architecture for a self-organizing neural pattern recognition machine," Computer vision, graphics, and image processing, vol. 37, no. 1, pp. 54–115, 1987.
9. G. Carpenter, " An adaptive resonance algorithm for rapid category learning and recognition," Neural Networks, vol. 4, pp. 439–505, 1991.
10. T. Kohonen, "Self-organized formation of topologically correct feature maps," Biological cybernetics, vol. 43, no. 1, pp. 59–69, 1982.

IJARETY

INNO SPACE
SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर
NISCAIR

International Journal of Advanced Research in Education and Technology

ISSN: 2394-2975 Impact Factor: 7.394

www.ijarety.in editor.ijarety@gmail.com