Risk Management in the Financial Sector: An Artificial Intelligence-Based System for Fraud Detection

Avadhoot Ukirde[1], Pratham Gaikwad[2], Sarthak Shinde and Amruta Hingmire

{avdhootukirde499@gmail.com, prathamgaikwad2011@gmail.com, shindesarthak026@gmail.com, ahhingmire_comp@jspmrscoe.edu.in}

Department of Computer Engineering, JSPM's Rajarshi Shahu college of Engineering, Pune, India.

Abstract. Banking fraud is a serious and ongoing problem that involves attempting to deceive financial institutions in order to gain money or other benefits. Every year, banks lose millions of dollars due to various types of fraud, such as fake documents and other forms of deception. Online transaction fraud and fraudulent bank loan applications are among the most common types of fraud. To address this issue, a study has been conducted to investigate a system that utilizes machine learning techniques to identify suspicious activities and detect irregularities in online transactions. By analyzing large amounts of data, this system can quickly and accurately identify potential fraud, helping banks to minimize financial losses and protect their customers' assets. In addition to detecting fraud, this technology also improves risk management for banks and their customers.

Keywords: Banking fraud, fraud-related activities, online transaction fraud, fraudulent loan applications, machine learning techniques, fraud detection, fraud prevention, pattern recognition, risk management etc.

1 Introduction

Bank or money, concentrated places are the main targets for people that want to commit fraud. To minimize the risk, The Risk management system plays an important role to avoid any fraudulent activity. Nevertheless, fraudster people continue their invasion by defeating every

[1] Corresponding author. Email: avdhootukirde499@gmail.com

ICISML 2024, January 05-06, Pune, India

DOI 10.4108/eai.5-1-2024.2341831

existing and currently developed anti-fraud techniques. They recognize fraud systems and other similar scams by the industry. In the past 15-20 years various types of frauds have been done by giving wrong personal information to cheat the system which is illegal [2]. Until now there were very few techniques which prevented banking frauds. By the development of fraud detection algorithms

Many businesses today use graphical databases to solve a variety of data problems, including fraud detection. Additionally, the objective was to demonstrate how it would affect the prompt and accurate detection of any suspicious transactions. [1]. These shady transactions were viewed as banking system outliners. In this research, We have created a web-based program for fraud detection. The program serves as a focal point via which users and banks may quickly identify risk areas. Banking/financial sectors are developing fraud detection algorithms to save consumers from suspicious transactions in response to the scenario. This paper searches for various types of frauds, the limitation of existing detecting systems and the merits with the help of artificial intelligence and machine learning [4]. These challenging heterogeneous graph data cannot be handled well by conventional machine learning algorithms. The current strategy is to model the data as a heterogeneous information network for the identification of common traits and organizational structures among fraudsters. [9]

In our work the task of detecting credit card fraud is first described. It investigates the performance implications of training class distributions. then go over our multi-classifier meta-learning method and empirical findings. In real-world data mining applications, databases with skewed class distributions and non-uniform cost per error are typical. To solve these three problems, we developed a multi-classifier meta-learning strategy. Our empirical findings from a task involving the identification of credit card fraud show that the method can dramatically reduce loss brought on by fraudulent transactions.

Many different types of credit card fraud occur frequently. Before machine learning or deep learning gained popularity, it was challenging for businesses and banks to implement an efficient fraud detection system. [11]. Fraudsters are highly skilled and active individuals. This paper will identify application fraud, which occurs when a person provide false information about themselves to obtain a credit card, as part of the traditional strategy. To evaluate which algorithm works best and can be modified by credit card merchants for recognizing fraud transactions, logistic regression, decision trees, and random forests [14]. Customers may post reviews of their goods or services using online product review platforms.

However, fake reviews posted by dishonest persons frequently deceive buyers & cost businesses money.

This paper provides a comprehensive overview of intelligent financial fraud practices. It describes various types of fraud risk caused by the covid-19 pandemic and review to develop of data types used in detection practices from quantitative data [6], detection of frauds is essential for every business. And, fraud detection is possible for commercial industry and bank with the advanced technology. With the availability of increasing processing power, advancement in statistical modelling, capacity to capture and store voluminous data organizations are adopting technology to detect various fraud. Online Deception, Types of Deceptions, Techniques to Find Deception also useful to detect suspicious activities [5]

.

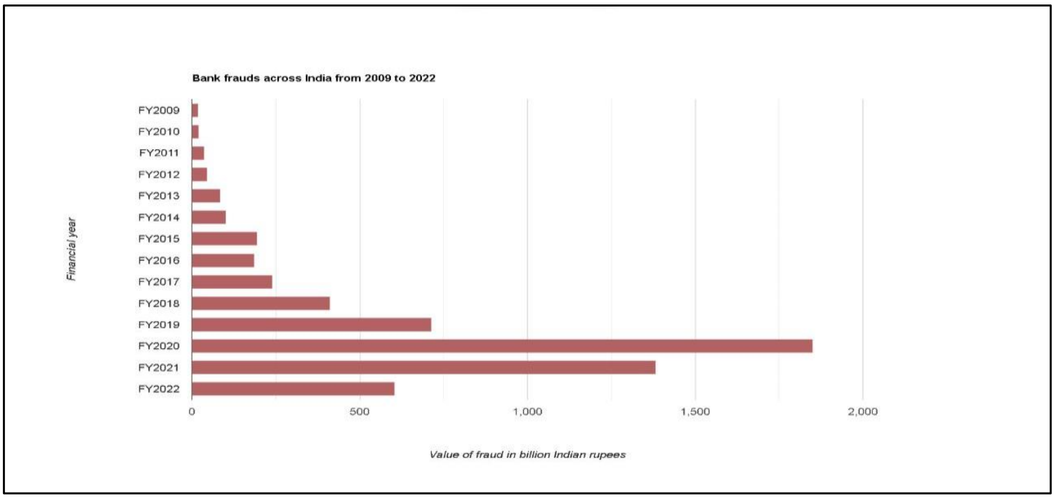


Figure 1. Bank Fraud across India (2009-2022)

According to statistics, the RBI detected bank frauds of 604 billion Indian rupees in 2022. As a result, the value of bank frauds reversed the trend that had been steadily expanding in India during the previous 10 years, both in terms of the total number of frauds and their value. Figure 1 shows that the cost of bank fraud in FY 2009 was around 20 billion Indian rupees. As more payments are made online, there has been an increase in fraud involving the banking industry. Due to COVID-19, the most of the transactions in FY2020 were completed online, which greatly increased bank fraud and resulted in losses of around 1800 billion Indian rupees. Thus, it must be under control.[22]

2. Literature Review

Financial Risk Management can be performed on various levels. Based on the source of risk factors, it is conventional to classify risk into four high-level categories:

A. Market risk,

B. Volatility measurement and forecasting:

C. Credits Risks:

D. Operational risk

A. Managing Market Risk:

Volatility, which is defined as the standard deviation of the log return of an asset, is one of the important metrics for managing market risk. An options financial derivative that is used as insurance or leverage to reduce potential loss recursively manages this risk. A portfolio of options is used in the common risk management technique known as hedging to lessen exposure to risk. Businesses may also adopt dynamic asset allocation systems in order to reduce these market risks and increase business return at the same time.

B. Volatility measurement and forecasting:

Higher volatility denotes higher market risk. Volatility is a statistical measure used to describe the dispersion of return of a financial asset or portfolio generally. It is the most crucial element in figuring out option prices. Volatility is essentially a measurement of unpredictability entering the contact centre. Understanding future volatility helps prevent losses for both professionals and individuals.

C. *Credits Risks:*

Credit risk is the likelihood that a borrower will suffer a loss. He is unable to make loan payments or fulfil contractual commitments. It specifically refers to the possibility that a bank may not receive the principal and interest owed, which could result in a disruption of cash flows and higher collection costs. Credit scoring, default detection, and bankruptcy detection are all parts of credit risk. Credit risks can be reduced through classification and clustering.

D. Operational Risks: Operational risk consists of three types of risks that are

1. *People Risk:* This People risks consist of any fraudulent activity by user, or customer of bank or by mistakenly any wrong information. People risk can be avoidable.

2. Process Risk is the risk occurred when there is any fault in the system.

3. Legal compliance risk Operational Risks consist of fraud detection having anomaly detection, Binary classification, and text mining.
4. We have conducted study on a variety of survey paper types for our work. The effort has been split into two phases: the first is the detection of credit card fraud, and the second is the detection of fraud in loan applications. Different machine learning algorithms, such as decision trees, random forests, and logistic regression, are used to detect credit card fraud. We use optical character recognition (OCR) to enter data for loan application fraud detection, and we can identify erroneous data using a machine learning method.

Table 1 shows the standard datasets for credit risk assessment that are commonly used in machine learning research. Table 2 represents Comparison of Accuracy Results from a Survey of Machine Learning Techniques for Credit Card Fraud Detection and/ Loan Defaults.

Table 1: Standard Datasets used for assessment of Credit Risk using machine Learning

Dataset Name	**Number of Samples**	**Target Attribute**
[15] German Credit	1,000	Credit Risk (Good/Bad)
[16] Australian Credit	690	Credit Risk (Approved/Not Approved)
[17] Lending Club Loan	1,480,000	Loan Default (Default/Non-Default)
[18] Home Equity Line of Credit	5,960	Loan Default (Default/Non-Default)
[19] Default of Credit Card Clients	30,000	Credit Default (Default/Non-Default)
[20] FICO HMEQ	5,960	Loan Default (Default/Non-Default)
[21] Credit Approval	690	Credit Risk (Approved/Not Approved)

3. Proposed Methodology for Risk Management System in Financial System

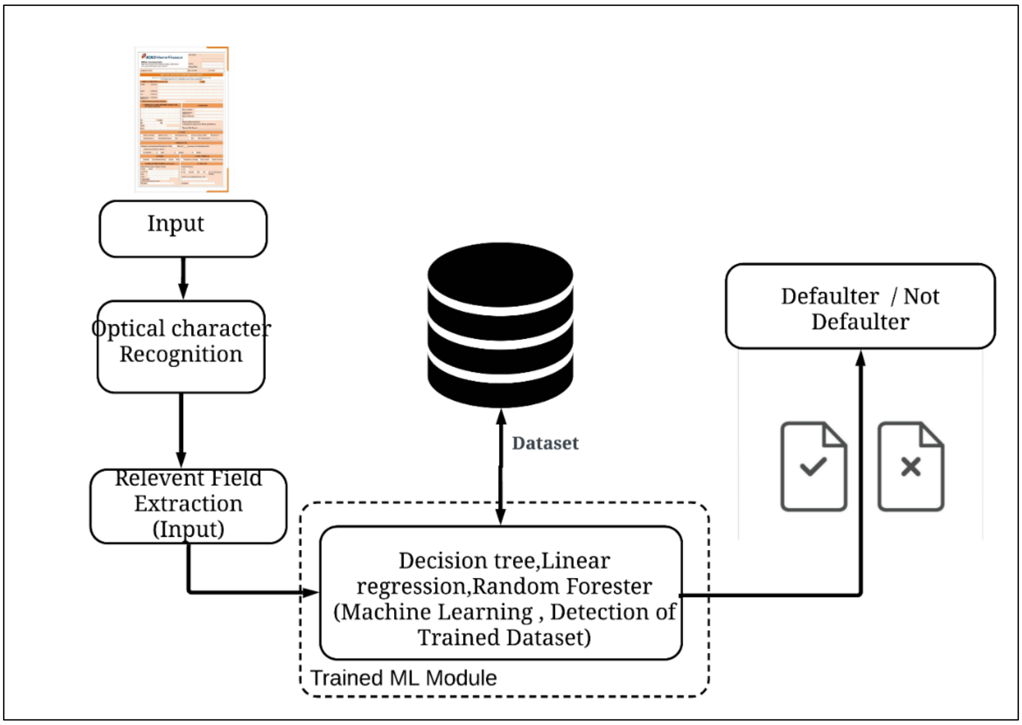
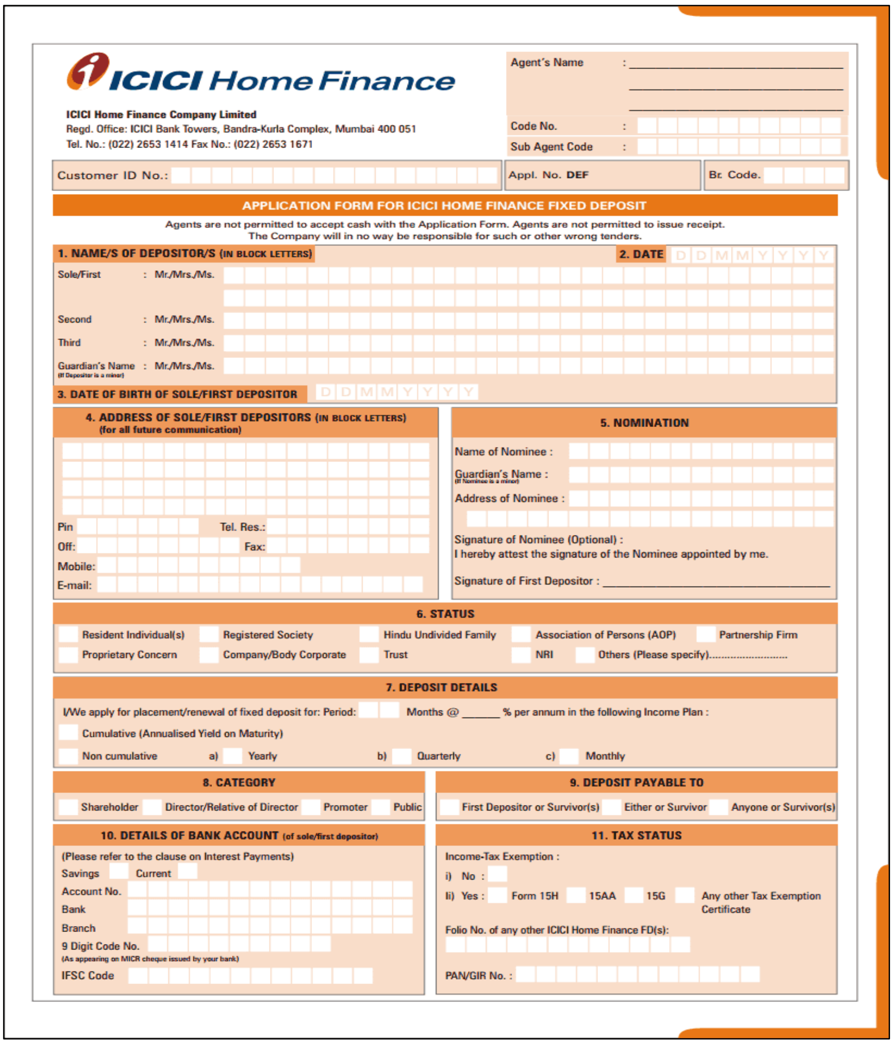

Input
Optical character Recognition
Relevent Field Extraction (Input)
Dataset
Decision tree,Linear regression,Random Forester (Machine Learning , Detection of Trained Dataset)
Trained ML Module
Defaulter / Not Defaulter

Fig 2. Architecture of Risk Management system for classification of Fraudulent and Non-Fraudulent activity.

The figure 2 shows the proposed mechanism for fraud detection. The input module and the detection module are the two main modules that make up the proposed system's architecture. The input data when entered by the legitimate authority will be done in the input module using the various (optical character recognition) OCR tools. There after the input from the OCR tool will be passed on to the natural processing engine for extracting the appropriate data from the raw input coming from the OCR. These relevant data is then stored in the database for reusing in any further operations. Next when the employee wants to check if the applicant is eligible for granting loan the data is then retrieved and then passed to the multiple machine learning models (Decision tree, Random Forest) in which the applicant is classified as eligible or non-eligible on the basis of their credit score, period of employment, annual income etc.



ICICI Home Finance

ICICI Home Finance Company Limited
Regd. Office: ICICI Bank Towers, Bandra-Kurla Complex, Mumbai 400 051
Tel. No.: (022) 2653 1414 Fax No.: (022) 2653 1671

Agent's Name : ____________________

Code No. : □□□□□□□□□□

Sub Agent Code : □□□□□□□□□□

Customer ID No.: □□□□□□□□□□□□□□□□ Appl. No. **DEF** Br. Code. □□□□

APPLICATION FORM FOR ICICI HOME FINANCE FIXED DEPOSIT

Agents are not permitted to accept cash with the Application Form. Agents are not permitted to issue receipt.
The Company will in no way be responsible for such or other wrong tenders.

1. NAME/S OF DEPOSITOR/S (IN BLOCK LETTERS) **2. DATE** D D M M Y Y Y Y

Sole/First : Mr./Mrs./Ms.

Second : Mr./Mrs./Ms.

Third : Mr./Mrs./Ms.

Guardian's Name : Mr./Mrs./Ms.
(If Depositor is a minor)

3. DATE OF BIRTH OF SOLE/FIRST DEPOSITOR D D M M Y Y Y Y

4. ADDRESS OF SOLE/FIRST DEPOSITORS (IN BLOCK LETTERS)
(for all future communication)

Pin Tel. Res.:
Off: Fax:
Mobile:
E-mail:

5. NOMINATION

Name of Nominee :
Guardian's Name :
(If Nominee is a minor)
Address of Nominee :

Signature of Nominee (Optional) :
I hereby attest the signature of the Nominee appointed by me.

Signature of First Depositor : ____________________

6. STATUS

□ Resident Individual(s) □ Registered Society □ Hindu Undivided Family □ Association of Persons (AOP) □ Partnership Firm
□ Proprietary Concern □ Company/Body Corporate □ Trust □ NRI □ Others (Please specify)..........................

7. DEPOSIT DETAILS

I/We apply for placement/renewal of fixed deposit for: Period: □□ Months @ ______ % per annum in the following Income Plan :
□ Cumulative (Annualised Yield on Maturity)
□ Non cumulative a) □ Yearly b) □ Quarterly c) □ Monthly

8. CATEGORY

□ Shareholder □ Director/Relative of Director □ Promoter □ Public

9. DEPOSIT PAYABLE TO

□ First Depositor or Survivor(s) □ Either or Survivor □ Anyone or Survivor(s)

10. DETAILS OF BANK ACCOUNT (of sole/first depositor)

(Please refer to the clause on Interest Payments)
Savings □ Current □
Account No.
Bank
Branch
9 Digit Code No.
(As appearing on MICR cheque issued by your bank)
IFSC Code

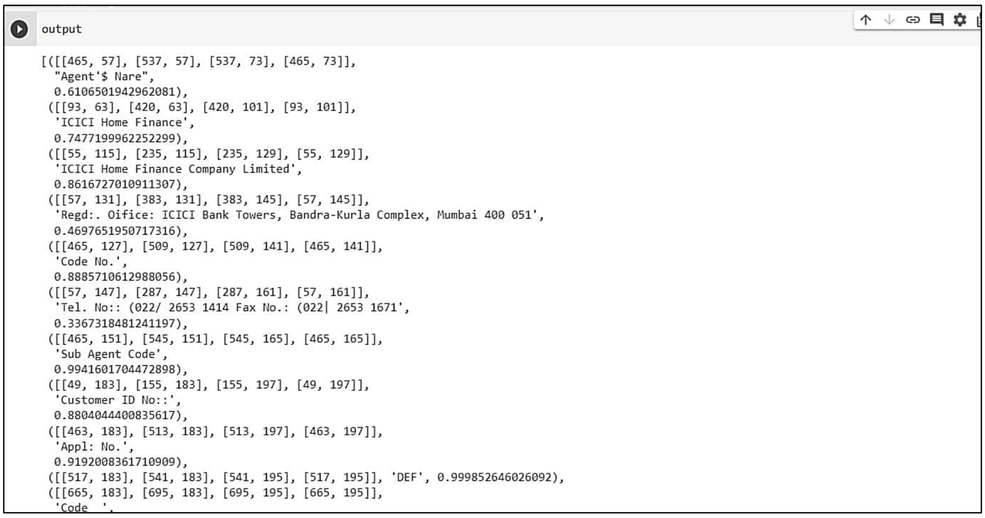
11. TAX STATUS

Income-Tax Exemption :
i) No : □
Ii) Yes : □ Form 15H □ 15AA □ 15G □ Any other Tax Exemption Certificate

Folio No. of any other ICICI Home Finance FD(s):

PAN/GIR No. :

Fig 3. A sample input image of Loan Application



output

```
[([[465, 57], [537, 57], [537, 73], [465, 73]],
  "Agent'$ Nare",
  0.6106501942962081),
 ([[93, 63], [420, 63], [420, 101], [93, 101]],
  'ICICI Home Finance',
  0.7477199962252299),
 ([[55, 115], [235, 115], [235, 129], [55, 129]],
  'ICICI Home Finance Company Limited',
  0.8616727010911307),
 ([[57, 131], [383, 131], [383, 145], [57, 145]],
  'Regd:. Oifice: ICICI Bank Towers, Bandra-Kurla Complex, Mumbai 400 051',
  0.4697651950717316),
 ([[465, 127], [509, 127], [509, 141], [465, 141]],
  'Code No.',
  0.8885710612988056),
 ([[57, 147], [287, 147], [287, 161], [57, 161]],
  'Tel. No:: (022/ 2653 1414 Fax No.: (022| 2653 1671',
  0.3367318481241197),
 ([[465, 151], [545, 151], [545, 165], [465, 165]],
  'Sub Agent Code',
  0.9941601704472898),
 ([[49, 183], [155, 183], [155, 197], [49, 197]],
  'Customer ID No::',
  0.8804044400835617),
 ([[463, 183], [513, 183], [513, 197], [463, 197]],
  'Appl: No.',
  0.9192008361710909),
 ([[517, 183], [541, 183], [541, 195], [517, 195]], 'DEF', 0.999852646026092),
 ([[665, 183], [695, 183], [695, 195], [665, 195]],
  'Code  ',
```

Fig 4. OCR generated output for various input fields of input application.

After detection, the information is transmitted to the appropriate authorities for human review. If the information is accepted, it is then forwarded for additional processing, in case the information is needed for documentation. The data is subsequently sent for revaluation, where the machine learning model is further enhanced to boost its accuracy, and the data is reprocessed, if the processed information meets the authority's requirements. OCR, or optical character recognition, is a method that converts a text image into a sample of text that can be read by computers. For instance, if you scan X image, your computer will save the image file. A text editor cannot be used to edit, count, or search the words in the file. The physical form of a document is processed by a scanner in optical character recognition.

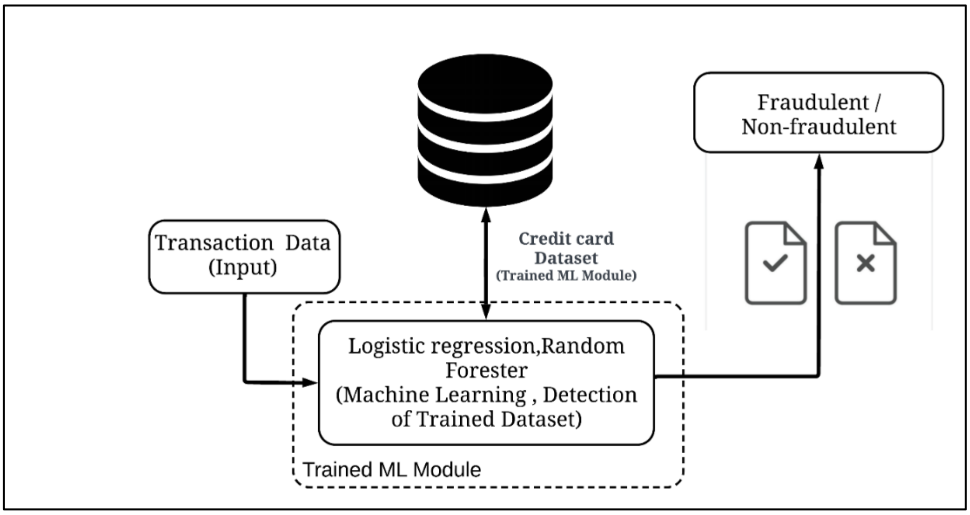


Figure. 5 Architecture of Risk Management system for classification of Fraudulent and Non- credit card fraudulent activity.

Following are some machine learning algorithms that can be used to find risk in datasets. For this we are using combined new dataset having nearly 1.2M. Entries in it the attributes are credit card no, Marchant, Category, amount, first name, middle name, Last name, gender, street, city, city Pop, Job, DoB, trans_nums, State unix_time, merch_lat, zip, Lat, long, merch long, is fraud. With the help of we can predict Credit card fraud. In case of checking if the performed transaction is fraudulent or not our system uses decision tree and A.R.I.M.A to classify the transaction into fraudulent or non-fraudulent activity. The machine learning model also keeps in mind the previous spending habits of the individual and according manipulates the classification outcome

Logistic Regression for Credit Risk Assessment:

The first stage is to collect information on previous loans and borrower characteristics in order to create a logistic regression model for credit risk assessment. The borrower's income, employment situation, credit history, debt-to-income ratio, and other pertinent details should all be included in this data. The data is cleansed and preprocessed after it has been collected to get rid of any incorrect or superfluous values. A training set and a testing set are generated from the data. The logistic regression model is trained using the training set, and its performance is assessed using the testing set.

The logistic regression model gains the capacity to forecast the likelihood of default based on characteristics of the borrower during training phase. This is accomplished by utilizing a method known as maximum likelihood estimation to fit the model to the training set of data. Finding the coefficients for each variable that increase the likelihood of the observed data is the objective.

Experimentation with Logistic Regression:

The model can forecast the likelihood of default for new borrowers once it has been trained. The borrower's attributes are input into the model, which then generates a probability score between 0 and 1, where 0 indicates a low likelihood of default and 1 indicates a high likelihood. The performance of the model may be evaluated using metrics like accuracy, precision, recall, and F1 score. These indicators show how accurately the model can categorize borrowers as low risk or high risk. Overall, logistic regression is a potent technique for assessing credit risk that can assist lenders in making better choices regarding loan approvals and interest rates. Lenders can more effectively manage their risk and minimize financial losses by using data to estimate the likelihood of default.

Logistic regression is a popular method for credit risk assessment using machine learning. A mathematical model for logistic regression on the German Credit dataset can be represented as follows:

- Let there be n observations, with m features and a binary target variable y, where y = 1 indicates that the loan was granted, and y = 0 indicates that the loan was not granted.
- Let X be the n x m matrix of input features, where each row represents an observation, and each column represents a feature.
- Let β be the (m x 1) vector of coefficients for the logistic regression model.

The logistic regression model can be represented as:

$$P = 1 / (1 + \exp(-X\beta)) . \qquad (1)$$

P: The predicted probability of the loan being granted

The coefficients β can be estimated by using maximum likelihood estimation.

The objective function for maximum likelihood estimation is:

$$L(\beta) = \prod (p\_i)\hat{}y\_i * (1 - p\_i)\hat{}(1 - y\_i) . \qquad (2)$$

i :index for each observation,

p_i : predicted probability of the loan being granted for observation i.

The coefficients β can be estimated by maximizing the log-likelihood function :

$$\log L(\beta) = \sum y\_i \log p\_i + (1 - y\_i) \log (1 - p\_i) . \qquad (3)$$

The logistic regression model can then be used to predict the probability of a loan being granted for new observations, based on their input features. The predicted probability can be used as a measure of credit risk, with higher probabilities indicating lower credit risk.

Following is the output by using logistic regression.

Name of Algorithm	**Accuracy Achieved for Classification**
CART	87.97 %
Gradiant Boosting	87.83 %
KNN	86.67 %
Logistic Regression	86.38 %
MLP	85.65 %
SVM	85.51 %
Random Forest	85.36 %

Decision Tree for Credit Risk Assessment:

A decision tree is a tree-like model that uses recursive grouping of the data into ever-smaller groups based on the values of the input features to make decisions or predictions. A test on one of the input features is run at each node of the tree, dividing the data into two or more groups.The test that is chosen is the one that best separates the data based on the desired outcome, such as minimizing the error or maximizing the information gain.

The splitting process continues until the data in each leaf node is homogeneous or as pure as possible, meaning that all the samples in the node belong to the same class or have the same label. The decision tree can then be used to make predictions on fresh data by following the path from the root node to the leaf node, which corresponds to the values of the input features. The anticipated outcome is the class or label assigned to the leaf node. Decision trees, which can accommodate both category and numerical input data, are extremely straightforward to comprehend and visualize. They can also be applied to problems involving classification and regression. However, overfitting is a risk with decision trees that can be reduced by employing strategies like pruning, ensemble methods, or regularization. For this credit card fraud dataset is used.

Name of Algorithm	**Accuracy of Classification**
Decision tree classifier	95.57%

*Random Forest for Credit Risk assessment***:**

Different decision trees are combined using the ensemble learning method Random Forest to create a more accurate and dependable model. The method picks a subset of features and a portion of training data at random for each tree in the forest. Each decision tree is trained on a different subset of data and uses a random subset of the available features at each split in order to reduce correlation across the trees and improve overall model performance. The forecast is created by averaging the forest's individual trees' forecasts, weighted by each one's individual accuracy, when a new sample is presented to the model for classification or regression. Both categorical and numerical data can be handled by Random Forest, which also handles missing values and noisy data without the need for pre-processing. In addition, it is more resistant to outliers and data noise and less prone to overfitting than a single decision tree.

The number of trees in the forest, which can be adjusted to reach the desired level of accuracy and generalization performance, is a key hyper-parameter in Random Forest. The maximum depth of the trees, Additional hyper-parameters that can be changed include the minimum number of samples required to divide a node and the minimum number of samples required to be at a leaf node. All things considered, Random Forest is a strong and adaptable algorithm that is frequently employed in numerous tasks like classification, regression, feature selection, and anomaly detection.

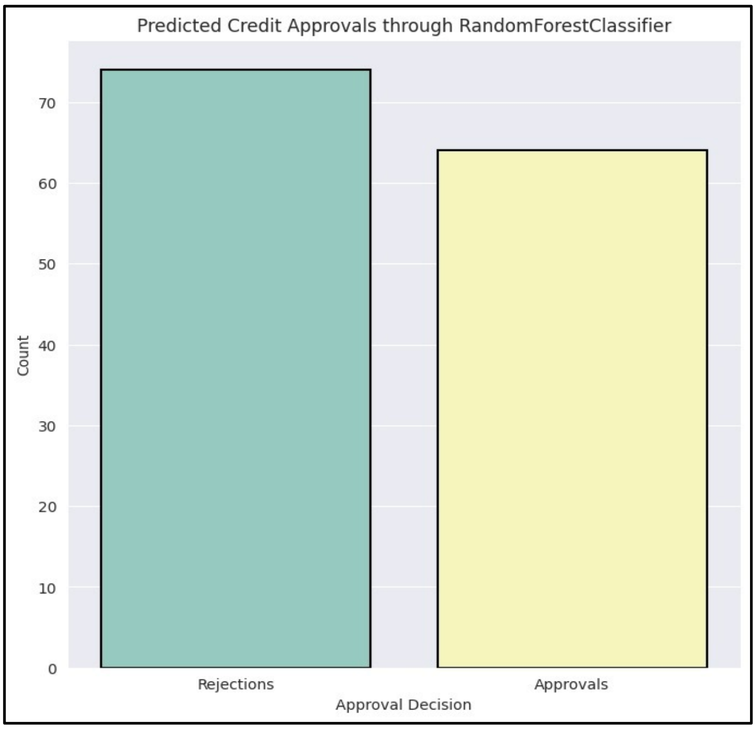


Fig.6: Predicted Credit approval by Random Forest Classifier

4. Conclusion

In summary, our paper introduces a comprehensive Risk Management system tailored for the financial sector to address the pervasive issue of search rank fraud in online services. Through meticulous exploration, we have elucidated the system's key components, notably focusing on the integration of optical character recognition for loan application scanning. By rigorously evaluating different classifiers including Decision Tree, Random Forest, and others, we have substantiated the efficacy of our approach. Notably, our findings demonstrate that the Decision Tree classifier achieves an impressive 95.57% accuracy in efficiently distinguishing between fraudulent and non-fraudulent loan applicants.

Furthermore, our investigation extends to the realm of irregular credit card transactions, where we employ an array of classifiers including CART, Gradient Boosting, KNN, Logistic Regression, MLP, SVM, and Random Forest. The results are compelling, with the CART classifier emerging as a standout performer, exhibiting an 87.971% accuracy in accurately categorizing irregular credit card transactions as legitimate or non-legitimate. This achievement underscores the robustness and versatility of our Risk Management system in tackling multifaceted challenges within the financial domain.

References

[1] C. Wang and H. Zhu, "Representing Fine-Grained Co-Occurrences for Behavior-Based Fraud Detection in Online Payment Services."(2020).

[2] Proceedings of the Second International Conference on Inventive Research in Computing Applications (ICIRCA-2020), IEEE Xplore, Part Number: CFP20N67-ART; ISBN: 978-1-7281-5374-2.(2020).

[3] M. Sánchez-Aguayo, L. Urquiza-Aguiar, and J. Estrada-Jiménez, "Review Fraud Detection Using the Fraud Triangle Theory and Data Mining Techniques: A Literature Review," International Journal of Advanced Science and Technology, vol. 29, no. 4s, pp. 38-46, 2020.(2020).

[4] V. Ghai and S. S. Kang, "Role of Machine Learning in Credit Card Fraud Detection," in Proceedings of the 2021 3rd International Conference on Advances in Computing, Communication Control and Networking (ICAC3N), pp. 939-943(2021).

[5] M. Singh Ahuja and Lovepreet Singh, "Online Fraud Detection - A Review," International Research Journal of Engineering and Technology (IRJET),(2020).

[6] B. Liu et al, "Credit Card Fraud Detection Using Lightgbm Model," in IEEE 2020 International Conference on E-Commerce and Internet Technology (ECIT), pp. 232-236, (2020).

[7] D. Ge, J. Gu, S. Chang, and J. Cai, "Credit Card Fraud Detection Using Lightgbm Model," in IEEE 2020 International Conference on E-Commerce and Internet Technology (ECIT), pp. 232-236, (2020).

[8] "A Survey of Deep Learning based Online Transactions Fraud Detection Systems," in 2020 International Conference on Intelligent Engineering and Management (ICIEM), (2020).

[9] S. Tang, L. Jin, and F. Cheng, "Fraud Detection in Online Fraud via Heterogeneous Graph Transform," Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai, China.(2021)

[10] İpek Erdoğan,Orhan Kurto,Alican Kurt,Şerif Bahtıyar(2020) credit card fraud detection(2020)

[11] X. Yu, X. Li, Y. Dong, and R. Zheng, "A Deep Neural Network Algorithm for Detecting Credit Card Fraud," in IEEE 2020 International Conference on Big Data, Artificial Intelligence and Internet of Things Engineering (ICBAIE), pp. 181-183, 2020.(2020)

[12] Adriano Perirera, "Methodology for the Fraud Detection in Electronic Transaction."(2020)

[13] M. Rahman, N. Hernandez, B. Carbunar, and D. H. Chau, "Towards De-Anonymization of Google Play Search Rank Fraud," IEEE Transactions on Knowledge and Data Engineering, pp. 1-1, 2020.(2020)

[14] "Machine Learning for Credit Card Fraud Detection System," International Journal of Applied Engineering Research, vol. 13, no. 24, pp. 16819-16824, 2018.(2020)

[15] M. Hofmann and R. Klinkenberg, "The German Credit Data Set," in Proceedings of the International Conference on Knowledge Discovery and Data Mining, 1999.(2020)

[16] K. Bache and M. Lichman, "UCI Machine Learning Repository," University of California, School of Information and Computer Science, 2013.(2020)

[17] C. Zhang, G. Xu, and D. Zhu, "Machine Learning-Based Credit Scoring: A Systematic Literature Review," Expert Systems with Applications, vol. 145, p. 113129, 2020.(2021)

[18] S. Helal and S. Zhang, "Credit Risk Assessment Using Statistical and Machine Learning: Basic Methodology and Risk Modeling Applications," in International Conference on Computational Science and Its Applications, pp. 910-918, Springer, 2005.(2020).

[19] I. C. Yeh and C. H. Lien, "The Comparisons of Data Mining Techniques for the Predictive Accuracy of Probability of Default of Credit Card Clients," Expert Systems with Applications, vol. 36, no. 2, pp. 2473-2480, 2009.(2021).

[20] "FICO Score High-Risk Credit Score," Fair Isaac Corporation.(2020).

[21] K. Bache and M. Lichman, "UCI Machine Learning Repository," University of California, School of Information and Computer Science, 2013.(2020).

[22] Reserve Bank of India, "Value of Bank Frauds across India from Financial Year 2009 to 2022," [Online]. Available: https://www.statista.com/statistics/1012762/india-value-of-bank-fraud/.(2022).