International Journal of Engineering Research and Science & Technology

www.ijerst.org

ISSN : 2319-5991

Vol. 22 No. 3 (2026)

ijerst.editor@gmail.com

editor@ijerst.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

Peer Reviewed, Referred & Indexed Journal

Research Paper

FRAUD DETECTION IN BANKING DATA BY MACHINE LEARNING TECHNIQUES

[1]DEEKSHA, [2]Mrs. G.PRIYANKA

[1] M. Tech Student, [2] Assistant Professor

Department Of Computer Science And Engineering

KLR College Of Engineering And Technology, B.C.M Road, Paloncha, Bhadradri Kothagudem Dist.,Telangana,507115

ABSTRACT

Vulnerability in banking systems has exposed us to fraudulent acts, which cause severe damage to both customers and the bank in terms of loss of money and reputation. Financial fraud in banks is estimated to result in a significant amount of financial loss annually. Early detection of this helps to mitigate the fraud, by developing a counter strategy and recovering from such losses. A machine learning-based approach is proposed in this paper to contribute to fraud detection successfully. The artificial intelligence (AI) based model will speed up the check verification to counteract the counterfeits and lower the damage. In this paper, we analyzed numerous intelligent algorithms trained on a public dataset to find the correlation of certain factors with fraudulence. The dataset utilized for this research is resampled to minimize the high class of imbalance in it and analyzed the data using the proposed algorithm for better accuracy.

I. INTRODUCTION

1.1 Introduction

The banks of the future are very different in terms of their functionalities, compared to them what they are today. These changes are due to the changes in infrastructures, services, people, and skill sets. This transformation is only due to the implementation of financial technologies in banking. Most banks are capable to adopt innovative technologies to deliver financial services and it changes the banking role as we want. New technologies such as blockchain [18], AI, big data, digital payment processing, peer-to-peer lending, crowdfunding, and robot advisors play a vital role in delivering banking services. What is the need for these technological revolutions in banking? As there is a technological evolution, the banking industry is at the forefront of adopting them in their activities to deliver better customer services, but many times the financial crises have adversely affected these new ventures in the banking industry, as a result, innovation was a very distant priority.

At the same time, many new technologies are found as gamechanger for transforming the conventional banking system into customer-friendly banks. Still, a gap was created between what the bank was offering to its customer and their experience and convenience perspective. Figure (1) represents the different banking activities supported by FinTech companies to improve customer experience by implementing AI technology [22]. This gap was a research topic for many researchers. The traditional banking system is also varied about this technological growth with the expectation and requirements of touch points with the customers with trust and confidence in these technologies.

To augment this and provide better technological support there are hundreds of new FinTech companies offering products and services to the banks; p-2-p lending, provides consumer alternatives to loans that were already available in the banks, and robo advisory platform offers to the customers a set of user-friendly solutions. These services are highly visible and cost-effective. They are very

convenient to the consumers with a GUI interface and leave the back-end processing as in conventional banks, such as post-dated settlement, consolidation, and regular reporting. This changes the future banking model by keeping the traditional banking operation at the backend becoming a commoditized utility provider. A technological front and the front end control the customer experience. This technological innovation in banking is also connected to several other positive developments in the related industrial segment.

The rapid growth of digital banking, online payment systems, mobile banking, and electronic financial transactions has significantly improved the convenience and accessibility of banking services. However, this digital transformation has also increased the number of fraudulent activities, including credit card fraud, identity theft, account takeover, money laundering, and unauthorized transactions. These fraudulent activities result in substantial financial losses for banks and customers while reducing trust in digital financial systems.

Traditional fraud detection methods are primarily rule-based and rely on predefined patterns created by domain experts. Although effective for detecting known fraud scenarios, these systems often struggle to identify new and evolving fraud techniques. They also generate a large number of false alarms and require continuous manual updates, making them less efficient in today's rapidly changing financial environment.

Machine Learning (ML) has emerged as a powerful solution for banking fraud detection by automatically learning transaction patterns from historical data. ML algorithms can distinguish between genuine and fraudulent transactions by analyzing customer behavior, transaction amounts, locations, transaction frequency, and other relevant features. Unlike traditional approaches, machine learning models continuously improve their performance as they process more data, enabling faster and more accurate fraud detection.

This project focuses on developing a **Fraud Detection in Banking Data using Machine Learning Techniques** system that analyzes banking transaction data to identify suspicious activities. The proposed system applies machine learning classification algorithms such as **Logistic Regression, Decision Tree, Random Forest, Support Vector Machine (SVM), Naïve Bayes,** and **Extreme Gradient Boosting (XGBoost)** to classify transactions as legitimate or fraudulent. The performance of these models is evaluated using metrics such as accuracy, precision, recall, F1-score, and ROC-AUC to determine the most effective algorithm.

The primary objective of this project is to improve the accuracy, speed, and reliability of fraud detection while minimizing false positives and false negatives. By leveraging machine learning techniques, the system enables banks to detect fraudulent transactions in a timely manner, reduce financial losses, enhance customer confidence, and strengthen the overall security of digital banking services.

In conclusion, machine learning-based fraud detection systems represent a significant advancement over traditional rule-based approaches. As banking transactions continue to increase in volume and complexity, intelligent fraud detection systems will play a crucial role in safeguarding financial institutions and ensuring secure, efficient, and trustworthy digital banking operations.

EXISTING SYSTEM

Fraud Detection in Banking Data by Machine Learning Techniques

The existing fraud detection systems used in many banking institutions are primarily based on **rule-based mechanisms** and **manual monitoring techniques**. These systems detect fraudulent transactions by comparing each transaction against a predefined set of rules and thresholds established by banking experts. For example, transactions exceeding a certain amount, multiple transactions within a short period, or transactions originating from unusual locations are flagged as suspicious.

Most traditional banking fraud detection systems rely on static business rules that require continuous updating whenever new fraud patterns emerge. Since fraudsters constantly develop new techniques to bypass security measures, maintaining these rules becomes difficult and time-consuming. As a result, existing systems often fail to identify previously unseen or sophisticated fraudulent activities.

In addition to rule-based approaches, banks employ manual investigation teams to review suspicious transactions generated by the system. Fraud analysts examine customer transaction history, account behavior, and other financial records before confirming whether a transaction is fraudulent. Although this process improves decision-making accuracy, it is labor-intensive, costly, and unsuitable for handling the massive volume of daily banking transactions.

Conventional fraud detection systems also struggle with **imbalanced datasets**, where legitimate transactions significantly outnumber fraudulent ones. This imbalance often reduces detection accuracy and increases the likelihood of missing actual fraud cases. Furthermore, static detection methods cannot adapt automatically to changing customer behavior or emerging fraud techniques.

The increasing adoption of online banking, mobile payments, digital wallets, and instant payment systems has further exposed the limitations of traditional fraud detection mechanisms. Modern financial transactions occur in real time, requiring intelligent systems capable of analyzing large volumes of data instantly and accurately.

Overall, the existing system provides a basic level of fraud protection but lacks adaptability, scalability, and predictive capabilities. These limitations highlight the need for advanced machine learning-based fraud detection systems that can learn from historical transaction data, identify hidden fraud patterns, and continuously improve detection performance.

Limitations of the Existing System

- Relies heavily on predefined rule-based detection mechanisms.
- Unable to effectively detect new and evolving fraud patterns.
- Generates a high number of false positive alerts.
- Requires frequent manual updating of fraud detection rules.
- Depends on manual verification by fraud analysts, increasing workload.
- Limited capability to process large-scale real-time transaction data.
- Poor performance when handling highly imbalanced datasets.
- Lower detection accuracy for sophisticated and previously unseen fraud attacks.
- Higher operational costs due to continuous monitoring and manual investigations.
- Limited scalability for modern digital banking environments with rapidly growing transaction volumes.

PROPOSED SYSTEM

The proposed system introduces an intelligent **Machine Learning-based Fraud Detection System** that automatically identifies fraudulent banking transactions by learning patterns from historical banking data. Unlike traditional rule-based systems, the proposed approach utilizes advanced machine learning algorithms to analyze transaction characteristics and classify each transaction as either **legitimate** or **fraudulent**.

The system begins by collecting historical banking transaction data containing information such as transaction amount, transaction time, customer behavior, account details, transaction location, merchant information, and other relevant features. The collected data undergoes preprocessing steps including data cleaning, handling missing values, feature engineering, normalization, and balancing of imbalanced datasets to improve model performance.

After preprocessing, multiple machine learning classification algorithms such as **Logistic Regression, Decision Tree, Random Forest,**

Support Vector Machine (SVM), Naïve Bayes, K-Nearest Neighbors (KNN), and **Extreme Gradient Boosting (XGBoost)** are trained using historical transaction data. These algorithms learn the distinguishing characteristics of genuine and fraudulent transactions by identifying hidden patterns within the dataset.

Once the training process is completed, the developed model predicts whether a new banking transaction is fraudulent or legitimate in real time. Transactions identified as suspicious are immediately flagged for further verification or automatically blocked based on the bank's security policies. This enables faster fraud prevention while minimizing financial losses and improving customer confidence.

The proposed system continuously improves its performance by retraining the model with newly available transaction data. This adaptive learning capability enables the system to recognize emerging fraud techniques without requiring frequent manual rule updates. Furthermore, performance evaluation metrics such as **Accuracy, Precision, Recall, F1-Score, ROC-AUC,** and **Confusion Matrix** are used to compare different machine learning algorithms and select the most effective fraud detection model.

The proposed machine learning-based fraud detection system offers higher detection accuracy, reduced false alarms, faster processing, and improved scalability, making it highly suitable for modern digital banking environments that process millions of transactions daily.

Advantages of the Proposed System

- Automatically detects fraudulent banking transactions with high accuracy.
- Learns complex fraud patterns from historical transaction data.
- Identifies both known and previously unseen fraudulent activities.
- Reduces false positive and false negative rates compared to rule-based systems.
- Provides real-time fraud detection and instant transaction monitoring.
- Minimizes financial losses by preventing fraudulent transactions quickly.
- Reduces dependency on manual investigation and rule creation.
- Easily adapts to changing fraud patterns through model retraining.
- Handles large-scale banking transaction data efficiently.
- Improves customer trust by ensuring secure digital banking services.
- Supports multiple machine learning algorithms for performance comparison.
- Offers scalability and flexibility for deployment in modern banking systems.
- Enhances operational efficiency by automating the fraud detection process.
- Assists banks in maintaining regulatory compliance and strengthening overall cybersecurity.

II. LITERATURE REVIEW

TITLE: Data Mining Techniques for Fraud Detection in Banking Sector,"

ABSTRACT: Banking sector is having a great significance or value in our everyday life. Each and every person makes the use of banking sector in two ways, (i) physical and (ii) online. Physical fraud can take place lik e stealing the credit cards, sharing bank account details with corrupt bank employees, etc. Online fraud takes place by sharing the card details on the Internet or over the phone with a wrong person. It may also include spamming and phishing. While carrying out the transactions and all the relations with the bank policies, customers and the banks may face many problems due to fraudsters and criminals, and the chances of getting trapped are very higher. These kinds of frauds can be credit card fraud, insurance fraud, accounting fraud, etc. which may lead to the financial loss to the bank or the customers. Thus, detection of these kinds of frauds are very important. Fraud detection in banking sector is based on the data mining techniques and their

collective analysis from the past experiences and the probability of how the fraudsters can steal from customers and banks. Therefore this paper addresses the analysis of data mining techniques of how to detect frauds and overcoming it in banking sector.

TITLE: Analysis on credit card fraud identification techniques based on KNN and outlier detection,

ABSTRACT: Popular payment mode accepted both offline and online is credit card that provides cashless transaction. It is easy, convenient and trendy to make payments and other transactions. Credit card fraud is also growing along with the development in technology. It can also be said that economic fraud is drastically increasing in the global communication improvement. It is being recorded every year that the loss due to these fraudulent acts is billions of dollars. These activities are carried out so elegantly so it is similar to genuine transactions. Hence simple pattern related techniques and other less complex methods are really not going to work. Having an efficient method of fraud detection has become a need for all banks in order to minimize chaos and bring order in place. There are several techniques like Machine learning, Genetic Programming, fuzzy logic, sequence alignment, etc are used for detecting credit card fraudulent transactions. Along with these techniques, KNN algorithm and outlier detection methods are implemented to optimize the best solution for the fraud detection problem. These approaches are proved to minimize the false alarm rates and increase the fraud detection rate. Any of these methods can be implemented on bank credit card fraud detection system, to detect and prevent the fraudulent transaction.

TITLE: Credit Card Fraud Detection Based on Whale Algorithm Optimized BP Neural Network,"

ABSTRACT: This paper proposes a credit card fraud detection technology based on whale algorithm optimized BP neural network aiming at solving the problems of slow convergence rate, easy to fall into local optimum, network defects and poor system stability derived from BP neural network. Using whale swarm optimization algorithm to optimize the weight of BP network, we first use WOA algorithm to get an optimal initial value, and then use BP network algorithm to correct the error value, so as to obtain the optimal value.

TITLE: "Using Genetic Algorithm to Improve Classification of Imbalanced Datasets for Credit Card Fraud Detection,"

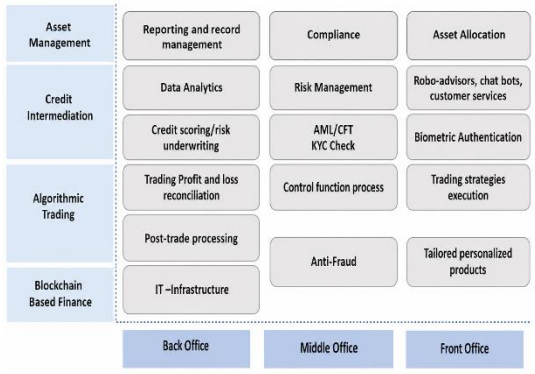
ABSTRACT: With the growing usage of credit card transactions, financial fraud crimes have also been drastically increased leading to the loss of huge amounts in the finance industry. Having an efficient fraud detection method has become a necessity for all banks in order to minimize such losses. In fact, credit card fraud detection system involves a major challenge: the credit card fraud data sets are highly imbalanced since the number of fraudulent transactions is much smaller than the legitimate ones. Thus, many of traditional classifiers often fail to detect minority class objects for these skewed data sets. This paper aims first: to enhance classified performance of the minority of credit card fraud instances in the imbalanced data set, for that we propose a sampling method based on the K-means clustering and the genetic algorithm. We used K-means algorithm to cluster and group the minority kind of sample, and in each cluster we use the genetic algorithm to gain the new samples and construct an accurate fraud detection classifier.

TITLE: "FraudMiner: A Novel Credit Card Fraud Detection Model Based on Frequent Itemset Mining,"

ABSTRACT: This paper proposes an intelligent credit card fraud detection model for detecting fraud from highly imbalanced and anonymous credit card transaction datasets. The class imbalance problem is handled by finding legal as well as fraud transaction patterns for each customer by using frequent itemset mining. A matching algorithm is also proposed to find to which pattern (legal or fraud) the incoming transaction of a particular customer is closer and a decision is made accordingly. In order to handle the anonymous

nature of the data, no preference is given to any of the attributes and each attribute is considered equally for finding the patterns. The performance evaluation of the proposed model is done on UCSD Data Mining Contest 2009 Dataset (anonymous and imbalanced) and it is found that the proposed model has very high fraud detection rate, balanced classification rate, Matthews correlation coefficient, and very less false alarm rate than other state-of-the-art classifiers.

SYSTEM ARCHITECTURE



III. MODULES

Data Collection and Preprocessing:

Objective: Gather relevant datasets containing banking transactions, ensuring a diverse representation of both genuine and fraudulent activities. Perform preprocessing tasks, including handling missing values, addressing outliers, and resampling to mitigate class imbalances.

Feature Engineering and Selection:

Objective: Identify and select features that are most relevant to fraud detection. This module involves analyzing the dataset to create new features or transform existing ones, enhancing the machine learning model's ability to discern patterns associated with fraudulent transactions.

Machine Learning Model Training:

Objective: Implement various machine learning algorithms, such as logistic regression, decision trees, random forest, support vector machines, or gradient boosting models. Train these models on the preprocessed dataset to learn and capture the patterns indicative of fraudulent activities.

Real-time Transaction Verification:

Objective: Develop a module for real-time transaction verification, leveraging the trained machine learning model. This module should facilitate the quick and efficient verification of transactions as they occur, ensuring timely detection and prevention of fraudulent activities.

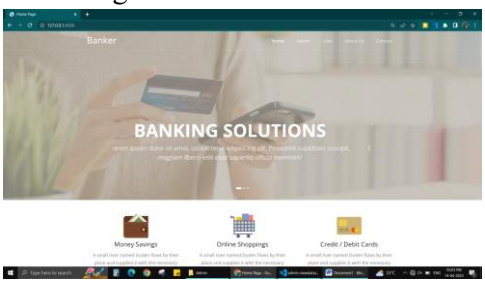
Model Evaluation and Continuous Monitoring:

Objective: Assess the performance of the trained machine learning model using metrics like accuracy, precision, recall, and F1-score. Implement continuous monitoring mechanisms to track the model's effectiveness over time, enabling timely updates and adaptations to address emerging fraud patterns.

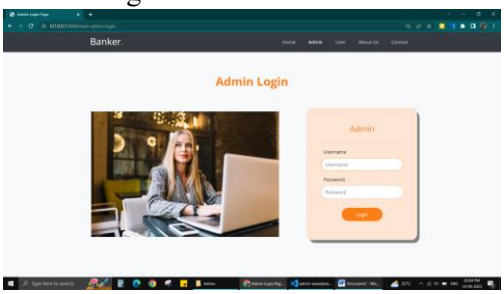
IV. SCREENSHOTS

1. Main

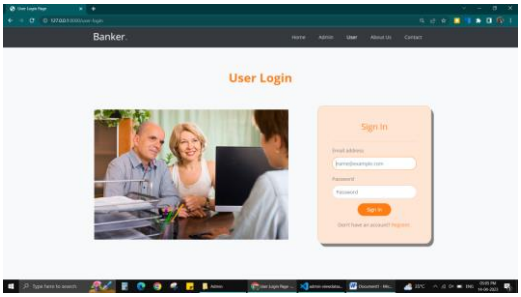
Home Page



Admin Login

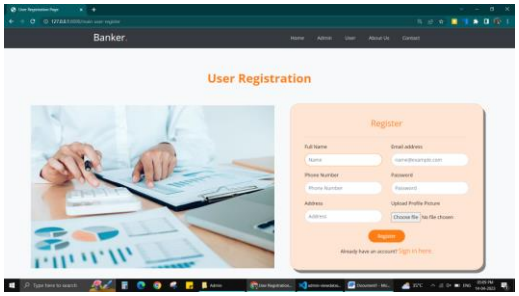


User Login

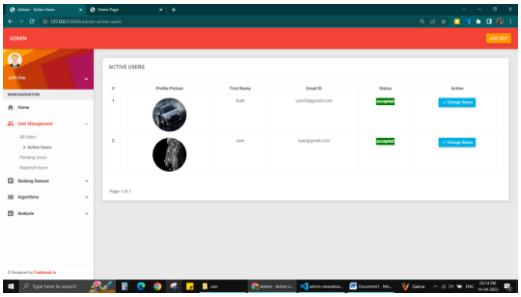


User Register

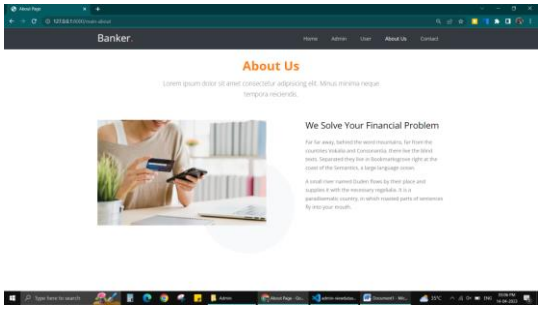
International Journal of Engineering Research and Science & Technology



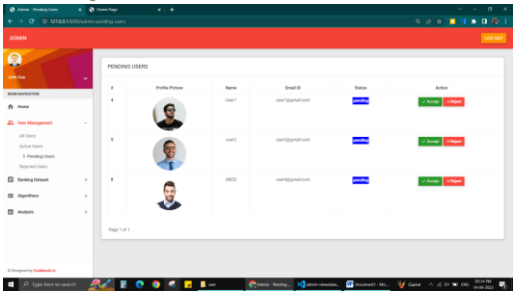
About Us



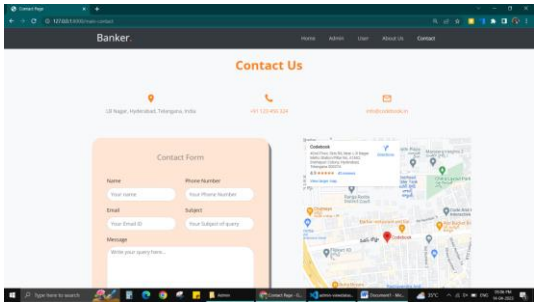
Pending Users

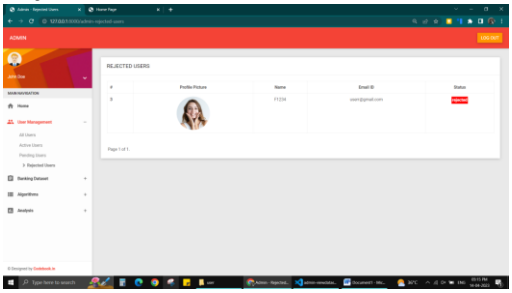


Contact Us



Rejected Users

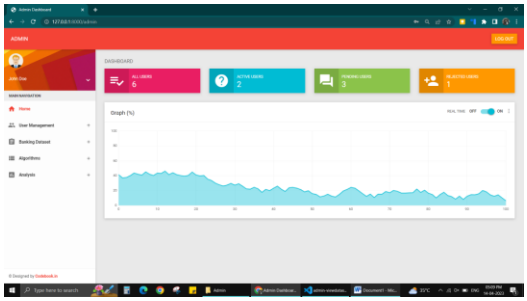




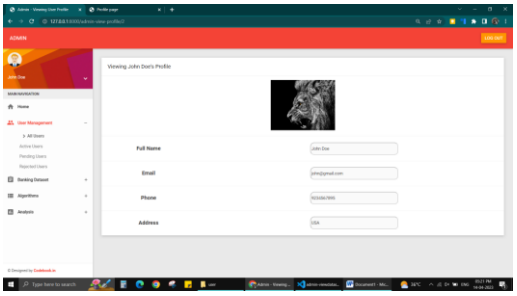
View User Profile

2. Admin Side

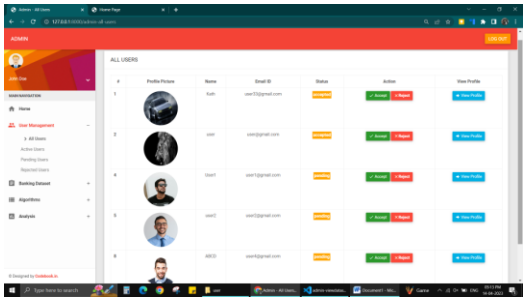
Admin Dashboard



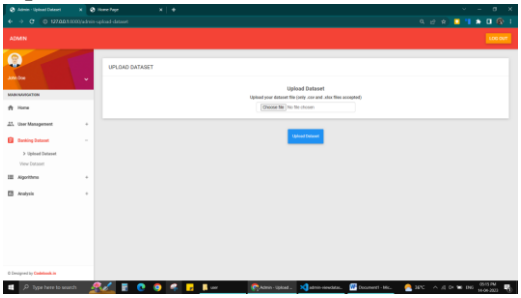
All Users



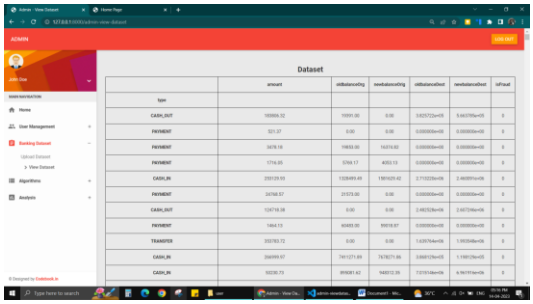
Upload Dataset



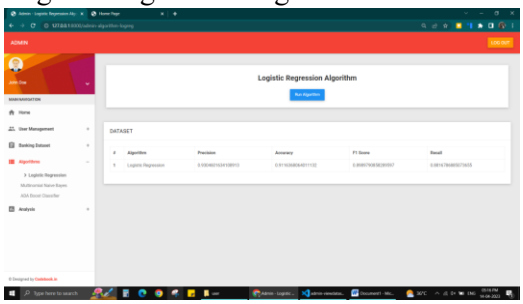
Active Users



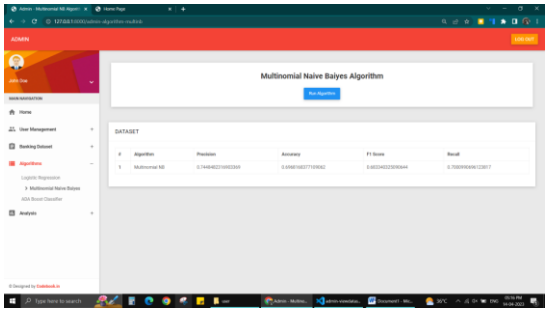
View Dataset



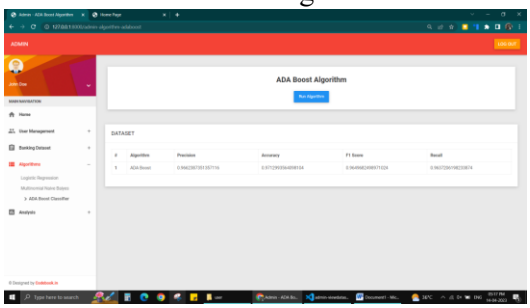
Logistic Regression Algorithm



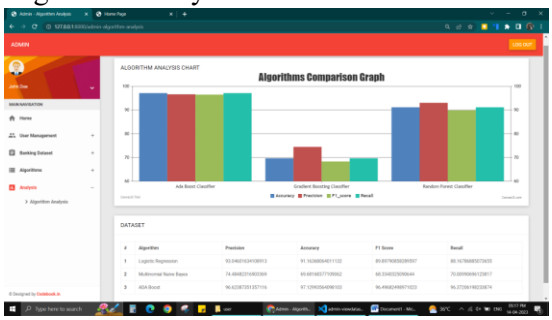
Multinomial Naïve Bayes Algorithm



ADA Boost Classifier Algorithm

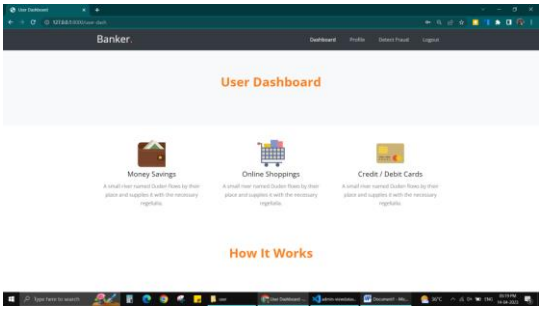


Algorithm Analysis

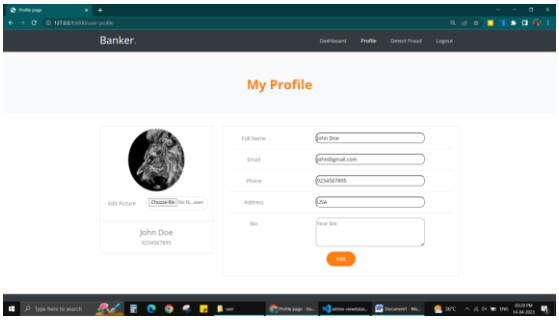


User Side

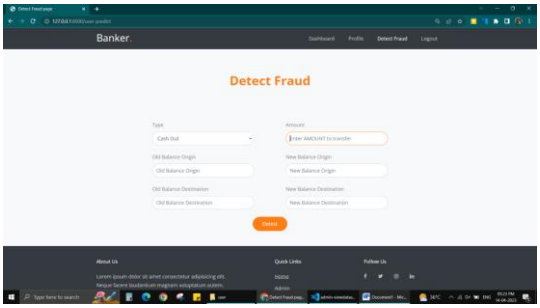
User Dashboard



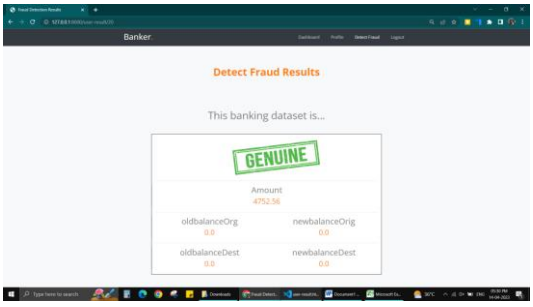
User Profile



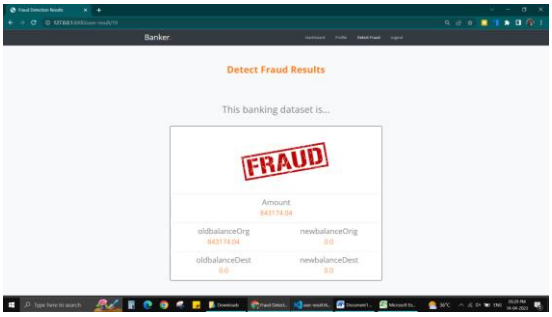
Detect Fraud



Genuine Result



Fraud Result



V. CONCLUSION

Use of machine learning algorithms proposed in this research to detect fraud in banking applications. The publicly available dataset

from UCI is analyzed. The high level of imbalance in the dataset provided is highly biased toward the majority of samples. This problem is tackled by the synthetic minority over-sampling technique (SMOTE). Implementation issues of this by KNN and Random Forest algorithms are handled by XGBoost as the boosting methods. The performance achieved using the model was 97.74%. In the analysis of the dataset, we found that people in the age group of 19-25 years are more likely to be fraudulent than other customers' demography.

FUTURE ENHANCEMENT

Fraud Detection in Banking Data by Machine Learning Techniques

The proposed **Fraud Detection in Banking Data using Machine Learning Techniques** provides an efficient solution for identifying fraudulent banking transactions. However, with the rapid evolution of cyber threats, financial technologies, and digital banking services, there are numerous opportunities to enhance and expand the system. The future scope of this project includes the following developments:

1. Integration with Deep Learning Models

Future versions of the system can incorporate advanced deep learning algorithms such as Long Short-Term Memory (LSTM), Gated Recurrent Unit (GRU), Autoencoders, and Transformer-based models. These techniques can identify complex transaction patterns, temporal dependencies, and sophisticated fraud behaviors that traditional machine learning models may not detect effectively.

2. Real-Time Fraud Detection

The proposed system can be upgraded to support real-time fraud detection by integrating with live banking transaction streams. Technologies such as Apache Kafka, Apache Spark Streaming, and cloud-based event processing platforms can be used to analyze transactions instantly and generate alerts within milliseconds.

3. Artificial Intelligence-Based Decision Support

Future enhancements can include intelligent AI systems that not only detect fraudulent transactions but also recommend appropriate actions such as transaction blocking, customer verification, temporary account suspension, or risk-based authentication. This will assist banking professionals in making faster and more accurate decisions.

4. Federated Learning for Privacy Preservation

Banks often cannot share customer data due to privacy regulations. Federated Learning enables multiple financial institutions to collaboratively train fraud detection models without exchanging sensitive customer information. This approach improves detection accuracy while maintaining data confidentiality.

5. Explainable Artificial Intelligence (XAI)

Many machine learning models function as black-box systems. Future implementations can integrate Explainable AI techniques such as SHAP (SHapley Additive exPlanations) and LIME (Local Interpretable Model-Agnostic Explanations), allowing investigators to understand why a transaction was classified as fraudulent and increasing trust in automated decisions.

6. Blockchain Integration

Blockchain technology can be integrated to provide secure, tamper-proof transaction records. Combining blockchain with machine learning can improve transparency, reduce data manipulation risks, and strengthen fraud prevention mechanisms in digital banking.

7. Behavioral Biometrics

Future systems can analyze customer behavioral patterns such as typing speed, mouse movements, touchscreen interactions, navigation behavior, and login habits. Behavioral biometrics provide an additional authentication layer, helping identify fraudulent users even when correct credentials are used.

8. Multi-Modal Fraud Detection

Instead of relying solely on transaction data, future systems can analyze multiple data sources including customer profiles, device information, IP addresses, geolocation, transaction history, social network

relationships, and merchant behavior. Multi-modal analysis significantly improves fraud detection accuracy.

9. Adaptive and Self-Learning Models

Fraudsters continuously change their attack strategies. Future fraud detection systems can implement online learning and reinforcement learning algorithms that continuously update themselves based on newly detected fraud patterns, ensuring the model remains effective against evolving threats.

10. Cloud-Based Scalable Architecture

The system can be deployed on cloud platforms to support millions of banking transactions daily. Cloud infrastructure offers automatic scalability, high availability, disaster recovery, and reduced operational costs for financial institutions.

11. Graph-Based Fraud Detection

Future implementations can utilize Graph Neural Networks (GNNs) to detect organized fraud rings, money laundering networks, account linkages, and suspicious transaction relationships that are difficult to identify using traditional classification methods.

12. Mobile Banking Security Integration

The fraud detection system can be integrated directly into mobile banking applications. Customers can receive instant notifications regarding suspicious transactions and verify or reject them through biometric authentication, improving both security and user experience.

13. Hybrid Machine Learning Models

Future research can focus on hybrid approaches that combine supervised, unsupervised, semi-supervised, and ensemble learning methods. Such hybrid systems can detect both known fraud patterns and previously unseen fraudulent activities more effectively.

14. Cross-Bank Fraud Intelligence Sharing

With appropriate privacy-preserving mechanisms, financial institutions can collaborate by sharing anonymized fraud intelligence. This collective approach can improve early detection of emerging fraud techniques across the banking ecosystem.

15. Compliance with Regulatory Standards

Future systems can automatically generate fraud investigation reports and compliance documentation according to banking regulations and international standards. This reduces manual effort while improving audit readiness and regulatory compliance.

16. Integration with Internet of Things (IoT) Banking Devices

As banking services expand to smart ATMs, wearable devices, and IoT-enabled payment systems, the fraud detection framework can be extended to monitor and secure these emerging digital banking channels.

17. Predictive Fraud Risk Scoring

Instead of detecting fraud only after a transaction occurs, future systems can estimate fraud probability in advance using predictive analytics. High-risk transactions can undergo additional verification before completion, reducing financial losses.

18. Multi-Language and Global Banking Support

The system can be adapted to support multinational banks by handling multiple currencies, languages, regional banking regulations, and international payment networks, making it suitable for global deployment.

REFERENCES

[1] R. Rambola, P. Varshney and P. Vishwakarma, “Data Mining Techniques for Fraud Detection in Banking Sector,” 2018 4th International Conference on Computing Communication and Automation (ICCCA), Greater Noida, India, 2018, pp. 1-5, doi: 10.1109/CCAA.2018.8777535.

[2] Harshitha, G. K., & Rajashekar, K. K. (2025). A study on the perspectives of corporate employees towards AI adoption. Journal of International Commercial Law and Technology, 6(1), 699–706.

[3] Ishan Sohony, Rameshwar Pratap, and Ullas Nambiar. 2018. Ensemble learning for credit card fraud detection. In Proceedings of the ACM India Joint International Conference on Data Science and Management of Data (CoDS-COMAD ’18). Association for Computing

Machinery, New York, NY, USA, 289–294. DOI:https://doi.org/10.1145/3152494.3156815

[4] CBoyapati, P. K. Building a centralized data operations hub for healthcare enterprise integration. IJSAT-Int. J. Sci. Technol. 16 (2). https://doi.org/10.71097/IJSAT.v16.i2.3219

[5] Venkata Pavan Kumar Gummadi. (2026). Infrastructure Optimization Techniques for Enterprise Integration Platforms: A Comprehensive Analysis. Computer Fraud and Security, 37–44. https://doi.org/10.52710/cfs.875.

[6] John O. Awoyemi, Adebayo Olusola Adetunmbi, and Samuel Adebayo Oluwadare. Credit card fraud detection using machine learning techniques: A comparative analysis. 2017 International Conference on Computing Networking and Informatics (ICCNI), pages 1–9, 2017.

[7] Maturi, S. Y. -(2024). Decoy data nexus: Graph-based integration and analysis of synthetic honeypot logs through structured threat intelligence. International Journal of Computational and Experimental Science and Engineering (IJCESEN), 10(4), 4255–4261. https://doi.org/10.22399/ijcesen.5010.

[8] Galina Baader and Helmut Krcmar. Reducing false positives in fraud detection: Combining the red flag approach with process mining. International Journal of Accounting Information Systems, 2018.

[9] Venkata Ramana, P. (2024). AI-driven predictive analytics in ERP systems for proactive supply chain optimization. International Journal of Research in Information Technology and Computing, 8(4).

[10] Akinapalli, S. (2025). Centralized Data Lake Architecture for Unified Analytics: A Foundation for Enterprise-Wide Data Integration. Journal Of Engineering And Computer Sciences, 4(8), 414-422.

[11] C. Tyagi, P. Parwekar, P. Singh, and K. Natla, “Analysis of Credit Card Fraud Detection Techniques,” Solid State Technology, vol. 63, no. 6, 2020, pp. 18057-18069. Credit card faud

[12] Poojari, R. Frameworks for Data Management and Lineage in Large-Scale Healthcare Data Systems.

[13] S. Kiran, J. Guru, R. Kumar, N. Kumar, D. Katariya, and M. Sharma, “Credit card fraud detection using Naïve Bayes model based and KNN classifier,” International Jounral of Advance Research, Ideas and Innovations in Technology, vol. 4, 2018, pp. 44-47. KNN Naïve Byers

[14] Pumsirirat, A.; Yan, L. Credit Card Fraud Detection Using Deep Learning based on Auto-Encoder and Restricted Boltzmann Machine. Available online: https://thesai.org/Downloads/Volume9No1/Paper_3-Credit_Card_Fraud_Detection_Using_Deep_Learning.pdf (accessed on 23 February 2021). DL

[15] Gajula, S. (2025, December). Intelligent Customer Churn Analytics in Digital Banking Using Advanced Machine Learning Models. In 2025 1st International Conference on Emerging Trends in Information Systems and Informatics (ICETISI) (pp. 1-6). IEEE.

[16] Pourhabibi, T.; Ongb, K.L.; Kama, B.H.; Boo, Y.L. Fraud detection: A systematic literature review of graph-based anomaly detection approaches. Decis. Support Syst. 2020, 133, 113303. Fraud detection.

[17] Bhagwat, V. B. (2026). Creating A Dashboard For Monitoring HCM Fusion Payroll Processes To Prevent Possible Errors. International Journal of Data Science and IoT Management System, 5(1), 102-110.

[18] Podgorelec, B.; Turkanovi´c, M.; Karakati˘c, S. A Machine Learning Based Method for Automated Blockchain Transaction Signing Including Personalized Anomaly Detection. Sensors 2020, 20, 147. Anomaly detection.

[19] Gaddam, S. From Fixed Specifications to Self-Adapting Systems: A Machine Learning Perspective on Software Engineering.

[20] Srikanth Kavuri. (2024). Probabilistic Generative Modeling for Synthesizing High-Coverage Test Data in Safety-Critical Software

Applications. Computer Fraud and Security, 633–642. https://doi.org/10.52710/cfs.838.

[21] Puh, M.; Brki´c, L. Detecting Credit Card Fraud Using Selected Machine Learning Algorithms. In Proceedings of the 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia, 20–24 May 2019. Credit card fraud detection.

[22] Babburi, S. Lightweight Distributed Provenance Framework for Edge and IoT Data Systems.

[23] Xuan, S.; Liu, G.; Li, Z.; Zheng, L.; Wang, S.; Jiang, C. Random Forest for Credit Card Fraud Detection. In Proceedings of the 2018 IEEE 15th International Conference on Networking, Sensing and Control (ICNSC), Zhuhai, China, 27–29 March 2018. RF. [24] Huang, D.; Mu, D.; Yang, L.; Cai, X. CoDetect: Financial Fraud Detection with Anomaly Feature Detection. IEEE Access 2018, 6, 19161–19174. Financial fraud detection.