



Preventing Bank Fraud Using Intelligent Machine Learning Models

V. Ramya *, Dr. Nazimunnisa †

Email Correspondence*: v.ramya24@gmail.com

¹ PG Scholar, Department of Computer Science and Engineering, Sree Dattha Institute of Engineering and Science, Sheriguda, Ibrahimpatnam, Telangana 501510.

² Assistant Professor, Department of Computer Science and Engineering, Sree Dattha Institute of Engineering and Science, Sheriguda, Ibrahimpatnam, Telangana 501510.

Abstract:

The presence of vulnerabilities in banking systems has rendered us susceptible to fraudulent activities, resulting in significant financial and reputational harm for both clients and the bank. Financial institutions suffer substantial financial losses each year due to financial fraud. Early identification of this issue aids in mitigating fraudulent activities by formulating a proactive approach and recuperating any monetary damages incurred. This research introduces a machine learning methodology that has the potential to greatly assist in the precise identification of fraudulent activity. The use of AI-driven technique will expedite the process of verifying checks in order to combat counterfeiting and minimize the consequent harm. This paper provides a comprehensive analysis of many intelligence algorithms that were trained using a publicly available dataset. The objective was to determine the relationship between certain characteristics and the occurrence of fraudulent behavior. In this study, the dataset undergoes resampling to tackle the issue of class imbalance. Afterwards, the suggested method is used to assess the dataset in order to improve accuracy.

Keywords: Digital Signal Processing, Noise Suppression, Noise Estimation, Wiener Filtering, Speech Recognition.

1. Introduction

Future banks possess unique roles in contrast to their current counterparts. These changes have occurred due to alterations in infrastructures, services, persons, and skill sets. The only reason for this transformation is the incorporation of financial technology in the banking industry. Most banks possess the capacity to use state-of-the-art technology to provide financial services, therefore modifying the role of banking as intended. Emerging technologies such as blockchain, artificial intelligence (AI), big data, digital payment processing, peer-to-peer lending, crowdfunding, and robot advisors play vital role in enabling the delivery of financial services. What is the justification for these technological developments in banking? Due to continuous technological breakthroughs, the banking sector has been leading in the integration of new technologies into its operations to improve customer service. Nevertheless, the presence of financial crises has often impeded the advancement of these novel endeavors in the banking industry, resulting in a dearth of emphasis on innovation. Multiple developing technologies are now being praised as transformational tools that have the potential to overhaul the conventional banking sector, enhancing its user-friendliness

*PG Scholar, Department of Computer Science and Engineering, Sree Dattha Institute of Engineering and Science, Telangana.

†Assistant Professor, Department of Computer Science and Engineering, Sree Dattha Institute of Engineering and Science, Telangana.

and customer- centric approach. Nevertheless, there existed a extensively researched gap. The traditional banking system is also worried about the influence of technological improvements on customer relations, highlighting the need of trust and confidence in emerging technologies. Emerging FinTech enterprises are increasingly providing a disparity between the services provided by the bank and expectations and convenience of their clientele. Figure (1) depicts the several banking procedures that FinTech companies enable to improve customer experience via the use of AI technology [22]. Various researchers have diverse variety of products and services to banks in order to strengthen and improve technological help. P2P lending offers customers alternative loan possibilities beyond those now offered by traditional banks, while a robot advising platform offers users a variety of user-friendly solutions.

2. System Analysis

Currently, in the financial domain, fraud detection techniques generally depend on conventional approaches, such as rule-based algorithms or human verifications. Typically, these systems are responsive rather than proactive, since they detect fraudulent transactions only after they have already taken place. This might result in substantial financial losses and harm to the bank's image. Moreover, these systems have difficulties in terms of scalability and efficiency, particularly when dealing with substantial amounts of transaction data. A primary obstacle encountered by current systems is the substantial discrepancy between the number of fraudulent transactions and real ones, leading to a huge class imbalance in the data. This disparity presents challenges in precisely identifying fraud, leading to an increased probability of false negatives, when fraudulent behavior remains unnoticed. Generally, the current systems do not possess the necessary level of complexity and speed to successfully counter the advanced methods used by individuals engaged in fraudulent activities.

3. Proposed System

This paper proposes a machine learning methodology that leverages artificial intelligence (AI) to enhance the detection of fraudulent activities in financial systems, with the goal of addressing the shortcomings of existing fraud detection methods. The objective of the proposed system is to identify fraudulent transactions, with a special emphasis on check verification, in a manner that is efficient and automated. The purpose is to reduce the potential damage caused by fraud. The system employs a range of advanced algorithms that have been trained on a publicly accessible dataset including historical financial transaction data. To address the issue of class imbalance, the dataset is resampled to provide machine learning models in detecting fraudulent actions.

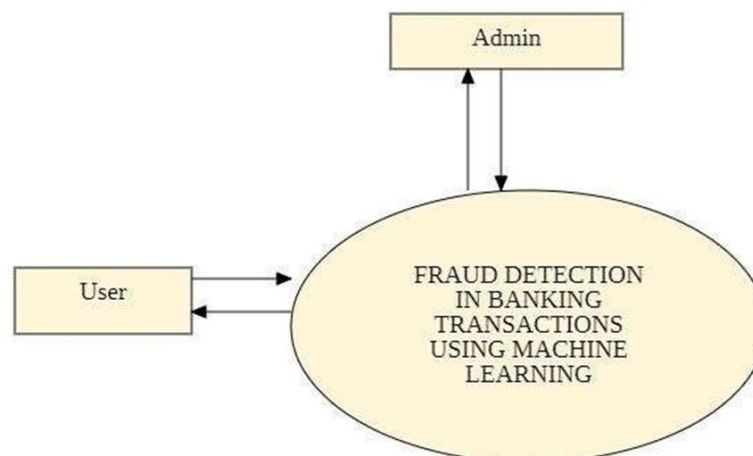


Figure-1 Proposed System

The AI model employs sophisticated algorithms to analyze the correlation between various factors and cases of fraud, enabling it to identify repeating patterns that might indicate fraudulent behavior. The proposed system provides a more balanced representation of both fraudulent and lawful transactions throughout the training phase. Resampling improves the accuracy and reliability of automates the detection process, leading to a faster, more efficient, and more precise method for identifying and reducing fraud in financial systems. This aids in mitigating financial losses and preserving the bank's image.

4. Screenshots

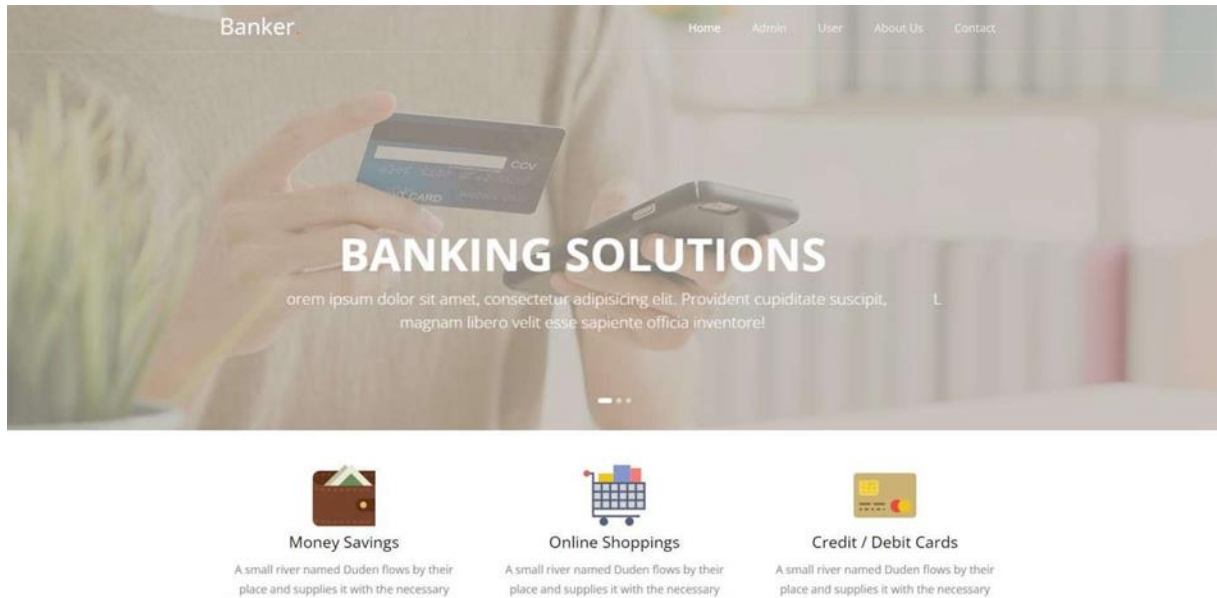


Figure-2 Homepage

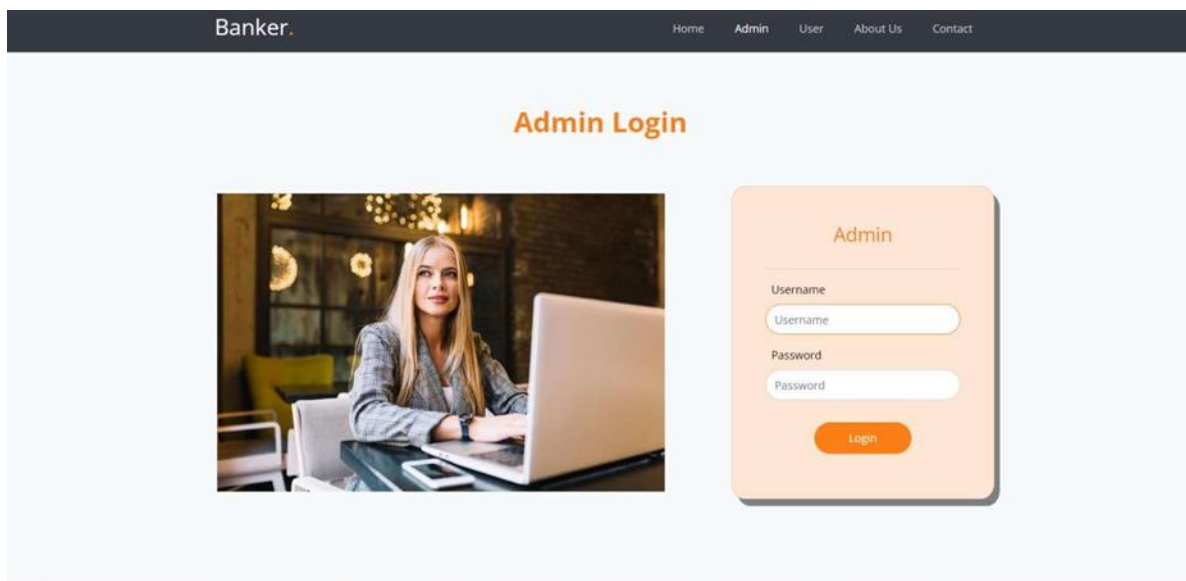


Figure-3 Admin Login

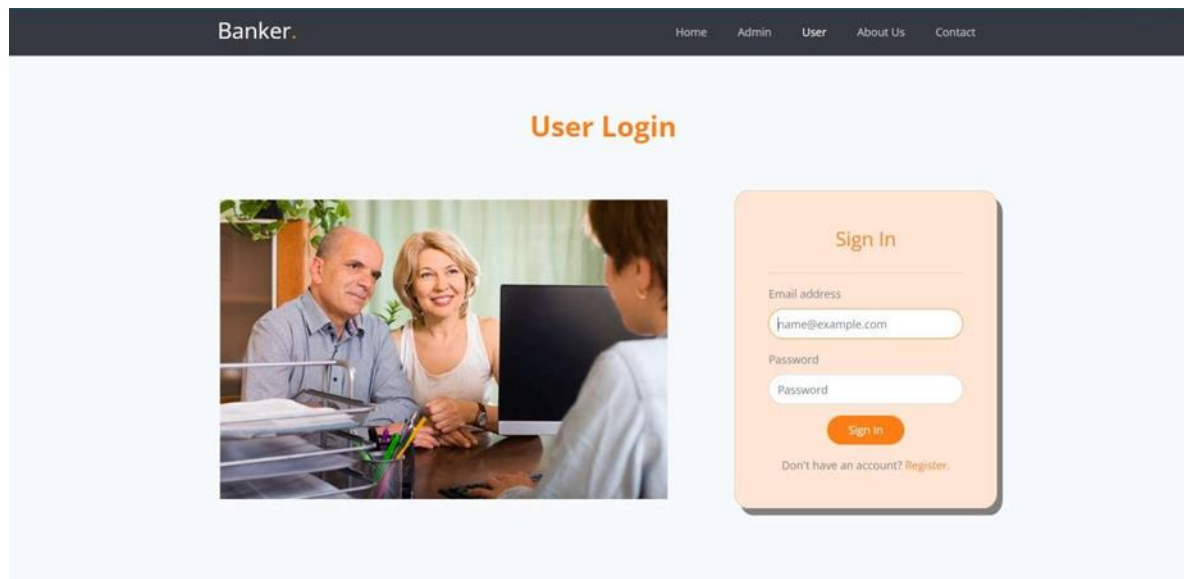


Figure-4 User Login



Figure-5 User Registration

5. Conclusion

This study proposes the use of machine learning methods to identify deceptive activities in banking applications. Analyzed the publicly accessible dataset provided by UCI. The dataset shown exhibits a significant imbalance, characterized by a prominent bias towards the majority of samples. The issue at hand is addressed by the synthetic minority over-sampling method (SMOTE). XGBoost effectively addresses the implementation challenges associated with KNN and Random Forest algorithms by using them as boosting techniques. The model had a precision accuracy of 97.74%. Upon analyzing the data, we

discovered that individuals between the ages of 19 and 25 have a higher propensity for engaging in fraudulent activities compared to other consumer demographic groups.

7. References

- [1] Rambola, R., Varshney, P., & Vishwakarma, P. (2018). Data mining techniques for fraud detection in banking sector. In 2018 4th International Conference on Computing Communication and Automation (ICCCA) (pp. 1–5). IEEE. <https://doi.org/10.1109/CCAA.2018.8777535>
- [2] Malini, N., & Pushpa, M. (2017). Analysis on credit card fraud identification techniques based on KNN and outlier detection. In 2017 Third International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB) (pp. 255–258). IEEE. <https://doi.org/10.1109/AEEICB.2017.7972424>
- [3] Sohony, I., Pratap, R., & Nambiar, U. (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) (pp. 289–294). Association for Computing Machinery. <https://doi.org/10.1145/3152494.3155681>
- [4] Wang, C., Wang, Y., Ye, Z., Yan, L., Cai, W., & Pan, S. (2018). Credit card fraud detection based on whale algorithm optimized BP neural network. In 2018 13th International Conference on Computer Science Education (ICCSE) (pp. 1–4). IEEE. <https://doi.org/10.1109/ICCSE.2018.8468855>
- [5] Benchaji, I., Douzi, S., & ElOuahidi, B. (2018). Using genetic algorithm to improve classification of imbalanced datasets for credit card fraud detection. In 2018 2nd Cyber Security in Networking Conference (CSNet) (pp. 1–5). IEEE. <https://doi.org/10.1109/CSNET.2018.8602972>
- [6] Awoyemi, J. O., Adetunmbi, A. O., & Oluwadare, S. A. (2017). Credit card fraud detection using machine learning techniques: A comparative analysis. In 2017 International Conference on Computing Networking and Informatics (ICCNI) (pp. 1–9).
- [7] Carcillo, F., Dal Pozzolo, A., Le Borgne, Y. A., Caelen, O., Mazzer, Y., & Bontempi, G. (2018). SCARFF: A scalable framework for streaming credit card fraud detection with Spark. *Information Fusion*, 41, 182–194.
- [8] Baader, G., & Krcmar, H. (2018). Reducing false positives in fraud detection: Combining the red flag approach with process mining. *International Journal of Accounting Information Systems*.
- [9] Ravisankar, P., Ravi, V., Raghava Rao, G., & Bose, I. (2011). Detection of financial statement fraud and feature selection using data mining techniques. *Decision Support Systems*, 50(2), 491–500.
- [10] Seeja, K., & Zareapoor, M. (2014). FraudMiner: A novel credit card fraud detection model based on frequent itemset mining. *The Scientific World Journal*, 2014, 1–10.
- [11] Tyagi, C., Parwekar, P., Singh, P., & Natla, K. (2020). Analysis of credit card fraud detection techniques. *Solid State Technology*, 63(6), 18057–18069.
- [12] Chee, C., Jaafar, J., Aziz, I., Hassan, M., & Yeoh, W. (2019). Algorithms for frequent itemset mining: A literature review. *Artificial Intelligence Review*, 52, 2603–2621.
- [13] Kiran, S., Guru, J., Kumar, R., Kumar, N., Katariya, D., & Sharma, M. (2018). Credit card fraud detection using Naïve Bayes model based and KNN classifier. *International Journal of Advance Research, Ideas and Innovations in Technology*, 4, 44–47.
- [14] Pumsirirat, A., & Yan, L. (2019). Credit card fraud detection using deep learning based on auto-encoder and restricted Boltzmann machine. *International Journal of Advanced Computer Science and Applications*, 9(1). https://thesai.org/Downloads/Volume9No1/Paper_3-Credit_Card_Fraud_Detection_Using_Deep_Learning.pdf

8. Conflict of Interest

The authors declare that there are no conflicts of interest regarding the publication of this article.

9. Funding

No external funding was received to support or conduct this study.