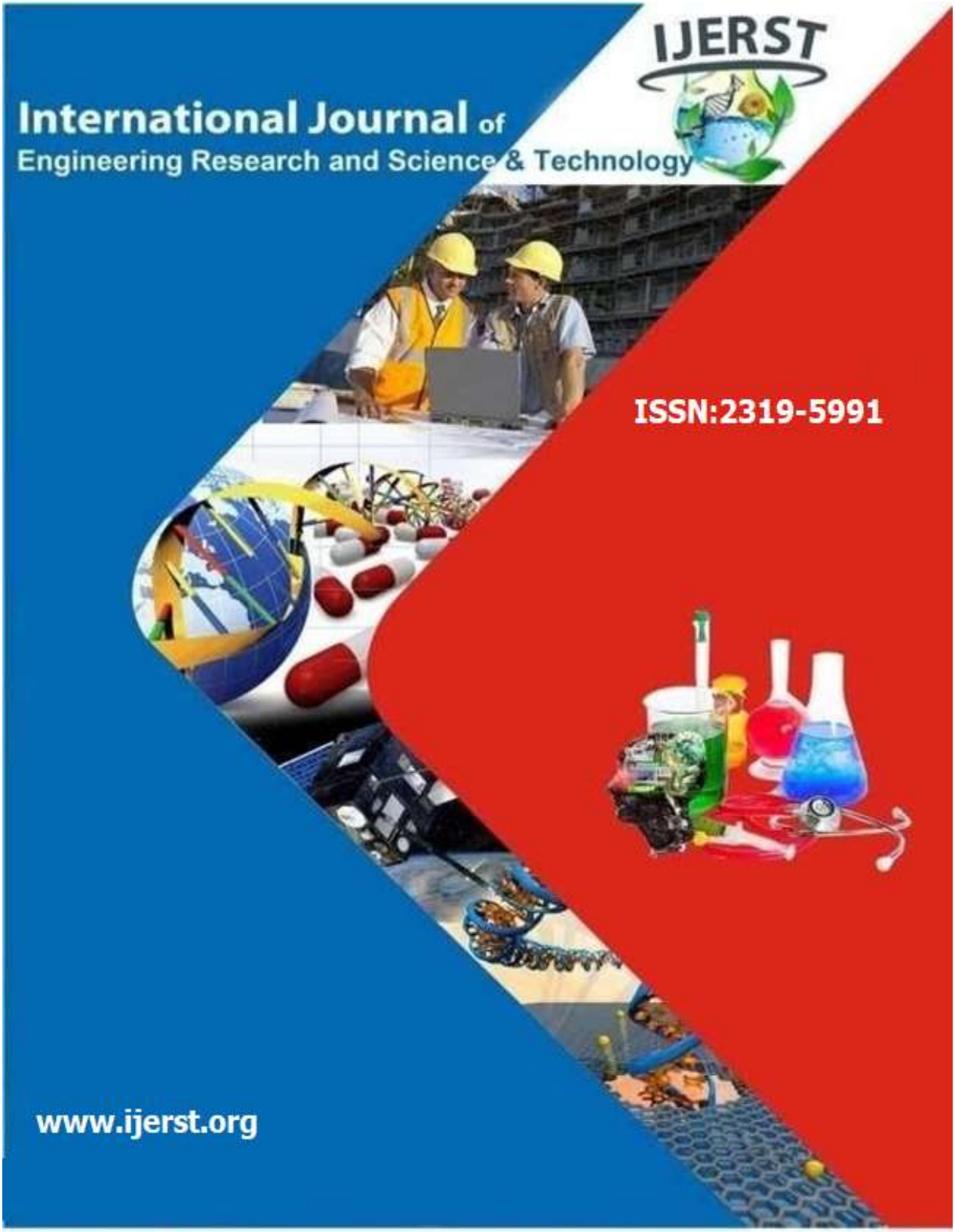

E-mail: editor@ijerst.org or ijerst.editor@gmail.com

ISSN 2319-5991 www.ijerst.com

Vol. 21, Issue 2, 2025

FRAUD DETECTION IN BANKING TRANSACTIONS USING MACHINE LEARNING

1Dr. T. CHARAN SINGH, 2J. MANOJ KUMAR, 3S. SAI KEERTHI

4K. SHIVA, 5V. SAICHARAN NAIK

1Associate Professor, Department of CSIT, Sri Indu College of Engineering and Technology-Hyderabad

2345Under Graduate, Department of CSIT, Sri Indu College of Engineering and Technology-Hyderabad

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

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, 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. This gap was a research topic for many researchers. The traditional banking system is also varied about

ISSN 2319-5991 www.ijerst.com

Vol. 21, Issue 2, 2025

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.

II. LITERATURE SURVEY

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 like 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 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: "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

ISSN 2319-5991 www.ijerst.com

Vol. 21, Issue 2, 2025

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.

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: "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. 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.

III. SYSTEM ANALSIS

EXISTING SYSTEM

- In case of bank fraud detection, the existing system is detecting the fraud after fraud has been happen. Existing system maintain the large amount of data when customer comes to

know about inconsistency in transaction, he/she made complaint and then fraud detection system start it working. It first tries to deZtect that fraud has actually occur after that it transactions that was used to fraud detection mechanism developed by master and visa cards.

- A machine learning paradigm classification, with Bank Fraud Detection being the base.
- Intrusion detections to track fraud location and so on. In case of existing system there is no confirmation of recovery of fraud and Customer satisfaction.

ISSN 2319-5991 www.ijerst.com

Vol. 21, Issue 2, 2025

- Secure electronic system used to analyze the behavior of legitimate users.
- Data Mining mechanisms to classify and preprocess the user's data.

DISADVANTAGES

- Each payment system has its limits regarding the maximum amount in the account, the of transactions per day and the amount of output.
- If Internet connection fails, you cannot get to your online account.
- If you follow the security rules the threat is minimal. The worse situation when the of processsing company has been broken because it leads to the leak of personal data on and its owners.
- The information about all the transactions, including the amount, time and recipient are stored.
- In the database of the payment system. And it means the intelligence agency has access this information. Sometimes this is the path for fraudulent activities.
- Imbalanced Datasets: Imbalance in the distribution of normal and fraudulent transactions can pose challenges. The model may be biased towards the majority class, leading to lower accuracy in detecting the minority (fraudulent) class.
- Dynamic Nature of Fraud: Fraud patterns evolve over time, and models may struggle to adapt to new types of fraudulent activities that were not present in the training data. Continuous model monitoring and updating are crucial.
- False Positives and Negatives: Striking a balance between minimizing false positives (genuine transactions flagged as fraudulent) and false negatives (fraudulent transactions not detected) is challenging but crucial for a successful fraud detection system.
- Regulatory Compliance: Adhering to regulatory requirements and compliance standards in the banking sector is essential. Ensuring that the model meets legal and ethical guidelines is a significant consideration.
- Adversarial Attacks: Fraudsters may attempt to manipulate the system by understanding its weaknesses. Developing models robust to adversarial attacks is an ongoing challenge.

PROPOSED SYSTEM

The proposed system aims to enhance fraud detection in banking transactions through the implementation of a machine learning-based approach. The motivation for this system lies in addressing the vulnerabilities within banking systems that expose both customers and financial institutions to fraudulent acts, causing substantial financial loss and damage to reputation. The goal is to enable early detection of fraudulent activities, allowing for the development of effective counter-strategies and recovery plans.

Key Components of the Proposed System:

- Machine Learning Algorithms: The system incorporates various intelligent machine learning algorithms. These algorithms are trained on a carefully selected dataset that includes both genuine and fraudulent transactions. The choice of algorithms is critical in identifying patterns and correlations associated with fraudulent activities.

ISSN 2319-5991 www.ijerst.com

Vol. 21, Issue 2, 2025

• Data Analysis and Correlation: Extensive data analysis is conducted on the dataset to identify correlations between specific factors and fraudulent transactions. The system leverages artificial intelligence (AI) to analyze the data efficiently, speeding up the verification process and enhancing the accuracy of fraud detection.

• Resampling Techniques: To address class imbalance within the dataset, the proposed system employs resampling techniques. This helps mitigate the challenges associated with an uneven distribution of normal and fraudulent transactions, ultimately improving the model's ability to detect fraud accurately.

• Counterfeit Check Verification: A significant feature of the proposed system is its ability to counteract counterfeit transactions. The AI-based model is designed to expedite the verification process, thereby reducing the impact of counterfeit activities and minimizing potential damage.

• Model Training and Accuracy: The system undergoes rigorous training using the resampled dataset and employs the proposed algorithm to enhance accuracy. The goal is to create a robust and reliable model capable of effectively differentiating between genuine and fraudulent transactions.

• Adaptability and Speed: Recognizing the dynamic nature of fraud, the proposed system is designed for adaptability. It can evolve and learn from emerging fraud patterns, ensuring that it remains effective in the face of evolving threats. The emphasis on speed in check verification is crucial for real-time fraud detection.

Expected Benefits:

• Early Fraud Detection: The proposed system aims to detect fraudulent transactions at an early stage, allowing for prompt intervention and mitigation strategies.

• Improved Accuracy: Through the utilization of advanced machine learning algorithms and careful dataset preprocessing, the system is expected to achieve higher accuracy in identifying and classifying fraudulent activities.

• Reduced Damage and Losses: By accelerating the check verification process and countering counterfeits, the system contributes to minimizing the financial losses incurred by both customers and the banking institution.

• Enhanced Trust and Reputation: Successful implementation of the proposed system contributes to building and maintaining trust among customers and stakeholders, safeguarding the reputation of the banking institution.

ADVANTAGES

• To eliminate real time fraud to the lowest level.

• To increase the confidence of customers in the banking system especially for online transactions.

• To deter both current and potential fraudsters.

• Early Fraud Detection: The system's utilization of advanced machine learning algorithms enables the early detection of fraudulent transactions. This early identification allows for timely intervention and the implementation of counter-strategies,

ISSN 2319-5991 www.ijerst.com

Vol. 21, Issue 2, 2025

mitigating potential financial losses and reputational damage.

• Improved Accuracy and Precision: Through rigorous training on a carefully selected and resampled dataset, the proposed system is expected to achieve higher accuracy and precision in distinguishing between genuine and fraudulent transactions. This accuracy reduces false positives and negatives, providing a more reliable fraud detection mechanism.

• Efficient Counterfeit Check Verification: The incorporation of artificial intelligence in the system expedites the check verification process, specifically countering counterfeit transactions. The increased speed in verification enhances the system's ability to identify and prevent fraudulent activities in real-time, reducing the potential damage caused by counterfeits.

• Enhanced Customer and Stakeholder Trust: Successful implementation of the proposed system contributes to building and maintaining trust among customers and stakeholders. The system's ability to protect against fraudulent activities safeguards the financial interests of customers and reinforces the reputation of the banking institution, fostering a sense of security and confidence.

IV. IMPLEMENTATION AND RESULTS

MODULE DESCRIPTION

Fraud Detection in Banking Transactions Processor:

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

• Model Evaluation and Continuous Monitoring: 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.

View and Authorize Users (Admin)

In this module, the admin can view the list of users who all registered. In this, the admin can view the user’s details such as, user name, email, address and admin authorizes the users.

Online User: In this module, there are n numbers of users are present. User should register before doing any operations. Once user registers, their details will be stored to the database. After registration successful, he

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

Vol. 21, Issue 2, 2025

has to login by using authorized user name and password. Once Login is successful user will do some operations like REGISTER AND LOGIN, Predict Fraud in Banking Transactions Status, VIEW YOUR PROFILE.

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 SCOPE

1. Enhanced Model Accuracy with Advanced Algorithms: Future research can focus on developing hybrid machine learning models that combine deep learning and ensemble techniques to improve fraud detection accuracy and minimize false positives.
2. Real-time Fraud Detection Systems: Implementing AI-driven real-time transaction monitoring can help detect fraudulent activities instantaneously, reducing financial losses and improving customer trust.
3. Cross-Bank Data Sharing for Fraud Prevention: A collaborative fraud detection

ISSN 2319-5991 www.ijerst.com

Vol. 21, Issue 2, 2025

framework across multiple banks using federated learning can help in identifying patterns across institutions while preserving data privacy.

4. Application of Generative AI for Synthetic Fraud Analysis: The use of generative models to create synthetic fraudulent data can help improve fraud detection models by training them on more diverse fraud scenarios.

5. Adaptive Learning Models for Evolving Fraud Tactics: Self-learning AI models that continuously adapt to new fraud patterns can improve fraud detection by keeping up with the ever-evolving tactics of fraudsters.

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. C. Wang, Y. Wang, Z. Ye, L. Yan, W. Cai, and S. Pan, “Credit Card Fraud Detection Based on Whale Algorithm Optimized BP Neural Network,” 2018 13th International Conference on Computer Science Education, Colombo, 2018, pp. 1-4, doi: 10.1109/ICCSE.2018.8468855.

3. ssFabrizio Carcillo, Andrea Dal Pozzolo, Yann-A¨el Le Borgne, Olivier Caelen, Yannis Mazzer, and Gianluca Bontempi. Scarff: a scalable framework for streaming credit card fraud detection with spark. Information Fusion, 41:182–194, 2018.

4. 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.

5. Ravisankar P, Ravi V, Raghava Rao G, and Bose, Detection of financial statement fraud and feature selection using data mining techniques, Elsevier, Decision Support Systems Volume 50, Issue 2, p491-500 (2011) SVM.

6. C. Chee, J. Jaafar, I. Aziz, M. Hassan, and W. Yeoh, “Algorithms for frequent itemset mining: a literature review,” Artificial Intelligence Review, vol. 52, 2019, pp. 2603–2621. Litrature review AI.

7. 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.

8. Lucas, Y.; Jurgovsky, J. Credit card fraud detection using machine learning: A survey. arXiv 2020, arXiv:2010.06479. Credit card fraud.

9. 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.