2023 International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE) | 978-1-6654-9260-7/23/$31.00 ©2023 IEEE | DOI: 10.1109/IITCEE57236.2023.10091067

Fraud Detection in Banking Transactions Using Machine Learning

Rathnakar Achary[1]
Alliance College of Engineering and Design
Alliance University, Bangalore, India
[1]rathnakar.achary@alliance.edu.in

Chetan J Shelke[2]
Alliance College of Engineering and Design
Alliance University, Bangalore, India
[2]chetan.shelke@alliance.edu.in

***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.**

Keywords – Credit card fraud, fraudulent transactions, KNN classifier, Random Forest, XGBoost, Blockchain, Artificial intelligence

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 [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.

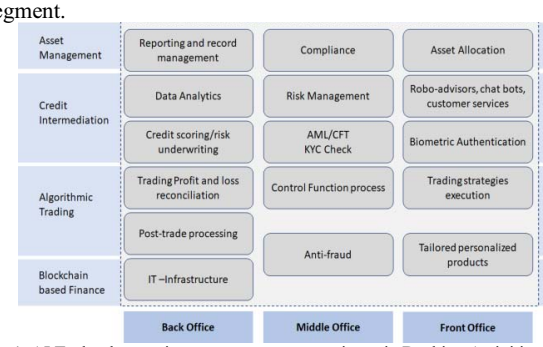


Fig.1. AI Technology to improve customer experience in Banking Activities

AI-powered chatbots that mimic human conversation and messaging apps are replacing the activities of the backend services in call centers. Biometric data and iris scanning are used as an alternative to passwords and tokens used for transactions. The other technologies enabled with FinTech are IoT, wearable technologies and ben-in-banking are common things in day-to-day banking operations, most of them with gamification service to the end users. To service their customers, banks today need to change their mode of service. By adopting advanced technologies, they may succeed in the evolution of the banking industry and embed them in their operations as their culture and innovation across the organization. This has consequences in many folds. The City bank analysis represents that, for the next 10 years 30% of the bank jobs will disappear. Some research estimated this job loss will be more than 50%. This has a consequence for many financial institutions across the globe. It is not just a job loss, but also connected with several economic aspects around it, like accounting firms, law firms, hotels, and services businesses. The profiles of the new jobs created in the FinTech industry are very small in number, but they are entirely different with very different skill sets. Those are very essential for today's banking systems. Considering all the above-said challenges in banking one of the common challenges faced by most of the banks today are fraudulent transactions and malicious behavior of the users. The fraudulent transaction is a rising challenge for the banking industry with an estimated financial loss and damage to the reputation. This survey report presents that about 56% of the fraud in banking is only reported [15]. It clearly indicates that a better fraud detection

model is of paramount requirement in most banks either small or big in size.

This research work aims to design an intelligent system with a machine learning model, that will be predictive and adaptive to detect the fraudulent activities of the customer in banking transactions. The paper is structured with the following sections. In section II we described the literature review with the related work completed by other researchers and in section III technological impact on banking and the digital revolution in India. Section IV describes the role of AI in risk management and governance and section V, the fraud analysis using machine learning algorithms followed by a conclusion.

II. LITERATURE REVIEW

Statistical methods can be used for fraud detection. Here the statistical distribution of the dataset is analysed for anomalous behavior of the fraudulent by using Linear Discriminant Analysis and Logistic regression [1]. The authors used a variety of data mining techniques in real-time fraud detection using historical data [1]. The research work [2] describes the methods to detect fraud by using KNN algorithm and outlier finding mechanism. The model helps in the detection of malicious behavior of the fraudulent. The authors in [3] used an ensemble technique including the Random Forest model to analyze the normal transactions and compare the performance of the fraudulent transaction detection method by neural networks. Fraud detection in [4] presented the method for credit card transactions and analyzed the data using Wale-algorithm optimized backpropagation. The authors in [4][6] have analyzed already classified results for detecting credit card fraud using an imbalanced dataset. K means clustering is used for sampling groups of fraudulent transaction samples. Authors also used genetic algorithms for group fraudulent transactions. The researcher used multiple machine learning algorithms such as KNN, Logistic regression, and Naïve Bayes for analyzing the available dataset. An enhanced study of this has demonstrated, the represents that KNN outperforms the other two methods [2][6]. The performance was assessed by precision, recall, Mathew correlation coefficient, and balanced classification rate specificity. A unique fraud detection technique is proposed in [7] using Big data technology with a new method known as Scalable Real-time Fraud Finder (SCARFF) using different data analysis tools such as Spark, Cassandra, and Kafka. Real-time data analysis is possible with a large amount of transaction data. The advantage of this system proposed holds higher accuracy, fault tolerance, and scalability. In [8] the researcher presented a feature engineering method to minimize the number of false positive rates, that are normally used in the anomaly-detecting algorithm [16].

III. TECHNOLOGICAL IMPACT ON BANKING

Figure (2) shows a global banking technology radar, these disruptive technologies will shape the future of banking. The different cutting-edge technologies are pivotal for today's banking system. Augmented reality: to enhance customer experience, Blockchain: enable multiple parties to access the same data simultaneously using distributed ledger[18]. Robotic process automation: to mimic human action and judgment but at a higher speed, scale, and quality. Quantum computing: to work out complex current complex data operations. Artificial intelligence: to make a better decision even by using historical data. API platforms: designed to work through API when a front-end experience is connected to backend execution. Prescriptive Security: to analyze the early visibility of threats and cyber-attacks. Hybrid cloud: Designed to allow the bank to offer innovative new offerings to its customers. Instant payment: to provide ubiquitous online transactions. The AI in financial services initiative sets out to explore the multiplicative impacts of emerging technologies.

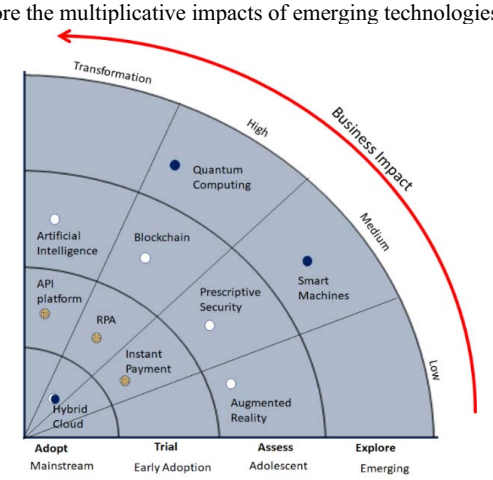
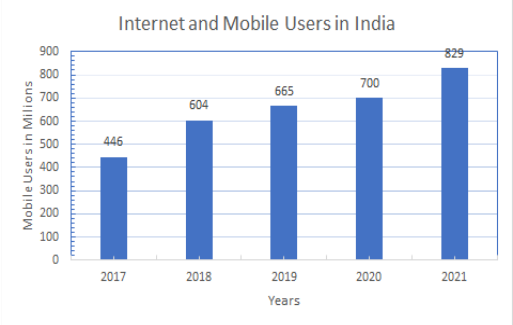


Fig.2. Global banking technology radar

A. India Digital Revolution

With the momentum of the digital revolution in the world, India also gained a defining momentum. It was estimated that the growth in the digital sector is estimated to double in 2025. Complete digitalization is expected to faster world spread economic growth and enhance employability through incremental value addition across various industrial sectors, such as manufacturing, healthcare, education, and logistic. In the last decade, there is a significant change in the field of digitalization in India. This technological disruption has been enabled by massive growth in the IT sector and the demography of the end users. The country has witnessed the world's second-largest digital ecosystem with 700 million internet users and is estimated to reach up to 829 million by the end of 2021 and an equal number of mobile users.



Source: Ministry of Electronics and IT

Fig.3. Internet and Mobile users in India

This rapid shift is due to the catalytic role played by the Government in moving its services to digital platforms. Some of the key achievements of this are India becoming the second fastest digital adopter among the top 17 digital economies, e-governance and digital identities, e-commerce growth and penetration of mobile internet access, growth of mobile and internet access, and adoption of digital media by citizens. With a faster pace of changes, there is exponential growth in the

county's digital economy which is almost doubled by 2020 as compared to 2017 and is expected to become a USD 5 trillion in 2024 and a leap of USD 1 trillion by 2025.

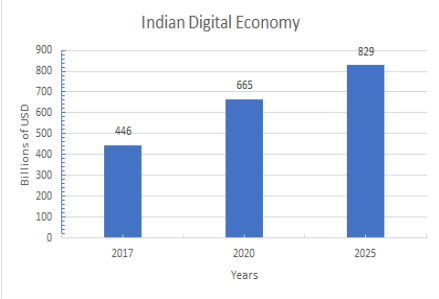


Fig.4. Indian Digital Economy

The concept of AI in banking applications will emulate human capabilities to demonstrate a higher level of intelligence and accuracy. Its impact on the banking sector is analyzed on three levels.

i. The process the bank adopts

ii. The different banking services and products provided to its customers.

iii. The user experiences the bank offers to their customers and employees.

Nealy 75% of the leading banks with a financial capacity over USD 100 billion are started implementing AI on a massive scale, compared to the banks with a financial capacity of less than USD 100 billion.

B. Artificial intelligence

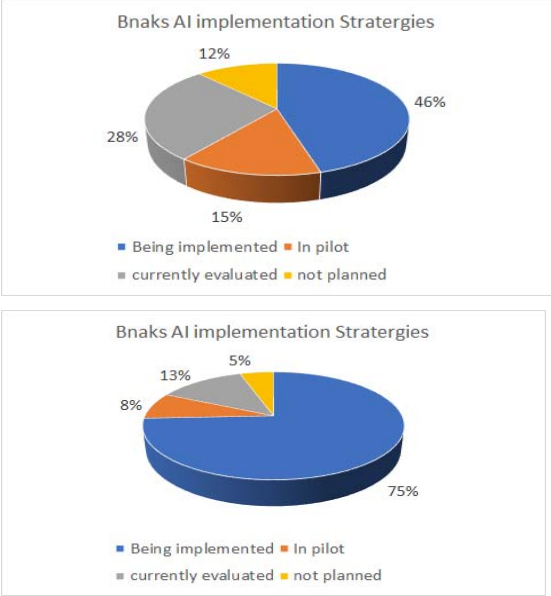


Fig.5. Asset Size – Above USD 100 Billion

A survey report from Microsoft Asia and IDC Asia-pacific study to the Financial Services Industry (FSI) found that 41% of the banks have started observing the competition three years after adopting AI and another 52% have initiated the AI implementation. These banks implementing AI-based systems in different domains already started to see an improvement of nearly 17% to 26% in better customer engagement, higher margin, higher competitiveness, and better management. As a result of this there is a significant amount of cost saving, which is estimated at about USD 447 billion in 2023, by the implementation of AI applications in front-end, back-end, and middle-end operations as 45%, 7%, and 50% respectively. The frontend operation includes a customer interface, personalized services, user authentication, and validations and wealth management. Back-end operations aim to signify the backend process, business and strategy insights, and regulating compliances.

The middle layer operation does crucial tasks such as the detection of fraudulent behavior of the customers, risk identification and mitigation, AML, loan approval, and KYC verification. Figure (6) indicates the four major areas that benefitted from the use of AI (USB evidence lab).

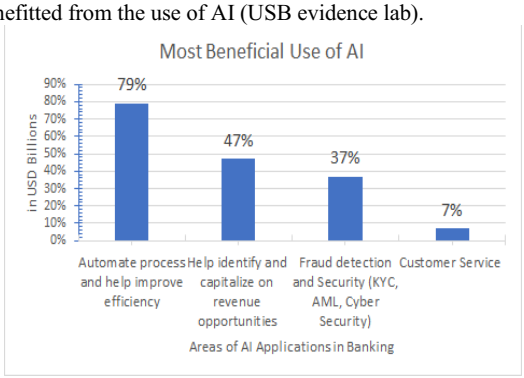


Fig.6. Four Major Areas Benefited by using AI

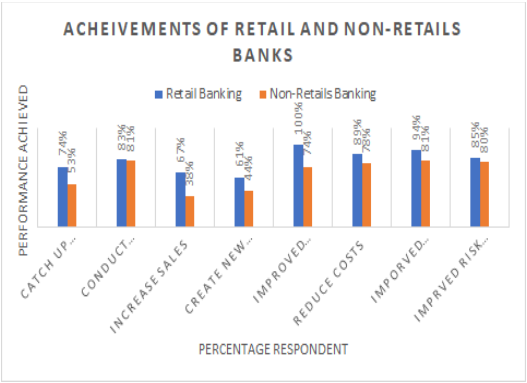
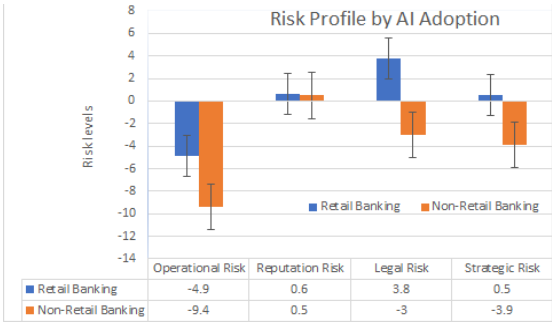


Fig.7. Retails and Non-Retail Banks

To develop a banking solution using AI or its subset machine learning, which uses historical data to make predictions or to make decisions with the help of programming modules such as *Keras*, *Tensorflow*, Pandas, and *Numpy*. These machine learning technologies generally use data generated by normal business operations [25], which may be structured or unstructured in nature to generate an accurate result. The research report represents that the major reason for the implementation of AI is, it enables the banking solution a key driver for both retail and non-retail banking for improving their risk management and improving customer experience. In retail banking, the main implementation of AI is for KYC verification and AML investigation of the OPEX and maximizing the performance. The survey report also indicates that 80% of the retail and non-retail banks achieved their intended tasks as mentioned above. Figure (7) indicates the accomplishment of bank objectives after AI implementation.

IV. ROLE OF AI IN RISK MANAGEMENT AND GOVERNANCE

There are other potential benefits and opportunities provided by AI implementation. Consequently, there are challenges that need to be properly managed. Analysis shows that the main risks faced by retail banks by the quality of the data used for analysis, and the confidentiality of the data taken from the data store for analysis. No AI model can result from better accuracy unless the quality of the data considered for analysis is appropriate and reliable. To protect the privacy of the customer data a high level of confidentiality is to be maintained during the data analysis. Validation of the model uses is also another important requirement to achieve better performance and a high degree of interoperability to gain support from management and regulators. More adaptation of AI applications in banking operations leads to new challenges in the areas of operational, legal reputation, and strategies. The level of these risks is different for different types of banking services. Some of the retail banks believe that the implementation of AI may substitute human operators, and may add legal risks, but its impact on the reputation may be minimal.



	Operational Risk	Reputation Risk	Legal Risk	Strategic Risk
Retail Banking	-4.9	0.6	3.8	0.5
Non-Retail Banking	-9.4	0.5	-3	-3.9

Fig.8. Risk profile by AI adoption in banks

V. FRAUD ANALYSIS

Most banks adopt traditional rule-based methods of fraud analysis. Today due to the availability of advanced technologies the number of fraudsters is increasing, which is also an increased threat level to the banking industry. Fraud patterns are changing due to inconsistency in the banking systems. Fraud detection is possible with a valuable dataset and a high-performance machine learning algorithm. The data are gathered from a public dataset and categorized, based on these we can classify the users as benign or fraudulent. Figure (9) gives the details about the fraud detection and prevention market size in 2016 – 2022, worldwide. Many statistical and machine learning models are used to analyze the fraudulent and non-fraudulent in each dataset. In this paper, we analyze popular statistical and machine-learning methods for the detection of a fraudulent transactions.

The most popular among these is Benford's law for modeling and the other machine learning modules for classification and binary decision trees [12]. These models help to determine benign and fraudulent transactions.

A. Benford's law

This law is used to determine patterns in a particular set of transactions or datasets[19]. Using this dataset can detect fraudulent transactions or anomalies. In Benford's law, the universal value of the data depends on the units. If there exists a universal probability distribution P(x), then it must be invariant under a change of scale as

$$P(k\,x) = f(k)P(x)$$

If $\int P(x)dx = 1 \quad then \int P(k\,x)dx = \frac{1}{k}$

Normalization denotes $f(k) = \frac{1}{k}$

Differentiating with respect to k and setting k = 1, we get $xP^1(x) = -P(x)$ with the solution $P(x) = \frac{1}{x}$

This does not represent the proper probability distribution. The distribution of the first digit is shown as a percentage in figure (10). The frequency of the first digits follows the logarithmic relations as

$$Fa = log\left(\frac{a+1}{a}\right)$$

Fa is the frequency of the digit 'a' in the first place of used number. Table (1) gives the observed and computed frequencies.

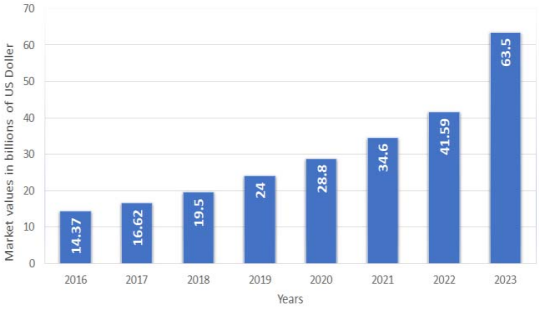


Fig.9. Fraud detection and prevention market worldwide

The probability of the first digit D is given by a logarithmic distribution

$$P_D = \frac{\int_D^{D+1} P(x)dx}{\int_1^{10} P(x)dx} = log_{10}\left(1+\frac{1}{D}\right)$$

For D = 1, ……., 9 For the second digit it is represented as

$$P_{D=D2} = \sum_{D1=1}^{9} log_{10}\left[1+\left(\frac{1}{D1\,D2}\right)\right]$$

$D2$ = 1, ……., 9 and so on

When plugging in the digits 1 through 9, each subsequent digit has a diminishing probability that it will be the leading digit with 1 being the most common and 9 being the least.

Benford's law is widely used in executing accounting transactions and detecting fraud. Using Benford's curve income statement, general ledger, and inventory listing can be assessed and compared to the curve to determine its genuineness.

B. Machine learning classification algorithm

Under machine learning determining whether the transaction is fraudulent or benign is considered a classification problem. Different machine learning algorithms play a crucial role in fraud detection[21]. This includes Logistic regression, *k*-nearest neighbor algorithms, Random Forest (RF) Classifier, Support Vector Machine (SVM), and Naïve Bayes classifier. Among this algorithm it was found that Naïve Bayes classifier got the best accuracy. The comparative analysis of these classification algorithm is given in the figure (11).

C. Dataset

In this analysis of fraud detection, we used UCI dataset with balanced features like customer ID and the demographics details such as Customers' origin referring to zip code, type of the customer, age, gender, category, and amount of purchase when committed the crime. To avoid the imbalance in the

dataset one can, perform oversampling or undersampling. We perform an exploratory data analysis on the dataset to capture its features. In data cleansing, the available categorical features are transformed into numerical values. An oversampled technique called SMOTE (Synthetic Minority Over-sampling Technique) is used here. It will create new data points from the minority class using the neighbour instances so that generated samples are not biased and the base accuracy score will improve.

Number interval	Observed frequency	Logarithmic interval
1 to 2	0.306	0.301
2 to 3	0.185	0.176
3 to 4	0124	0.125
4 to 5	0.094	0.097
5 to 6	0.080	0.079
6 to 7	0.064	0.067
7 to 8	0.051	0.058
8 to 9	0.049	0.051
9 to 10	0.047	0.046

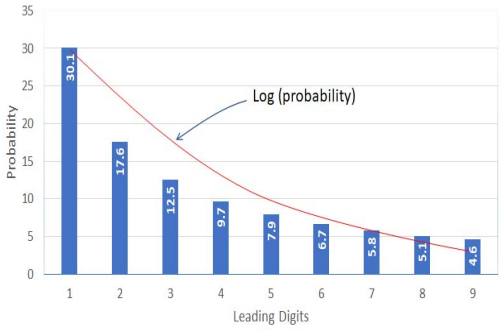


Fig.10. Observed and Computed Frequencies. Frad detection using leading digits in Benford's law

Sl. No.	Algorithms	Accuracy
01	Logistic Regression	89.34%
02	K-nearest neighbors	93.45%
03	Support vector machine	94.89%
04	Decision Tree	96.81%
05	Random forest classifier	97.50%
06	Naïve Bayer's classifier	98.23%

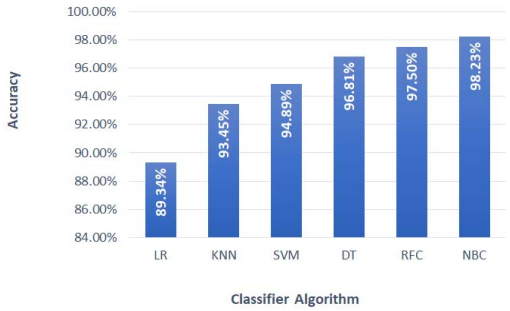


Fig.11. Classification Algorithms and their Accuracy

The KNN algorithm identifies similar things that exist in proximity[2]. The data points are closer to each other. The similarity can be calculated based on the distance functions such as Euclidean for the continuous variable as

$$d(x,y) = \sqrt{\sum_{i=1}^{m}(x_i - y_i)^2}$$

The distance between the training data and the test data is obtained from the above equation, also then the k values related to the test data. Similarly, the distance between all the training cases with new value are calculated the in terms of distance.

Fig. 12. Age versus Fraud

Random forest – RF is an ensemble classifier used in this both for classification and regression task. It involves the concept of bagging method, which is a collection of many weak learners. In RF they are considered as decision trees. One of the constraints of a decision tree is that they perform better for part of the dataset, but with a high variance due to greedy approaches of the model, because of this the approach may continuously select the best split at each level and it may not consider the current level. As a result of this there is a chance of overfitting. With this the performance of the model is better in training data and low in test data.

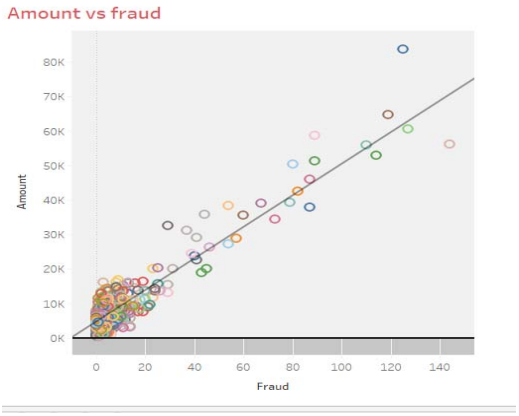


Fig. 13. Fraud Amounts

In RF this problem can be mitigated by using the bootstrapping method. In which the training data are trained randomly, where a different subsample of the data is used to train each decision tree. XGBoost – XGBoost is a gradient-

boosting algorithm used in the research, which combines a weak learner with a strong learner. In which the multiple iterations involved to process the weak learner and predict the value of the class labels and, then calculate the loss. This process repeats until a certain threshold, hence known as gradient decent optimization problem or gradient boost. XGBoost is such as gradient boosting technique minimizing the overfitting. Its speed of processing is much faster due to parallel processing than conventional gradient boosting.

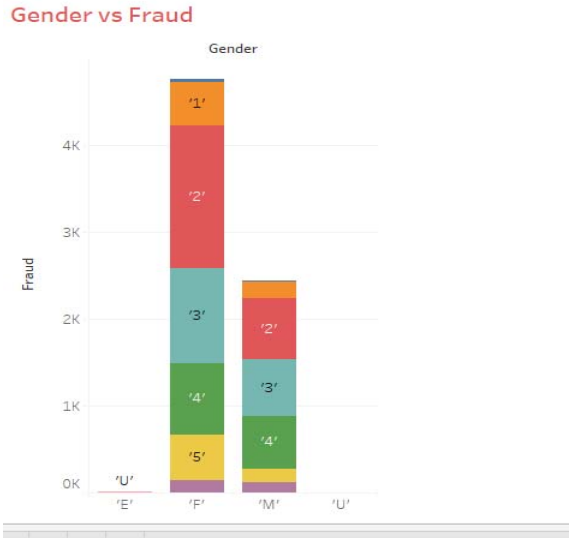


Fig 13. Fraud based on gender

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.

REFERENCE

[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] N. Malini and M. Pushpa, "Analysis on credit card fraud identification techniques based on KNN and outlier detection," 2017 Third International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB), Chennai, 2017, pp. 255-258, doi: 10.1109/AEEICB.2017.7972424.

[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] 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 (ICCSE), Colombo, 2018, pp. 1-4, doi: 10.1109/ICCSE.2018.8468855

[5] I. Benchaji, S. Douzi and B. ElOuahidi, "Using Genetic Algorithm to Improve Classification of Imbalanced Datasets for Credit Card Fraud Detection," 2018 2nd Cyber Security in Networking Conference (CSNet), Paris, 2018, pp. 1-5, doi: 10.1109/CSNET.2018.8602972.

[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] Fabrizio 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.

[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] 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

[10] K. Seeja, and M. Zareapoor, "FraudMiner: A Novel Credit Card Fraud Detection Model Based on Frequent Itemset Mining," The Scientific World Journal, 2014, pp. 1-10. KNN, SVM

[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] 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

[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] PwC's Global Economic Crime and Fraud Survey 2020. Available online: https://www.pwc.com/fraudsurvey (accessed on 30 November 2020). Fraud surver.

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

[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] Synthetic Financial Datasets for Fraud Detection. Available online: https://www.kaggle.com/ntnu-testimon/paysim1 (accessed on 30 November 2020). Fraud detection.

[20] Ma, T.; Qian, S.; Cao, J.; Xue, G.; Yu, J.; Zhu, Y.; Li, M. An Unsupervised Incremental Virtual Learning Method for Financial Fraud Detection. In Proceedings of the 2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA), Abu Dhabi, United Arab Emirates, 3–7 November 2019; pp. 1–6. Financial fraud detection.

[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] Ryman-Tubb, N.F.; Krause, P.J.; Garn, W. How Artificial Intelligence and machine learning research impacts payment card fraud detection: A survey and industry benchmark. Eng. Appl. Artif. Intell. 2018, 76, 130–157. Credit card fraud detection.

[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.

[25] Amarasinghe, T.; Aponso, A.; Krishnarajah, N. Critical Analysis of Machine Learning Based Approaches for Fraud Detection in Financial Transactions. In Proceedings of the 2018 International Conference on Machine Learning Technologies (ICMLT'18), Nanchang, China, 21–23 June 2018; pp. 12–17. Machine learning for fraud detection