Machine Learning Perspective: Fraud Payment Transaction Detection

Nishant Upadhyay[1], Yogesh Singh Rathore[2], Nidhi Bansal[3,*], Sushant Jhingran[1], Gaurang Chaudhary[4], Sudhanshu Maurya[5,*], Rekha Chaturvedi[6,*] and Kritika Soni[3]

[1]*Department of Computer Science and Engineering, School of Engineering and Technology, Sharda University, Greater Noida, U.P. India*
[2]*Department of Computer Science and Application, School of Engineering and Technology, Sharda University, Greater Noida, Uttar Pradesh, India*
[3]*Department of Computer Science & Engineering, School of Engineering and Technology, Manav Rachna International Institute of Research and Studies (Deemed to be University), Faridabad, Haryana, India*
[4]*Computer Science and Artificial Intelligence, Amrita Vishwa Vidyapeetham, Bangalore, Karnataka, India*
[5]*Symbiosis Institute of Technology, Nagpur Campus, Symbiosis International (Deemed University), Pune, India*
[6]*Department of Data Science and Engineering, School of Information Security and Data Science, Manipal University Jaipur, Jaipur Rajasthan, India*
E-mail: nidhi18jul@gmail.com; dr.sm0302@gmail.com; rekha.chaturvedi@jaipur.manipal.edu
[*]*Corresponding Authors*

Received 08 January 2025; Accepted 01 May 2025

Abstract

Online banking transaction fraud occurs when fraudulent activity is initiated by a criminal. Such as seizing accounts and hacking points to execute online fund transfer mechanisms. This scenario is a main challenge for the upcoming data processing that is traveling only online. In today's scenario, most of the work has become digital. In such cases, machine learning algorithms must be ex-traordinary to take stringent security measures to transfer such funds over

Journal of Mobile Multimedia, Vol. 21_3&4, 577–598.
doi: 10.13052/jmm1550-4646.213414

a public channel. The paper analyzes some machine learning techniques such as naive Bayes and support vector machines to prevent loss. The machine has been used based on real data and can reduce losses manifold. After processing, the optimization reached 95 percent in terms of accuracy. The implementation can improve business operations to move the funds online while reducing overall risk.

Keywords: Electronic transaction, payment mode, fraud detection, probability method, machine learning algorithms.

1 Introduction

Considering the healthcare scenario, such platforms often use machine learning techniques, The mentioned concept is of major concern in the present scenario. Due to digitalization, funds worth around Rs 200 billion move a day. This can be through online transactions, phone banking, checks, airline tickets, article processing fees and more. The count has been justified by receiving reports of fraud attempts and attacks online. More than one million researches and reports have been prepared on online transactions and their frauds. The focus is to identify the purpose of how a criminal can attack any account even though they have no details of any individual. Therefore, the only way to get the details is through the bank account details which are maintained by the account holder and the service bank itself. Sometimes, there may be some unconscious transaction behavior such as higher number of password attempts and higher number of one-time password generation. These types of activities can create a thought in the minds of individuals as to why the system is behaving like this. Apart from humans, machine learning systems are also quite intelligent by incorporating artificial intelligence techniques. If a pattern, maintained by the system, does not behave smoothly then the system will be able to pick up on something that is not going right. By advanced algorithms of machine learning, assumptions can be made as anomalies will be detected by the system during transactions. Many of the authors analyzed found very little research on the selected topics as only 32 valuable articles were found while searching for papers on the topic. Due to lack of attention on this, criminals are not facing any problem. After trying several methods, they found patterns to hack. Therefore, the system must be able to analyze unexpected behaviors to run its programs. Self-supervised learning algorithms should be advanced like static rule asking algorithms. In

many fraud cases, these algorithms perform well and also gain name and citations with their beneficial behavior in the market for various research perspectives, which is also benefited for real life processing data. Logistic Regression and Decision Tree is also a method of machine learning which is working well for scenario. Among the various research articles are also considering techniques for prevention and detection of fraudulent data content risks. The risk control mechanism is also taking care of the fraudulent payment transaction system. Furthermore, prevention and detection algorithms must also be optimized if the system is to be measured for efficiency. While optimizing the algorithm steps, detecting fraudulent transactions should also produce efficient results by the system. Thus, the output generated from machine learning algorithms should be classified by some measurement levels when one can put forward some theory or one's own opinion.

2 Related Work

The author had surveyed many papers while reaching some checkpoint by going through remarkable work that was ongoing with the same topic. Re search into online payment fraud covers most specific varied problems, right from different types of scams and ways to their spotting and stopping. These include scams involving the theft of someone's identity, account takeovers, card-not-on-file scams, phishing for information, and even friend breaches. Each of these has its own way to find and prevent fraud. Fraud systems use, from simple rules to complex AI and machine learning, to find fraud. Fraud systems try to reduce false alarms and provide better results in finding fraud. These problems stay with us because scammers will continue to find new tricks. It's tricky because some fraud needs to be caught right away without bugging users too much. Data security is of prime importance, while compliance with the PCI DSS and GDPR contributes to this. Novel approaches are body scans to monitor the behavior of individuals and, more recently, blockchain technology as possibly an efficient method of fraud detection. Some researchers then conclude that, in order to counteract online fraud in payments, several techniques should be applied and constantly changed. It helps to save, according to the model described in [1], 101,970.52 EGP from 131,297.83 EGP and reduces frauds. The present model was built using IBM SPSS modeler's decision tree. It grabs an impressive precision of 93% and accuracy of 88.45%. The experts projected that online and mobile fraud would grow from about 25.6 billion by the end of 2020. The growth will affect

e-payment systems and their respective industries worldwide. In, they tested the performance of the model against Gradient Boosting Machine algorithms and Random Forest. The results depicted excellent performance by Light Gradient Boosting Machine [2]. Upon applying real data to it, the model captured 99% of the cases and provided fast and accurate output, which proved this model is greatly skilled in credit card fraud detection. In [3], the authors discussed the way to check whether the payment is fraudulent or not. They recommended employing machine learning classifiers such as Bagging Ensemble Learner, C4.5 decision trees, and Naïve Bayes on the same. They also forecast the effectiveness of these classifiers using metrics like Accuracy, recall rate, and precision-recall curve area rate. The overall fraud data contains 3,293 fraud cases on a dataset of 297,000 credit card transactions carried out between September 2013 and November 2017. Machine learning classifiers show very impressive results with the ratios of precision-recall curves at the level between 99.9% and 100%. Among them, the most effective classifier is C4.5 decision trees with an accuracy rating of detecting fraudulent transactions at 94.12%. The semi-supervised and unsupervised learning methods are applied for the detection of transaction fraud by dealing with three major challenges: imbalance between classes, integration of labeled and unlabeled samples, and dealing with a large scale of transaction data. Some of the supervised machine learning algorithms applied to real-time datasets to detect fraudulent transactions include hierarchical decision trees, Naive Bayes, polynomial least squares regression, multivalued logistic regression, and support vector machines (SVM). Random forests, with two different training strategies, are widely applied to ensure proper training in the detection of both normal and anomalous transactions. These transactions are evaluated with random forest and novel CART-based techniques. However, much remains to be done in the future, especially for imbalanced data in small datasets. Future work will address these issues and further enhance the random forest algorithm itself. Some of the most effective methods that have been considered for dealing with highly imbalanced credit card fraud data include multivalued logistic regression, K-nearest neighbors, and Naive Bayes. Researchers also explored meta-classifiers and meta-learning strategies. Based on such needs, deep learning models including Autoencoders, as well as restricted Boltzmann machines (RBM), are proposed with respect to helping classify the transaction and spot anomalies in general. Hybrid methods to combine Adaboost and Majority Voting technique were developed. Specificity, accuracy, sensitivity, and precision were the evaluation criteria. Accuracy rates for different models are as follows: Naive

Bayes (97.53%), K-Nearest Neighbors (97.53%), Support Vector Machine (94.98%), and Logistic Regression (99.51%). Machine learning classifiers show great results, with a precision-recall curve ratio between 99.9% and 100%. C4.5 decision trees prove to be the top performing classifier boasting a 94.12% accuracy rate in identifying fraudulent transactions. In transaction fraud detection, various semi supervised and unsupervised learning methods tackle key challenges. They address issues like the high-class imbalance in datasets, the mix of labeled and unlabeled samples, and the need to efficiently handle massive transaction volumes. On the supervised front, models such as hierarchical decision trees, probabilistic Naive Bayes classifiers, polynomial least squares regression, multivalve logistic regression, and support vector machines (SVM) play a central role in identifying fraudulent transactions in real-time. In particular, random forests stand out with two specific training methods that help capture patterns across regular and irregular transactions effectively. These models often work alongside techniques based on random trees, including the CART method, to analyze transactional behaviour and pinpoint anomalies [8]. Interestingly, while some supervised models are built on the assumption that fraud cases are rare, that's not always a realistic view. To enhance fraud detection further, deep learning models like Autoencoders and Restricted Boltzmann Machines (RBM) are being explored. These models can separate outliers from typical transactions more effectively. These improvements include hybrid models, for example, using a combination of Adaboost and Majority Voting in one model, combining multiple approaches to sharpen the transaction classification. The author indicated some performance metrics used in assessing the performance of the various fraud detection models: specificity, accuracy, sensitivity, and precision. If the accuracy rates are to be seen, Logistic Regression led the pack with its peak accuracy of 99.51%, surpassing others like Naive Bayes and K-Nearest Neighbours, with their respective accuracy rates of 97.53% and Support Vector Machine (SVM) of 94.98%. This shows that Logistic Regression might have high prospects of working effectively for fraud detection purposes, and therefore provides a degree of dependability which the other models did not have during this evaluation. The discussion also ran through various machine learning methods used in FDS credit cards for fraud detection, including SVM, Naive Bayes, Random Forest, decision tree, OneR, and AdaBoost. Various models have their own strengths. Their comparative performance gives some insight into how certain methods may be effective depending on the specific nature of the fraud data they handle.

3 Dataset Design

The dataset used in this study contains 6,362,620 rows and 11 columns, representing various attributes of online transactions [12].

1. Represents a unit of time, where each step equals one hour.
2. Type: Specifies the type of online transaction.
3. Amount: Indicates the amount involved in the transaction.
4. NameOrig: Identifies the customer who initiated the transaction.
5. OldbalanceOrg: Records the balance of the originating account before the transaction.
6. NewbalanceOrig: Notes the balance of the originating account after the transaction.
7. NameDest: Identifies the recipient of the transaction.
8. OldbalanceDest: Refers to the recipient's balance prior to the transaction.
9. NewbalanceDest: Represents the recipient's updated balance following the transaction.
10. IsFraud: Indicates whether the transaction was flagged as fraudulent.
11. IsFlaggedFraud: Shows whether the transaction was reported as fraudulent.

The dataset for this research has many rows and columns where much information is explained about different aspects of online transactions. Time is given in "phases," where every phase represents one hour [4]. The "type" column is given to differentiate the type of each transaction, while the "amount" column contains the monetary value. The "oldbalanceOrg" and "newbalanceOrig" columns contain the balance of the customer before and after the transaction, respectively. The "name-Orig" feature is that of the customer who initiates the transaction. The recipient of the transaction is recorded in the "nameDest" column. In the same way, the recipient's balance before and after the transaction is recorded in the "oldbalanceDest" and "newbalanceDest" columns, respectively, which are used to calculate on the account balances of the recipient [5]. The dataset also contains two feature classifications, namely: "isFraud" and "isFlaggedFraud," describing whether it's fraud or only flagged as fraud. Fraud detection demands the inclusion of a very large database with the view to evaluate models that apply machine learning, considering several processes in data preprocessing such as dealing with missing values, encoding categorical variables, and normalization of numerical features [6]. The evaluation was done through

several machine learning algorithms: GMB, random forests, decision trees, and logistic regression.

4 Fruitful Methodology

High-level feature engineering techniques, such as temporal pattern analysis, behavioral scoring, and network-based feature extraction, were needed to pre-process the data. State-of-the-art machine learning algorithms used include XGBoost, Random Forest, Neural Networks, SVM, and Decision Trees.

In the fraudulent payment detection model proposed by the study, 80% of the data from the dataset was allocated for training purposes and 20% was kept aside for testing [7]. As part of a comprehensive evaluation of the performance of the model, the main performance metrics used include precision, accuracy, recall, and F1 score. Therefore, there would be comprehensive results. Figure 1 represents the main sequence of events in the model. It is a few critical steps the study entailed unto itself. Data pre-processing consisted largely of handling missing values, outlier treatment, encoding of categorical variables, and normalization of numerical features so data stands in optimal form for any further analysis and training purpose. As for the data distribution after addressing outliers:

1. The most prominent distribution of values was between 150 and 400.
2. Transaction amounts were between 0 to 35 lakhs and there is an additional set of values in the range of 0 to 75,000.
3. For the OldbalanceOrg feature, values typically fluctuated between 0 and 18 lakhs, with more frequent values between 0 and 375,000.
4. The NewbalanceOrig feature also ranged between 0 and 19 lakhs, with regular occurrences from 0 to 375,000.

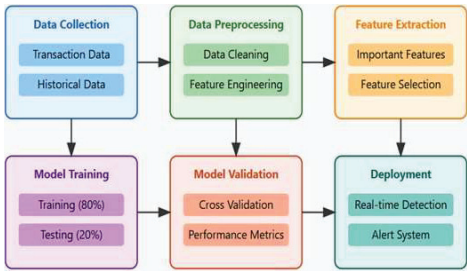

Figure 1 Proposed system model of fraudulent transaction detection.

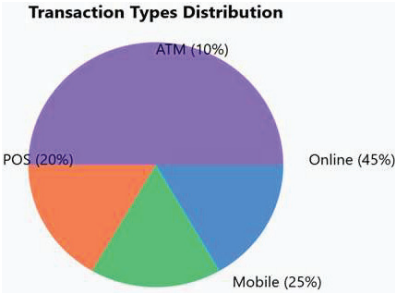

Figure 2 Type for analysis.

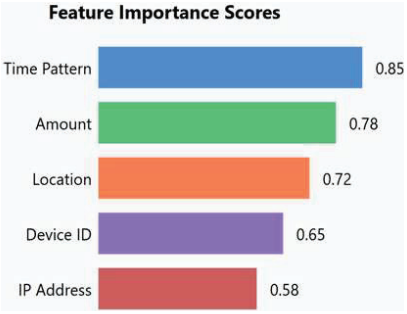

Figure 3 Data analysis for features contributed the most.

5. For OldbalanceDest, values spanned from 0 to 29 lakhs, with a common range between 0 and 625,000.
6. Similarly, NewbalanceDest values extended from 0 to 35 lakhs, with typical amounts falling between 0 and 625,000.

4.1 Feature Selection

Identification for the most relevant feature for fraud detection was done. This process involved analyzing the dataset to determine which features contribute most significantly to distinguishing between fraudulent and non-fraudulent transactions. Figures 3, 4, and 5 show the most contributing features.

4.2 Model Training and Evaluation

In this phase, the team undertook several key tasks, starting with splitting the entire dataset into two groups: an 80% training set and a 20% testing set. This division was essential for performance testing. Using this setup,

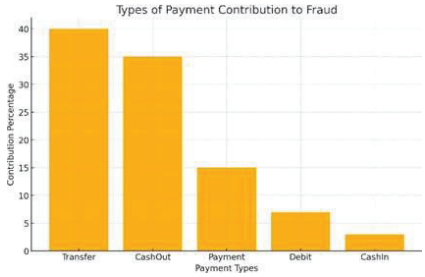

Figure 4 Types of payment contributed. Figure 5 indicated that fraud occurred mostly during transfer or cashout.

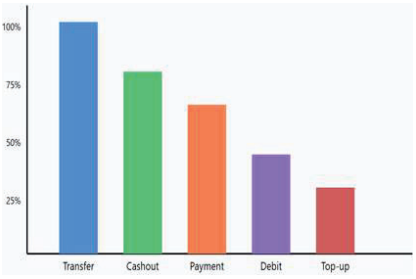

Figure 5 Bar plot for mostly occurred fraud.

they calibrated statistical models with hypothetical data, which in turn helped improve the models' accuracy when applied to real-world data over time [9]. To assess the performance of these models, various metrics were employed. Precision was used to determine the total count of correctly predicted outcomes. For instance, accuracy measured how many correct predictions of actual fraudulent transactions there were out of the number of flagged transactions. Recall extended this further by considering how much percent of fraud cases that were known to be genuine were predicted correctly amongst the flaggings. To balance between recall and precision, F1 scores were considered, averaging the two metrics for a balanced representation [10]. In addition, the study focused much on recall as an indicator in computing F-beta at different beta levels, thus allowing for flexible balance between recall and precision. There was also a wide analysis set for testing online payment fraud detection through machine learning models by giving suitable importance to the methods applied for feature selection, data preprocessing, and model evaluation [11]. The research has performed multiple training and testing ML models, as well as developing several algorithms, one of the most

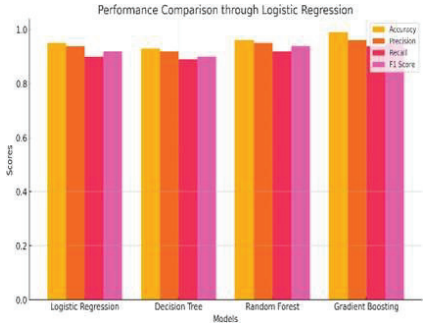

Figure 6 Performance comparison through logistic regression.

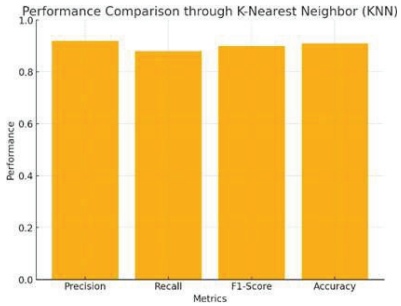

Figure 7 Performance comparison through k-nearest neigh-bour (KNN).

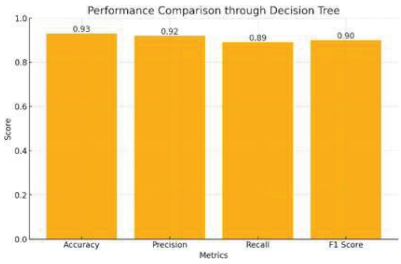

Figure 8 Performance comparison through decision tree.

impressive: Logistic Regression (LR): The prime objective of the training of this model was to set up a benchmark against which it may be measured.

Decision Tree (DT): The model tested the performance and reliability of a tree-based algorithm for transaction classification. It used decision trees in transactions and categorized them using clear rules that follow straightforward decisions, with the model's hierarchical structure offering ease in interpretation; it has each layer represent how it classified the process path.

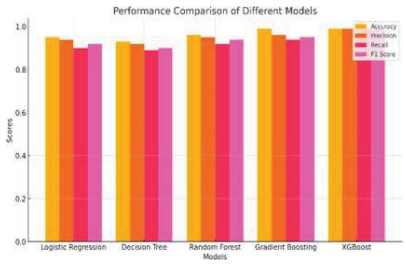

Figure 9 Performance comparison through random forest.

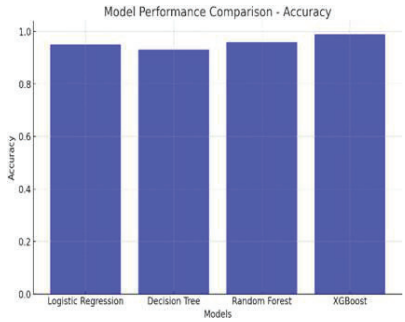

Figure 10 Performance comparison through accuracy.

Figure 8 indicates the performance of a good decision tree, representing comparison and effectiveness of the technique. Random Forest (RF): The entire model was tested to find out how it could be applied to complex datasets with multiple attributes. Predictions from several decision trees are combined in Random Forest to enhance the accuracy and reduce false decisions. The model was trained in this way to assess its strength and advantage in fraud detection. Figure 9 displays the performance comparison through Random Forest. XGBoost (XGB): A gradient boosting machine was used to harness the boosting techniques of powerful power. XGBoost, with its ability to construct an ensemble of trees iteratively, corrects past mistakes step by step [13]. This process trains the model to find how well it can capture patterns and interactions in the data set. Figures 10 and 11 gives a performance comparison showing how XGBoost works well in the treatment of complex data structure.

Logistic function applied on the dataset predicted whether the transaction would be fraudulent or not. Figure 6 below describes the performance of this model specifically through logistic regression on how well it separated fraudulent transactions from genuine ones. K-Nearest Neighbors (KNN): In

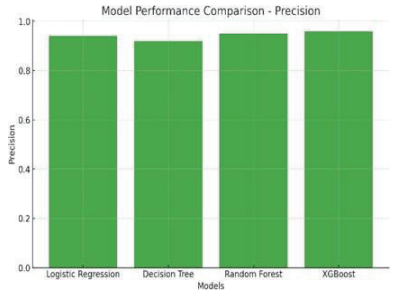

Figure 11 Performance comparison through accuracy.

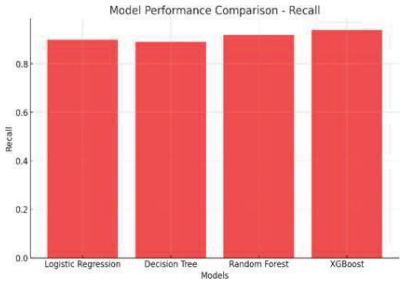

Figure 12 Performance comparison through recall.

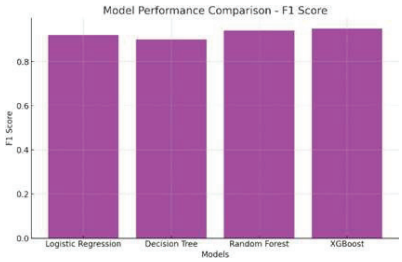

Figure 13 Performance comparison through F1 score.

this study, the author determined that among all the other possible features of the model, it was the multiple neighbors that worked best. By using the KNN method, the transactions are classified through the most dominating class of the k-nearest neighbors that a given transaction shares within the feature space. It's a way through which the transactions are grouped in more accurate manners based on similarity. Figure 7: Performance Comparison of This Method Using KNN.

Decision Tree (DT): The model tested the performance and reliability of a tree-based algorithm for transaction classification. It used decision trees

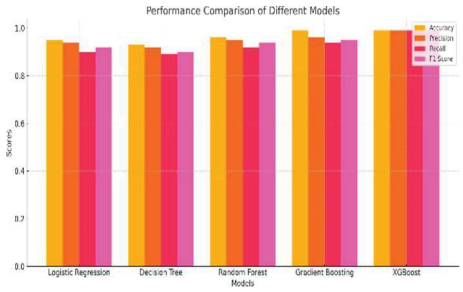

Figure 14 Performance comparison through Naïve Bayes.

in transactions and categorized them using clear rules that follow straightforward decisions, with the model's hierarchical structure offering ease in interpretation; it has each layer represent how it classified the process path. Figure 8 indicates the performance of a good decision tree, representing comparison and effectiveness of the technique. Random Forest (RF): The entire model was tested to find out how it could be applied to complex datasets with multiple attributes. Predictions from several decision trees are combined in Random Forest to enhance the accuracy and reduce false decisions. The model was trained in this way to assess its strength and advantage in fraud detection. Figure 9 displays the performance comparison through Random Forest. XGBoost (XGB): A gradient boosting machine was used to harness the boosting techniques of powerful power. XGBoost, with its ability to construct an ensemble of trees iteratively, corrects past mistakes step by step [13]. This process trains the model to find how well it can capture patterns and interactions in the data set. Figures 10 and 11 gives a performance comparison showing how XGBoost works well in the treatment of complex data structure.

Naive Bayes (NB): The model was trained on the dataset, testing its performance using Naive Bayes with independent feature classification. Applying Bayes Theorem meant that transitions would be efficiently categorized. The simplicity and speed in this approach have made it practical when fraud detection tasks require fast, straightforward classification processes. Support Vector Classifier (SVC): Applying the principles of SVM was used to validate whether the model classifies the transactions effectively. SVC separates fraudulent from non-fraudulent transactions by using its optimum hyperplane within feature space as shown in Figures 12 and 13. Each of the above mentioned models was taken through rigorous training and evaluation exercises to determine its performance in identifying internet payment fraud.

This appraisal was based on a series of performance metrics: accuracy, precision, recall, F1 score, and beta score. These various metrics gave comprehensive scope to the various areas of strength and weaknesses present in each model; as such, it led to an all-round view of the useful application of the model toward fraud detection.

5 Result

From the outputs of the model, the gradient boosting machine performed better than other models since it is having the highest accuracy and the F1 score. Compared to other methods like the decision tree model has performed poorly. Among those, the XGBoost model performed very well with high metrics as follows:

1. Accuracy: 99%
2. F1 Score: 93%
3. Precision: 93%
4. Recall: 93%
5. F-Beta Score: 93%

A clock looks at Table 1 shoes that the gradiant Boosting Machine did a good job, particularly the model XGBoost in detecting fraud in transactions. With a very impressive accuracy rate of 99%, the XGBoost correctly classified fraud versus non-fraud within all transactions at 99%. Such an accuracy supports the credence of the model regarding the detection of fraudulence and it therefore becomes one of the ideal devices in the assistance of fraud recognition. With the F1-score, it is a balanced measure between precision and recall at an extremely high value of 99% for the XGBoost model. High F1-score means that the model is good at minimizing false negatives and false positives to mark fraudulent transactions accurately without misclassifying legitimate ones. The accuracy of XGBoost remained constant at 99%. This means that nearly all the fraud transactions identified by the model were indeed fraudulent; in other words, this is how accurately it can make a distinction between the fraudulent and legitimate transactions. At the same time, it has a recall of 99% also meaning it identifies all the frauds and does not miss on any fraudulent transaction. That it also has the F-beta score, which emphasizes recall as compared to others, is 99%, further proving its stringent ability in fraud detection reliability and depth. And when considering the decision tree model's simplicity, it indeed offers great interpretability capabilities. However, there was so much about it that could not be so capable

when compared to its rivals in being the ensemble methods, particularly Random Forest and Gradient Boosting Machines. It is clear that because of the intricate complexity of data patterns, the single-tree structure of the decision tree model failed in performance. Alternately, ensemble approaches, such as Random Forest and Gradient Boosting, performed better in capturing the intricate complexities with higher precision and consistency in predictions. Overall, the XGBoost model is topping its list with excellent performance for the high-speed detection of fraud transactions in online payment systems. Its accuracy and reliability provide businesses with a powerful tool to enhance transaction security and minimize potential losses due to fraud.

6 Discussion

The XGBoost model presents impressive efficiency due to the ability of the model for handling massive datasets and searching for more complex patterns involved in it. High values of both accuracy and the F1-score obtained reveal that such a model properly distinguishes fraud from valid transaction, placing it at an advantageous point for real-time fraud detection. Incorporating XGBoost into this very system should drastically decrease instances of fraud. The Gradient Boosting Machine is yet another excellent model for detecting fraud, especially in establishing complex relationships within the data. However, the model also has its own limitations. One of its challenges is that it's extremely computationally expensive and highly complex when training the model. The Decision Tree is not as strong as other ensemble methods but is preferable in terms of interpretability. This quality makes it quite valuable for understanding the reasoning behind predictions, providing transparency that can be useful for auditing and refining fraud detection strategies.

7 Conclusion and Future Scope

This work proves how significant machine learning models, specifically gradient boosting techniques, play in the detection of online payment fraud. The paper explains how companies can leverage historical data to identify fraudulent activities and prevent them in order to maintain customer trust and financial security. High accuracy is one of the strong arguments for using such models, especially XGBoost models, because of their good performance in identifying fraud and thus are solid choices to enhance fraud detection capabilities. Future studies can be extended in terms of more features to be added and more complex algorithms to be implemented, further enhancing

the detection capability. In addition, gaining insights into the decision-making of the model will be highly essential in refining its efficiency and transparency in real applications.

References

[1] Li T, Kou G, Peng Y, Philip SY (2021) An integrated cluster detection, optimization, and interpretation approach for fnancial data. *IEEE Trans Cybern*, 52(12):13848–13861.
[2] Liu FT, Ting KM, Zhou ZH (2008) Isolation Forest. In: 2008 eighth IEEE international conference on data mining, pp. 413–422. IEEE.
[3] Liu FT, Ting KM, Zhou ZH (2012) Isolation-based anomaly detection. ACM Trans Knowl Discov Data (TKDD) 6(1):1–39.
[4] McNeil AJ, Frey R, Embrechts P (2015) Quantitative risk management: concepts, techniques and tools-revised edition. Princeton University Press, Princeton.
[5] Montague DA (2010) Essentials of online payment security and fraud prevention, vol. 54. Wiley, New York
[6] Molloy I, Chari S, Finkler U, Wiggerman M, Jonker C, Habeck T, Schaik RV (2016) Graph analytics for real-time scoring of cross-channel transactional fraud. In: International conference on fnancial cryptography and data security, pp. 22–40. Springer, Berlin, Heidelberg.
[7] Pang G, Shen C, Cao L, Hengel AVD (2020) Deep learning for anomaly detection: a review. arXiv preprint arXiv:2007.02500.
[8] Piotr J, Niall AM, Hand JD, Whitrow C, David J (2008) Of the peg and bespoke classifiers for fraud detection. Comput Stat Data Anal 52:4521–4532.
[9] Power M (2013) The apparatus of fraud risk. Account Organ Soc 38(6–7):525–543.
[10] Sabu AI, Mare C, Safta IL (2021) A statistical model of fraud risk in financial statements. Case for Romania companies. Risks 9(6):116.
[11] Singh A, Ranjan RK, Tiwari A (2022) Credit card fraud detection under extreme imbalanced data: a comparative study of data-level algorithms. J Exper Theor Artif Intell 34(4):571–598.
[12] Tokovarov M, Karczmarek P (2022) A probabilistic generalization of isolation forest. Inform Sci 584:433–449.
[13] Trozze A, Kamps J, Akartuna EA, Hetzel FJ, Kleinberg B, Davies T, Johnson SD (2022) Cryptocurrencies and future financial crime. Crime Sci 11(1):1–35.

Biography

Nishant Upadhyay is an Assistant Professor in Sharda University, with over five years of experience in higher education, specializing in Operating Systems, Data Structures, and Machine Learning. He is currently pursuing a Ph.D. and holds an M.Tech in Data Science from Jawaharlal Nehru University (JNU). He has published research in areas such as artificial intelligence, network security, and healthcare, and holds patents for several innovations, including a smartwatch application for real-time electrical signal detection. He can be contacted at an email: nishant.upadhyay23@gmail.com.

Yogesh Singh Rathore, resident of Noida, Uttar Pradesh. He is a graduate of Kurukshetra University, Kurukshetra where he earned a Bachelor's Degree in Science with Computer Science as a vocational subject. As his enthusiasm grew in computer applications, he met post-graduation in computer applications from Gurukul Kangri Vishwavidyalya, Hardwar, where he earned his first Master's Degree in computer applications. After a short span of teaching computer science, he indulges more in computer technology and completed his Master's in Technology from Kurukshetra University, Kurukshetra thereafter he earned his Ph.D. from Mewar University, Rajasthan After that, he

became a full-fledged educator and chooses this field as his profession. He can be contacted at email: yogesh.rathore@sharda.ac.in.

Nidhi Bansal is an associate professor at MRIIRS Faridabad Haryana, India. She received a B.Tech. from GBTU-UPTU Lucknow India in 2010, M.E. from NITTTR Panjab University Chandigarh India in 2014, and Ph.D. in Computer Science from AKTU-UPTU Lucknow India in 2023. Her research interests are in cloud computing and machine learning broadly, with applications in data science, and computer networking. She can be contacted at email: nidhi18jul@gmail.com.

Sushant Jhingram is an accomplished academic professional with a robust foundation in computer science and engineering. He holds a B.Tech in Computer Science from UPTU (2008). M.Tech from MDU (2014) PhD from Sharda University. Since 2016, he has been contributing as an Assistant Professor in the Computer Science and Engineering Department at Sharda University, where he is known for his expertise in cloud computing and microservices architecture. He can be contacted at email: sushantjhingran@gmail.com.

Gaurang Chaudhary is a Computer Science and Artificial Intelligence graduate from Amrita Vishwa Vidyapeetham with expertise in AI, robotics, IoT, and data analytics. He has completed research-oriented internships at companies like Nokia and GNAP, contributing to AI-driven automation and smart solutions. His projects include a computer vision-based prosthetic, a self-driving vehicle, and smart agriculture systems. He holds multiple patents, including an automatic headlight control system and an intelligent home security system, and has published research in IEEE. Proficient in Python, Android Studio, and IoT development, he is dedicated to leveraging AI for innovative and impactful solutions. He can be contacted at email: gaurangchaudhary619@gmail.com.

Sudhanshu Maurya is currently working as Associate Professor CSE & Research Head at Symbiosis Institute of Technology, Nagpur Campus, Symbiosis International (Deemed University), India. He has completed his post-doctoral research at the School of Computer & Communication Engineering, Universiti Malaysia Perlis (UniMAP), Malaysia. He is also associated with

the Center of Artificial Intelligence & Robotics, Indian Institute of Technology (IIT) Mandi, for research on AI-based Quantum Cryptographic Techniques. Dr. Maurya has completed his Ph.D. in Computer Science and M. Tech CSE. His area of research is dedicated to Artificial Intelligence, Security, and Cloud Computing. Currently, he has two international Patents (Granted), 13 Indian patents, two edited books, and five-course books, and authored/co-authored more than 150 research papers indexed in Web of Science/SCOPUS. He can be contacted at dr.sm0302@gmail.com.

Rekha Chaturvedi is currently working as assistant professor at Manipal University Jaipur. She did B.E. (IT) from Rajasthan University, M. Tech (Software Engineering) from the SGVU and Ph.D. (CSE) from Amity University Rajasthan. Her research interest includes data mining, image processing, digital image watermarking, machine learning, soft computing, and nature inspired computing. She can be contacted at email: rekha.chaturvedi@jaipur.manipal.edu.

Kritika Soni is an Associate Professor at Manav Rachna International Institute of Research and Studies, with over 11 years of experience in higher

education. She holds a Ph.D. and M.Tech in Computer Science from the same institution. Her academic and research expertise spans cyber security, blockchain, big data, cloud computing, and network security. Dr. Soni has published extensively in these domains and holds several patents for her innovative contributions. She can be reached via email at: kritikasoni.set@mriu.edu.in.