Online Payment Fraud Identification using Machine Learning Techniques

1. Ravi R, MCA Student,

PES Institute of Technology and Management, Shivamogga, Karnataka, India

2. Mr. Ajith G L Assistant professor, MCA,

PES Institute of Technology and Management, Shivamogga, Karnataka, India

Abstract

The convenience and accessibility of payments that are available at any location around the globe has been placed into the convenience of online transactions in the current day and age. Electronic payments have increased by a huge factor over the years. Although e payment systems are of benefit to consumers through fast and easy transactions, it also benefits businesses in terms of their revenue growth. But, this is also a convenience not without its own risks, most especially the online fraud. It is also through the ease of initiating digital payments that fraudulent activities are more easily committed. As a consumer, becoming a victim of such kind of a fraud is not only a loss of money but also involves personal data exposure, inconvenience of reporting it, and having to block or modify payment systems. To businesses, fraud may lead to customer dissatisfaction, loss of trust and even the possibility of having to give refunds to customers to retain them. Consequently, consumers and enterprises need to remain aware regarding possible online frauds. To find a answer to this ever-increasing fear, this research paper would suggest a ML model that has the potential to identify a legitimate or a fraudulent transaction through an online medium. An understanding of different features is considered in the model to make the correct prediction, including the nature of the transaction, who the recipient is, and others.

Keywords: Financial transaction fraud, detection methods, machine learning, prediction, Random Forest classifier, online fraud payment

1. Introduction

Online payments became a phenomenon of huge popularity over the past decades. People have found them convenient in the sense that irrespective of place and time, people can easily send money. This has made them a favorite to some. This transition was also fueled by the COVID-19 pandemic which has forced more customers and companies into digital transactions. Research indicates that the trend will probably persist and e-commerce and online payments are on the rise in the future. But this resulted in online payment fraud. With the increased use of digital facilities when it comes to managing finances, cybercriminals have discovered new avenues to attack users and systems. People have to ensure that their money is ended up where it is supposed to be and by honest people. Otherwise, failure to do that, may cause fraud, blocking the accounts, leaking personal data, and occasionally even worse outcomes. Business can also be at risk particularly when the business customers become victims of fraudsters. Companies usually end up compensating customers as this ensures the trust and satisfaction of the customers and this aspect can give a company both financial and image related stresses. Though companies have come up with different fraud detection tools in a bid to solve this problem, not many of them are indeed effective in preventing and detecting such frauds. No matter how digital security maintains a steady rise, fraudsters are closely on its heels and they tend to perceive new ways of overcoming protective measures. As an example, a study conducted by Zanin et al. (2018) revealed that the planet has seen a steady rise in the number of losses incurred due to fraudulent bank card operations between the years 2014 and 2017. Other works, such as the one conducted by Kalbande et al. (2021), revolve around a different concept, concept drift, a term indicating that data patterns and behaviours change over time. Like customers can adapt and alter their attitude in consumer behaviour, fraudsters will also adapt and practice their strategies. Nevertheless, cybersecurity analysts labor hard, in an attempt to detect these changing trends and sensitize the users against being hapless victims.

A deliberate and illegal initiative to intend to deceive and obtain something, leads to an extremely and bright fraud detection systems (FDS). These systems are maintained to continuously check the transactions, and raise doubts to identify any suspicious activity. Here machine learning algorithms are crucial, as they get to know the past data to decide upon the possibility of a new transaction being a fraud. Data mining methods assist in the discovery of trends. the differences between legitimate and inauthentic transactions, and together with machine learning, they can substantially increase the ability of detecting fraud.

2. Literature survey

[1] Keeping a customer information and transaction details is increasingly important in the current digital world where internet money transfers are happening at every second. Bahnsen, A.C., Aouada, D., Stojanovic, A. and Ottersten, B.(2016) argue that an area of significant concern as far as online shopping is concerned is credit cards theft. it is focusing with identifying fraud cases related to usage of credit cards in e-business.

[2] It is a complicated task to design correct models of detecting fraudulent online transactions. That can be said particularly because of the nature of datasets utilized and the divergent outcomes associated with the same. Among the most important obstacles, the following can be noted: gaining access to relevant information, making it ready to process, choosing the right algorithms, and understanding the end results (Behera, T.K and Panigrahi et al., 2020). Among the main issues, it is necessary to note that real payment data may include very sensitive personal data. Such data are normally open to authorized financial institutions and other third-party services only (Ranjan et al., 2022).

[3] Fraudsters continuously change their methods. As some scams become widely known, users begin recognizing suspicious patterns. Similarly, as customer behavior shifts over time, fraud detection systems must evolve to keep up. This makes it essential to frequently update fraud detection algorithms (Choi, D. and Lee, K 2019). While real-time data is crucial for creating effective models, obtaining such data is difficult due to its sensitive nature. Only the entities managing transactions have the authority to access it.

[4] Ileberi et al. (2021) improves the performance of the model with AdaBoost, along with logistic regression, decision trees, and SVM. XGB- AdaBoost attained a Matthews correlation coefficient (MCC) of 0.99 in a successful handling of the occurrence of class imbalance. They also showed the significance of sensitivity, specificity, accuracy and error rate performance measures in their analysis. The cross-validation scores of Logistic Regression model and XGBoost were 94.16 and 93.76 percent respectively. This research used only 10 % of the available data hence the potential of more research involving complete body of data.

[5] Ileberi, E., Sun, Y.et al. (2021) achieved a finding that gossip learning failed to be effective since there was no control in its process, but, on the contrary, federated learning was more successful as it was semi-decentralized. Jain et al. (2020) noted that there are two typical types of fraud in the case of a Cash Out transfer or a merchant transaction when the funds may end up flowing to scammers.

[6] In their work, Yee et al. (2018) tested the performance of a number of machine learning algorithms, using accuracy, precision, and specificity to measure their respective efficacies. This research mainly revealed that Random Forest model was outstanding, and it registered a precision of 99.7 and 96.2 accuracy.

[7] Thennakoon et al. (2019) provided the structure of a three-component fraud detection system comprising a data warehouse, an API module, and ML-based detection model of fraud. The modules exchange real-time information and raise alerts using GUI. The users receive the information that some fraudulent activity is suspected, and judges record their commentary as the reference.

[8] Singh et al. (2021) offered the possibility to apply an intelligent fraud detection model that is designed to recognize four varieties of scams with the help of the best fitting algorithms.

[9] Rambola et al. (2018) discussed how to combine the data of different sources and how to format it as part of data mining. They utilized neural networks in detecting fraud through the clustering of transactional data regarding customer profiles.

[10] Wang et al. (2015) presented two ensembles approaches (OOB and UOB) based on re-sampling and time decay to overcome the problems of class imbalance. They noticed that data distribution is vital in producing high performing models. Even though the outcomes are quite encouraging, false positives, or the incorrect identification that a legitimate transaction is actually fraudulent, continue to haunt many fraud detection systems (Behera & Panigrahi, 2015). It subjects customers and businesses to inconvenience and difficulties. In order to minimize this false alert the research suggested usage of fuzzy c-means cluster and the usage of neural networks since the fuzzy algorithm simply clusters similar data and conversely the neural network is mainly used in the correct classification.

[11] Singh et al. (2021), have compared numerous machine learning patterns such as KNN, SVM, Random Forest, they concluded that the most successful option is a random forest with 99.9 percent accuracy and the lowest false warnings. However, the reports by Jain et al. (2020) cannot be discounted even though their study was not done using real-time data as it will be applied in future enhancements on the fraud control systems.

[12] Kaur et al. (2021) recognized the fact that the increasing risk of cybercrime via digital payments becomes the most dangerous threats to financial organizations and tech practitioners. In their study, the authors used several machine learning and data mining algorithms to separate legitimate transactions and fraudulent based on behavioral patterns; these algorithms were CART, C4.5, and Naive Bayes (Yan et al., 2020)

3. Proposed Methodology

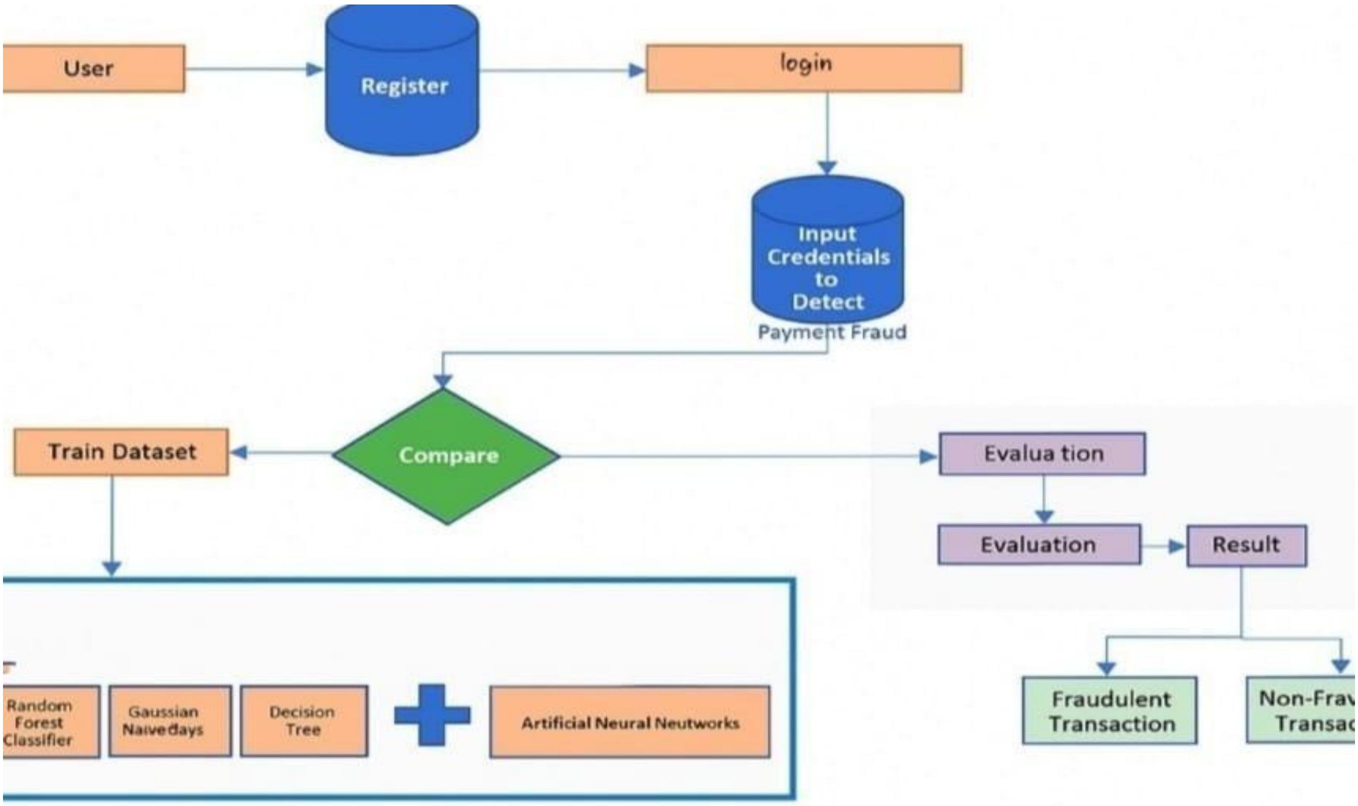


Figure 3.1: Flowchart of Proposed Implementation

The online payment fraud detection can be done when a user register and created a account to predict the transaction. After registration a user can get his email id and password, and then a user can able to login using his credentials, then a web interface will opens, then a user must enter the essential credentials as input for detecting whether the transaction is fraud or safe. Then the user entered credentials is compared with trained data and This data is then divided into two: a training data and a testing data. The training set is utilized in the training of different ML algorithms that are the Logistic Regression, Random Forest Classifier, Gaussian Naive Bayes, Decision Tree and the Artificial Neural Network. The above mentioned models are educated to pick up transaction patterns that are suggestive of fraudulent behavior. In the interim, they depend on the testing dataset through which they assess the performance of these trained models when applied to new, unseen data. The analysis assists in measuring the accurateness and reliability of the models. The system uses evaluation results to predict whether a transaction is fraudulent or legitimate. The result of this procedure is a definite categorization of every transaction to be either a fraudulent transaction or non-fraudulent transaction, and provide actions to be taken in time and establish even more security of online payment systems. Online transactions are very perceptive to fraud; this is why appropriate analysis of data is important. The machine learning technology is fast becoming an option used by financial institutions like banks, among other companies, to strengthen their protection systems against these threats. A lot of organizations are committing resources on developing smart systems capable of detecting mischievous transactions before they hurt. Such systems do not only aid the detection of fraud but also protect customers against possible financial losses. To conduct the present research, the data was collected using the open-access service Kaggle, Because it is challenging. to get access to real-time financial data and regulatory authorities restrict such access in terms of security and privacy. The data base that is being utilized contains more than 1 million rows of 11 various features. Among the most important features are a type of transaction, its amount, identity of the sender (nameOrig), his or her prior to and after the transaction balances (oldbalanceOrg and newbalanceOrig), identity of the recipient (nameDest), and their respective balances (oldbalanceDest and newbalanceDest). FraudThe target variable specifying whether the given transaction is authentic (0) or fraudulent (1) is the one based on which the fraud detection models are trained and tested.

4. Mathematical Formula

The main goal of this paper is to evaluate whether combining supervised machine learning models with Artificial Neural Networks (ANN) can increase the speed and efficiency of fraud detection systems compared to traditional methods. To assess this, two separate experiments were carried out. The first experiment involved training the models using all available features in the dataset. In the second, we excluded two less relevant features—nameDest and nameOrig—to analyze how their removal affects model performance.

To fairly compare the results, we used a set of evaluation metrics: recall, specificity, F1-score, AUC score, AUC-ROC curve, and the geometric mean of recall and specificity. Since the dataset consists of many false values (with far more legitimate transactions than fraudulent ones), accuracy alone wouldn't provide a reliable assessment. Instead, metrics like recall (how many actual frauds were correctly identified) and AUC (how well the model separates the classes) were prioritized. To interpret model results more clearly, we used the confusion matrix, which breaks predictions down into four categories:

- **True Positive (TP)**: Accurately recognizing a genuine transaction as safe.
- **False Positive (FP)**: Failing to detect a fraudulent transaction
- **False Negative (FN)**: Mistakenly marking a genuine transaction as fraudulent
- **True Negative (TN)**: Correctly detecting a fraudulent transaction.

Metrics such as precision and specificity help in understanding how accurately frauds are being identified. Meanwhile, recall shows the proportion of real frauds that the model catches, and F1-score balances both precision and recall—ideally aiming for a value close to 1. We also used the geometric mean of recall and specificity to ensure fair evaluation in the presence of class imbalance. After applying various techniques and preparing the final dataset, We tested each model with the formulas. This helped us understand The effect of under sampling and feature elimination on performance, providing deeper insight into which approach yields the most reliable result

$$\text{Recall/Sensitivity} = \frac{TP}{TP+FN}$$

$$\text{Precision/Specificity} = \frac{TP}{TP+FP}$$

$$\text{F1-Score} = \frac{2 * Recall * Precision}{Recall + Precision}$$

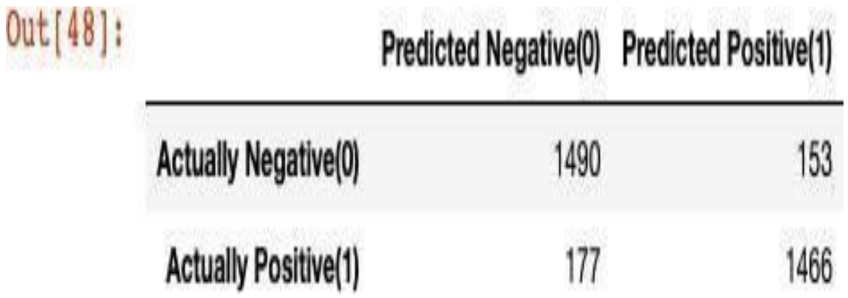
$$\text{Geometric Mean(GM)} = \sqrt{Sensitivity * Specificity}$$

5. Graphs

Module Accuracy Comparison:

Logistic Regression

The logistic Regression provided accuracy of 89.9 percent preciseness of 86 percent. The following confusion matrix provides the answers of logistic regression confusion matrix: The ROC value of the model is

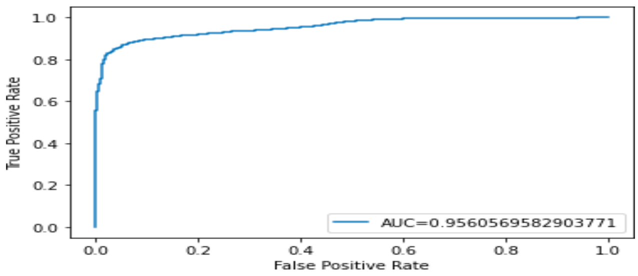


Out[48]:

	Predicted Negative(0)	Predicted Positive(1)
Actually Negative(0)	1490	153
Actually Positive(1)	177	1466

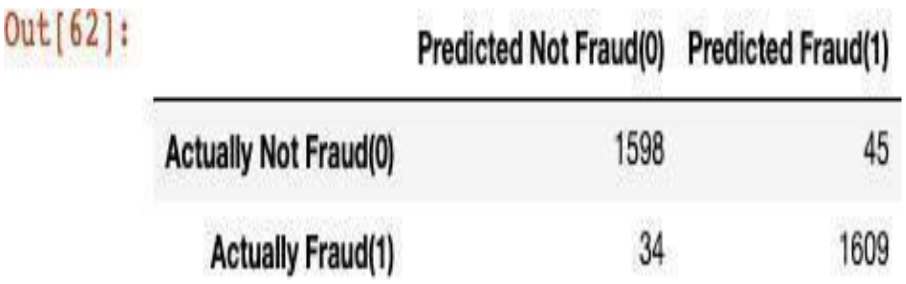
Figure 1: Confusion Matrix out to be 95 percent

The following graph illustrates:



Random Forest Classifier

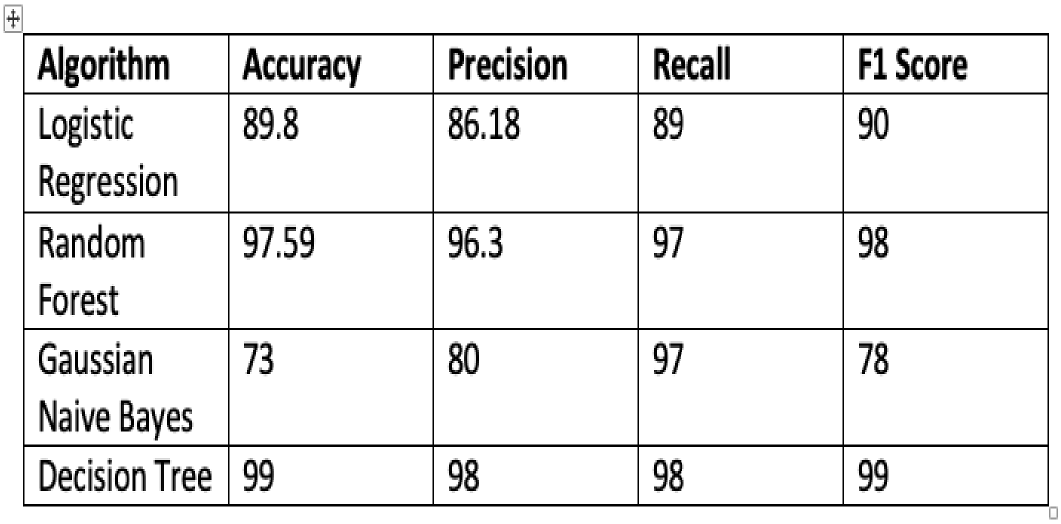
Random Forest was the second classifier, achieving an accuracy of 87%, a precision of 96.3%, and an AUC of 99%. Its confusion matrix is presented below:



Out[62]:

	Predicted Not Fraud(0)	Predicted Fraud(1)
Actually Not Fraud(0)	1598	45
Actually Fraud(1)	34	1609

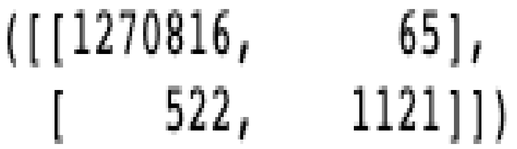
Figure 2: Confusion Matrix of the Random Forest model



Algorithm	Accuracy	Precision	Recall	F1 Score
Logistic Regression	89.8	86.18	89	90
Random Forest	97.59	96.3	97	98
Gaussian Naive Bayes	73	80	97	78
Decision Tree	99	98	98	99

Artificial Neural Networks

ANN were also implemented into our dataset. Another comparative study on machine learning model and Neural Network performance on fraud identification in the research by Yan et al. (2021) was also available.



```
([[1270816,      65],
  [    522,    1121]])
```

Figure 3: Confusion Matrix for ANN

After ANN was applied, the confusion matrix is figure 16 and the accuracy rate was successful by 99 percent. The number of transactions that were estimated to be non-fraudulent and ended up being fraudulent amounts to 65 and the number of transactions that were estimated not to be fraudulent yet arrived as being fraudulent amounted to 522.

6. Results

In this part of the research paper, the question of how the fraud detection system was in fact constructed and tested is addressed. It describes the process that was followed to clean the data, select most pertinent features and perform machine learning models. To create this research, the Python coding language (version 3.7) was deployed, and Google Colab was utilized as a platform of development. Python was chosen for its readability and ease of understanding, as well as its vast library support, particularly in the field of machine learning. It is also easy to resolve problems since it has strong community support. In the given project, the dataset is publicly available in CSV extended data format and consists of 11 features, including the target column which shows whether the transaction is a fraud or not. We imported this data into a Pandas DataFrame, cleaned the data and scaled the coefficients. Using visualizations, we explored the patterns and relationships between the features and the target variable. We transformed categorical data into numerical or numeric values so that the dataset becomes ready to undergo machine learning by performing one-hot encoding on the data. Once the data was prepared, it was then classified as training, validation and test sets. We found out that imbalance the proportion of the ratio of legitimate transactions exceeded by far the one of fraudulent ones. To deal with this we applied under sampling where the majority class of more than 6 million records was cut down to the minority class size of 8,213. After that, we implemented different ML algorithms in the balanced dataset; among these models are Logistic Regression, Random Forest, Decision Tree, Gaussian Naive Bayes, and Artificial Neural Networks (ANN). We aimed to compare the performances of these models in detecting fraud. We also trained the models to cover the significance of particular features with and without.

i.e. without two less important fields nameOrig and nameDest. As metrics we relied on the following ones: specificity, sensitivity (recall), F1-score, AUC-ROC, and geometric mean, to be used in performance evaluation. The confusion matrix was an important tool that was in aid of determining the number of true positives and false negatives that were to be forecasted and gave us some role on the accuracy and the reliability of the models in real life conditions in detecting fraud.

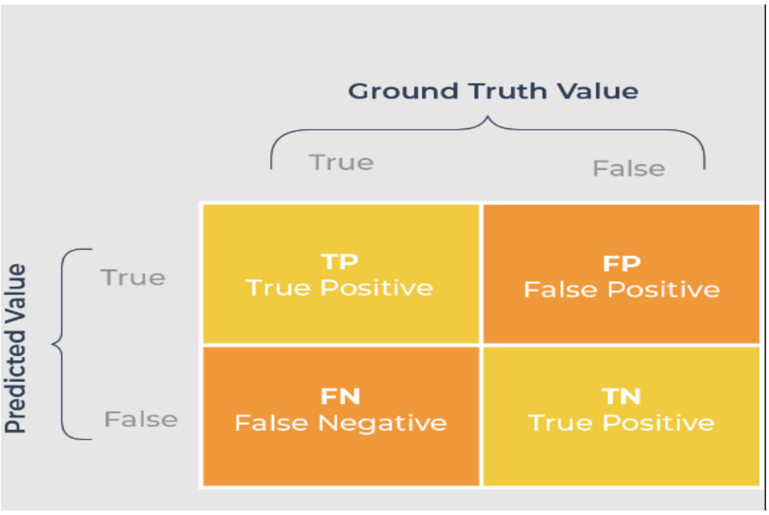


Fig 6.2 : Results of prediction

7. Conclusion

Over the last few years, Online payment fraud has been among the most common financial crimes. In this research paper, the results are founded on research carried on utilizing ML to detect such fraudulent activities. Feature selection is a key finding of this research, as it positively impacts model accuracy while reducing the number of false alarms. We successfully respond to the question of how ML can detect fraud and how well this model is accepted among audiences by checking various ML models, to detect fraudulent transactions. A reliable fraud detection system should not only be precise but must correctly detect the fraud and make fewer errors. We focused to develop a model that will balance it and help to achieve safer online transactions.

8. Future Enhancement

To enhance the performance of our models, we applied several techniques, such as Selecting features and managing class imbalance, to prioritize the most meaningful data. We used the confusion matrix to evaluate our models' performance, and the results were promising, we weren't able to completely eliminate false positives or false negatives. For financial institutions, achieving zero errors is crucial, as misclassifying transactions can lead to customer dissatisfaction and financial losses due to refunds. In the future, this research can be extended to further reduce these errors. Exploring hybrid models or combining multiple algorithms may help improve accuracy and provide even more reliable fraud detection.

9. References

[1] Bahnsen, A. C., Aouada, D., Stojanovic, A. and Ottersten, B. (2016). Detecting credit card fraud using periodic features.

[2] Behera, T. K. and Panigrahi, S. (2015). Credit card fraud detection: A hybrid approach using fuzzy clustering neural network.

[3] Choi, D. and Lee, K. (2017). Machine learning based approach to financial fraud detection process in mobile payment system, IT CoNvergence PRActice (INPRA) 5.

[4] Ileberi, E., Sun, Y. and Wang, Z. (2021). Performance evaluation of machine learning methods for credit card fraud detection using smote and adaboost, IEEE Access 9.

[5] Jain, V., Agrawal, M. and Kumar, A. (2020). Performance analysis of machine learning algorithms in credit cards fraud detection.

[6] Kalbande, D., Prabhu, P., Gharat, A. and Rajabally, T. (2021). A fraud detection system using machine learning.

[7]Kaur, P., Sharma, A., Chahal, J. K., Sharma, T. and Sharma, V. K. (2021). Analysis on credit card fraud detection and prevention using data mining and machine learning techniques.

[8] Kolodiziev, O., Mints, A., Sidelov, P., Pleskun, I. and Lozynska, O. (2020). Automatic machine learning algorithms for fraud detection in digital payment systems, Eastern- European Journal of Enterprise Technologies 5.

[9] Rai, A. K. and Dwivedi, R. K. (2020). Fraud detection in credit card data using unsu- pervised machine learning based scheme.

[10] Rambola, R., Varshney, P. and Vishwakarma, P. (2018). Data mining techniques for fraud detection in banking sector.

[11]Ranjan, P., Santhosh, K., Kumar, A. and Kumar, S. (2022). Fraud detection on bank payments using machine learning.

[12] Saputra, A. and Suharjito (2019). Fraud detection using machine learning in e-commerce, International Journal of Advanced Computer Science and Applications 10.

[13] Singh, P., Chauhan, V., Singh, S., Agarwal, P. and Agrawal, S. (2021). Model for credit card fraud detection using machine learning algorithm.

[14] Thennakoon, A., Bhagyani, C., Premadasa, S., Mihiranga, S. and Kuruwitaarachchi, N. (2019). Real-time credit card fraud detection using machine learning.

[15] Wang, S., Minku, L. L. and Yao, X. (2015). Resampling-based ensemble methods for on- line class imbalance learning, IEEE Transactions on Knowledge and Data Engineering 27.

[16] Yan, T., Li, Y. and He, J. (2021). Comparison of machine learning and neural network models on fraud detection.

[17] Yee, O. S., Sagadevan, S. and Malim, N. H. A. H. (2018). Credit card fraud detection using machine learning as data mining technique, Journal of Telecommunication, Electronic and Computer Engineering 10.

[18] Taranjyot Singh Chawla, 2022, Online payment fraud detection using machine learning techniques, MSc Research paper, Data analytics.