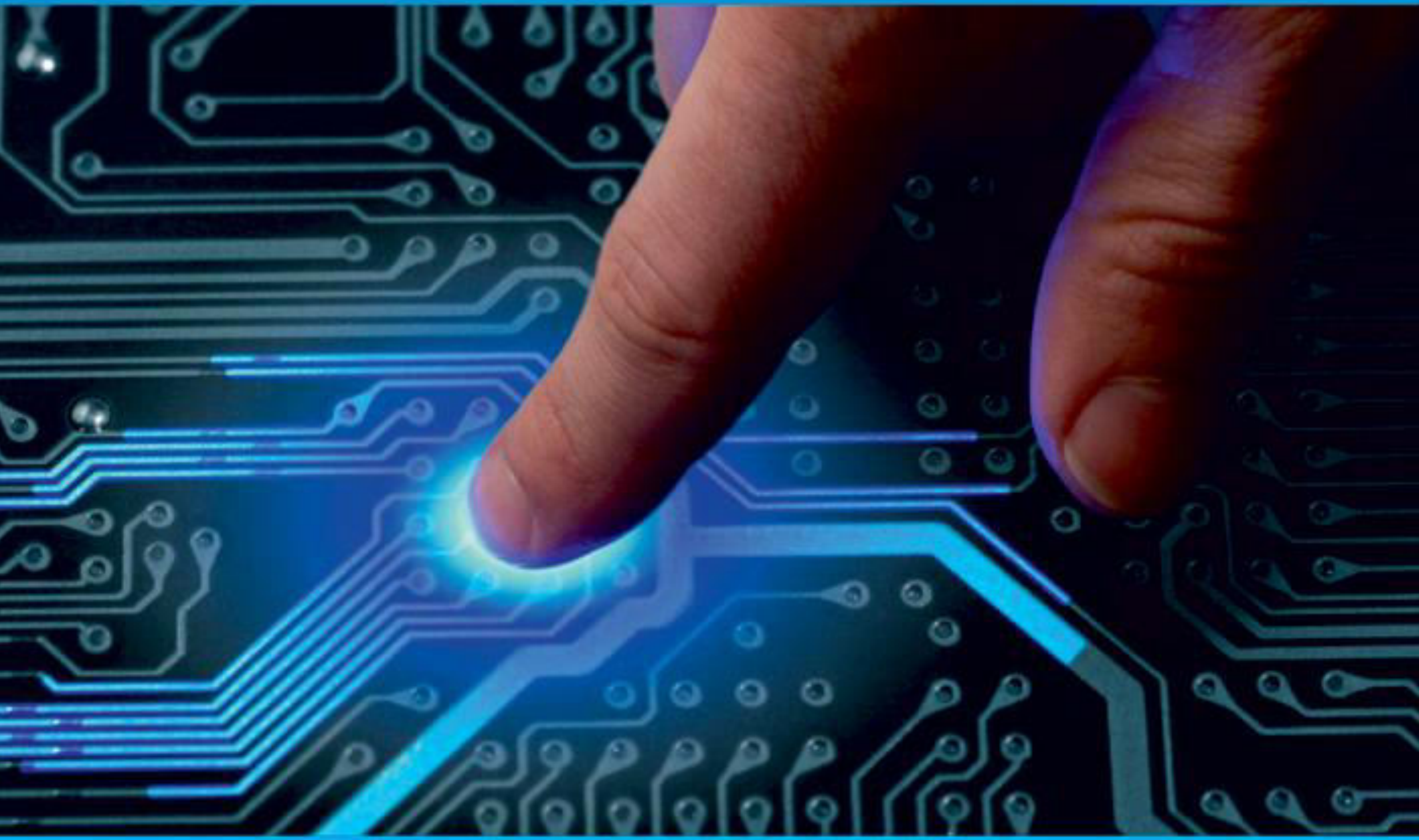
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 12, December 2024

INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 8.625

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Online Payment Fraud Detection

Shivani Joshi, Gori Khandelwal, Yash Barai, Prof. Sandeep Kulkarni

Bachelor of Computer Applications (Big Data Analytics), Ajeenkya D Y Patil University, Pune, India

Bachelor of Computer Applications (Big Data Analytics), Ajeenkya D Y Patil University, Pune, India

Bachelor of Computer Applications (Big Data Analytics), Ajeenkya D Y Patil University, Pune, India

Assistant Professor & Research Guide, Ajeenkya D Y Patil University, Pune, India

ABSTRACT: Detection of Online Payment Fraud Businesses and customers alike are now very concerned about the possibility of payment fraud due to the quick growth of e-commerce and online transactions. The creation and deployment of an online payment fraud detection system using cutting-edge machine learning is the main goal of this project.

learning data analytics methods and algorithms. The system seeks to detect and stop fraudulent activity in real time by examining transactional data, user behaviour patterns, and contextual information. The system learns to differentiate between authentic and fraudulent transactions through feature engineering, model training, and data preparation. A variety of machine learning techniques are used to find irregularities and patterns suggestive of fraudulent activity, such as logistic regression, random forest, and neural networks.

To evaluate the system's performance and make sure it is efficient in identifying fraudulent transactions while reducing false positives, evaluation metrics including precision, recall, and F1-score are employed. Furthermore, the project

investigates how to further improve the system's fraud detection capabilities by integrating behavioural biometrics, anomaly detection methods, and real-time data streams. In the end, the created online payment fraud detection system is an essential instrument for safeguarding consumers and companies against monetary losses and maintaining confidence in online payment ecosystems.

KEYWORDS: Online Payment Fraud, Machine Learning, Fraud Detection, E-commerce Security, Anomaly Detection, Data Analytics Real-time Monitoring, Behavioural Biometrics.

I. INTRODUCTION

Both consumers and businesses now enjoy previously unheard-of convenience thanks to the explosive expansion of e-commerce and online transactions. The security and reliability of digital payment systems are seriously threatened by the rise in online payment fraud that has coincided with this expansion. Fraudulent actions may lead to significant monetary losses, harm to the reputation of the company, and a drop in customer confidence. As a result, creating strong fraud detection systems has become essential for companies looking to protect their operations and clientele . The goal of this project is to use data analytics and cutting-edge machine learning techniques to create and implement an online payment fraud detection system. The system looks for and stops fraudulent transactions in real time by examining enormous volumes of transactional data and user behaviour patterns.

Data preprocessing, feature engineering, and the use of several machine learning methods, including logistic regression, random forest, and neural networks, are all part of the detection process. These models have been taught to

identify trends and irregularities that point to fraud so that preventative action can be done. To improve the precision and effectiveness of fraud detection, the project investigates the integration of behavioural biometrics and real-time data streams in addition to conventional machine learning techniques. Metrics including precision, recall, and F1-score are used to assess the system's performance, making sure that identifying fraudulent transactions and reducing false positives are balanced. This project helps shield companies and customers against online payment fraud by offering a complete and scalable solution, which eventually promotes a safer digital commerce environment.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

1.1 EXISTING SYSTEM

The majority of the current systems for detecting online payment fraud are based on simple statistical models and rule-based techniques. To detect suspicious transactions, these systems employ preset criteria and thresholds. For example, they may flag transactions from odd sources or exceeding a specific threshold. Although these techniques can be

Although they are good at spotting established fraud trends, they frequently have trouble keeping up with the latest and changing strategies employed by scammers. Rule-based systems may also produce a large number of false positives, which could upset customers and raise operating expenses for companies. These systems' static structure further restricts their capacity to identify complex fraud schemes involving numerous transactions or minute behavioural shifts.
Consequently, there is an increasing demand for more sophisticated and flexible systems that can precisely identify.

1.1.1 CHALLENGES

The dynamic nature of fraud makes it difficult for detection systems to stay ahead of the game because scammers are always changing their strategies.
High Transaction Volume: Systems must handle the enormous volume of online transactions and evaluate data instantly, which calls for effective infrastructure and algorithms.
Data Imbalance: Since fraudulent transactions are typically few in comparison to genuine ones, the datasets are unbalanced, which might impair the accuracy and training of models.
False Positives and Negatives: To preserve consumer trust and prevent needless interventions, it's imperative to strike the correct balance between identifying fraudulent transactions and preventing false positives.
Data privacy and security: Strict adherence to data protection laws and strong security measures are necessary when handling private and sensitive financial information.
Scalability: As e-commerce expands, the system must be able to accommodate growing transaction volumes.

1.2 PROPOSED SYSTEM

The suggested approach improves the detection of online payment fraud by utilizing data analytics and sophisticated machine learning techniques. In contrast to conventional rule-based systems, this method makes use of advanced models such as neural networks, random forests, and logistic regression to examine transactional data, user behaviour patterns, and background data. To enhance the caliber and applicability of the training data, the system goes through extensive feature engineering and data preprocessing. The technology can more rapidly and precisely detect irregularities and fraudulent activity by combining behavioural biometrics with real-time data streams. Furthermore, model upgrades and ongoing learning guarantee that the system adjusts to changing fraud strategies. The goal of the suggested system is to offer a reliable, scalable, and effective solution that can identify and stop fraudulent transactions, protecting companies and customers in
the digital payment ecosystem.

1.2.1 ADVANTAGES:

Enhanced Accuracy: By learning from a variety of data patterns, machine learning algorithms offer a higher accuracy rate in identifying fraud.

- **Real-time Detection:** Potential fraud can be stopped right away by the system's ability to recognize and report suspicious transactions in real-time.
- **Adaptability:** The system can adjust to new and developing fraud schemes thanks to ongoing learning and model changes.
- **Decreased False Positives**: Sophisticated algorithms and thorough feature engineering reduce false positive rates, improving the user experience.
- **Scalability:** The system is appropriate for expanding enterprises since it can manage high transaction volumes.
- **Thorough Data Analysis:** By utilizing contextual data and behavioural biometrics, a deeper comprehension of user behaviour is obtained, enhancing detection capabilities.
- **Integration Capability:** The system can function seamlessly by being integrated with the current security and payment infrastructure.

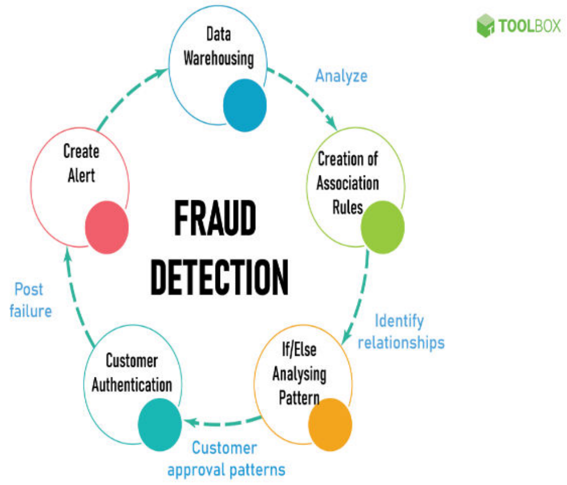


Fig 1: Fraud Detection

II. LITERATURE REVIEW

The architecture and implementation of an online payment fraud detection system using machine learning involve a multi-layered approach, integrating various components and technologies to achieve real-time, accurate fraud detection. The foundational step in developing such a system begins with data collection and preprocessing. Transactional data, including attributes like transaction amount, location, time, and user behaviour, is aggregated from multiple sources. This data often contains noise and missing values, necessitating robust preprocessing techniques such as data cleaning, normalization, and imputation. The use of exploratory data analysis (EDA) tools helps in understanding the distribution and relationships within the data, which is crucial for effective feature engineering. Feature engineering plays a pivotal role in the architecture, as the quality and relevance of features directly impact the performance of machine learning models. Features such as transaction frequency, velocity, and user-specific behaviour patterns are derived to distinguish between legitimate and fraudulent transactions. Advanced techniques like feature selection and dimensionality reduction, using methods such as Principal Component Analysis (PCA) and Recursive Feature Elimination (RFE), are employed to optimize the feature set and enhance computational efficiency. Behavioural biometrics, capturing unique user patterns like typing speed and mouse movements, are increasingly integrated to add a layer of security by verifying user identity based on behavior. The core of the system involves the deployment of machine learning models. A variety of algorithms are considered, each offering different strengths in detecting fraud. Logistic regression provides a straightforward, interpretable model ,while decision trees and random forests offer more complex decision-making capabilities and robustness against overfitting. Ensemble methods, particularly those involving gradient boosting and random forests, are popular due to their ability to improve predictive accuracy by combining multiple models. More recently, deep learning approaches, such as Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), have been employed to capture intricate patterns and temporal dependencies in transaction sequences. These models are trained on labeled datasets, using supervised learning techniques where the goal is to distinguish between fraudulent and non-fraudulent transactions. Given the challenge of class imbalance, where fraudulent transactions are rare, techniques like oversampling, under sampling, and synthetic data generation (e.g., SMOTE) are used to balance the training data. Real-time detection capability is a critical aspect of the system architecture. The implementation involves stream processing frameworks that can handle high-velocity data and provide timely responses. Technologies such as Apache Kafka and Apache Spark are often utilized for this purpose, enabling the system to ingest, process, and analyze data in real-time. The model deployment pipeline includes monitoring and updating mechanisms to ensure that the models remain effective against evolving fraud tactics. This is achieved through continuous learning and periodic retraining with new data. The evaluation of the fraud detection models is conducted using a variety of metrics. Precision, recall, F1-score, and Area Under the Receiver Operating Characteristic Curve (AUC-ROC) are commonly used to measure the system's performance. These metrics provide insights into the trade-offs between catching fraudulent transactions and minimizing false positives. High precision is crucial to avoid flagging legitimate transactions as fraudulent, which can lead to

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

customer dissatisfaction and loss of business. Conversely, high recall ensures that most fraudulent transactions are detected.The tools and technologies employed in building and deploying the system are diverse, encompassing data analytics, machine learning, and big data frameworks. Python is a popular programming language for developing the machine learning models, with libraries such as scikit-learn, TensorFlow, and PyTorch providing extensive functionality for model building and evaluation. For data processing and feature engineering, tools like pandas and NumPyare widely used. The system's infrastructure often relies on cloud platforms such as AWS, Azure, or Google Cloud, which provide scalable resources and tools for machine learning deployment, including managed services like AWS SageMaker or Azure ML .In conclusion, the architecture and implementation of an online payment fraud detection system are complex and involve several critical steps, from data collection and preprocessing to model training and realtime deployment. The integration of advanced machine learning techniques, real-time processing capabilities, and robust evaluation metrics ensures that the system is both effective and efficient. The use of cutting-edge tools and technologies, combined with a well-designed architecture, enables the detection of fraudulent activities, protecting businesses and consumers in the digital payment landscape.

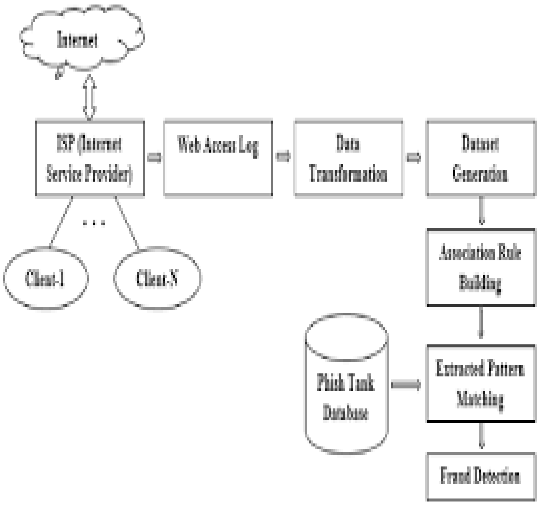


Fig 2: Fraud Detection

III. METHODOLOGY

The methodology for developing an online payment fraud detection system involves a comprehensive and systematic approach, beginning with data collection and culminating in the deployment and continuous improvement of the detection models. Initially, transactional data is gathered from various sources, including payment gateways, financial institutions, and user devices. This data includes details such as transaction amount, time, location, device information, and user behaviour patterns. The first step is data preprocessing, which involves cleaning the data to remove inconsistencies, handling missing values, and normalizing the data to ensure uniformity across different scales and units. This is followed by exploratory data analysis(EDA) to understand the underlying patterns and distributions, aiding in the identification of key features relevant to fraud detection .Feature engineering is a critical phase where raw data is transformed into meaningful features that can enhance model performance. This includes creating derived features such as transaction velocity, frequency, and customer profiles based on historical behaviour. Advanced feature selection techniques, like Principal Component Analysis (PCA) and Recursive Feature Elimination (RFE), are used to reduce dimensionality and eliminate redundant features, thereby improving the efficiency and accuracy of the models. The core of the methodology involves selecting and training machine learning models capable of distinguishing between legitimate and fraudulent transactions. A variety of algorithms are explored, including logistic regression for its simplicity and interpretability, decision trees and random forests for their ability to model complex decision boundaries, and ensemble methods like gradient boosting for enhanced predictive accuracy. Deep learning models, such as Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), are also considered for their strength in capturing temporal patterns and non-linear relationships in the data. Given the imbalanced nature of the dataset, where fraudulent transactions are relatively rare, techniques like oversampling, undersampling, and the use ofsyntheticdata generation methods (e.g., SMOTE) are employed to ensure balanced training.The trained models are then validated and evaluated using a separate

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

test dataset. Performance metrics such as precision, recall, F1-score, and Area Under the Receiver Operating Characteristic Curve (AUC-ROC) are used to assess the models' effectiveness. These metrics help determine the trade-offs between identifying fraudulent transactions and minimizing false positives, which is crucial for maintaining a positive user experience and operational efficiency.In the deployment phase, the models are integrated into a real-time processing pipeline capable of handling high-velocity data streams. Technologies like Apache Kafka and Apache Spark are utilized to ensure low- latency data ingestion and processing. The deployed system continuously monitors incoming transactions, applying the trained models to detect potential fraud. To maintain the system's relevance and accuracy, a continuous learning framework is implemented,where models are periodically retrained on new data to adapt to evolving fraud patterns and tactics.The methodology also includesrobust security measures to protect sensitive financial and personal data, ensuring compliance with data protection regulations suchas GDPR and PCI DSS. The entire process is supported by a scalable infrastructure, often leveraging cloud platforms like AWS, Azure, or Google Cloud for their robust computing resources and machine learning services.In summary, the methodology combinesdata preprocessing, feature engineering, machine learning model selection, and realtime deployment to create an effective online payment fraud detection system. Continuous evaluation and model updating ensure the system remains robust against new fraud techniques, providing reliable protection for businesses and consumers in the digital payment space.

3.1 INPUT

The inputs for the online payment fraud detection system consist of a diverse set of data points that capture various aspectsof each transaction and the associated user behavior. Key inputs include transactional details such as the amount, date and time, payment method, and geographic location. These are supplemented with user-related information, such as account history, device ID, IP address, and browsing patterns. Additionally, metadata such as transaction velocity (e.g., the number of transactions in a short period) and frequency (e.g., typical transaction amounts) are crucial for understanding normal versus abnormal activity. Behavioral biometrics, like keystroke dynamics, mouse movements, and navigation patterns, are also collected to help identify anomalies in user behavior. The system may also use contextual data, such as the type of merchant or product being purchased, which can provide further insight into the legitimacy of the transaction. All these inputs are gathered from various sources, including payment gateways, banking institutions, and user devices, and are crucial for accurately identifying potential fraudulent activities.

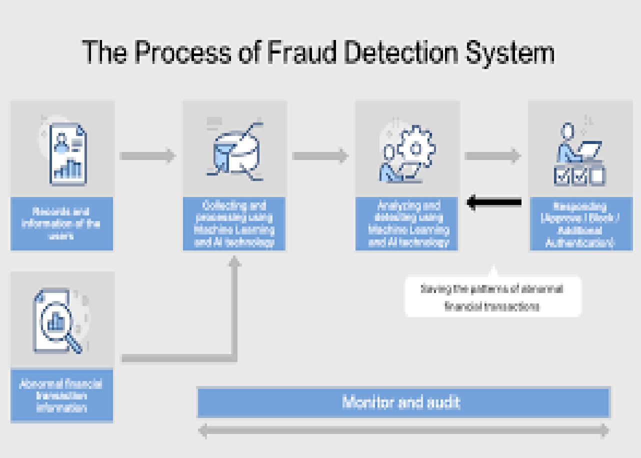
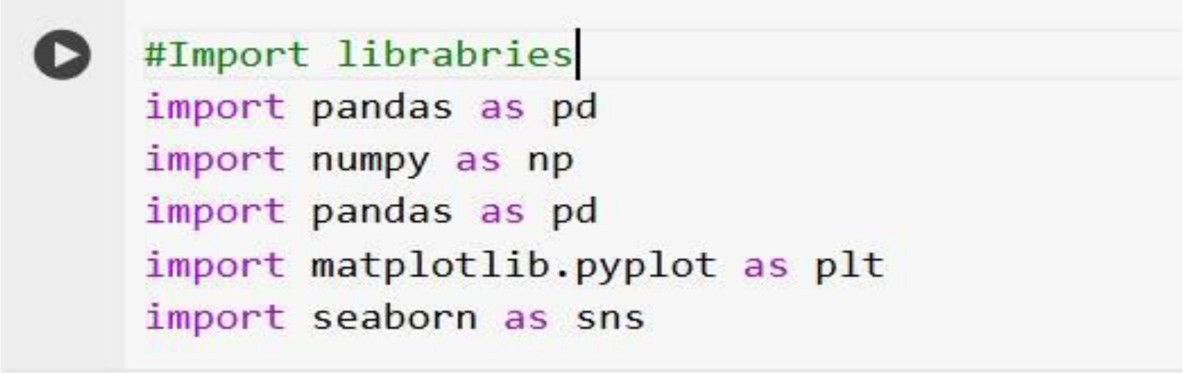

The Process of Fraud Detection System
Records and information of the users
Collecting and processing using Machine Learning and AI technology
Analyzing and detecting using Machine Learning and AI technology
Responding (Approve / Block / Additional Authentication)
Saving the patterns of abnormal financial transactions
Abnormal financial transaction information
Monitor and audit

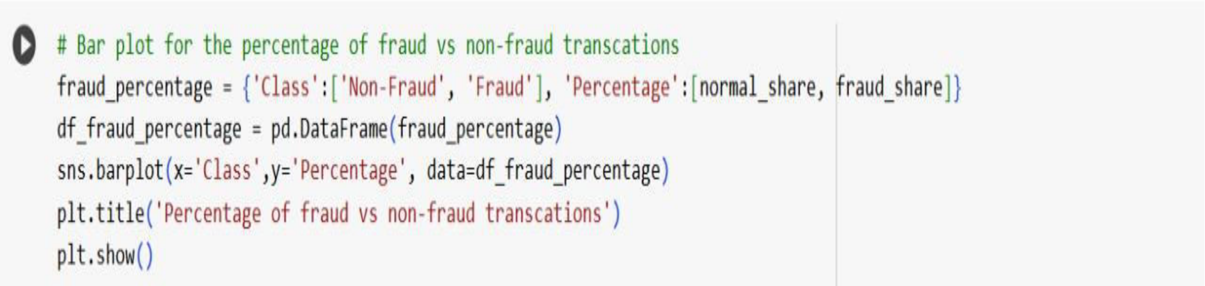
Fig3: Process of the Fraud Detection

3.2 OUTPUT

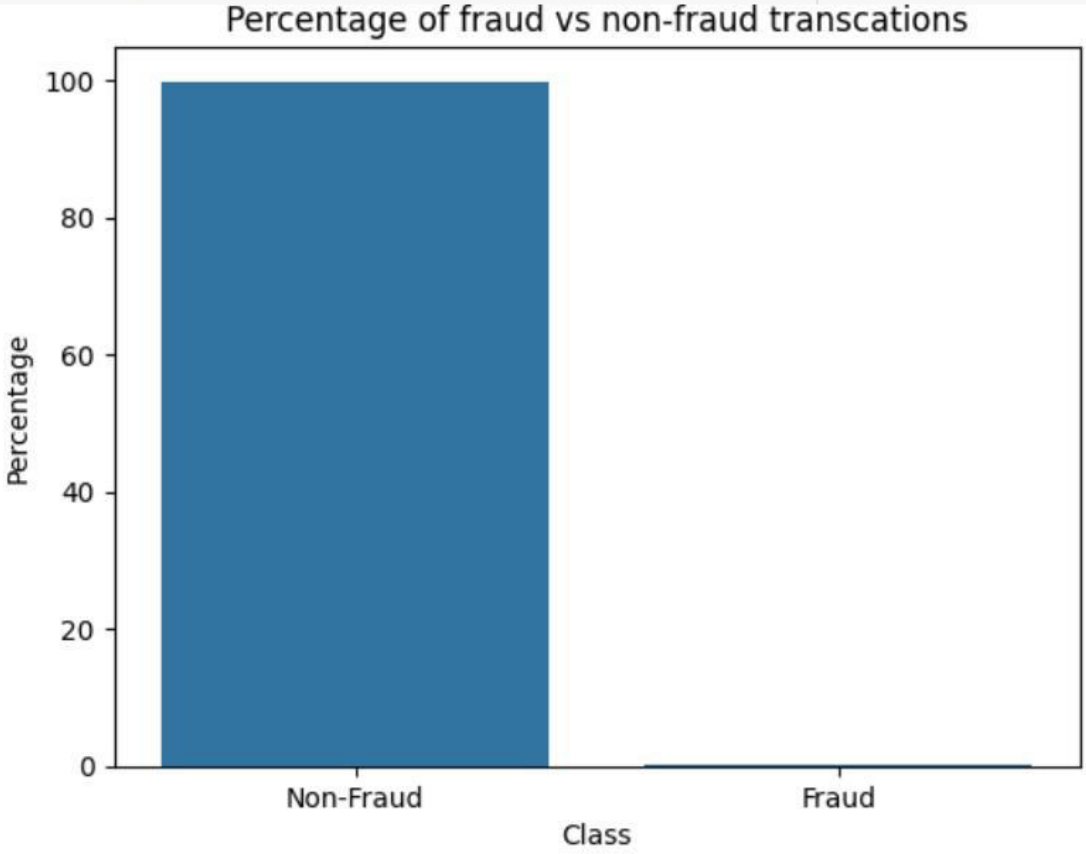
A fraud detection research paper typically presents methodologies, algorithms, and experimental results aimed at identifying fraudulent activities in various domains like finance, e-commerce, and insurance. The output highlights the proposed models (e.g., machine learning, deep learning, or statistical approaches), their performance metrics (e.g., accuracy, confusion, precision, recall, F1-score), and comparisons with existing techniques. It may also include datasets used, feature engineering techniques, and real-world applicability of the fraud detection system, emphasizing its scalability and effectiveness in reducing false positives while maintaining high detection rates.

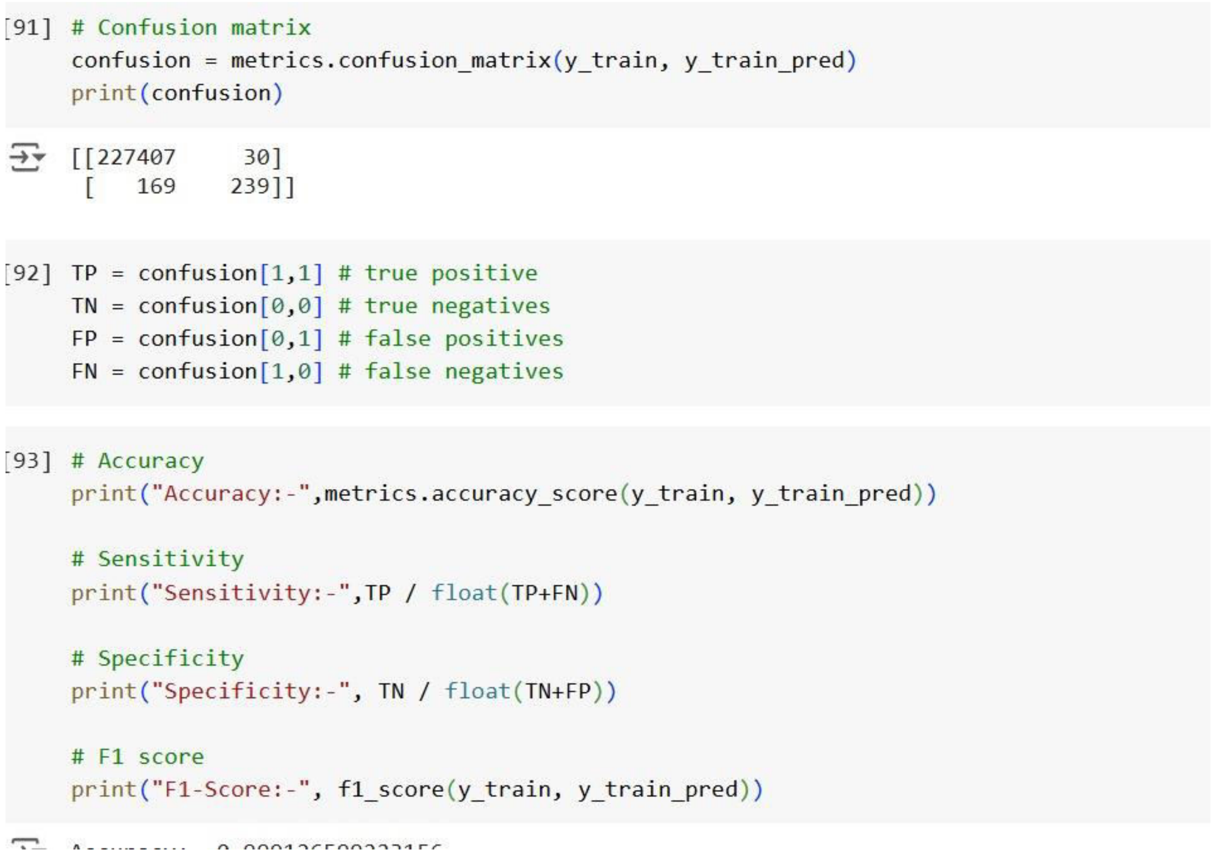


```
#Import librabries
import pandas as pd
import numpy as np
import pandas as pd
import matplotlib.pyplot as plt
import seaborn as sns
```

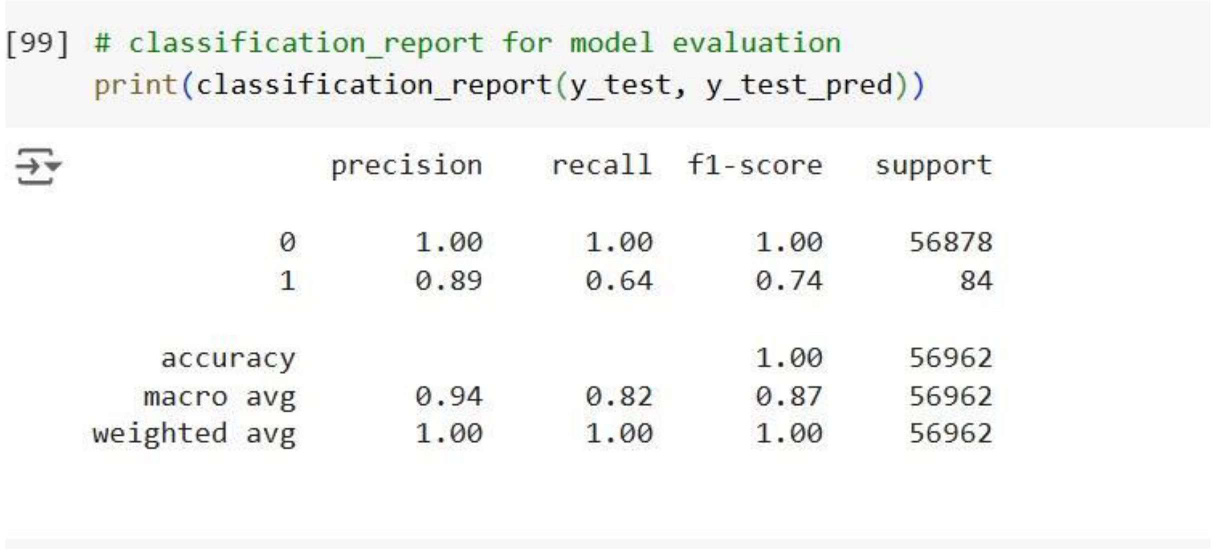


```
# Bar plot for the percentage of fraud vs non-fraud transcations
fraud_percentage = {'Class':['Non-Fraud', 'Fraud'], 'Percentage':[normal_share, fraud_share]}
df_fraud_percentage = pd.DataFrame(fraud_percentage)
sns.barplot(x='Class',y='Percentage', data=df_fraud_percentage)
plt.title('Percentage of fraud vs non-fraud transcations')
plt.show()
```

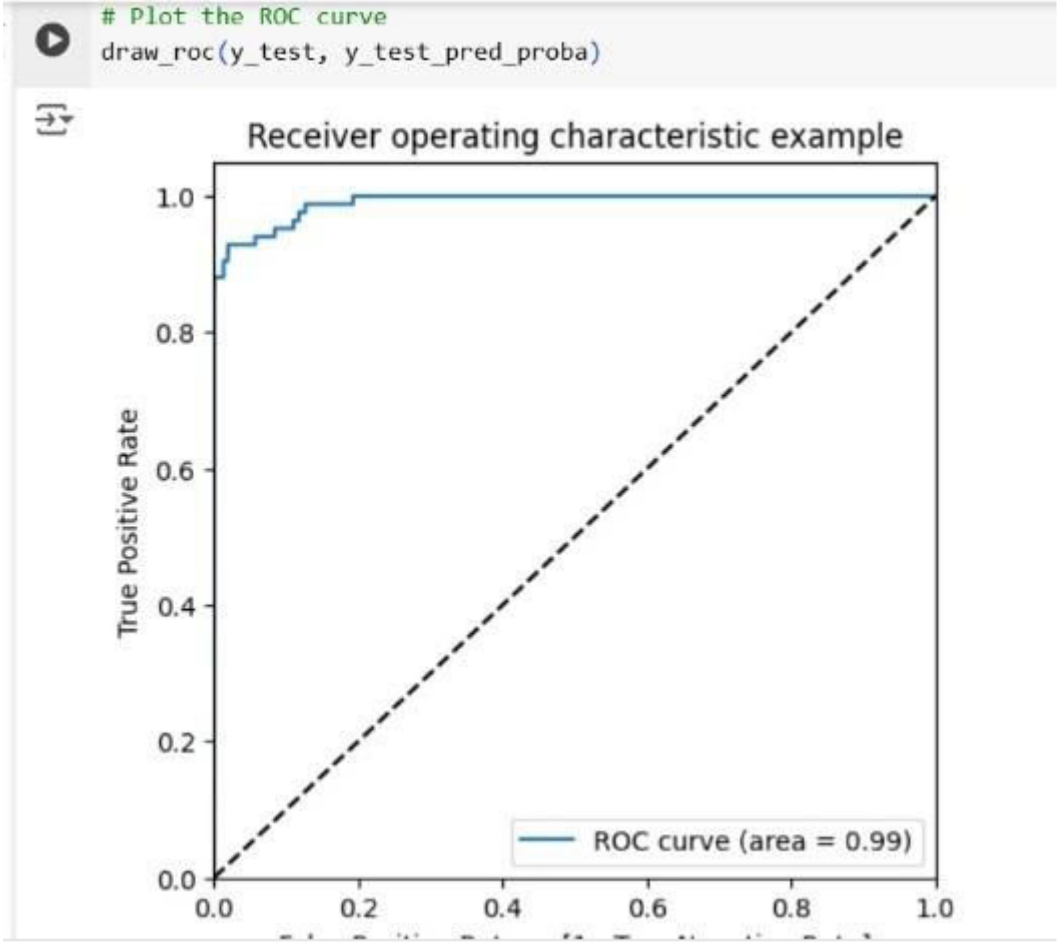




```
[91] # Confusion matrix
     confusion = metrics.confusion_matrix(y_train, y_train_pred)
     print(confusion)

     [[227407     30]
      [   169    239]]

[92] TP = confusion[1,1] # true positive
     TN = confusion[0,0] # true negatives
     FP = confusion[0,1] # false positives
     FN = confusion[1,0] # false negatives

[93] # Accuracy
     print("Accuracy:-",metrics.accuracy_score(y_train, y_train_pred))

     # Sensitivity
     print("Sensitivity:-",TP / float(TP+FN))

     # Specificity
     print("Specificity:-", TN / float(TN+FP))

     # F1 score
     print("F1-Score:-", f1_score(y_train, y_train_pred))

     Accuracy:- 0.9991265992233156
```



```
[99] # classification_report for model evaluation
     print(classification_report(y_test, y_test_pred))

                   precision    recall  f1-score   support

               0       1.00      1.00      1.00     56878
               1       0.89      0.64      0.74        84

        accuracy                           1.00     56962
       macro avg       0.94      0.82      0.87     56962
    weighted avg       1.00      1.00      1.00     56962
```



```
# Plot the ROC curve
draw_roc(y_test, y_test_pred_proba)
```

IV. CONCLUSION

The online payment fraud detection project represents a significant advancement in safeguarding digital transactions through the application of advanced machine learning techniques and real-time data processing. The integration of sophisticated algorithms, including logistic regression, random forests, and deep learning models, has improved the accuracy and efficiency of detecting fraudulent activities compared to traditional rule-based systems. By incorporating real-time processing and behavioural biometrics, the system enhances its ability to respond promptly to suspicious transactions while adding an extra layer of security. However, the project also highlights ongoing challenges, such as the inherent class imbalance in transaction data, which affects model performance and requires continuous refinement. The scalability of the system to handle increasing transaction volumes and the need for effective integration with other security measures remain critical considerations. Additionally, ensuring data privacy and regulatory compliance is essential to maintaining user trust and protecting sensitive information. Looking ahead, the project's future scope includes further advancements in machine learning techniques, exploration of multi-modal data sources, and improvements in real-time processing capabilities. Personalizing fraud detection and enhancing the system's ability to adapt to evolving fraud tactics are also crucial areas for development. Addressing these challenges and leveraging new technologies will continue to enhance the effectiveness and resilience of fraud detection systems, ultimately providing better protection for businesses and consumers in the dynamic landscape of online transactions.

V. FUTURE SCOPE

The future scope for the online payment fraud detection system is promising, with several key areas for advancement and enhancement. Continued innovation in machine learning techniques, such as the development of more sophisticated deep learning models and the application of unsupervised learning methods, holds potential for improved detection accuracy and adaptability to new fraud tactics. Integrating multi-modal data sources, including social media activity and device fingerprints, can provide a more comprehensive understanding of user behaviour and enhance fraud detection capabilities. Additionally, advancing real-time processing technologies and leveraging cloud and edge computing can address scalability challenges, ensuring the system remains effective as transaction volumes grow. Personalizing fraud detection models to individual user behaviours and ensuring robust privacy and compliance measures will be crucial for maintaining user trust and operational effectiveness. Exploring these future developments will enable the system to stay ahead of emerging threats and continue to offer robust protection in the evolving landscape of online payments.

REFERENCES

BOOK REFERENCES

1) Ben Ameur, H., Ftiti, Z., Jawadi, F., & Louhichi, W. (2020). Measuring extreme risk dependence between the oiland gas markets. Annals of Operations Research. https://doi.org/10.1007/s10479-020-03796-1

2) Bernard, P., De Freitas, N. E. M., & Maillet, B. B. (2019). A financial fraud detection indicator for investors: an IDeA. Annals of Operations Research. https://doi.org/10.1007/s10479-019-03360-6A book on Field Guide to the Weather: Learn to Identify Clouds and Storms, Forecast the Weather, and Stay Safe Consultant by Ryan Henning inthe year 2019 link: http://surl.li/oknndt

3) RapidMiner. (2018). Optimize Selection (RapidMiner Studio Core) [Online].

ARTICLE REFERENCES

4) V. Kanade, What is fraud detection? definition, types, applications, and best practices |Spiceworks. Spiceworks(2021, June 11.); www.spiceworks.com. https://www.spiceworks.com/itsecurity/vulnerability- management/articles/what-is-fraud-detection/

5) D.A. Williams, Credit card fraud in Trinidad and Tobago. J. Financ. Crime 14(3), 340–359(2007). https://doi.org/10.1108/13590790710758521

6) S. Mahdi, A. Zhila, Fraud detection and audit expectation gap: Empirical from Iranian bankers. Int. J. Bus.Manag 3(10), 65–67 (2008)

7) C. Singh, Frauds in the Indian Banking Industry. Working Paper, IIMB, WP N0. 505, March 2016

8) B.A. Badejo, B.A. Okuneye, M.R. Taiwo, Fraud detection in the banking system in Nigeria challenges andprospects. J. Econ. Bus. 2(3), 255–282 (2017)

9) Y. Lucas, J. Jurgovsky, Credit card fraud detection using machine learning: a survey. arXiv preprintarXiv:2010.06479 (2020)

10) B. Alghamdi, F. Alharby, An intelligent model for online recruitment fraud detection. J. Inf. Secur. 10(03)(2019). https://doi.org/10.4236/jis.2019.103009

11) Y. Cai, D. Zhu, Fraud detections for online businesses: A perspective from blockchain technology. Financ.Innov 2(1) (2016). https://doi.org/10.1186/s40854-016-0039-4

12) J. Cui, C. Yan, C. Wang, Learning transaction cohesiveness for online payment fraud detection. ACM InternationalConference Proceeding Series, PartF168982 (2021). https://doi.org/10.1145/3448734.3450489

13) J. Cui, C. Yan, C. Wang, ReMEMBeR: Ranking metric embedding-based multicontextual behavior profiling foronline banking fraud detection. IEEE Trans. Comput. Soc. Syst 8(3) (2021). https://doi.org/10.1109/TCSS.2021.3052950

14) S.M. Darwish, An intelligent credit card fraud detection approach based on semantic fusion of two classifiers. Soft.Comput. 24(2) (2020). https://doi.org/10.1007/s00500-019-03958-9

15) M. Huang, L. Wang, Z. Zhang, Improved deep forest mode for detection of fraudulent online transaction. Comput.Inform 39(5) (2021). https://doi.org/10.31577/CAI_2020_5_1082

16) F. Mohammed Aamir Ali, M.A. Azad, M.P. Centeno, F. Hao, A. van Moorsel, Consumer-facing technology fraud:Economics, attack methods and potential solutions. Futur. Gener. Comput. Syst. 100, 408 (2019)

17) S.K. Saddam Hussain, E.S.C. Reddy, K.G. Akshay, T. Akanksha, Fraud detection in credit card transactions usingSVM and Random Forest Algorithms, in 2021 Fifth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), (2021), pp. 1013–1017. https://doi.org/10.1109/ISMAC52330.2021.9640631

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

18) N. Cveticanin, Credit card fraud statistics: What are the odds? | DataProt. Dataprot; dataprot.net (2022, March8). https://dataprot.net/statistics/credit-card-fraud-statistics/
19) J. Chunhua, N. Wang, Research on credit card fraud detection model based on similar coefficient sum, in First InternationalWorkshop on Database Technology and Applications, DBTA 2009, Wuhan, Hubei, China, April 25-26,2009, Proceedings, (2009), pp. 295–298 20) E.W.T. Ngai, H. Yong, Y.H. Wong, Y. Chen, X. Sun, The application of data mining techniques in financial frauddetection: A classification framework and an academic review of literature. Decis. Support. Syst. 50(3), 559–569 (2011)
21) Kanika, J. Singla, A survey of deep learning based online transactions fraud detection systems, in Proceedings ofInternational Conference on Intelligent Engineering and Management, ICIEM 2020, (2020). https://doi.org/10.1109/ICIEM48762.2020.9160200
22) A. Fernández, S. García, M. Galar, R.C. Prati, B. Krawczyk, F. Herrera, Learning from Imbalanced DataSets (Springer, 2018)
23) G. Haixiang, L. Yijing, G. Jennifer Shang, H.Y. Mingyun, G. Bing, Learning from classimbalanced data: Reviewof methods and applications. Expert Syst. Appl. 73, 220–239 (2017)
24) S. Jha, M. Guillen, J.C. Westland, Employing transaction aggregation strategy to detect credit card fraud. ExpertSyst. App 39(16), 12650–12657 (2012)
25) Cheema J, Raza K (2021) Data preprocessing techniques in machine learning: a comprehensive review. Int JComput Intell Syst 14(1):944–971. https://doi.org/10.2991/ijcis.d.210327.001
26) Fan W, Liu K, Liu H, Ge Y, Xiong H, Fu Y (2021) Interactive reinforcement learning for feature selection with decision tree in the loop. IEEE Trans Knowl Data Eng. https://doi.org/10.48550/arXiv.2010.02506. Accessed 03May 2023
27) Ge D, Gu J, Chang S, Cai J (2020) Credit card fraud detection using lightgbm model. In: International conference onE-commerce and internet technology (ECIT), IEEE, pp 232–236. https://doi.org/10.1109/ECIT50008.2020.00060

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING