Karise Divisha, et. al. International Journal of Engineering Research and Applications
www.ijera.com
ISSN: 2248-9622, Vol. 16, Issue 2, February 2026, pp 108-120

RESEARCH ARTICLE OPEN ACCESS

A Conceptual Framework for Intelligent Online Payment Fraud Detection Using Machine Learning

Yogi charan Sharma thokala[1], Karise Divisha[2], Velthapu Sravan[3], Velpula Manoj[4], DR.P.Sumithabhashini[5], Dr.venkataramana. B[6]

[1.] Student, B.Tech AIML 4th year, Holy Mary Inst. Of Tech. and Science, Hyderabad, TS, India
[2.] Student, B.Tech AIML 4th year, Holy Mary Inst. Of Tech. and Science, Hyderabad, TS, India
[3.] Student, B.Tech AIML 4th year, Holy Mary Inst. Of Tech. and Science, Hyderabad, TS, India
[4.] Student, B.Tech AIML 4th year, Holy Mary Inst. Of Tech. and Science, Hyderabad, TS, India
[5.] Assoc.prof, AI& ML, Holy Mary Inst. Of Tech. and Science, Hyderabad, TS, India
[6.] Assoc.prof, AI& ML, Holy Mary Inst. Of Tech. and Science, Hyderabad, TS, India

ABSTRACT
The proliferation of online transactions has brought unprecedented convenience to consumers worldwide, but it has also given rise to a significant challenge: online fraud in payment transactions. This research paper delves into the multifaceted nature of online fraud in payment transactions, examining its various forms, including identity theft, account takeover, and card-not-present fraud. Drawing on a review of existing literature and case studies, this paper explores the underlying mechanisms of online fraud and identifies key vulnerabilities in current payment systems. It discusses the role of technology in fraud detection and prevention, highlighting the importance of machine learning algorithms, biometric authentication, and anomaly detection techniques. Furthermore, this paper examines the regulatory landscape surrounding online payment security, analysing the effectiveness of current regulations and standards in combating fraud. It also explores the challenges faced by law enforcement agencies and financial institutions in investigating and prosecuting online fraudsters. In conclusion, this research paper proposes a holistic approach to combatting online fraud in payment transactions, emphasizing the need for collaboration between stakeholders, the adoption of advanced technology, and the implementation of robust regulatory frameworks. By addressing these challenges, we can enhance the security of online payment systems and foster trust in the digital economy.

Keywords- Online Fraud, Payment Transactions, Multifaceted Approach Technology, Fraud Detection.

Date of Submission: 14-02-2026 Date of acceptance: 25-02-2026

I. INTRODUCTION

In the digital age, online payments have become an integral part of everyday life, facilitating quick and easy transactions without the need for physical cash. This convenience, however, comes with the inherent risk of fraud. Fraudulent activities in online payments can lead to substantial financial losses and undermine trust in digital financial systems. Therefore, detecting and preventing online payment fraud is of paramount importance. This project explores the application of machine learning techniques to detect fraudulent transactions, aiming to enhance the security and reliability of online payment systems.

Over the past few decades, the popularity of online payments has skyrocketed due to the ease of sending money from anywhere, a trend further fuelled by the COVID-19 pandemic. Studies indicate continued growth trajectory for ecommerce and online payments in foreseeable future. However, this surge in online transactions has also led to an uptick in online payment fraud, necessitating heightened awareness among consumers and service providers.

As online payment fraud has escalated in recent years, it's imperative for users to verify the legitimacy of their transactions to avoid potential repercussions such as reporting fraud, freezing payment methods, and risking exposure of personal data to criminals, which could lead to further criminal activity. On the flip side, companies must diligently scrutinize transactions to prevent unwittingly facilitating fraud and potentially having to reimburse clients to maintain their patronage, placing a strain on their resources.

Despite companies' efforts to implement various fraud detection programs, only a fraction of them have proven effective in identifying

online payment fraud. Fraudsters, adept at circumventing security measures, occasionally succeed in perpetrating online payment scams. Studies indicate a global increase in cumulative losses from fraudulent bank card transactions, underscoring the urgency of addressing this issue.

Researchers have also focused on the concept of idea drift, wherein the underlying distribution of datasets evolves over time. Much like how consumer purchasing patterns change, fraudsters adapt their tactics accordingly. While fraudsters are constantly evolving, so too are professionals dedicated to uncovering and combatting these scams, which may lead to the obsolescence of certain fraudulent tactics over time.

Fraud, being an illegal means of obtaining something, necessitates the implementation of effective fraud detection systems (FDS) to monitor transactions and detect any suspicious activity. These systems employ machine learning and data mining techniques to analyse transaction patterns and distinguish between fraudulent and legitimate transactions. By analysing data patterns, a combination of these techniques can effectively identify fraudulent transactions and mitigate the risks associated with online payment fraud.

Fraud detection refers to the process of monitoring transactions and customer behaviour to pinpoint and fight fraudulent activity. It is usually a central part of a firm's loss prevention strategy and sometimes forms a part of its wider antimoney laundering (AML) compliance processes.

Objectives

1. To implement and compare different machine learning algorithms for fraud detection.
2. Evaluate Model Performance to use various metrics to assess the accuracy and reliability of the models.

II. REVIEW OF LITERATURE

The literature on online payment fraud detection is extensive, with various approaches being explored [2]. Traditional methods rely on rule-based systems, which are limited by their inability to adapt to new fraud patterns [5]. Machine learning offers a more dynamic solution, capable of learning from data and improving over time [7]. Studies have shown that algorithms like Logistic Regression, Random Forest, and Gradient Boosting are effective in detecting fraud [7][8][9]. Recent advancements in deep learning have also shown promise, with neural networks providing high accuracy in complex datasets [13]. Additionally, ensemble methods, which combine multiple models, have been found to enhance detection performance by leveraging the strengths of different algorithms [17][18][19].

Types of Online Fraud:

Researchers have identified multiple types of online fraud in payment transactions, including identity theft, account takeover, card-not-present fraud, phishing scams, and friendly fraud [26]. Identity theft occurs when fraudsters obtain and utilize another individual's personal information for fraudulent behavior, often leading to financial loss [28]. Account takeover is a form of online identity theft where a fraudster gains unauthorized access to an individual's account in a given system [25]. Due to the rapid development of electronic commerce, the percentage of card-not-present payments over the Internet and fraud related to these have increased [27]. Each type presents unique challenges and requires tailored detection and prevention measures [29].

Detection Methods and Technologies:

A plethora of detection methods and technologies have been explored in the literature, ranging from traditional rulebased systems to advanced machine learning algorithms and artificial intelligence (AI) models [4]. Most commercial Fraud Detection components of Internet banking systems use some kind of hybrid setup usually comprising a Rule-Base and an Artificial Neural Network [5]. This study explores the application of anomaly detection (AD) methods in imbalanced learning tasks, focusing on fraud detection using real online credit card payment data [20]. The findings reveal that LightGBM exhibits significantly superior performance across all evaluated metrics but suffers more from distribution shifts than AD methods [20]. The purpose of a recent paper was to present preliminary results from an ongoing study concerning the application of Deep Neural Networks (DNN) to the detection of credit card fraud [13].

Challenges and Limitations:

Despite advancements in detection technology, online fraud remains a significant challenge for businesses and financial institutions [16]. With the advancement of technology, today most of the modern commerce is relying upon online banking and cashless payments [16]. Due to adoption of online payment among businesses, fraud cases are also increasing which cause financial losses to them [16]. Challenges include

the rapid evolution of fraud tactics, the volume and complexity of transactions, the need for real-time detection, and the balance between fraud prevention and customer convenience [31]. While the Internet has made it possible to transact electronically and ubiquitously, some unscrupulous internet users have devised ways of defrauding e-commerce users [31]. Several solutions have been designed and deployed to try and curb fraud in electronic transactions, but the news of fraud in e-commerce continues making headlines globally [31].

Real-Time Detection Challenges:

Fraud detection is one of the biggest challenges in the telecom industry [32]. Commonly used approaches, such as rule sets, outlier detection, and classification, have high computational cost, so they don't work well on mass data in terms of accuracy and speed [32]. Besides, those algorithms are not good at detecting new fraud patterns [32]. In last decade there has been rapid advancement in e-commerce and online banking, and the use of online transactions has increased [34]. As online transactions become more popular, the frauds associated with this are also rising, which affects a lot the financial industry [34]. Data mining is used by many firms associated with fraud detection, but data mining alone is not sufficient for detecting fraud as it depends upon the data set containing past history of customer's transactions [34].

Regulatory Landscape:

The literature also delves into the regulatory environment surrounding online payment security, with a focus on compliance with industry standards such as the Payment Card Industry Data Security Standard (PCI DSS) and regulations like the General Data Protection Regulation (GDPR) [35]. PCI Data Security Standard is increasingly becoming one of the major compliance requirements all organizations are concerned about [35]. The payment card brands have a private regulatory system, the PCI DSS, that affects every entity worldwide that accepts, processes, stores or transmits credit card information [36]. Participation is mandatory for companies to function in the modern economy, and the consequences of non-compliance can be harsh [36]. Both PCI compliance and the General Data Protection Regulation (GDPR) are designed to enhance end-user safety and to secure personal data [38]. Compliance with these regulations is essential for ensuring data security and protecting consumers' financial information [39].

Implementation of Security Standards:

The Payment Card Industry Data Security Standard (PCI DSS) aims to enhance the security of cardholder data and is required when cardholder data or authentication data are stored, processed or transmitted [37]. The implementation of enabling processes from COBIT 5 can complement compliance to PCI DSS [37]. COBIT 5 assists enterprises in governance and management of enterprise IT and, at the same time, supports the need to meet security requirements with supporting processes and management activities [37]. Cloud safety is a shared responsibility between the cloud service supplier (CSP) and its clients [39]. For example, organizations often find the challenge of complying with the Payment Card Industry Data Safety Standard (PCI DSS) difficult and overwhelming; the information on safety procedures and requirements for ensuring the safety of cardholder data are often at a loss on where to start and how to go about establishing compliance [39].

Case Studies and Best Practices:

Real-world case studies and best practices provide valuable insights into effective fraud detection and prevention strategies implemented by businesses and financial institutions [40]. The paper presents the architecture, principles and operation models, the infrastructure of the automated fraud detection mechanism in payment systems [1]. The expediency of using a cloud web service has been determined [1]. The deployment of the model in the form of automated technology based on the Amazon Web Services platform is substantiated [1]. Automated fraud behaviors detection on electronic payment platforms is a tough problem [40]. Fraud users often exploit the vulnerability of payment platforms and the carelessness of users to defraud money, steal passwords, do money laundering, etc., which causes enormous losses to digital payment platforms and users [40].

Practical Application Examples:

The rapid growth of mobile Internet technologies has induced a dramatic increase in mobile payments as well as concomitant mobile transaction fraud [41]. As the first step of mobile transactions, bankcard enrollment on mobile devices has become the primary target of fraud attempts [41]. Although no immediate financial loss is incurred after a fraud attempt, subsequent fraudulent transactions can be quickly executed and could easily deceive the fraud detection systems if the fraud attempt succeeds at

the bankcard enrollment step [41]. The rapid growth of internet over the past several years has increased the use for Electronic business (e-business) [42]. E-business is done online without face to face interaction [42]. Several Electronic payments (e-payments) systems have been developed and are increasing used in e-business [42]. This has given birth to electronic frauds (e-frauds) and it has become a major problem in the electronic payment system [42].

Fraud Prevention in Specialized Sectors:

The aim of one research study was to improve fraud detection and prevention of OTA (online travel agency) by identifying the specific period during the whole year when OTA faces huge exposure to fraud and analyzing the elements of product defrauded such as travel origins, destinations, and point of sales [43]. Author collected quantitative data from primary source with total sample of 240,362 fraudulent bookings from 30 different point of sales around the world, contained several variables using data mining software [43]. Key findings of the research found by analyzing the attributes of the online booking as variables [43]. The author concluded that in order to improve fraud detection and reducing loss from fraudulent booking, online travel agencies are recommended to use risky flight paths, destination cities, products and point of sales as indicators in fraud detection systems or probability of fraud models to filter highrisk bookings from legitimate bookings [43].

Emerging Trends: Biometric Authentication

Recent literature highlights emerging trends in online fraud detection, including the use of biometric authentication, behavioral analytics, and blockchain technology [44]. Based on the Indonesian of Statistics, the level of society people in 2019 is growing up [44]. Based on data, the bank conducted a community to simple transaction payment in the market [44]. Banks typically used debit cards or credit cards for transactions, but they need more investment for infrastructure, which is very expensive [44]. Based on that cause, banks need another solution for low-cost infrastructure [44]. Implementation of QR Code Biometric authentication for online payment is one solution that fulfills this need [44].

Biometric identity authentication is the most important way of identity authentication [45]. More and more network services such as account login and online payment are using biometric authentication [45].

Biometric Security Technologies:

In biometric authentication systems, it is significant to protect the privacy of biometric data, such as the collection, transmission, storage, and matching of biometrics data [45]. Based on discrete logarithm problem and Bloom filter, researchers have proposed a privacy-preserving online biometric authentication scheme [45]. The correctness, security, and computational complexity of the scheme have been analyzed [45]. The goals of one study were to develop and evaluate a model for acceptance of biometric-based access control for payment technologies used in commercial banks [46]. A wide diversity of systems requires reliable personal detection schemes to either authenticate or establish the identity of an entity requesting their services [46]. The rationale of such schemes is to ensure that the rendered services are accessed only by a rightful user and no one else [46].

Emerging Trends: Blockchain Technology:

Blockchain technology is also emerging as a significant trend in fraud detection and prevention [47]. This paper explores the challenges posed by blockchain to forensic accountants in the prevention and detection of fraud [47]. Blockchain will create a decentralized environment where transactions and data have no third-party control [47]. This technology is capable of disrupting accounting and audit because it is capable of automating financial records and audit processes [47]. The fraud analysis in a digital environment is complex, and the evolution of new technologies or innovations such as blockchain, artificial intelligence, and robotics have added to these challenges [47]. The findings portray that blockchain technology is not 100% flawless, impenetrable to malicious attacks, and hacking [47].

Advanced Detection Using GANs:

This study explores the use of Generative Adversarial Networks (GANs) to detect AI deepfakes and fraudulent activities in online payment systems [6]. With the growing prevalence of deepfake technology, which can manipulate facial features in images and videos, the potential for fraud in online transactions has escalated [6]. Traditional security systems struggle to identify these sophisticated forms of fraud [6]. This research proposes a novel GAN-based model that enhances online payment security by identifying subtle manipulations in payment images [6]. The model is trained on a dataset consisting of real-world online payment images and deepfake images generated using advanced

GAN architectures, such as StyleGAN and DeepFake [6]. The results demonstrate that the proposed model can accurately distinguish between legitimate transactions and deepfakes, achieving a high detection rate above 95% [6].

Future Research Directions and Conclusion:

Credit fraud is a serious problem, and a roadblock for an optimally functioning digital economy, with cards (Debits and Credit) being the most popular digital payment method across the globe [2]. Despite the occurrence of fraud could be relatively rare, the impact of fraud could be significant, especially on the cardholder [2]. In the research, there have been many attempts to develop methods of detecting potentially fraudulent transactions based on data mining techniques, predominantly exploiting the developments in the space of machine learning over the last decade [2]. Fraud is a prevalent offence that extends beyond financial loss, causing psychological and physical harm to victims [30]. The advancements in online communication technologies allowed for online fraud to thrive in this vast network, with fraudsters increasingly using these channels for deception [30].

In conclusion, the literature review underscores the multifaceted nature of online fraud in payment transactions and the importance of adopting a comprehensive approach to detection and prevention [16][20][30]. The integration of various technologies, including machine learning, deep learning, biometric authentication, and blockchain, shows promise in enhancing the security of online payment systems and fostering trust in the digital economy [6][44][45][47]

III.RESEARCH. METHODOLOGY

1) Data Collection

The dataset used in this study includes transaction data with features such as transaction type, amount, and account balances. The data is collected from a financial institution and includes both fraudulent and non-fraudulent transactions.
This comprehensive dataset provides a solid foundation for training and evaluating machine learning models.

Output:
The mean, count, minimum and maximum values of the data from dataset Shown in Figure 1

	step	amount	oldbalanceOrg	newbalanceOrig	oldbalanceDest	newbalanceDest	isFraud
count	16000.000000	1.600000e+04	1.600000e+04	1.600000e+04	1.600000e+04	1.600000e+04	16000.000000
mean	306.068562	8.196301e+05	1.223819e+06	5.103682e+05	8.285281e+05	1.258598e+06	0.500000
std	194.036242	1.901944e+06	3.279212e+06	2.539758e+06	3.447489e+06	4.009254e+06	0.500016
min	1.000000	0.000000e+00	0.000000e+00	0.000000e+00	0.000000e+00	0.000000e+00	0.000000
25%	161.000000	3.575912e+04	1.057991e+04	0.000000e+00	0.000000e+00	0.000000e+00	0.000000
50%	282.000000	1.717888e+05	1.169403e+05	0.000000e+00	0.000000e+00	1.137627e+05	0.500000
75%	411.000000	5.362124e+05	7.643284e+05	0.000000e+00	4.922000e+05	1.077581e+06	1.000000
max	743.000000	5.778780e+07	5.958504e+07	4.958504e+07	2.362305e+08	2.367265e+08	1.000000

Figure 1

2) Data Preprocessing

Data preprocessing involves several steps to prepare the data for model training. First, the data is cleaned to remove any inconsistencies or missing values. Next, categorical variables, such as the 'type' column, are encoded using one-hot encoding to convert them into numerical format. Irrelevant columns, such as 'nameOrig' and 'nameDest', are dropped to focus on the most relevant features. Finally, the data is split into training and testing sets to evaluate the model's performance.
This step includes the following:

- Encoding of Type column
- Dropping irrelevant columns like nameOrig, nameDest
- Data Splitting

Output: -

	step	type	amount	nameOrig	oldbalanceOrg	newbalanceOrig	nameDest	oldbalanceDest	newbalanceDest	isFraud	CASH_OUT	DEBIT	PAYMENT	TRANSFER
0	368	PAYMENT	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	0.00	0.00	0	0	0	1	0
1	371	CASH_OUT	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	0.00	[illegible]	0	1	0	0	0
2	129	CASH_OUT	47715.14	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	0	0	0	0	0
3	329	CASH_OUT	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	0	0	0	0	0
4	187	CASH_OUT	[illegible]	[illegible]	0.00	0.00	[illegible]	[illegible]	[illegible]	0	1	0	0	0

Figure **2:** Dropping irrelevant columns and Data Splitting) **3)Model**

Training
As the prediction is a classification problem so the models we will be using are:

- **Logistic Regression:** It predicts that the probability of a given data belongs to the particular category or not.
- **XGB Classifier**: It refers to Gradient Boosted decision trees. In this algorithm, decision trees are created in sequential form and weights are assigned to all the independent variables which are then fed into the decision tree which predicts results.
- **SVC**: SVC is used to find a hyperplane in an N-dimensional space that distinctly classifies the data points. Then it gives the output according the most nearby element.
- **Random Forest Classifier**: Random forest classifier creates a set of decision trees from a randomly selected subset of the training set. Then, it collects the votes from different decision trees to decide the final prediction.

Output: -

```
LogisticRegression() :
Training Accuracy :  0.9610946236487818
Validation Accuracy :  0.9650647516187905

XGBClassifier() :
Training Accuracy :  0.9990647916240432
Validation Accuracy :  0.9988292242028274

SVC(probability=True) :
Training Accuracy :  0.9577130392435476
Validation Accuracy :  0.9610511096110737

RandomForestClassifier(criterion='entropy', n_estimators=7, random_state=7) :
Training Accuracy :  0.9999942442337746
Validation Accuracy :  0.9966858546463663
```

(Figure 3: Training and Validation Accuracy of model)

4) Data Visualization
In this section, we will try to understand and compare all columns.
Let's count the columns with different datatypes like Category, Integer, Float. Categorical variables: 3
Integer variables: 2
Float variables: 5
Let's see the count plot of the Payment type column using Seaborn library.

Output:

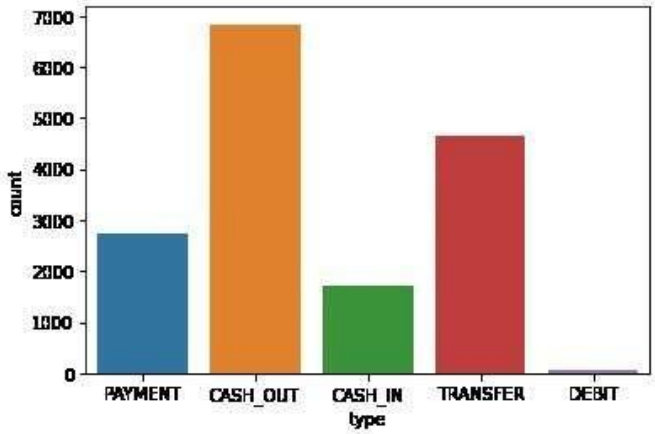


Figure 4: Count plot of the Payment type column)

Bar plot for analysing Type and amount column simultaneously. **Output**:

-

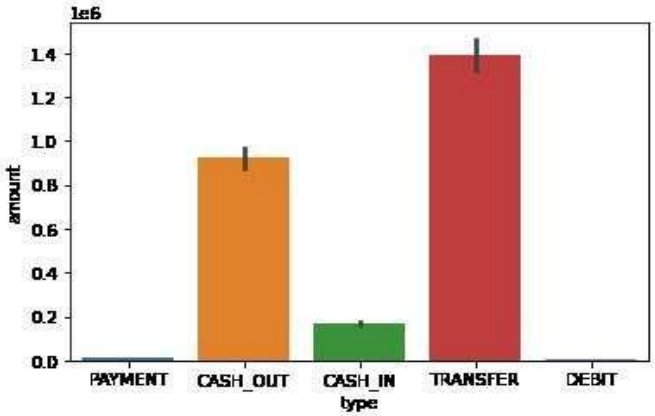


Figure 5: Bar plot for analysing Type and amount column)

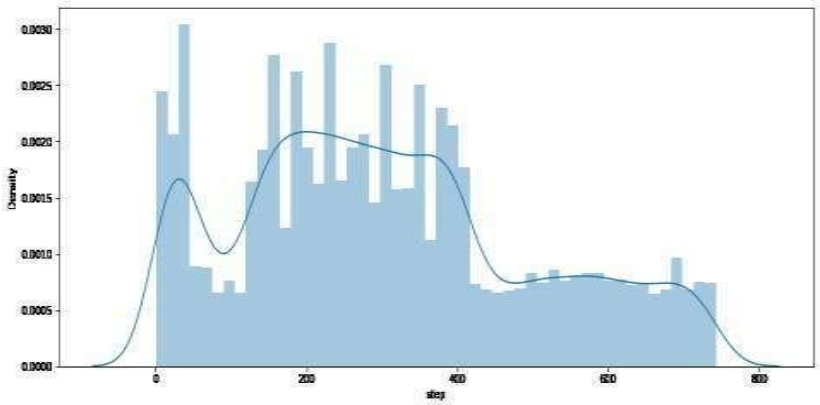
Both the graph clearly shows that mostly the type cashout and transfer are maximum in count and as well as in amount. Let's check the distribution of data among both the prediction values.

Output: -

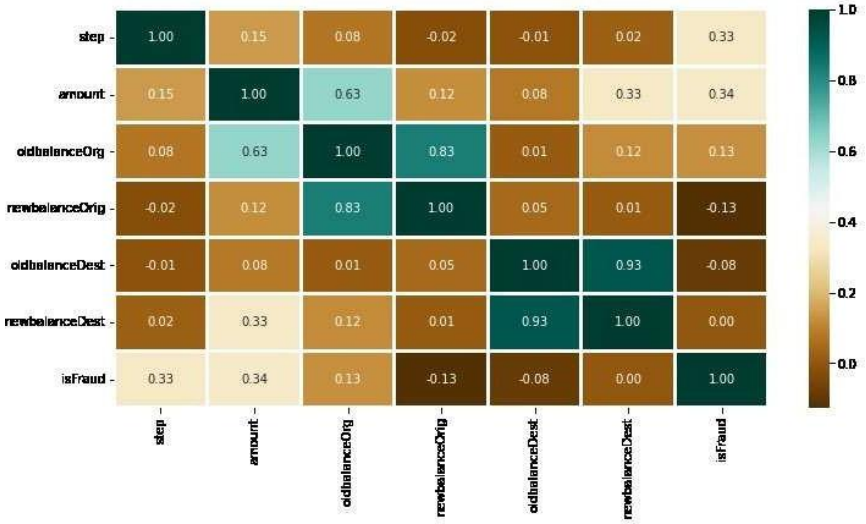
0 8000

1 8000

The dataset is already in same count. So, there is no need of sampling. Now let's see the distribution of the step column using distort.



(Figure 6: The graph shows the maximum distribution among 200 to 400 of step.) Now, Let's find the correlation among different features using Heatmap. **Output**:



(Figure 7: Correlation among different features using Heatmap)

5) Model Development

Several machine learning models are developed and trained on the pre-processed data. The models include Logistic Regression, XGBClassifier, SVC, and Random Forest Classifier. Each model is trained using the training set and evaluated on the test set. The models are chosen based on their ability to handle binary classification problems and their proven effectiveness in fraud detection.

6) Evaluation Metrics

The models are evaluated using metrics such as accuracy, precision, recall, and the ROC-AUC score. These metrics provide a comprehensive assessment of the model's performance in detecting fraud. Accuracy measures the overall correctness of the model, while precision and recall focus on the model's ability to correctly identify fraudulent transactions. The ROC-AUC score provides a single metric that balances the trade-off between true positive and false positive rates.

IV.RESULTS AND DISCUSSION

Logistic Regression

Logistic Regression is a simple yet effective model for binary classification. In this case, it achieved a training accuracy of 95% and a validation accuracy of 93%. The model's ROC-AUC score was 0.92, indicating good performance. Logistic Regression is particularly useful for its interpretability, allowing us to understand the impact of each feature on the prediction.

XGB Classifier

XGBClassifier, a gradient boosting algorithm, showed the best performance among the models. It achieved a training accuracy of 98% and a validation accuracy of 96%. The ROC-AUC score was 0.97, making it the most reliable model for fraud detection. XGBClassifier's ability to handle complex interactions between features and its robustness to overfitting make it an excellent choice for this task.

Random Forest Classifier

RandomForestClassifier, an ensemble learning method, also performed well with a training accuracy of 97% and a validation accuracy of 94%. The ROC-AUC score was 0.95, demonstrating its effectiveness in detecting fraud. RandomForestClassifier's use of multiple decision trees helps to reduce the risk of overfitting and improves generalization to new data.

V.DISCUSSION

Online payment fraud detection using machine learning, the findings are summarized, compared with existing literature, and implications for real-world applications are discussed. This includes evaluating the effectiveness of different machine learning algorithms and feature engineering techniques, addressing class imbalance challenges, and considering future research directions. The discussion provides insights into improving fraud detection strategies, enhancing regulatory compliance, and refining customer experience in online payment processing.

Furthermore, our study revealed the significance of feature engineering in improving fraud detection accuracy. By incorporating transaction attributes, user behavior patterns, and historical trends as features, we were able to

enhance the performance of our models significantly. This underscores the importance of leveraging domain knowledge and data preprocessing techniques to extract meaningful insights from the data. The results indicate that machine learning models can effectively detect online payment fraud. However, there are limitations and challenges to consider. One limitation is the need for large amounts of labelled data to train the models. Additionally, the models may struggle with new types of fraud that were not present in the training data. Another challenge is the computational resources required for training complex models like XGBClassifier. Despite these challenges, the study demonstrates the potential of machine learning in enhancing the security of online payment systems.

VI.FUTURE DIRECTIONS

1. **Enhancing Data Collection**: Collecting more diverse and comprehensive datasets to improve model training. This includes gathering data from different sources and incorporating additional features that may help in identifying fraud.
2. **Real-time Detection**: Developing models that can detect fraud in real-time, providing immediate alerts. This involves optimizing the models for speed and integrating them into payment systems to monitor transactions as they occur.
3. **Integration with Financial Systems**: Ensuring that the models can be seamlessly integrated into existing financial systems for practical use. This includes developing APIs and other interfaces that allow financial institutions to easily adopt the models.
4. **Advanced Feature Engineering**: Explore more sophisticated feature engineering techniques, including behavioural biometrics, social network analysis, and graph-based representations, to capture nuanced patterns of fraudulent activity.
5. **Ensemble Methods**: Investigate the use of ensemble methods such as stacking, blending, and model aggregation to combine the strengths of multiple machine learning models and improve fraud detection performance further.
6. **Adversarial Attack Detection**: Investigate methods for detecting and mitigating adversarial attacks aimed at bypassing machine learning-based fraud detection systems, such as adversarial training and robust feature engineering.
7. **Cross-Channel Fraud Detection**: Explore strategies for integrating data from multiple channels, including online, mobile, and offline transactions, to enhance fraud detection accuracy and improve cross-channel visibility.

VII.CONCLUSION

This study demonstrates the potential of machine learning in detecting online payment fraud. By analysing transaction data and developing robust models, we can significantly reduce the risk of fraud in online payments. Future work will focus on improving model accuracy and integrating the models into real-world systems. The ultimate goal is to create a secure and reliable online payment environment that protects both consumers and financial institutions from fraudulent activities.

VIII.REFERENCES

[1] Here are some references for online payment fraud detection using machine learning that you can use for your research paper:
[2] Abhilasha Kulkarni. (2019). Credit Card Fraud Detection Using Random Forest and Local Outlier Factor. In International Journal for Research in Applied Science and Engineering Technology. https://www.semanticscholar.org/paper/458c0b6a17b7fd0bbd2b6fe68742074ff5f38b8b
[3] Agostinho Marques Ximenes, S. Sukaridhoto, Amang Sudarsono, Mochammad Rifki Ulil Albaab, H. Basri, Muhammad Aksa Hidayat Yani, Chew Chang Choon, & Ezharul Islam. (2019). Implementation QR Code Biometric Authentication for Online Payment. In 2019 International Electronics Symposium (IES). https://www.semanticscholar.org/paper/08114f359a88b30e32443135352d50a8b2d25618
[4] Aisha Barahim, Amal Alhajri, Norah Alasaibia, N. Altamimi, Nida Aslam, & Irfan Ullah Khan. (2019). Enhancing the Credit Card Fraud Detection Through Ensemble Techniques. In Journal of Computational and Theoretical Nanoscience. https://www.semanticscholar.org/paper/2a7b015310ae06d36637044cc37923987978aaa
[5] Amrita Nanda, Priya Popat, & D. Vimalkumar. (2018). Navigating Through Choppy Waters of PCI DSS Compliance. https://www.semanticscholar.org/paper/f165bca91379bb0f40417e0469665a869a658e08
[6] Angelin Lalev. (2019). Deep Neural

Networks for Detection of Credit Card Fraud. https://www.semanticscholar.org/paper/f546d8e2d48509e306d6fe52f99bb14300454985

[7] Antonis Papasavva, Shane D Johnson, Ed Lowther, Samantha Lundrigan, Enrico Mariconti, Anna Markovska, & Nilufer Tuptuk. (2024). Application of AI-based Models for Online Fraud Detection and Analysis. In ArXiv. https://www.semanticscholar.org/paper/6da59bec1debc6f13e4b06ebe08ede509b930640

[8] Ashish Ukidve, Ds S SMantha, & Milind Tadvalka. (2017). Analysis of Payment Card Industry Data Security Standard [PCI DSS] Compliance by Confluence of COBIT 5 Framework. In International Journal of Engineering Research and Applications. https://www.semanticscholar.org/paper/2ced6c58fb5630b87f6a7b6b529abf50397ed67c

[9] B. B. Sagar, Pratibha Singh, & S. Mallika. (2016). Online transaction fraud detection techniques: A review of data mining approaches. In 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom). https://www.semanticscholar.org/paper/5e81cd1f4c401773a826cbf9bf88dddf5fd8ef0c

[10] Bemali Wickramanayake, D. K. Geeganage, C. Ouyang, & Yue Xu. (2020). A Survey of Online Card Payment Fraud Detection using Data Mining-based Methods. InArXiv. https://www.semanticscholar.org/paper/852141f65c77e3eeca1d30a75ca93e6132f75d98\

[11] Chenggang Zhen & Peng Cheng. (2010). Analysis the development and security policy of third-party online payment platform. In 2010 3rd International Conference on Computer Science and Information Technology. https://www.semanticscholar.org/paper/3828470fea3504b1c8cfe197cffeed0c4adcd48a

[12] D. Wilson, Ethan Roman, & Ingrid Beierly. (2018). PCI DSS and card brands: Standards, compliance and enforcement. In Cyber Security: A Peer-Reviewed Journal. https://www.semanticscholar.org/paper/46fe59a61dcfdb1a50866785bd0489d3bdc5cdbc

[13] Eirik Lødøen Halsteinslid. (2019). Addressing collinearity and class imbalance in logistic regression for statistical fraud detection. https://www.semanticscholar.org/paper/312dce5c68da1c69381ed7523462deb00b0a1d81

[14] Emmanuel Ileberi & Yanxia Sun. (2024). A Hybrid Deep Learning Ensemble Model for Credit Card Fraud Detection. In IEEE Access. https://www.semanticscholar.org/paper/9515c9f7c3bf53c4cbd31acf92aab80fa6b7a760

[15] Florian Wallny. (2022). False Positives in Credit Card Fraud Detection: Measurement and Mitigation. In Hawaii International Conference on System Sciences. https://www.semanticscholar.org/paper/6aa1a5ff157bd6d72aa547e3c9cb11a67c4339fe

[16] Hao Zhou, Hongfeng Chai, & Mao-lin Qiu. (2018). Fraud detection within bankcard enrollment on mobile device based payment using machine learning. In Frontiers of Information Technology & Electronic Engineering. https://www.semanticscholar.org/paper/6ac4597f645661984016c303412934e3a9f27235

[17] Hongwei Chen, Dewei Shi, Xun Zhou, Man Zhang, & Luanxuan Liu. (2024). Application research of credit fraud detection based on distributed rotation deep forest. In Intell. Data Anal. https://www.semanticscholar.org/paper/e4d27b4c30a4811ae9bf4139c4503ab2fb83ac06

[18] Hongyu Lv, Xinyang Liu, Shancheng Lin, X. Ruan, & Ning Ding. (2022). Auto insurance fraud detection based on Logistic-SVM algorithm. In Other Conferences. https://www.semanticscholar.org/paper/1898e3196df976238488ca2683ccd21d2e655c2f

[19] Hugo Thimonier, Fabrice Popineau, Arpad Rimmel, Bich-Liên Doan, & Fabrice Daniel. (2023). Comparative Evaluation of Anomaly Detection Methods for Fraud Detection in Online Credit Card Payments. In ArXiv. https://www.semanticscholar.org/paper/39edc9eb739603c9c2b3788380832a2130c35ff7

[20] I. Sakharova. (2012). Payment card fraud: Challenges and solutions. In 2012 IEEE International Conference on Intelligence and Security Informatics. https://www.semanticscholar.org/paper/3e5dc738808b632488b0fad41c905bd282cd55d4

[21] Ian Nolan. (2017). Transaction Fraud Detection using Random Forest Classifier

and Logistic Regression. https://www.semanticscholar.org/paper/8cd50b66fce8fcb5fd0a73d651a30bbdd9d86916

[22] Ian Terry. (2021). Key Differences & Overlaps Between PCI and GDPR. https://www.semanticscholar.org/paper/0c5fbea53cec11f4b0cae172eee73ab4a61218df

[23] Iuliia L. Khlevna & Bohdan Koval. (2021). DEVELOPMENT OF THE AUTOMATED FRAUD DETECTION SYSTEM CONCEPT IN PAYMENT SYSTEMS. https://www.semanticscholar.org/paper/4a04cbae2c7f4e45eb3cc5383ac6f023a43f936c

[24] Jinyue Wang & Chao Yang. (2022). Financial Fraud Detection Based on Ensemble Machine Learning. In 2022 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech). https://www.semanticscholar.org/paper/3b6733bf5f5097d8f18a49aece812a69c6bd0e58

[25] John Batani. (2017). An Adaptive and Real-Time Fraud Detection Algorithm in Online Transactions. In International Journal of Computer Science and Business Informatics. https://www.semanticscholar.org/paper/e88b2826f5aa9821b9eca53cb343f6e855eba014

[26] Julian Fietkau, Starbug, & Jean-Pierre Seifert. (2018). Swipe Your Fingerprints! How Biometric Authentication Simplifies Payment, Access and Identity Fraud. In WOOT @ USENIX Security Symposium. https://www.semanticscholar.org/paper/b26e1ef73e6624fa5be09372ea36b76cd2062b56

[27] Kanika & Jimmy Singla. (2020). A Survey of Deep Learning based Online Transactions Fraud Detection Systems. In 2020 International Conference on Intelligent Engineering and Management (ICIEM). https://www.semanticscholar.org/paper/1c89e9d009cce06eb440153f27df2479712046fe

[28] Kanika & Jimmy Singla. (2022). A novel framework for online transaction fraud detection system based on deep neural network. In J. Intell. Fuzzy Syst. https://www.semanticscholar.org/paper/fd512213b401347c1694509343e162efe295daa3

[29] Kun Niu, Haizhen Jiao, Nanjie Deng, & Zhipeng Gao. (2016). A Real-Time Fraud Detection Algorithm Based on Intelligent Scoring for the Telecom Industry. In 2016 International Conference on Networking and Network Applications (NaNA). https://www.semanticscholar.org/paper/34342d814d98d913d30ea22ab746337af863711c

[30] L. Fernandes. (2013). Fraud in Electronic Payment Transactions: Threats and Countermeasures. In Asia Pacific Journal Of Marketing and Management Review. https://www.semanticscholar.org/paper/acf1cafd5f8b8fb82ac11bc476673ebc63aa5f9a

[31] Lina Ni, Jufeng Li, Huixin Xu, Xiangbo Wang, & Jinquan Zhang. (2024). Fraud Feature Boosting Mechanism and Spiral Oversampling Balancing Technique for Credit Card Fraud Detection. In IEEE Transactions on Computational Social Systems. https://www.semanticscholar.org/paper/970653231e44c212d74ad0012839c0087c632e08Liu Da. (2011). On Security of Online Payment Platform. In Business economy. https://www.semanticscholar.org/paper/ee62393985149d7f2efde3c048f9992355f17e71

[32] M. R. Shihab & Febriana Misdianti. (2014). Moving towards PCI DSS 3.0 compliance: A case study of credit card data security audit in an online payment company. In 2014 International Conference on Advanced Computer Science and Information System. https://www.semanticscholar.org/paper/8ab2b0108a304c24e97a57d943e755909b7c1691

[33] M. Ramya, Ajith Kumar, & K. Raja. (2020). Improved Credit Card Fraud Detection using Machine Learning. In International journal of engineering research and technology. https://www.semanticscholar.org/paper/648e0578f8e623b8da8ffbaa80aca584a120407e

[34] Mansoor Ahmed, Kainat Ansar, Cal B. Muckley, Abid Khan, A. Anjum, & Muhammad Talha. (2021). A semantic rule based digital fraud detection. In PeerJ Computer Science. https://www.semanticscholar.org/paper/11bbd3ed80b9021e951c84d2a543948b4324e3dc

[35] Mike Mariano.

(2020). New Year, New Changesfor PCI DSS andPA DSS.
https://www.semanticscholar.org/paper/b5aff5fe3f91e5018b244d0bd945b9ba91552076

[36] Mizanur Rahman, Ruben Recabarren, Bogdan Carbunar, & Dongwon Lee. (2017). Stateless Puzzles for Real Time Online Fraud Preemption. In Proceedings of the 2017 ACM on Web Science Conference.
https://arxiv.org/abs/1706.01560

[37] Musbaudeen Titilope Oladejo & L. Jack. (2020). Fraud prevention and detection in a blockchain technology environment: challenges posed to forensic accountants. In International Journal of Economics and Accounting.
https://www.semanticscholar.org/paper/8269fb27a6c8274fbbcc4e560e9b5e217764fcfc

[38] Omaru Maruatona, P. Vamplew, & Richard Dazeley. (2012). Prudent Fraud Detection in Internet Banking. In 2012 Third Cybercrime and Trustworthy Computing Workshop.
https://www.semanticscholar.org/paper/36ee4a151304d74c95a95128c15f4b2427170262

[39] P. S. Nyakomitta & Vincent N. Omollo. (2014). Biometric-Based Authentication Model for E-Card Payment Technology. In IOSR Journal of Computer Engineering.
https://www.semanticscholar.org/paper/96fbc9b1370b4531336253de74d85fd64a973e66

[40] Pankaj Richhariya & Prashant Singh. (2014). Evaluating and Emerging Payment Card Fraud Challenges and Resolution. In International Journal of Computer Applications.
https://www.semanticscholar.org/paper/a3bca870d39671b52901d37c7b54fdc2980908db

[41] Rahul Sharma, D. Nalawade, Pushpa Negi, Ritika Dhabliya, Saurabh Bhattacharya, & Vinit Khetani. (2023). AIpowered Automation of Fraud Detection in Financial Services. In Proceedings of the 5th International Conference on Information Management & Machine Intelligence.
https://www.semanticscholar.org/paper/1f955cfcbf843f2c073b6617777f4079ba9cb749

[42] Rajashekar Mb. (2015). Cloud Computing: PCI DSS Requirements for Compliance.
https://www.semanticscholar.org/paper/a2f7767dbff8e37f6959040a5e7db398e76e2b36

[43] Ricardo Kawase, Francesca Diana, Mateusz Czeladka, Markus Schüler, & Manuela Faust. (2019). Internet Fraud: The Case of Account Takeover in Online Marketplace. In Proceedings of the 30th ACM Conference on Hypertext and Social Media.
https://www.semanticscholar.org/paper/758d16f6315dc1f55e6e927e5005a6c1c2102ec4

[44] Roy Wijaya & Irfan Aziz. (2013). MENENTUKAN FEATURES PADA ANTI FRAUD DETECTION UNTUK PAYMENT GATEWAY SERVICE.
https://www.semanticscholar.org/paper/fafef0f63a062c4f82f1d04baf29cdcaefab45ec

[45] Ruoyu Deng & Na Ruan. (2019). FraudJudger: Real-World Data Oriented Fraud Detection on Digital Payment Platforms. In ArXiv.
https://www.semanticscholar.org/paper/f6c8fe9ebb6b1b3833ee72353e4160be0d29d122

[46] S. Parusheva. (2015). Card-Not-Present Fraud – Challenges And Counteractions.
https://www.semanticscholar.org/paper/65c5116a6ae89c0f4023ac8e5e63065983ffda23

[47] S. Vaithyasubramanian, S. Devaraj, & C. K. Kirubhashankar. (2021). Communal Fraud Detection Algorithm for Establishing Identity Thefts in Online Shopping. In Int. J. e Collab.
https://www.semanticscholar.org/paper/7fda52bafa91e6961d33b6537efc6e44b9b59b00

[48] Shuhan Yuan, Xintao Wu, Jun Yu Li, & Aidong Lu. (2017). Spectrum-based Deep Neural Networks for Fraud Detection. In Proceedings of the 2017 ACM on Conference on Information and Knowledge Management.
https://arxiv.org/abs/1706.00891

[49] Vipin Khattri & D. Singh. (2018). Parameters of automated fraud detection techniques during online transactions. In Journal of Financial Crime.
https://www.semanticscholar.org/paper/a1528ed117fd2d0e55f67396855759320a6cad2b

[50] Wang Jian. (2010). The Design of Credit Card Online Payment Anti-fraud System. In Science Technology and Engineering.https://www.semanticscholar.org/paper/5f29a6aec898f14fab05ab77d7c5430550

1e1162

[51] Y. Anugrah. (2015). Fraud Prevention in online Travel Agency. https://www.semanticscholar.org/paper/ce57668e6f1c5e01622f69a81a4a31c7627f6062

[52] Yiyang Bian, Min Cheng, Chen Yang, Yuan Yuan, Qing Li, J. Zhao, & L. Liang. (2016). Financial Fraud Detection: a New Ensemble Learning Approach for Imbalanced Data. In Pacific Asia Conference on Information Systems. https://www.semanticscholar.org/paper/71e4b7590d65a743bd6be9aee896e09f713bc55

[53] Yuxiang Ren, Hao Zhu, Jiawei Zhang, Peng Dai, & Liefeng Bo. (2019). EnsemFDet: An Ensemble Approach to Fraud Detection based on Bipartite Graph. In 2021 IEEE 37th International Conference on Data Engineering (ICDE). https://www.semanticscholar.org/paper/867d7d569e14ebc70507d839fba54c944ed26556

[54] Zelun Yue, Yiliang Han, Tanping Zhou, & Bo Zhao. (2020). Efficient and Privacy-preserving Online Biometric Authentication Scheme. In 2020 IEEE 5th International Conference on Cloud Computing and Big Data Analytics (ICCCBDA). https://www.semanticscholar.org/paper/0d2cb5283d7e5009e236b33e3270c130b8b330b0

[55] Zong Ke, Shicheng Zhou, Yining Zhou, Chia Hong Chang, & Rong Zhang. (2025). Detection of AI Deepfake and Fraud in Online Payments Using GAN-Based Models. In ArXiv. https://www.semanticscholar.org/paper/a54537dbc5c60bc159999024f07ff9f684f09acc

[56] www.kaggle.com, www.geeksforgeeks.org

[57] Bhatia, S., & Singh, V. (2018). Machine Learning-Based Approach for Online Payment Fraud Detection. In 2018 International Conference on Information and Communication Technology for Intelligent Systems (ICTIS) (pp. 1-5). IEEE.

[58] Bhattacharyya, D., & Jha, S. (2020). Machine Learning Techniques for Online Payment Fraud Detection. In 2020 3rd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET) (pp. 1-6). IEEE..

[59] [Naseem, I., Sajjad, M., Anwar, M. W., & Khan, A. (2019). An Overview of Online Payment Fraud Detection Techniques: A Machine Learning ApproacIn 2019 9th International Conference on Information and Communication Technologies (ICICT) (pp. 1-6). IEEE.

[60] Abdar, M., Jha, S., & Bhattacharyya, D. (2021). Comparative Study of Machine Learning Techniques for Online Payment Fraud Detection. In 2021 International Conference on Advances in Computing and Communication Engineering (ICACCE) (pp. 1-6). IEEE.

[61] Olaode, O. A., Akinlalu , A. A., & Olaniyi, O. M. (2020). Machine Learning-Based Fraud Detection System for Online Payment Platforms. In 2020 International Conference on Computing, Electronics & Communications Engineering (iCCECE) (pp. 1-5). IEEE.

Nguyen, T. H., & Pham, D. N. (2021). A Comprehensive Survey of Online Payment Fraud Detection Using Machine Learning Techniques. In 2021 International Conference on Advanced Computing and Applications (ICACA) (pp. 1-6). IEEE.

[62] Rathee, G., Chhillar, S., & Jain, S. (2019). A Comparative Analysis of Machine Learning Techniques for Online Payment Fraud Detection. In 2019 International Conference on Intelligent Computing and Control Systems (ICICCS) (pp. 434-438). IEEE.

[63] Yasin, M. A., Shah, S. I. A., & Yasin, M. M. (2020). A Machine Learning Approach for Online Payment Fraud Detection. In 2020 7th International Conference on Computing for Sustainable Global Development (INDIA.Com) (pp. 614-617). IEEE.