Development of Generic Framework for Payment Gateway related to Consumer Applications

Dr. Rajashree Shettar, Avani Goyal, R V College of Engineering

Article Info
Page Number: 1304-1315
Publication Issue:
Vol. 71 No. 3 (2022)

Article History
Article Received: 12 January 2022
Revised: 25 Febuary 2022
Accepted: 20 April 2022
Publication: 09 June 2022

Abstract

Consumer Applications or E-commerce websites uses payment methods for the transaction, where users complete their payment using various methods like card payment, internet banking, unified payments interface (UPI) or cash payment. Many a times while transacting the process and payment fails due to various reasons as wrong One Time Password (OTP), UPI pin, passwords or Card Verification Value (CVV). This payment failure may happen due to misreading or sometimes when someone unauthorized person tries to access the personal accounts and enters wrong details.

Many organizations creates and work on their dashboard to analyze their product, sell/consumption and other factors of their web-app or business. This project mainly focuses on the creation of dashboard to analyze fraud detection and prediction using machine learning algorithm and neural network respectively.

The main objective to build is to analyze frauds happening in consumer application related to payment gateways along with future predictions related to frauds and some key performance indicators (KPI). The methodology used in the fraud detection is KNN classification algorithm which classifies if the payment is a fraud payment or the authentic payment. Along with this future trends of fraud was also predicted using LSTM neural network where a data generated from KPI and fraud detection was passed through it. The input data dataset have various number of defined classes in it, so that the detection and prediction of fraud will be easier along with the KPIs like return of investment, cart abandonment rate and payment conversion rate. The model detects the frauds in payment with 97% accuracy. The dataset used was custom and was used for testing and training purpose.

Key Terms—KNN, LSTM, KPI, Cart abandonment, payment conversion, return of investment, Fraud detection.

1.Introduction

Online transaction are increasing with UPI, cards, net banking as it is easier and saves time of the customer purchase. But as the online transaction is increasing so is the fraud. Hence using machine learning algorithms and ANN model, an attempt has been made to gain the

knowledge about the fraud and genuine transaction. With the increasing usage of ecommerce and online shopping, customer's vital information like card's CVV, UPI pin, OTP, passwords etc. are always vulnerable. The reason for rise in fraud cases is that fraudsters easily barge into the customers private information. Even the banking systems are vulnerable to frauds, also the fraudsters are finding new ways of fraud like identity theft from social media platform so the fraud prevention and detection is an ever evolving process. As the online frauds are ever increasing, the traditional way of detecting and preventing frauds are being replaced by various machine learning algorithms.

Usually fraud detection systems uses transaction rules to find the discrepancy in the transactions. Since it is a time consuming process, fraudsters take a good advantage of the time lag. The vital disadvantage of the system is occurrence of false positive. The false positive rate makes the genuine users fraudsters and blocks their account.

Deep learning and Machine learning also plays a vital role in the fraud detection system and its prediction. Larger the dataset more is the efficiency of the machine learning algorithms to detect the fraudulent transaction data. As it takes a lot of time to manually detect the fraud transaction machine learning algorithms and deep learning algorithms gives a faster and efficient solution and the results not only for fraud detection and prediction but for various real life problems like medical diagnosis, email spam, etc.

Every year organizations or people face loss in large digits. The idea is to analyze the fraud and to know the future trend of the fraud. So that the organizations can increase the authentication and security to reduce the frauds in the system. Also apart from just detecting and predicting frauds, gaining insights about the data and the organization will be helpful in the improvement.

2.Literature Survey

The author in the paper [1] give insights on the application of Big data analysis and Artificial intelligence in banking domain for increasing the customer experience. It shows the best approach used by Indonesian banking and as well global banking for using AI and BDA. Also they have marked the challenges faced during the research for ensuring the data quality for banks and the application of AI and BDA. If the data is not accurate it might not give the perfect analysis report. In [2] the author states how Artificial Intelligence is influencing and affecting the Banking domain. As AI has made processes easy by introducing Drive thru Banking, Passbook Updating, chatbot assistant, Fraud detection and Mobile Banking. As the research progressed it was analysed that the data collected was not that sufficient to analyse also it concluded that not many have the facility and knowledge about the e-banking or internet facility. In [3] authors describe the architecture of big data in banking systems, as well as the tools used to analyze the data, including as machine learning and cluster analytics. The major advantages and drawbacks of Big Data Analytics in the financial industry are also discussed, since the banking sector is still working in this field with AI and computer science, it is not easy to install technology and have employees comprehend and be educated for it all of a sudden.

An experimental universe of financial fraud is achieved by the variety in advanced simplicity to encouraging client dedication with organizations. Over the course of the last year, financial fraud has fundamentally expanded at banks and different foundations of money. As per the rate and setting of credit card use, the review in [4] investigates the chance of false transaction. In the space of computerized financial transaction, a work is made to make a reasonable division between misrepresentation location and the estimating of conceivable fake prospects.

The author in [5] proposes to use the Von Mises Distribution which helps to broaden the transaction aggregation approach and helps in developing some new features set which are basically based on periodic analysis of the time of transaction. Next, cutting-edge credit card fraud detection algorithms are examined, and it is compared to how different sets of characteristics affect the results, the dataset was given by major European card processing business which was authentic credit card fraud data. There was a 13% mean increase in the financial savings which was gained by adding the periodic characteristics in the process.

The research in [6] aims to distinguish between fraudulent and non-fraudulent transactions in terms of transaction time and amount by utilizing classification, computational machine learning and statistics algorithms (differentiation, chain rule, etc.), and linear algebra to build complex machine learning models for prediction and understanding of the data set.

Three significant contributions are made by the document in [7]. First, with assistance from an industry partner, a formalization of the fraud detection issue that precisely examines the circumstances under which Fraud Detection Systems monitors daily sample of credit card transactions. Moreover, shows the best performance metrics for fraud detection. The second point is the authors have created and tested a new learning technique that fortunately handles issues incorporating idea drift, class imbalance, and verification delay. Third, they show how conceptual biases and class imbalances have affected on the actual data with greater than 75 million transactions approved period for a period of 3 years in the trials.

Authors in [8] have trained a machine learning model based on the dataset using a variety of machine learning techniques, including Random Forest, Logistic Regression, Support Vector Machine (SVM), and Neural Network. The optimal algorithm to serve the same aim was projected using a comparative study of the F1 score. The artificial neural network (ANN) performs best, according to the study, with a F1 score of 0.91.

The goal of this project [9] is to recognize device learning algorithms in particular. Both the Adaboost collection of rules and the Random Woodland set of rules are utilized as algorithms. Accuracy, precision, recall, and F1-rating are entirely taken into account while determining the results of the two algorithms. The confusion matrix serves as the primary basis for the primary plotting of the ROC curve. When comparing the Random Forest and Adaboost algorithms, the set of rules with the best accuracy, precision, recall, and F1 score -rating is taken into account because it is the best set of rules that is utilized to identify fraud.

The author's in [10] draw attention to the crucial techniques and procedures used in fraud detection while also concentrating on recent research. The effectiveness of several techniques for spotting fraudulent transactions is examined and assessed. These techniques include Support Vector Machines (SVMs), Artificial Neural Networks (ANNs), k-Nearest Neighbour (k-NN), Decision Tree, naive Bayesian and Frequent Pattern Mining algorithms.

The authors in [11] looked at special machine learning methods to accurately and precisely predict the validity of financial transactions. For this investigation, the following algorithms were used: MLP Repressor, Random Forest Classifier, Complement NB, K Neighbors Classifier, Logistic Regression, Bagging Classifier, LGBM Classifier, Decision Tree

Classifier, Deep Learning, MLP Classifier, Gaussian NB and Bernoulli NB. The dataset was built up from the Kaggle repository. Random Forest Classifier was created using the pleasing classifier and an imbalanced dataset. The accuracy was 99.97%, the precession was 99.96%, the recall was 99.97%, and the F1 rating was 99.96%. The pleasing classifier, however, turned into the Bagging Classifier when the dataset was balanced. The accuracy was 99.96%, the precession was 99.95%, the recall was 99.98%, and the F1 rating was 99.96%.

In this study [12], the author suggests various data science techniques for generating new results for credit card fraud detection. The techniques suggested were the machine learning algorithms using Random Forest and the deep learning Convolutional Neural Network. Check the precision of the previously mentioned algorithms (RFA, CNN) to determine whether they are accurate, and provides with the user interface to determine if the transaction in the sector or the bank is real, genuine or fraudulent. Rise in the credit card frauds is genuine as the usage of e-commerce increases.

3. Methodology

The proposed system for detecting and predicting the frauds in the organization uses various parameters like OrderID, OrderDate, Category, SubCategory, CustomerName, Country, State, email, IP, PaymentMethod, where these inputs are fed into the K-nearest Neighbour classifiers to classify the data as fraud or no-fraud. Further the detected data is used for the prediction of the fraud trends using LSTM model where the model is fed with the fraud detection sample.

Here the KPIs created are based on the data and to gain the insights about the data like return on investment, cart abandonment rate and payment conversion rate. The KPIs are basically curated in order to know when and why the user did not complete the payment or what is the payment mode for the transaction and the rate at which the assets in carts are being abandoned.

4. Design

Figure 1 shows the system architecture of the dashboard for fraud detection, prediction and analysis. The dataset used was passed through the preprocessing pipeline after which it was passed to the models created for analytics and predictions. The data prepared was used to create a graph from samples and these plots were passed to the dashboard with sample counts and performance analysis. For evaluating performance of the system, Recall, precision , false positive, true positive, true negative and false negative were taken in consideration which were calculated using the values of confusion matrix.

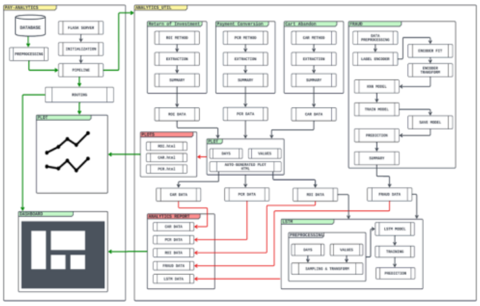


Fig. 1. System Design

Fraud Analyzer and predictor model is as shown in Fig 2. Data passes through the following modules in order to predict and detect the fraud.

- Data pre-processing
- Data analysis and fraud detection
- Fraud prediction
- Data rendering to dashboard

The pre-processing phase is the initial step where the data cleaning and other preprocessing steps are performed in order to make the data ready to feed the system. The output gained from pre-processed data is given as input for the analysis. In data analysis and fraud detection the preprocessed data is used for analyzing return on investment, payment conversion rate, cart abandonment rate and fraud detection, in fraud detection K-nearest Neighbour classifier is used where the data is classified as 0 or 1 for no-fraud or fraud respectively. In the next flow LSTM model takes the fraud detection and return on investment sample as the input to predict the fraud trend for next 30 days, later the data curated is used for further predictions by applying data sampling in the LSTM model. Further these samples generated are saved in the form of generated HTML files and are rendered to the dashboard.

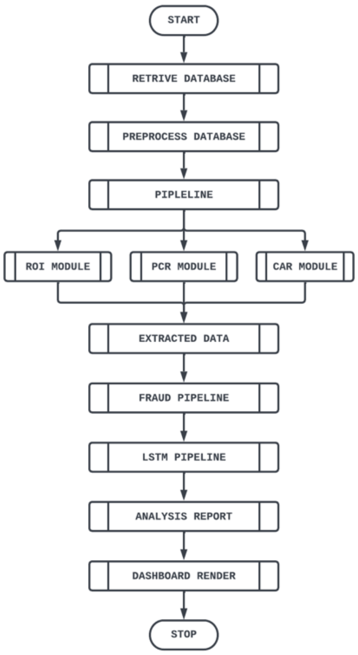
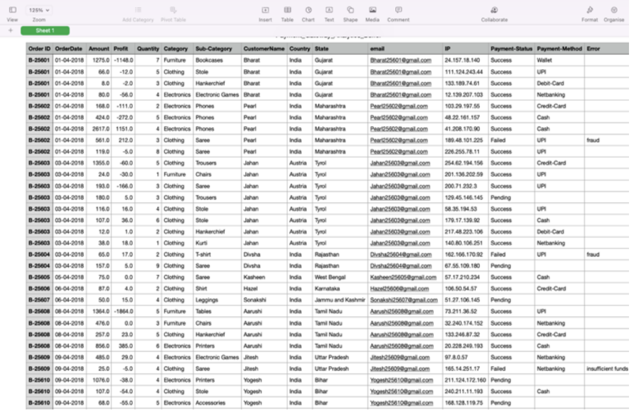


Figure 2 Flowchart of the proposed system

5. Proposed System

The dashboard was prepared on a dataset of size [4501, 15]. The data set is shown in the figure 3, it contains 15 attributes and 4501 data entry. The data attributes are like order_id, payment method, customer id, amount, quantity etc. This dataset was passed through the preprocessing pipelines where the missing values were treated. Further few Key Performance Indicators –

return on investment, payment conversion, cart abandonment was analyzed where the user can know how many customers did not proceed for payment or checkout from the cart or other insights regarding the data. The data summary and charts or graphs curated from these KPIs were saved in the form of an HTML file.



Order ID	OrderDate	Amount	Profit	Quantity	Category	Sub-Category	CustomerName	Country	State	email	IP	Payment-Status	Payment-Method	Error
B-25601	01-04-2018	1275.0	-1148.0	7	Furniture	Bookcases	Bharat	India	Gujarat	Bharat25601@gmail.com	24.157.18.140	Success	Wallet	
B-25601	01-04-2018	66.0	-12.0	5	Clothing	Stole	Bharat	India	Gujarat	Bharat25601@gmail.com	111.124.243.44	Success	UPI	
B-25601	01-04-2018	8.0	-2.0	3	Clothing	Hankerchief	Bharat	India	Gujarat	Bharat25601@gmail.com	133.189.74.61	Success	Debit-Card	
B-25601	01-04-2018	80.0	-56.0	4	Electronics	Electronic Games	Bharat	India	Gujarat	Bharat25601@gmail.com	12.139.207.103	Success	Netbanking	
B-25602	01-04-2018	168.0	-111.0	2	Electronics	Phones	Pearl	India	Maharashtra	Pearl25602@gmail.com	103.29.197.55	Success	Credit-Card	
B-25602	01-04-2018	424.0	-272.0	5	Electronics	Phones	Pearl	India	Maharashtra	Pearl25602@gmail.com	48.22.161.157	Success	Cash	
B-25602	01-04-2018	2617.0	1151.0	4	Electronics	Phones	Pearl	India	Maharashtra	Pearl25602@gmail.com	41.208.170.90	Success	Cash	
B-25602	01-04-2018	561.0	212.0	3	Clothing	Saree	Pearl	India	Maharashtra	Pearl25602@gmail.com	189.48.101.225	Failed	UPI	fraud
B-25602	01-04-2018	119.0	-5.0	8	Clothing	Saree	Pearl	India	Maharashtra	Pearl25602@gmail.com	226.255.78.11	Success	UPI	
B-25603	03-04-2018	1355.0	-60.0	5	Clothing	Trousers	Jahan	Austria	Tyrol	Jahan25603@gmail.com	254.62.194.156	Success	Credit-Card	
B-25603	03-04-2018	24.0	-30.0	1	Furniture	Chairs	Jahan	Austria	Tyrol	Jahan25603@gmail.com	201.136.202.59	Success	UPI	
B-25603	03-04-2018	193.0	-166.0	3	Clothing	Saree	Jahan	Austria	Tyrol	Jahan25603@gmail.com	200.71.232.3	Success	UPI	
B-25603	03-04-2018	180.0	5.0	3	Clothing	Trousers	Jahan	Austria	Tyrol	Jahan25603@gmail.com	129.45.146.145	Pending		
B-25603	03-04-2018	116.0	16.0	4	Clothing	Stole	Jahan	Austria	Tyrol	Jahan25603@gmail.com	58.35.194.53	Success	UPI	
B-25603	03-04-2018	107.0	36.0	6	Clothing	Stole	Jahan	Austria	Tyrol	Jahan25603@gmail.com	179.17.139.92	Success	Cash	
B-25603	03-04-2018	12.0	1.0	2	Clothing	Hankerchief	Jahan	Austria	Tyrol	Jahan25603@gmail.com	217.48.223.106	Success	Debit-Card	
B-25603	03-04-2018	38.0	18.0	1	Clothing	Kurti	Jahan	Austria	Tyrol	Jahan25603@gmail.com	140.80.106.251	Success	Netbanking	
B-25604	03-04-2018	65.0	17.0	2	Clothing	T-shirt	Divsha	India	Rajasthan	Divsha25604@gmail.com	162.166.170.92	Failed	UPI	fraud
B-25604	03-04-2018	157.0	5.0	9	Clothing	Saree	Divsha	India	Rajasthan	Divsha25604@gmail.com	67.55.109.180	Pending		
B-25605	05-04-2018	75.0	0.0	7	Clothing	Saree	Kasheen	India	West Bengal	Kasheen25605@gmail.com	57.17.210.234	Success	Cash	
B-25606	06-04-2018	87.0	4.0	2	Clothing	Shirt	Hazel	India	Karnataka	Hazel25606@gmail.com	106.50.54.57	Success	Credit-Card	
B-25607	06-04-2018	50.0	15.0	4	Clothing	Leggings	Sonakshi	India	Jammu and Kashmir	Sonakshi25607@gmail.com	51.27.106.145	Pending		
B-25608	08-04-2018	1364.0	-1864.0	5	Furniture	Tables	Aarushi	India	Tamil Nadu	Aarushi25608@gmail.com	73.211.36.52	Success	UPI	
B-25608	08-04-2018	476.0	0.0	3	Furniture	Chairs	Aarushi	India	Tamil Nadu	Aarushi25608@gmail.com	32.240.174.152	Success	Netbanking	
B-25608	08-04-2018	257.0	23.0	5	Clothing	Hankerchief	Aarushi	India	Tamil Nadu	Aarushi25608@gmail.com	133.246.87.32	Success	Credit-Card	
B-25608	08-04-2018	856.0	385.0	6	Electronics	Printers	Aarushi	India	Tamil Nadu	Aarushi25608@gmail.com	20.228.249.193	Success	Cash	
B-25609	09-04-2018	485.0	29.0	4	Electronics	Electronic Games	Jitesh	India	Uttar Pradesh	Jitesh25609@gmail.com	97.8.0.57	Success	Netbanking	
B-25609	09-04-2018	25.0	-5.0	4	Clothing	Saree	Jitesh	India	Uttar Pradesh	Jitesh25609@gmail.com	165.14.251.17	Failed	Netbanking	insufficient funds
B-25610	09-04-2018	1076.0	-38.0	4	Electronics	Printers	Yogesh	India	Bihar	Yogesh25610@gmail.com	211.124.172.160	Pending		
B-25610	09-04-2018	107.0	-54.0	4	Clothing	Stole	Yogesh	India	Bihar	Yogesh25610@gmail.com	240.211.11.193	Success	Cash	
B-25610	09-04-2018	68.0	-55.0	5	Electronics	Accessories	Yogesh	India	Bihar	Yogesh25610@gmail.com	168.128.119.75	Pending		

Figure 3: Dataset

In next flow the dataset was used for fraud detection where the preprocessed data was further encoded as fraud or no fraud data and was passed to the K-Nearest Neighbour Classifier model which a supervised learning model, where the algorithm calculates the similarity between new data/ case and already available data and further tag or put the new data into the category of most similar one. The algorithm does not learn immediately from the data set, rather it stores the data and while performing classification and performs the action accordingly, because of the mentioned reason the algorithm is also considered as Lazy Learning Algorithms. So, in dashboard attributes like order_id, email_id, IP address, country are passed for the classification. Which then returns the fraud related information as 0 or 1 for no fraud and fraud respectively. Figure 4 shows the confusion matrix for the analysis.

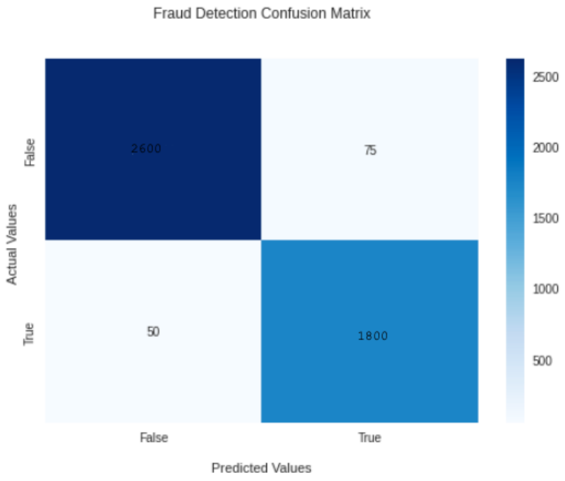


Figure 4: Fraud Detection Confusion Matrix

Further the samples collected from the Fraud detection and return on investment are passed to the LSTM model for the trend analysis of the data. Long Short-Term Memory is capable of learning long term dependencies for sequence data specially and also is a variety of recurrent neural network. It learns from the previous set of data which is achieved because the recurring module of the model. It predicts the data for next 30 days and saves the graph/chart in the form of HTML file. Later the plots are created and the analysis report is prepared.

STEP 1: Data pre-processing pipeline is created

STEP 2: KPI's (Return on Investment, Payment Conversion, cart abandonment, fraud detection) are created after passes it to the pre-processing pipelines and data summary is created after data extraction.

STEP 3: For fraud detection pre-processed data is encoded and is passed to the KNN model.

STEP 4: Return on investment data and fraud data is used for prediction the future fraud trends, using LSTM Model and data sampling is used for it.

STEP 5: KPI's data is used for plot creation

STEP 6: KPI's data and fraud data is used for creating analytics report.

STEP 7: data from step 5 and step 6 is passed to the dashboard using flask integration.

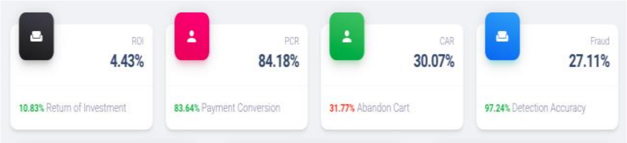
Figure 4: General Algorithm of the application

5. Results

1. RESULT FOR KPIs

The dataset which was preprocessed and was passed for data analysis, gives the various insights about the data on each KPI state on different aspects.

On considering Return on Investment (RoI) – it states that the net profit gained from the resources or the net cost. So if looked closely on the analysis it shows that the return on investment for a product according to the quantity is approximately 4.43% and the average return on investment for considering all the products and quantity is approximately 10% . In Payment Conversion Rate (PCR) it states the percentage of customer completed their payment on the platform using payment gateways. In PCR it shows approximately 84% payment conversion rate. If looked closely for cart abandonment rate it shows 30% of people leave their cart, as it is without checkout or payment. Figure 5 shows the analysis on the data for payment conversion rate, return on investment and cart abandonment rate.



ROI
4.43%
10.83% Return of Investment

PCR
84.18%
83.64% Payment Conversion

CAR
30.07%
31.77% Abandon Cart

Fraud
27.11%
97.24% Detection Accuracy

Figure 5: KPI RESULTS

As shown in figure 6, these results for KPI also shows the time graph of the data and the KPIs if required for the certain timeframe. Figure 6(a) shows the time graph for ROI, figure 6(b) shows the time graph for PCR and figure 6(c) gives the insight about CAR.

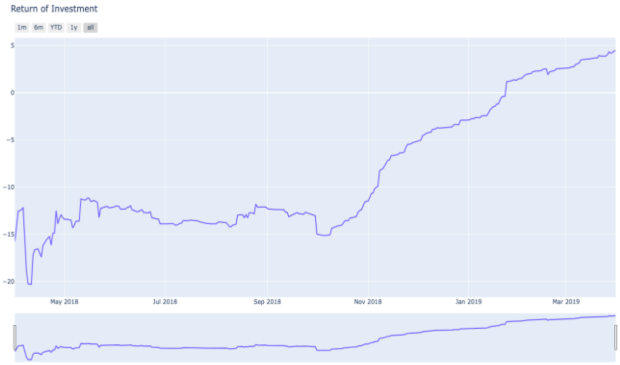


Figure 6(a) RETURN ON INVESTMENT

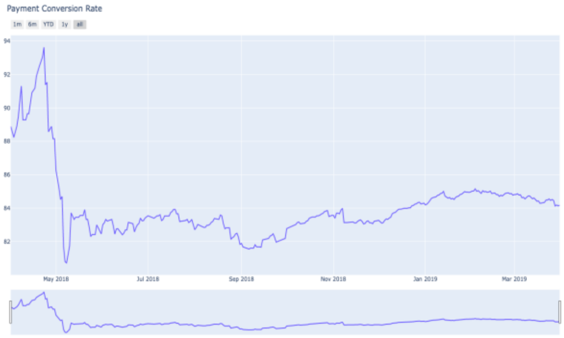


Figure 6(b) PAYMENT CONVERSION RATE

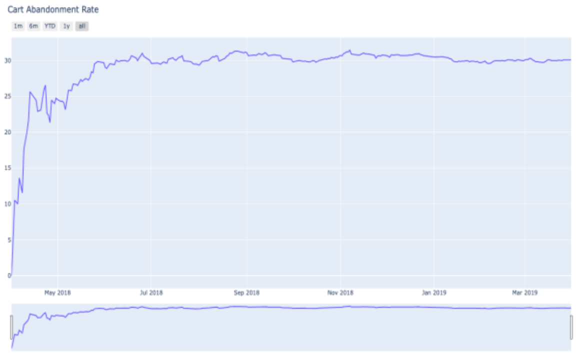


Figure 6(c) CART ABONDONMENT RATE

Further the statistical data for the KPIs shows the minimum and maximum values and according to the percentile of the data. Where Y- axis shows the ROI, PCR or CAR values with respect to percentile. As shown in figure 7

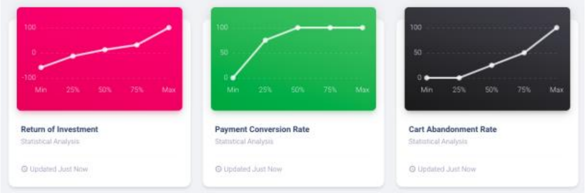


Figure 7 PERCENTILE GRAPHS FOR KPI

2. RESULT FOR FRAUD DETECTION

When the preprocessed data was passed into the K-Nearest Neighbours Classifiers the supervised method classifies and tags the data as fraud or no fraud, with 27% fraud identification and which was approximately 97% accurate. Where the fraud from a certain IP in most probable for the for the future fraud which is then later calculated in prediction. As shown in figure 5.

3. RESULT FOR FRAUD PREDICTION

The data from Return on investment and Fraud detection when sampled and passed through the LSTM model it predicts the fraud trend for the next 30 days as shown in figure 8. The model was trained with 200 epochs

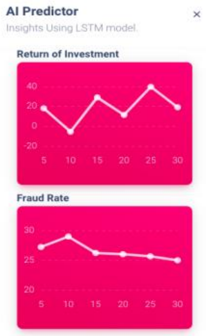
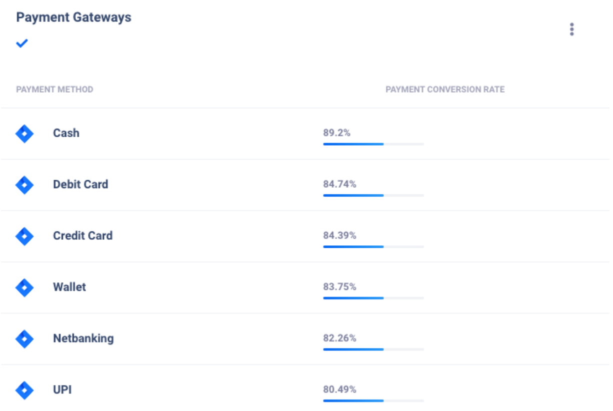


Figure 8 AI PREDICTORS

4. RESULTS OF OTHER ANALYSIS

Other analysis shows the payment conversion rate according to the payment method. There were various payment methods according to the dataset like cards, UPI, etc. The figure 9 shows the analysis for payment gateways.

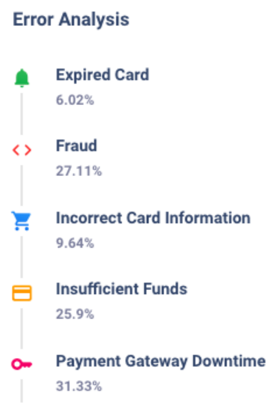
The final analysis in figure 10 is the error analysis which states the percentage of errors and the main reason behind the payment failure during the checkouts.



Payment Gateways

PAYMENT METHOD	PAYMENT CONVERSION RATE
Cash	89.2%
Debit Card	84.74%
Credit Card	84.39%
Wallet	83.75%
Netbanking	82.26%
UPI	80.49%

Figure 9 PAYMENT CONVERSION RATE



Error Analysis

Expired Card
6.02%

Fraud
27.11%

Incorrect Card Information
9.64%

Insufficient Funds
25.9%

Payment Gateway Downtime
31.33%

Figure 10 ERROR ANALYSIS

6. Conclusion

To improve the performance, services, operations and revenue many organizations and groups uses business analysis and data analysis in order to get the benefits of the technology and to improve their business goals. Similar like other organizations banking sector also uses this analysis techniques and have upgraded from their traditional technological approach and have increased their focus mainly in the digital transformation. By using Business analysis in payment services helps in improving the framework and provide better insights to the organization.

The dashboard was prepared to gain the insight of the organization and to know the scope of improvement. The dashboard give the fraud prediction and fraud detection analysis using LSTM model and K-Nearest Neighbour Classifier respectively along with various other analysis factors like return on investment, cart abandonment rate, payment conversion rate, error analysis etc.

Further scope of improvement for the dashboard can be including live data rather than static data with proper authorization and authentication of the user so that the organization just must feed the data and the analysis report will be rendered to the dashboard.

References

1. Elisa Indriasari; Ford Lumban Gaol; Tokuro Matsuo , “Digital Banking Transformation: Application of Artificial Intelligence and Big Data Analytics for Leveraging Customer Experience in the Indonesia Banking Sector”,presented at 2019 8th International Congress on Advanced Applied Informatics(IIAI-AAI) ,Toyanama, Japan,7-11 Year: 2019, pp: 863-868.
2. Dr. Navleen Kaur, Ms. Supriya Lamba Sahdev, “Banking 4.0: the influence of artificial intelligence on the banking industry & how AI is changing the face of modern day banks”, International Journal of Management (IJM) Volume 11, Issue 6, June 2020,pp 39-45.
3. Tushar Gupta; Naman Gupta; Ankit Agrawal; Aksh Agrawal; Kartik Kansal, “Role of Big Data Analytics In Banking”, 2019 International Conference on contemporary Computing and Informatics (IC3I).
4. Kaithekuzhical Leena Kurien*1 & Dr. Ajeet Chikkamannur, “Detection and Prediction of credit card fraud transactions using machine learning”, International Journal of Engineering Sciences & Research Technology (IJESRT), ISSN: 2277-9655, pp. 205-207
5. Correa Bahnsen, D. Aouada, A. Stojanovic, and B. Ottersten, “Feature engineering strategies for credit card fraud detection,” Expert Systems with Applications, vol. 51, pp. 134–142, 2016.
6. Varun Kumar K S, Vijaya Kumar V G, Vijay Shankar A, Pratibha K, “Credit Card Fraud Detection using Machine Learning Algorithms”, International Journal of Engineering Research & Technology (IJERT) ,Volume 09, Issue 07 (July 2020),pp 5-8.
7. Dal Pozzolo, G. Boracchi, O. Caelen, C. Alippi and G. Bontempi, “Credit Card Fraud Detection: A Realistic Modeling and a Novel Learning Strategy,” in IEEE Transactions on Neural Networks and Learning Systems, vol. 29, no. 8, pp. 3784-3797, Aug. 2018.
8. Pratyush Sharma, Souradeep Banerjee, Devyanshi Tiwari, and Jagdish Chandra Patni, “Machine Learning Model for Credit Card Fraud Detection- A Comparative Analysis”, The International Arab Journal of Information Technology, Vol. 18, No. 6, November 2021 , pp 789-790.
9. Ruttala Sailusha ; V. Gnaneswar ; R. Ramesh ; G. Ramakoteswara Rao ,”Credit Card Fraud Detection Using Machine Learning ”,2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS) ,19 June 2020

10. Kha Shing Lim, Lam Hong Lee and Yee-Wai Sim, “A Review of Machine Learning Algorithms for Fraud Detection in Credit Card Transaction”, IJCSNS International Journal of Computer Science and Network Security, Vol.21 No.9, September 2021, pp 32-37.

11. Mosa M. M. Megdad, Bassem S. Abu-Nasser and Samy S. Abu-Naser, “Fraudulent Financial Transactions Detection Using Machine Learning”, International Journal of Academic Information Systems Research (IJAISR) ISSN: 2643-9026 Vol. 6 Issue 3, March - 2022, Pages: 30-39.

12. A.Banupriya1, Divya.R2, M.Vinodhini3,”Credit Card Fraud Detection Using Data Science Techniques”, National E-Conference on "Communication, Computation, Control and Automation" (CCCA-2020) , ISSN : 2581-7175 pp 3-4.