Fraud Prediction [Draft White Paper]

- **Business Problem**

We do several transactions every day, in store to purchase things, in canteen for food, purchasing flight tickets etc. Transaction is involved everywhere. There are very minimum but some of the transactions that bank or credit card companies deal with are fraudulent. I am trying to fit a model on fraudulent transaction data, that I got in Kaggle.

- **Background/History**

While looking for several data sources, I found this data quite interesting and was thinking as if it was a real-life problem, I was thinking if I can solve this problem with the help of machine language models.

- **Data Explanation (Data Prep/Data Dictionary/etc)**

The dataset has several attributes which can be used to detect whether a transaction is fraudulent.

1. **Transaction ID**: A unique identifier for each transaction.
2. **Customer ID**: A unique identifier for each customer.
3. **Transaction Amount**: The total amount of money exchanged in the transaction.
4. **Transaction Date**: The date and time when the transaction took place.
5. **Payment Method**: The method used to complete the transaction (e.g., credit card, PayPal, etc.).
6. **Product Category**: The category of the product involved in the transaction.
7. **Quantity**: The number of products involved in the transaction.
8. **Customer Age**: The age of the customer making the transaction.
9. **Customer Location**: The geographical location of the customer.
10. **Device Used**: The type of device used to make the transaction (e.g., mobile, desktop).
11. **IP Address**: The IP address of the device used for the transaction.

12. **Shipping Address**: The address where the product was shipped.
13. **Billing Address**: The address associated with the payment method.
14. **Is Fraudulent**: A binary indicator of whether the transaction is fraudulent (1 for fraudulent, 0 for legitimate).
15. **Account Age Days**: The age of the customer's account in days at the time of the transaction.
16. **Transaction Hour**: The hour of the day when the transaction occurred.

- **Methods**

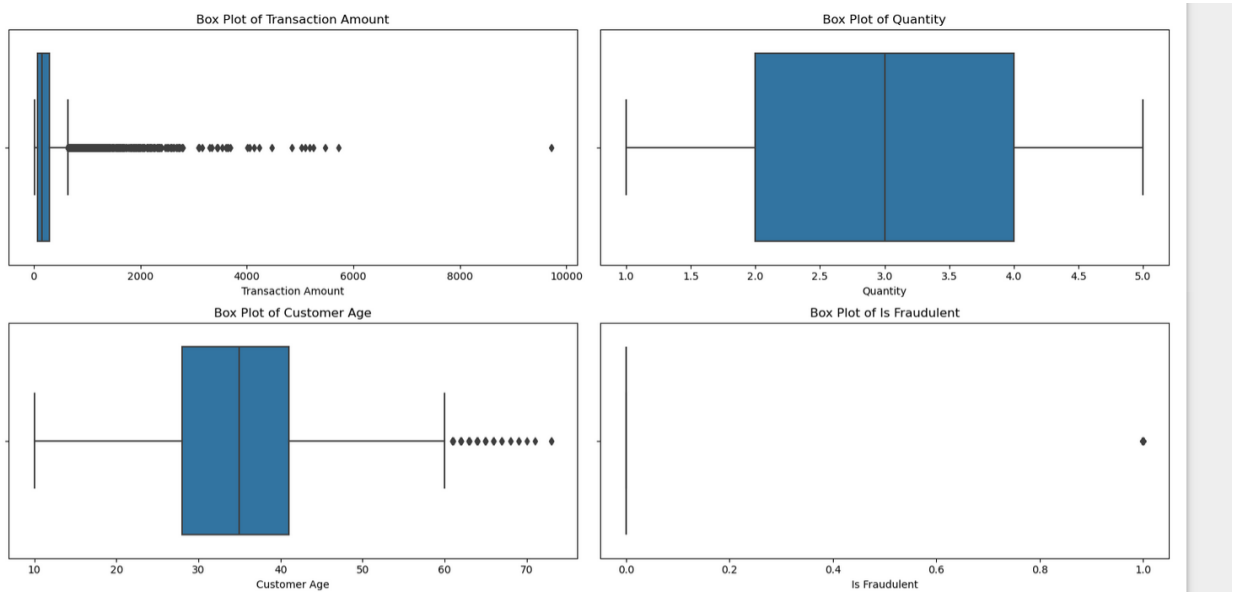
Here in this problem, I am trying to detect whether a transaction is fraudulent or not, so it is a classification problem, I have fit the random forest classification model for this. I have used several explanatory data analyses for analyzing the fraudulent transaction.

- **Analysis**

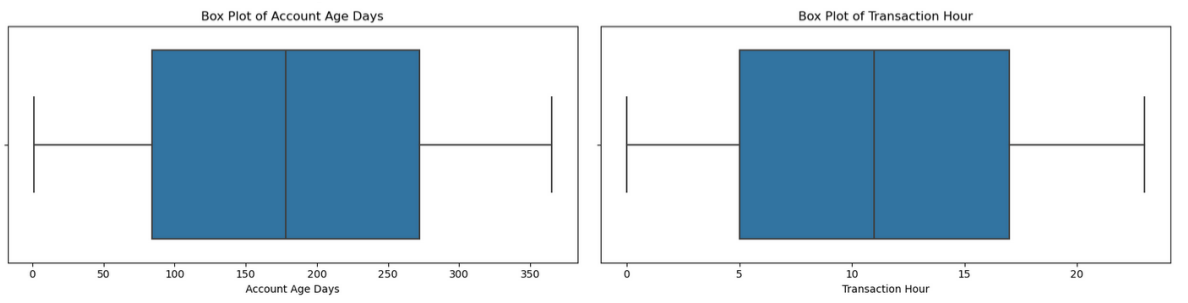
It's all about fraud, so the count of activities for the transaction is very less for fraud activities. When I looked for the percentage of output variable, the count for Is Fradulent is true are only for 5% records.

	Is Fraudulent
0	0.948295
1	0.051705

I did some exploratory data analysis on the data to identify different patterns on the data.

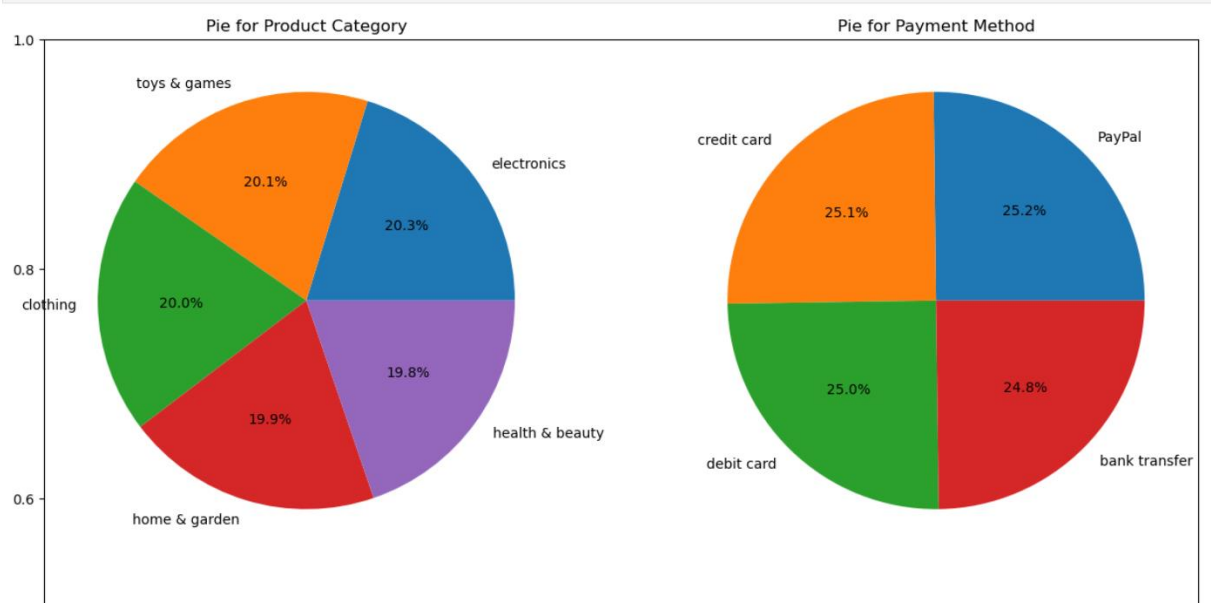


I have created some bar plot on the continuous variables like transaction amount, quantity i.e number of product involed in the transaction, customer age and Is Fraudulent field, i.e. If the transaction is a fraudulent transaction.
About the transaction amount, what I found is most of the transactions are less than 1000, the quantity of transactions is having average of 3, there are several outliers on customer age field.

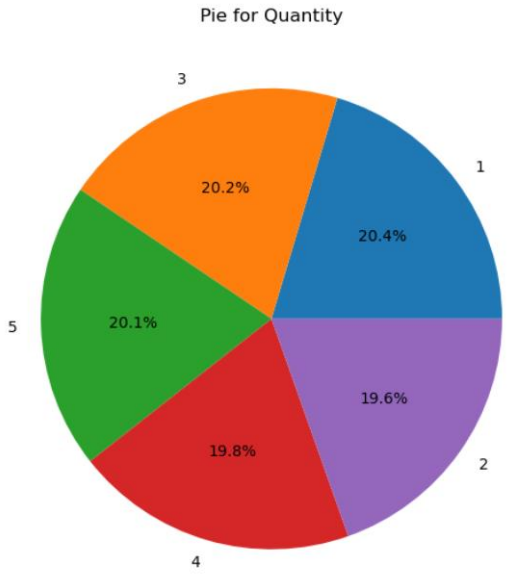


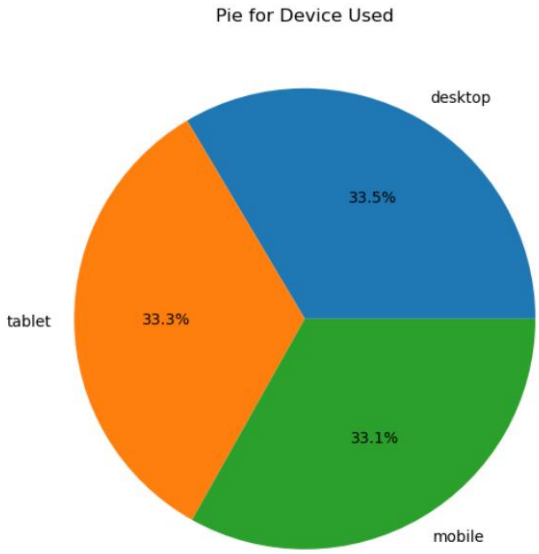
Among the other two continuous fields, account days in age has an average of 175 days and transaction hour having high volume between 5AM to 5PM.

Among the categorical field analysis, I did the pie diagram for product category and payment method. Overall looking at the pie diagram it looks like product categories and payment methods are mostly uniformly distributed among the transaction.



Similar scenario exists for quantity and device used for transaction.





- **Conclusion**

We have split the model into 80 and 20 for train and test, then fit the Random Forest classifier model into it after selecting some categorical and continuous variable. Then I test the model on test data. The accuracy of score came as `0.9553628093928496`. Which means 96% prediction is correct for the test data, when the model is fitted based on the selected training.

- **Assumptions**

The only assumption is that the encoded integer value for each variable should have an ordinal relation.

- **Limitations**

I have fitted this classification model based on the data, identifying fraud is not easy, and it must be very quick to find fraud transaction, so immediate action can be taken after the fraud occurs. One of the major limitations is data size, the data used for this model fitting is only from 2023 December for 2024 April, which is very less to identify this type of complex model.

- **Challenges**

Getting data for fraud is not easy, it took a reasonable amount of time to identify and choose data for this project. Another challenge was to identify the model, finally I chose the random forest classification model to detect the fraud.

- **Future Uses/Additional Applications**

As this model can be used for scoring transaction and identification of transactions whether it's a fraudulent transaction, we can create an application interface using this model and it can be called while transaction is in progress with an extra step for fraud validation.

- **Recommendations**

The accuracy of the model came out as 96%, which means 96 predictions out of 100 are correct, so it's a good, recommended model for fraud detection.

```
[186]: from sklearn.ensemble import RandomForestClassifier
       classifier_model = RandomForestClassifier(n_estimators = 10, random_state = 0)
       classifier_model.fit(train_x,train_y)

[186]: RandomForestClassifier
       RandomForestClassifier(n_estimators=10, random_state=0)

[187]: from sklearn.metrics import accuracy_score
       predictions = classifier_model.predict(test_x)
       accuracy_score(test_y, predictions)

[187]: 0.9553628093928496
```

- **Implementation Plan**

The best way to implement this model is by using application interface, the api will be called in the middle of traction and the API will return a binary value to identify whether the transaction is fraud or not.

- **Ethical Assessment**

'Fraud' is a very strong word, we have to be very careful and cautious before tagging a transaction with this flag, because its ways bring bad reputation to the customer. The transactions have personal identifiable information, so any false positives will bring bad reputation to the customer.

Another ethical concern is the reputation of banks and payment gateways like VISA, MASTERCARD, DISCOVERY etc., banks and payment gateways are very reputable organizations, any false positives may bring lots of questions on their security systems.