**Fraud detection models and trust level validation in Mobile Money Transaction (MMT)**

**Motivation:**

Recently, mobile money service has been increasingly popular. Mobile payments reduce the need for people to carry payment methods like cash and allow people to make transactions using smartphones, which provide great convenience for people. However, financial deception in mobile money transactions is a big issue. According to the study done by Javelin Strategy & Research and SAS in 2020, an increase of almost 35% in fraud attempts in mobile money transactions (2020). Recently, machine learning models have shown promising results for classification problems and fraud detection problems. We want to create a service agent to select the best machine learning models, perform functional validation processes, and assign trust levels.

**Problem Statement:**

The goal of this project is to develop a service module which can select k best machine learning models and a client module which can validate the functionality of selected models and assign trust levels for mobile money transaction fraud detection.

**Dataset:**

1. **Initial Data Statistics**

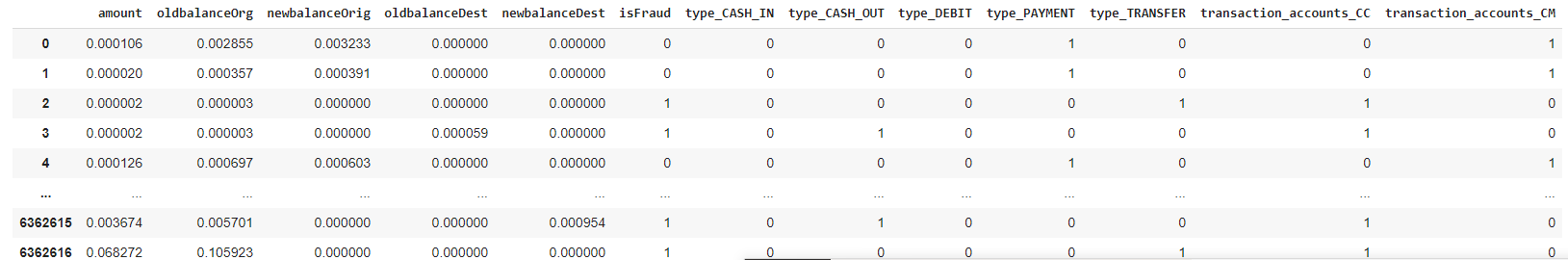
This project is using a Synthetic Financial Datasets For Fraud Detection generated by PaySim mobile money simulator from Kaggle (NTNU). There is a lack of publicly available datasets on financial services and specially in the emerging mobile money transactions domain. There are no publicly available financial transactions datasets. PaySim uses aggregated data from the private dataset to generate a synthetic dataset that resembles the normal operation of transactions and injects malicious behaviour to later evaluate the performance of fraud detection methods. This dataset has been constructed using real transaction data and also has a few fraudulent transactions inserted into them. The dataset contains 6,362,620 observations, 0.1291% of them are fraudulent transactions, and 11 features.

1. **Data Pre-processing**

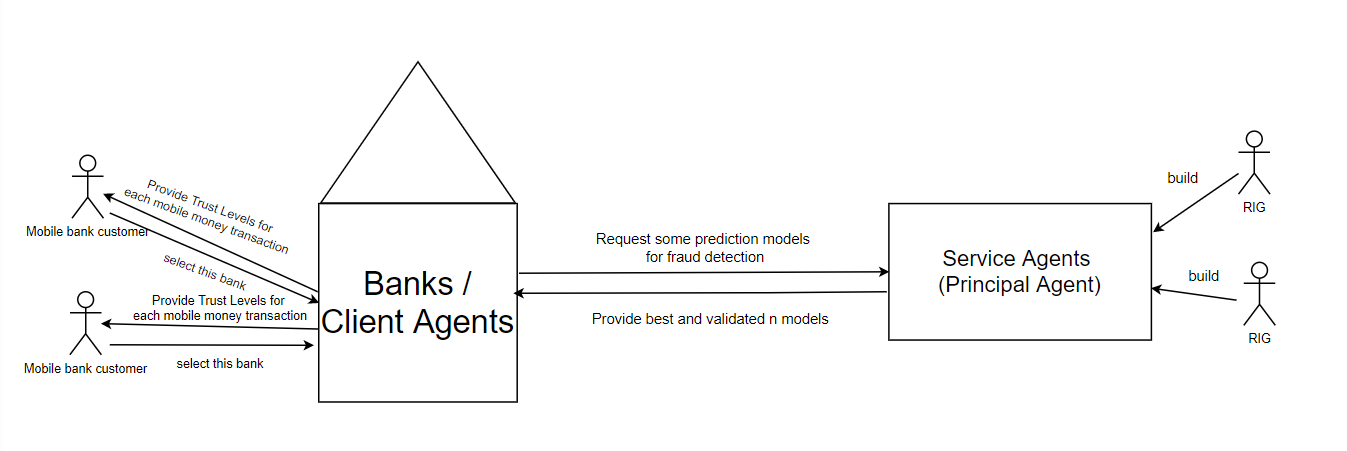
We perform the following pre-processing steps on our content variable. The work flow is briefly summarized as following:

* Created new variables
* Normalized numeric variables
* Dropped irrelevant features
* Performed One Hot Encoding for categorical variables

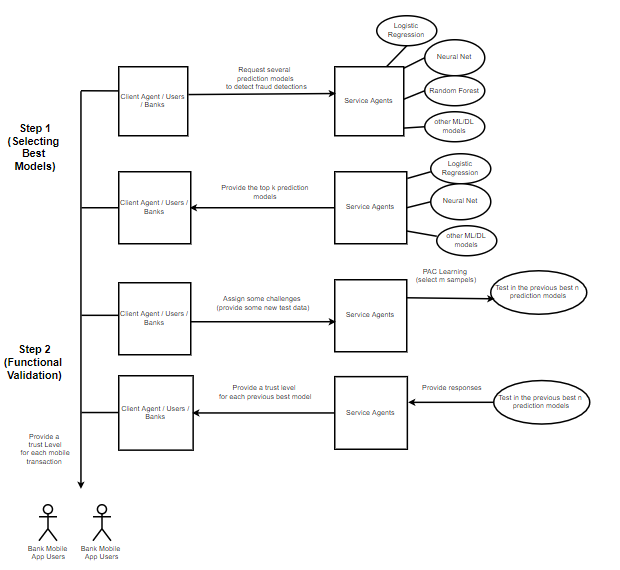
The final table contains 12 features and 6362620 data samples. The table is shown below.



**Architecture Diagram**

****

Recently, people tend to use mobile devices to make money transactions. However, electronic payment service has been a target for financial deception for several years. Having some accurate and validated fraud prediction model will help banks and bank customers to detect possible fraud transactions in mobile money transactions. There are two agents in our project, one is a client agent and another one is a service agent. Client agents can be banks. A service agent is a principal-agent in our project, which is built by RIG. Clients agents or banks will request some prediction models for fraud detection in mobile money transactions from the RIG service agent. After receiving the request from banks, the service agent will provide some best and validated fraud prediction models to banks. The banks can use these most accurate and verified machine learning models to predict fraud in mobile money transactions and assign a trust level for each mobile money transaction sample to customers.



There are three main parts (model selection, functional validation, and assigning trust level) in this project. In the step 1 or the model selection part, the client agents provide data to the service agent. Then, the service agent trains multiple machine learning models to predict fraud in mobile money transactions and chooses top k models based on test dataset performance. In the step 2 or the functional validation part, clients provide new labeled data to service agents. The service agent uses bootstrap resampling to generate N different test datasets. It then uses hypothesis testing to validate whether previously observed model performance is trustworthy or not. Based on the result from the model selection and functional validation, the service agent provides several most accurate and verified machine learning models for fraud detection to banks. Finally, banks or other client agents can use these accurate and verified prediction models to appropriately assign trust levels to new mobile money transactions.

**Step 1: Selecting K best models**

The first part of this project is to train several ML/DL fraud detection models and select top k models. Machine Learning and Deep Learning techniques can be used to determine the level of risk associated with a mobile transaction, to prevent fraud transactions, and provide better service for customers. We constructed 7 machine learning/deep learning models including Logistic regression, Bayesian classifier, Random Forests, Gradient Boosting, Adaboost, Support Vector Machine, and Neural nets. One biggest issue that we encounter is the data imbalance problem since only 0.1291% of data samples are fraudulent transactions. An Imbalanced dataset can cause a natural tendency to pick up the patterns in the most popular classes and ignore the least popular ones. In order to solve this problem, we use an oversample method which involves randomly duplicating examples from the minority class and adding them to the training dataset. We also use F1 score as a metric to measure accuracy. In this project, we decide to select the top 3 models and top 3 models are random forest, gradient boosting, and adaboost. These three trained models are saved for later use.

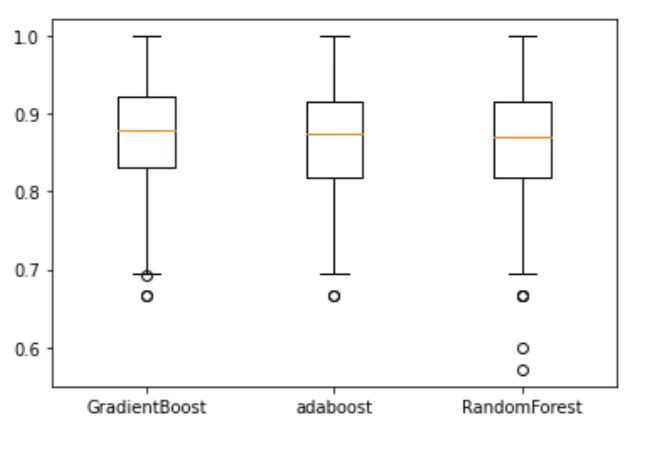


**Step 2: Functional Validation**

The second part of this project is to validate the functionality of previous selected top 3 models. The Functional Validation model can be used to determine whether the selected trained ML/DL models are appropriate models/computing services. Over time, fraudsters may use more advanced technologies to commit mobile financial deception and some previously trained ML/DL models may become not credible. Therefore, we develop a functional validation module that validates trust between the banks/client agents (bank/customers) and the service agents (RIG) in the MDM systems using a small number of data samples. Bootstrapping and hypothesis test techniques are used to double check the functionality of previous selected top 3 models.

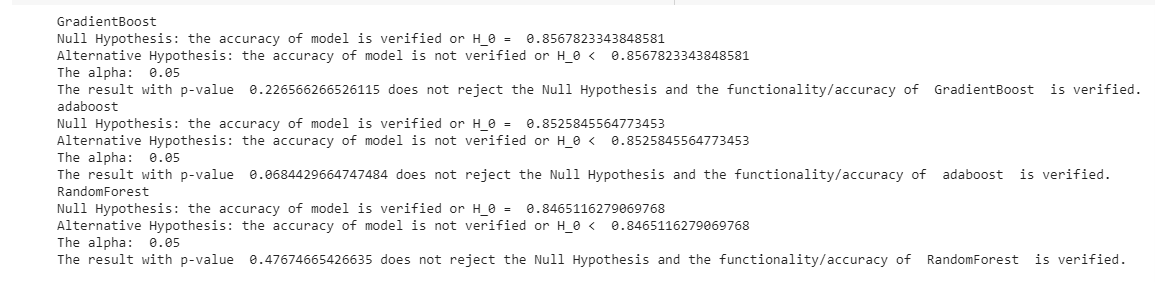
1. **Bootstrap**

Bootstrap is a resampling method which randomly and repeatedly selects data samples with replacement. We want to use it to generate many different test datasets based on one single labeled test dataset provided by clients and generate the F1 score/accuracy of these test datasets. Then, we get the variance of the sample distribution.



1. **Hypothesis Test**

Hypothesis testing in statistics is a way for you to test the results of a survey or experiment to see if you have meaningful results. In our project, we use hypothesis tests to determine whether the accuracy of current models with new mobile money transaction samples is less than the previous accuracy. If the accuracy of current models with new data samples is not significantly less than the previous accuracy or if the result does not reject the null hypothesis, the functionality of models are verified. In our project, all top 3 models are verified. The result is shown below.

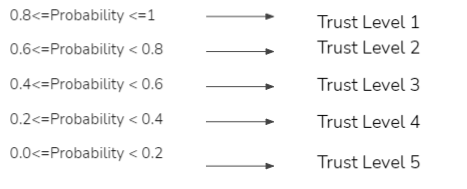


**Assign Trust Level**

We also build a trust model to show the risk / safety of each mobile money transaction. The trust model will also help customers and banks to determine which mobile money transactions are highly trustworthy and which transactions are vaguely defined. We assign a trust level from 1 to 5 for each data sample. A mobile money transaction sample with trust level 5 means this data sample is highly trustworthy. A mobile money transaction with trust level 1 means this data sample is highly risky. The machine learning models can predict the probability that a mobile money transaction sample is fraudulent. We use this probability to assign a trust level for each mobile transaction sample.

1. **Assign Trust Level using Top 3 Models**

We first assign trust using Top 3 models. If the probability is less than 0.2 which means the data sample is trustworthy and we will give a trust level 5 to this data sample. The rule is shown below.

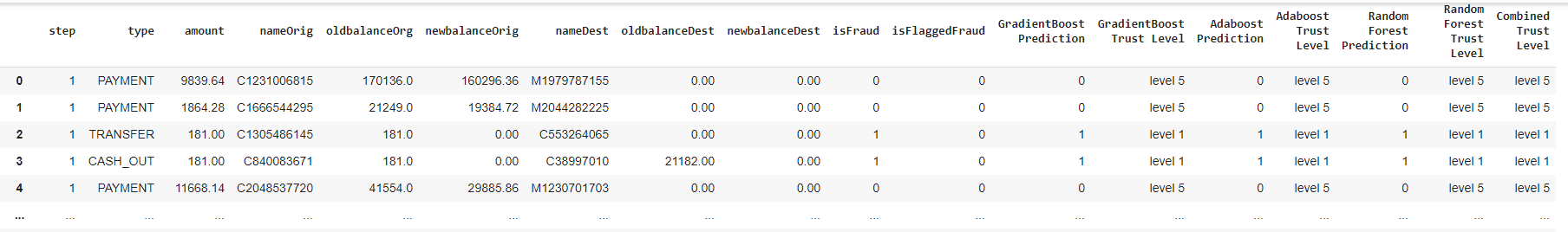


1. **Combine the Result from Top 3 Models**

The distribution of trust level prediction is skewed, so we use the ensemble method to improve prediction accuracy. In other words, we combine the results from random forest, adaboost, gradient boost together. We added together the trust levels from the top 3 models and average the combined value.

**Result and Conclusion**

In this project, we build a service agent to select well-performed machine learning models and validate the functionality of prediction models for mobile money transactions fraud detection. Finally, we build a trust model to help banks to clearly determine the safety of each mobile money transaction. Based on the result of this project, random forest, adaboost, and gradient boost are the most accurate models and the functionality of these three models is verified. A trust level is assigned to each mobile transaction sample using the selected and verified ML models. The final table is shown below. The final table contains the basic information about mobile money transaction samples and the trust levels predicted by top 3 models.



**Benefits and Usage**

* Seven different Machine Learning algorithms for RIG to select from
* Service agent as a Python class for easy reusability and integration in RIG’s dynamic trust service in MMT
* Use analytics engine Spark can help future RIG interns to shorten model training time when developing more complex systems
* Creative Bootstrapping based functional validation to help RIG’s clients use less data to generate more insights
* Ensemble dynamic trust decision to bring more trustworthy trust level assignments for RIG’s clients

**Limitations and Feature Work**

* Build a better/more complex deep learning models for fraud detection or use a pre-trained fraud detection deep learning models
* Build a visualization dashboard to better visualize the result and provide business insights for customers/companies
* Dynamically improve the models and assign trust levels, such as using adversarial learning technique
* Build a more meaningful trust model by using feature selections to determine important features or giving different weights for different ML models while combining the result from several top k models

**Acknowledgments**

We want to show great thanks to Ms. Emilia and Mrs. Jay for their kind help and understanding during this project. We also appreciate Dr. Cybenko, Dr. Decker, and other professionals for their technical support.

**References:**

NTNU. Synthetic Financial Datasets For Fraud Detection. Retrieved from <https://www.kaggle.com/ntnu-testimon/paysim1>

Javelin Strategy & Research and SAS (2020). *Study: Digital payments fraud surges during pandemic*. Retrieved from

<https://www.prnewswire.com/news-releases/study-digital-payments-fraud-surges-during-pandemic-301155991.html>