Review of: "Predicting Mobile Money Transaction Fraud using Machine Learning Algorithms"

Shahid Tufail[1]

1 Florida International University

Potential competing interests: The author(s) declared that no potential competing interests exist.

There are many editorial errors in the manuscript, I have provided my comments and suggestion in**Bold text**

3.1 Data Generation and Stimulation

Researchers have developed stimulators that use algorithms to

generate synthetic data from real-time observations to address this problem.

Fraud was coded as 1 = fraud and 0 = no fraud and is represented in equation 1.

The spelling of simulation is wrong.

The table provides information on the results of numerical features for money laundering transactions.

table 3 is not labeled

As can be seen in Figure 1, there are five unique types of transactions: cash-out, cash-in, payment, transfer, and debit.

Figure 1 is about scatter plot; I think authors are talking about figure 3 which is not labelled in the manuscript

Table 1: Independent Features and Description

As shown in Table 1, all the features except cash-in, debit, and payment type are

statistically significant at a *p-value* of 0.05 and with a confidence interval of 95%..

But table 1 is about independent features and description

again authors are talking about table 3 which is not labeled on page 14

The log(odd) in Table 1 lacks

Which table?

Table 1 provides an overview of the odds of the features and how they affect fraud.

is it second table on page 15?

Table 1 shows the results of the classifiers' performance

Table does not match the description is the text. page 16

As shown in Figure 1, the amount involved

in the transfer was again the top feature to predict suspicious transactions in mobile money transfers

Table does not match the description is the text. page 18

1. **The dataset used in the manuscript was generated using PaySim, my question is what factors does Paysim looks before flagging transaction as fraudulent or non fraudulent.**
2. **Some features were redundant and had to be dropped before model building. As a result, the features "nameorig" and "nameDest" are no longer relevant and must be removed. But, these two features can be used to determine the transaction as fraudulent or non fraudulent. For example, if A as sent some amount to B and the transaction was legitimate then it is most likely that future transactions between A and B will be legitimate. Moreover, if Z send some amount to another user then most of the transaction from Z are fraudulent so it is most likely that future transactions of Z will be fraudulent. So, my question is that is it a good idea to remove sender and receiver name from the transaction and if it's a privacy concern then these names can be encoded.**
3. **The accuracy of the training is 100% and test is 89% in the best case. This may be the signs of overfitting, so were any techniques used to protect the model from overfitting? Also, other model has lower train accuracy and higher test accuracy which is very uncommon. What was the dataset split for this study.**
4. **What was the ration of fraudulent to non-fraudulent in the dataset after smote technique was applied?**
5. **Why performance of neural network, SVM were not studied as literature shows them to be one of the best algorithms for classification tasks.**
6. **Was training time analysis performed?**