A machine learning approach to fraudulent payment detection of the payment aggregator business model in Sri Lanka

S. N. Rambukkanage

198768G

Master of Science in Information Technology
Department of Information Technology
Faculty of Information Technology
University of Moratuwa

June 2022

A machine learning approach to fraudulent payment detection of the payment aggregator business model in Sri Lanka

By

S. N. Rambukkanage

198768G

Dissertation submitted to the Faculty of Information Technology, University of Moratuwa, Sri Lanka for the partial fulfilment of the requirements of the Degree of Master of Science in Information Technology.

June 2022

A machine learning approach to fraudulent payment detection of the payment aggregator business model in Sri Lanka

June 2022

A research on detecting payments which are suspicious for fraud under card-not-present financial transactions of a special business model for payment acquiring services operating as a regulated payment aggregator in the financial technology industry in Sri Lanka

Research Report

IN 6900 Research Project

By S. N. Rambukkanage

198768G

Supervisor – Dr. S. C. Premaratne

Master of Science in Information Technology
Department of Information Technology
Faculty of Information Technology
University of Moratuwa

Declaration

I declare that this thesis is my own work and has not been submitted in any form for another degree or diploma at any university or other institution of tertiary education. Information derived from the published or unpublished work of others has been acknowledged in the text and a list of references is given.

Name of the Student: Signature of the Student:

S. N. Rambukkanage *UOM Verified Signature*

Date: 30/07 /2022

Supervised by: Signature of the Supervisor:

Dr. S. C. Premaratne *UOM Verified Signature*

Date: 30/07 /2022

Acknowledgement

First of all, I intend to extend my appreciation to my supervisor, Dr. Saminda Premaratne, Senior Lecturer, Faculty of Information Technology, University of Moratuwa for his supervision and advice given to improve my research project.

Next, I would like to thank the payment service provider who was willing to extend their support for my research study.

Finally, I wish to thank and acknowledge my family and friends for the support given for me to complete my research while balancing other work.

Abstract

When a payment aggregator is accepting payments on behalf of the merchants as a financial technology service provider, it is possible for a portion of those payments to be fraudulent payments. In order to detect fraudulent payments and avoid related losses, it is important to use an algorithm-based model which adapts to the changing circumstances instead of having fixed rules. This research uses machine learning concepts in order to detect a given card-not-present online transaction being a suspicious-for-fraud payment in the context of a Central Bank approved payment aggregator business model in Sri Lanka. Further to that, this research also investigates the conditions which are highly influential in deciding whether a given payment is suspicious for fraud under the payment aggregator model. Under machine learning, classification approach is used, as the dataset used is categorized as fraud and not fraud. The attributes related to the payment data are different given the context and feature engineering was required to obtain a meaningful outcome. It was discovered that the conditions which influence a payment to become suspicious for fraud are the name registered with the payment method being different to the name of the actual payee who made that particular transaction and the originating country of the transaction being different to the name of the country entered by the payee who made that particular transaction. Fourteen different supervised learning algorithms were tested on a payment dataset and were evaluated based on the accuracy of the predicted class label. As part of the outcome of this study, decision tree algorithm was identified as the most effective algorithm with the highest prediction accuracy and a model was built and saved using PyCaret for future use.

Keywords: *payment aggregator, fraudulent payments, machine learning, financial technology, card-not-present transactions*

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABBREVIATIONS

AVS: Address Verification Systems

Dtype: Data type

PA: Payment Aggregators

SVM: Support Vector Machine

Std: Standard Deviation

MCC: Matthew’s Correlation Coefficient