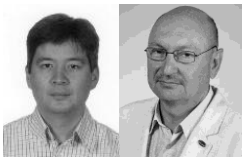
Fraud detection approaches in ecommerce

A Zhumabayev[1]*, R Muhamedyev[1,2,3]

[1]*Satbayev University, Kazakhstan, Almaty, Satpayev str., 22A*
[2]*ISMA University of Applied Sciences, Riga, Latvia*
[3]*Institute of Information and Computational Technologies. Kazakhstan, Almaty, Pushkin str*

**Corresponding author's e-mail: akylbekz@gmail.com, ravil.muhamedyev@gmail.com*



Abstract

Ecommerce industry has grown rapidly in last decades and it is still developing. Companies provide online services and products for customers. Cardholders can make purchases without need to be present at the point of sale. This characteristic of ecommerce is used by fraudsters to perform unauthorized transactions. Despite the fact that a lot of research is done in the area of fraud detection and many methods implemented the fraud is still a big threat. In the paper we analyse the current situation in this field and provide ideas for further improvements.

Keywords: ecommerce, fraud detection, machine learning

1 Introduction

Ecommerce transactions can be made online without presence of cardholder and card itself (CNP – card not present). There are methods for proving the identity such as user authentication, accepting electronically scanned documents or contacting with clients by phone. These methods are used by companies but have drawbacks that out of scope of this paper. Another approach is to use fraud detection (or fraud monitoring) system to recognize the abnormal transaction.

2 Overview

Fraud detection system is a component of online payment service that participate in the process of financial transaction. As an input this component has a data related to transaction such as amount, location, card number (also called pan) etc.

After processing the fraud detection system marks the transaction with the status: good, bad or suspicious. In case of a good status the payment system accepts the payment, in case of bad status the transaction is rejected and in case of suspicious status the transaction is hold until resolving (Figure 1) [1]. The process of resolving is time consuming as done usually manually by fraud specialists.

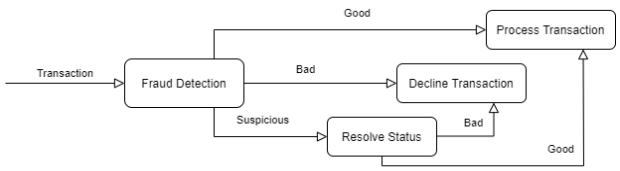


Figure 1 Fraud detection component

3 Rule-based approach

First fraud detection systems used rule-based approach. Earlier implementations were based on explicit constraints (also called limits) that represent different types of rules (generally with weights). Examples of such rules are white/black list, limits for amount, number of transactions etc.

Rule-based approach later was evolved in using of machine learning algorithms that can build rules in internal structure. The "state of the art" is using algorithms based on tree [2]. The rule-based approach is a popular solution. It is easy to understand and implement. In addition, it has a great performance.

The main problem with this approach is accuracy and lack of adaptation to changes in transaction environment. In case of rule-based approach we usually have a significant number of true negative results what means we reject many "good" transactions.

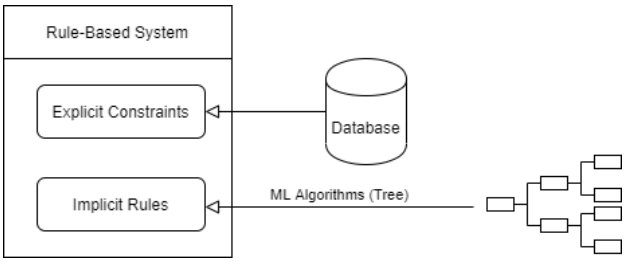


Figure 2 Rule-based approach

4 Pattern recognition

As next step of evolution the fraud detection systems start using pattern recognition approach. First, they used different statistical methods [3].

Nowadays, the behavior analysis is the winner. Best fit

for this approach is using a deep learning (Figure 3) [4]. The main issue of this approach is that financial system cannot trust deep learning algorithms as there is no clear information how the system come up with the result.

In the end, the payment system can recognize only two statuses from pattern recognition system: either good and suspicious or bad and suspicious (it depends on configuration of accuracy of machine learning algorithm).

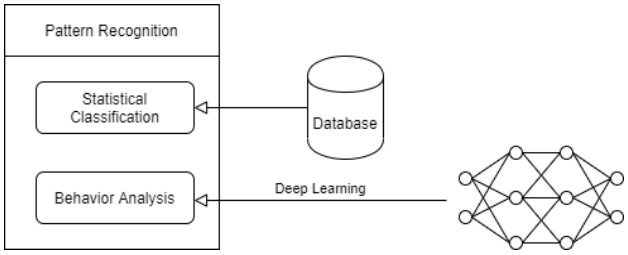


Figure 3 Pattern recognition approach

5 Addressing issues

A lot of research done by science community to deliver better solutions and address existing issues of rule-based and pattern recognition approaches [5]. The goal is to configure system in a way when it gives the best balance between accepting good transactions and declining bad transactions.

One of the approaches is to use algorithms based on cost (including cost of financial damage, cost of transaction processing, cost of missed client loyalty etc.) [6]. Another approach is to use probabilistic algorithms to cut the number of suspicious transactions [7]. Finally, we can represent the fraud detection system as a combination of three layers: rule-based, pattern recognition and filtering components (Figure 4).

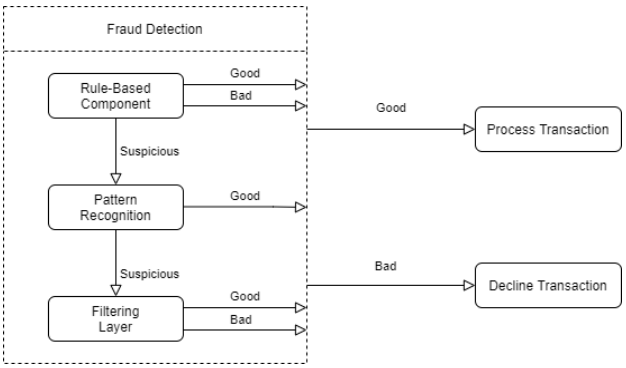


Figure 4 Fraud detection system components

6 Conclusion

We plan to analyse methods to decrease the number of transactions with suspicious status. The main idea is to use pattern recognition layer as a maximizer function for bas transactions (high recall) and filtering layer as reducer of suspicious transactions. One of the approaches is to use explainable AI approach [8, 9].

References

[4] Delamaire L, Abdou H, Pointon J 2009 Credit card fraud and detection techniques: a review *Banks and Bank Systems* **4**(2) 57-68

[5] Save P, Tiwarekar P, Ketan N, Mahyavanshi N 2017 A Novel Idea for Credit Card Fraud Detection using Decision Tree *International Journal of Computer Applications*. **161** 6-9

[6] Bolton R J, Hand D J 2002 Statistical Fraud Detection: A Review. *Statist. Sci.* **17**(3) 235-55

[7] Patidar R, Sharma L 2011 Credit card fraud detection using neural network *International Journal of Soft Computing and Engineering (IJSCE)* **1** 32-8

[8] Samaneh S, Zojaji Z, Ebrahimi Atani R, Monadjemi A 2016 *A Survey of Credit Card Fraud Detection Techniques: Data and Technique Oriented Perspective*

[9] Chan P, Stolfo S 1998 *Toward Scalable Learning with Non-uniform Class and Cost Distributions: A Case Study in Credit Card Fraud Detection*

[10] Falaki S, Alese B, Adewale O, Ayeni J, Aderounmu G, W O I 2015 Probabilistic Credit Card Fraud Detection System in Online Transactions *International Journal of Software Engineering and its Applications* **6**

[11] Farbmacher H, Loew L, Spindler M 2019 *An Explainable Attention Network for Fraud Detection in Claims Management* Technical Report, University of Hamburg

[12] Nguyen Q, Wai L, Divakaran D M, Low K, Chan M 2019 *GEE: A Gradient-based Explainable Variational Autoencoder for Network Anomaly Detection* 10.1109