ABSTRACT

Detecting frauds in credit card transactions is perhaps one of the best test-beds for computational intelligence algorithms. In fact, this problem involves a number of relevant challenges, namely: concept drift (customers' habits evolve and fraudsters change their strategies over time), class imbalance (genuine transactions far outnumber frauds), and verification latency (only a small set of transactions are timely checked by investigators). However, the vast majority of learning algorithms that have been proposed for fraud detection rely on assumptions that hardly hold in a real-world fraud-detection system (FDS). This lack of realism concerns two main aspects: 1) the way and timing with which supervised information is provided and 2) the measures used to assess fraud-detection performance. This paper has three major contributions. First, we propose, with the help of our industrial partner, a formalization of the fraud-detection problem that realistically describes the operating conditions of FDSs that everyday analyzes massive streams of credit card transactions. We also illustrate the most appropriate performance measures to be used for fraud-detection purposes. Second, we design and assess a novel learning strategy that effectively addresses class imbalance, concept drift, and verification latency. Third, in our experiments, we demonstrate the impact of class unbalance and concept drift in a real-world data stream containing more than 75 million transactions, authorized over a time window of three years.

TABLE OF CONTENTS

LIST OF FIGURES

ABBREVIATION

GUI	Graphical User Interface
PY	Python
OPP	Object Oriented Programming
DRY	Don't Repeat Yourself
PIP	Package Installer for Python
MRO	Method Resolution Order
PEP	Python Enhancement Proposals
BDFL	Benevolent Dictator For Life
REPL	Read-Eval-Print Loop