Journal of Cases on Information Technology
Volume 25 • Issue 1

Intelligent Anti-Money Laundering Fraud Control Using Graph-Based Machine Learning Model for the Financial Domain

Atif Usman, Department of Computer Science and Information Technology, Virtual University of Pakistan, Pakistan
https://orcid.org/0000-0002-8130-7957

Nasir Naveed, Department of Computer Science and Information Technology, Virtual University of Pakistan, Pakistan

Saima Munawar, Department of Computer Science and Information Technology, Virtual University of Pakistan, Pakistan*
https://orcid.org/0000-0002-2446-3670

ABSTRACT

Financial domains are suffering from organized fraudulent activities that are inflicting the world on a larger scale. Basel Anti-Money Laundering (AML) index enlists 146 countries, which are impacted by criminal acts like money laundering, and represents the country's risk level with a notable deteriorating trend over the last five years. Despite AML being a substantially focused area, only a fraction of such activities has been prevented. Because financial data related to this field is concealed, access is limited and protected by regulatory authorities. This paper aims to study a graph-based machine-learning model to identify fraudulent transactions using the financial domain's synthetic dataset (100K nodes, 5.3M edges). Graph-based machine learning with financial datasets resulted in promising 77-79% accuracy with a limited feature set. Even better results can be achieved by enriching the feature vector. This exploration further leads to pattern detection in the graph, which is a step toward AML detection.

KEYWORDS

Anti-Money Laundering, Machine Learning, Networks, Semi-Supervised Learning, Tensorflow, Transactions

1. INTRODUCTION

Financial domains travail from organized fraudulent activities, which in turn affects the economy of the organization as well as the national level (Truman & Reuter, 2004). These activities involve the financial sector as a medium to transfer funds, but the factual magnitude of money laundering is uncertain and even unknown in most cases. Every country is forced by law in this global fight against money laundering. UNO2 estimates the total amount of funds circulated under money laundering cover in a meta-analysis on drugs and crimes, about 2.7% of global GDP, i.e., 1.6 trillion USD (Pietschmann & Walker, 2011).

DOI: 10.4018/JCIT.316665
*Corresponding Author

Another analysis by Walkers in the late ’90s mentioned 2.85 trillion USD involved in money laundering worldwide. Money laundering is a method of obtaining money generated from criminal activity and masking these funds that appear to be clean and originated from a legitimate source, i.e., the process of illegally gaining assets appears legal (IMF, 2020). The most common criminal activities that the world faces nowadays are terrorist funding, drug smuggling, and human trafficking.

Figure 1 illustrates the concept of transactions performed by agents on different bank accounts and these transactions performed using cash, cheque, electronic banking (ATM) or mobile banking uses a banking system for fulfilment. Theoretically, these transactions can be used intelligently to train a machine learning model which used advanced learning capabilities to identify and even predict potential money laundering attempts. Basel AML index (Manning, Wong, &Jevtovic, 2020) shows the list of countries that are heavily victimized by this act and caused severe damage to economies. The annual report from the UN States department “The International Narcotics Control Strategy Report” (INCSR) estimates illicit financial flows put over $10bn in Pakistan (Rates, Guides, Center, Clinton, & Hotline, 2017). This shows the vast radius and substantial impact these fraudulent activities are generating on societies and economies over the globe (Omar, Johari, & Arshad, 2014), which makes this area fundamentally essential to detect at as early a stage as possible (Schott, 2006).

Act against Money laundering becomes obligatory for any country because of the impact that it can create e.g. government drop control over economic policies, elevating conceivable failure in the banking system, and small to medium-scale businesses (Qureshi, 2017). Another adverse effect it can cause is in the private sector. The inflow of out-sized capital provides an ability to the companies where marketing penetration can be achieved by lowering the cost prices of goods at a significant scale and gaining a competitive advantage over others where there is no one to match their prices. Such consequence hits adverse and damaging impacts on small to medium-scaled businesses. In the same way, the large inflow of money for a short time in a bank can cause liquidity problems, leading to bankruptcy. Further on, it has various other impacts on economic policies, the reputation of financial institutions, the corruption perception index (CPI), and social effects. Most of the work done to handle fraudulent scenarios within financial domains are alert systems focused on linear methods and designed with threshold rules to work with suspicious transactions. This means that the system generally ingests marketing data transactions and applies defined rules to mark them as faulty or fraudulent transactions. Following problems usually appear in such AML systems.

Figure 1. The overall architecture of the system outlining the scope and concept