# Deep Detection of Fraudulent Transactions

## Coordinators/Contacts:

sl. dr. ing. Dan Novischi (dan_marius.novischi@upb.ro)

## Description

Credit card fraud resulted in the loss of €1.80 billion in the EU and a soaring $3 billion in the US to financial institutions between 2017 and 2018 alone. The rise of digital payments systems such as Apple Pay, Android Pay, and Venmo has meant that loss due to fraudulent activity is expected to increase. Moreover, fraud prevention systems are insufficient to provide adequate security to the electronic commerce systems. However, the collaboration between detection and prevention systems might be effective to secure electronic commerce and keep losses a minimum. Nevertheless, there are many challenges that hinder the performance of fraudulent transaction detection, such as concept drift, real time detection, skewed distribution, large amounts of data and so on. Deep Learning presents a promising solution to this problem by enabling institutions to make optimal use of their historic customer data as well as real-time transaction details that are recorded at the time of the transaction.

The goal of this research project is to both develop an augmented balanced dataset of fraudulent transactions based on generative adversarial models and an adaptive deep solution for the detection of fraudulent transactions.

## References

[1] Ba, H. (2019). Improving Detection of Credit Card Fraudulent Transactions using Generative Adversarial Networks. arXiv preprint arXiv:1907.03355.

[2] Zeager, M. F., Sridhar, A., Fogal, N., Adams, S., Brown, D. E., & Beling, P. A. (2017, April). Adversarial learning in credit card fraud detection. In 2017 Systems and Information Engineering Design Symposium (SIEDS) (pp. 112-116). IEEE.

[3] Carneiro, N., Figueira, G., & Costa, M. (2017). A data mining based system for credit-card fraud detection in e-tail. Decision Support Systems, 95, 91-101.

[4] Abdallah, A., Maarof, M. A., & Zainal, A. (2016). Fraud detection system: A survey. Journal of Network and Computer Applications, 68, 90-113.