# A blue text on a black background Description automatically generatedClassification in Evolving Data Streams: Handling Concept Drift and Adversarial Attacks

#### GE461: Introduction to Data Science, Data Stream Mining Assignment, Spring 2024, Project 5

Görkem Kadir Solun, 22003214, [kadir.solun@ug.bilkent.edu.tr](mailto:kadir.solun@ug.bilkent.edu.tr)

[Classification in Evolving Data Streams: Handling Concept Drift and Adversarial Attacks 1](#_Toc166800468)

[1 INTRODUCTION 2](#_Toc166800469)

[2 RELATED WORKS 2](#_Toc166800470)

[REFERENCES 3](#_Toc166800471)

## 1 INTRODUCTION

Data stream mining has become an essential area of research in data science, addressing the need to process and analyze continuously arriving data in real time. Traditional batch learning methods, which assume access to the entire dataset at once, are unsuitable for dynamic environments where data is generated rapidly. In such settings, models must be updated incrementally to reflect new information, making data stream mining a crucial technique for applications like fraud detection, network monitoring, and adaptive user interfaces. This project focuses on building and evaluating evolving data stream classification models using the scikit-multiflow library, emphasizing the challenges of concept drift and adversarial attacks.

This assignment aims to implement and compare various data stream classification methods, specifically addressing concept drift and adversarial attacks. Concept drift refers to changes in the underlying data distribution over time, which can degrade model performance if not properly managed. Adversarial attacks, on the other hand, involve malicious data injections designed to mislead the model. This report presents the implementation of several classification models, including Adaptive Random Forest, SAM-kNN, Dynamic Weighted Majority, and a custom ensemble model. The performance of these models is evaluated using prequential evaluation on synthetic and real-world datasets, focusing on handling concept drift and mitigating the impact of adversarial attacks. The results are discussed through comparative analysis using plots and tables, providing insights into the effectiveness of different approaches in dynamic data stream environments.

## 2 RELATED WORKS

Data stream mining is a critical area of research that focuses on extracting meaningful patterns and knowledge from continuous data streams. Unlike traditional batch learning methods, data stream mining techniques must process data in real time, updating models incrementally as new data arrives. This real-time processing requirement poses unique challenges, such as handling concept drift and maintaining model accuracy over time. Concept drift, where the underlying data distribution changes, is a common issue in data streams that can significantly affect model performance if not adequately addressed. Various approaches have been proposed to handle concept drift, including adaptive algorithms and ensemble methods that dynamically adjust to changing data distributions [1], [2]**, [3]**.

In addition to concept drift, data stream mining models are also vulnerable to adversarial attacks, where malicious entities inject false data to corrupt the learning process. These attacks can masquerade as legitimate concept drift, challenging detection and mitigation. Recent studies have focused on developing robust algorithms that distinguish between genuine concept drift and adversarial attacks, thereby enhancing the resilience of data stream mining models [**4**]. By integrating drift detection mechanisms and adversarial defense strategies, researchers aim to create more reliable and secure data stream mining frameworks capable of operating effectively in dynamic and potentially hostile environments.

# REFERENCES

1. J. Gama, I. Žliobaitė, A. Bifet, M. Pechenizkiy, and A. Bouchachia, "A survey on concept drift adaptation," ACM Computing Surveys (CSUR), vol. 46, no. 4, pp. 1-37, 2014.
2. I. Žliobaitė, "Learning under concept drift: an overview," arXiv preprint arXiv:1010.4784, 2010.
3. K. Prasanna, M. Khan, S. Alshahrani, S. Alshahrani, P. Reddy, M. Alymani, and J. Babu, "Continual Learning Approach for Continuous Data Stream Analysis in Dynamic Environments," \*Applied Sciences\*, vol. 13, no. 14, p. 8004, 2023.
4. Ł. Korycki and B. Krawczyk, "Adversarial concept drift detection under poisoning attacks for robust data stream mining," Machine Learning, vol. 112, no. 10, pp. 4013-4048, 2023.