

# Anomaly Detection to Improve Security of Big Data Analytics

Tom Slooff, Fabien Brocheton, Antonio Parodi, Radim Cmar, Francesco Regazzoni

## Motivation

Big data analytics largely rely on data. Because of their central role, it is fundamental to ensure the security and correctness of data used in these applications. Anomaly detection could help to increase the security of big data analytics applications.

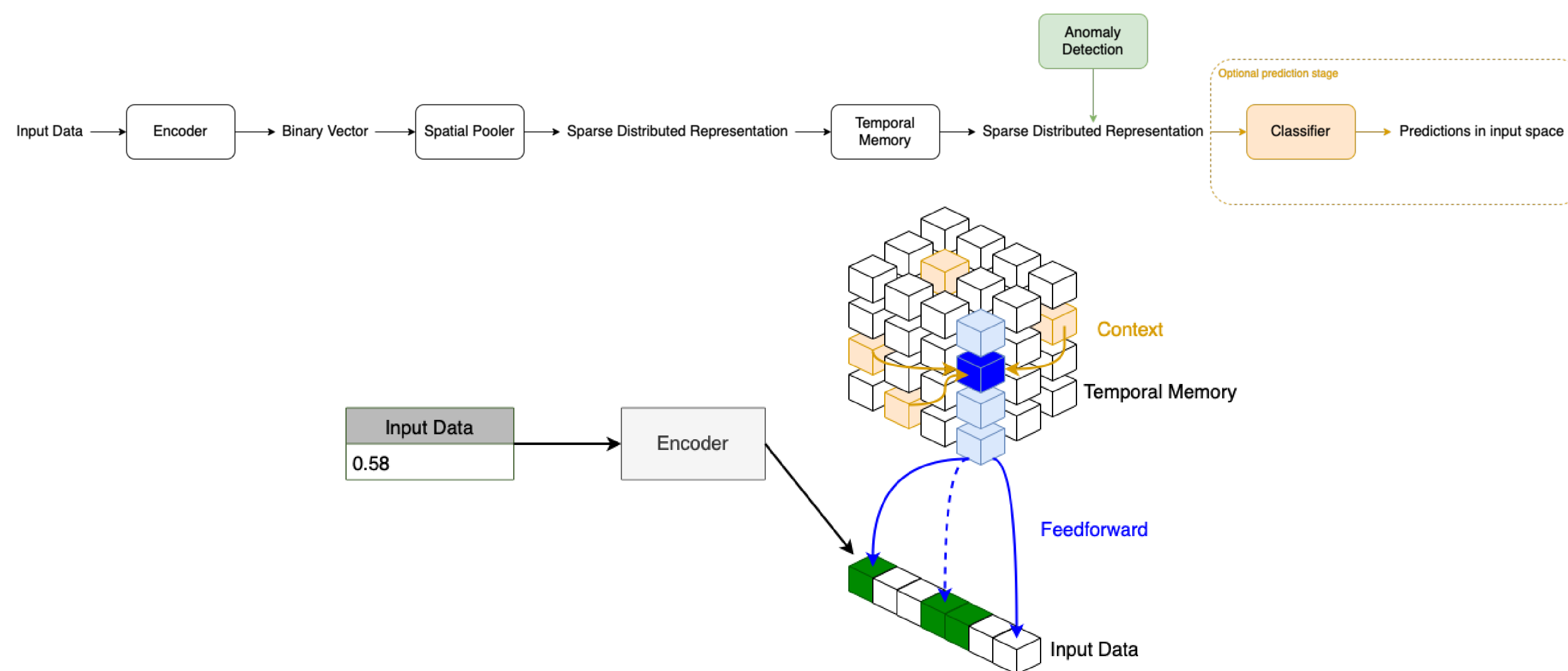
## Goal

There is a high variety in workflows and data which all put different requirements on the anomaly detection. Applying anomaly detection requires a designer to select a technique, implement it, and train it for their use-case. In this work we explore the possibility of providing a library of anomaly detection techniques that are universally applicable. Such a library may not reach the performance of the previous approach, but could drastically simplify the task of the designer while giving adequate performance for the application.

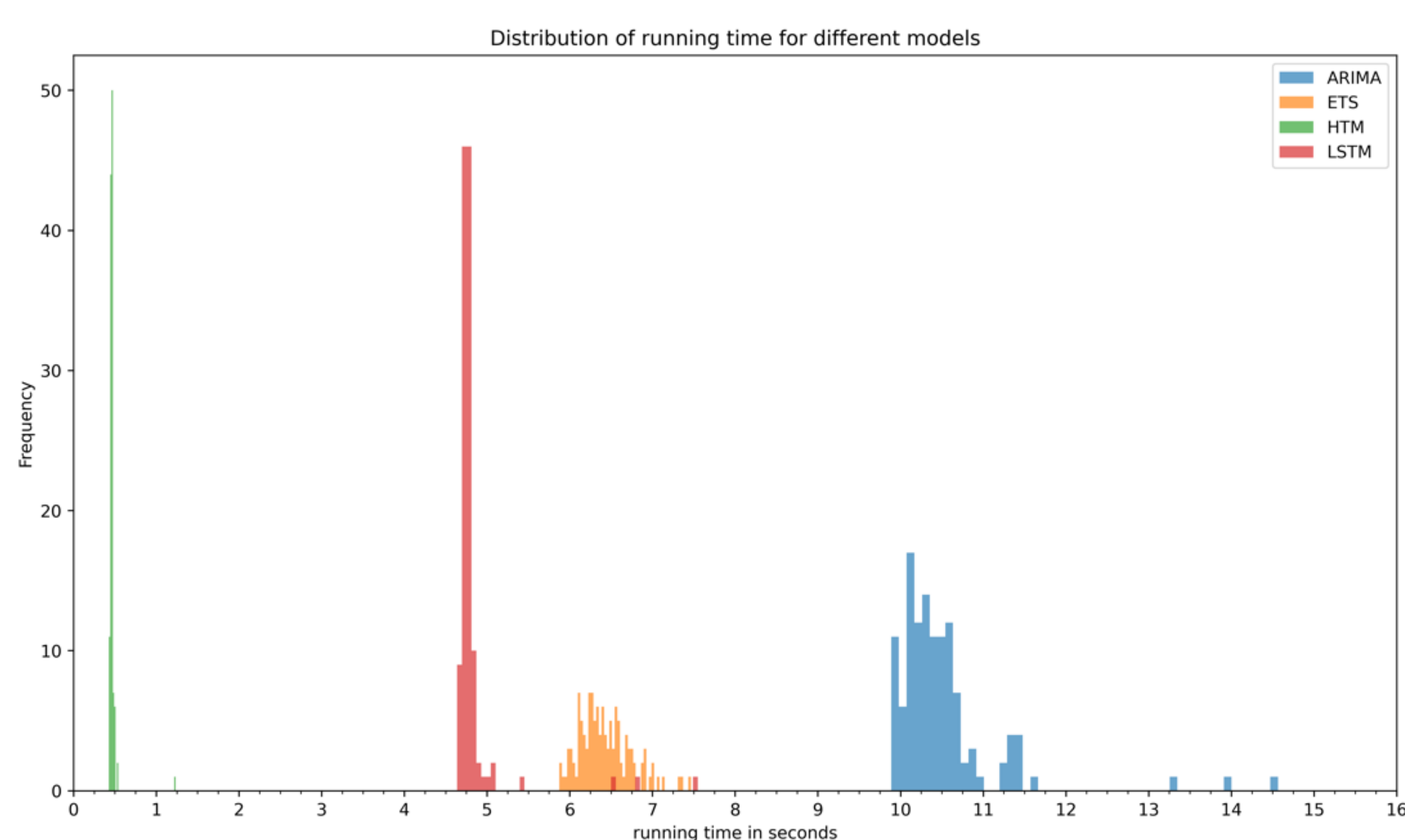
## Improved Security

Protection of data can be ensured through cryptographic primitives, which provide confidentiality, authentication, and integrity. In addition to this, anomaly detection can play a pivotal role. In a nutshell, anomaly detection learns the normal patterns of data and detects data points which fall outside of the norm. When used for security purposes, anomaly detection allows to identify anomalies in the data themselves, possibly introduced by malicious actors which exploit legitimate access to the system.

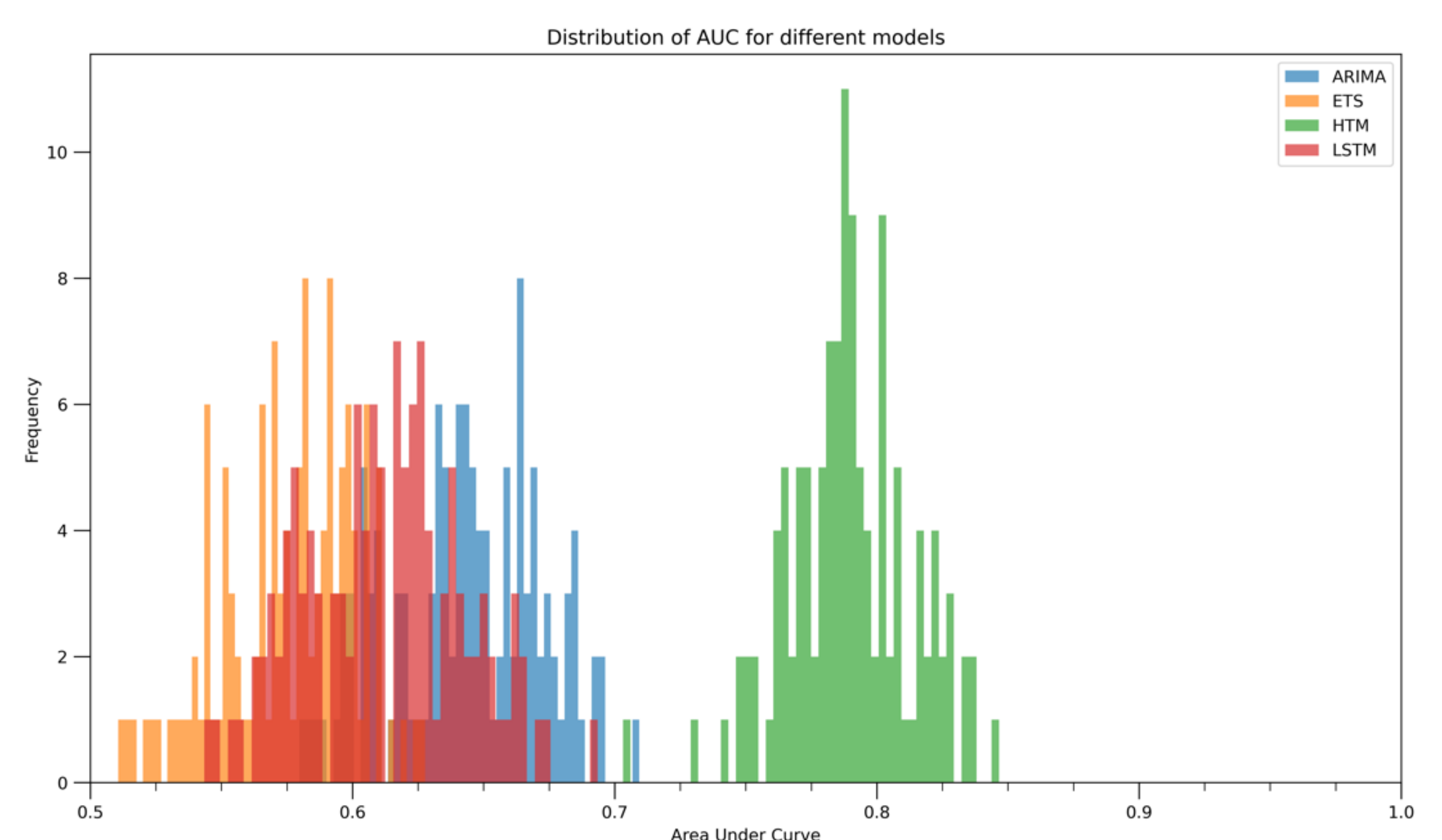
## Hierarchical Temporal Memory



## Running Time



## Anomaly Detection



## Conclusions

Anomaly detection is an interesting tool to enhance security in big data analytics. We focused on HTM as a universally-applicable technique for anomaly detection because the encoders allow it to handle a wide variety of input data similarly. The preliminary results show excellent performance of this technique compared to other popular anomaly detection methods.

## Paper



## Contact



This work is partially supported by the European Union Horizon 2020 Program under the EVEREST project (grant agreement No 957269)

Tom Slooff (tom.slooff@usi.ch), Francesco Regazzoni  
Computing Frontiers 2022. May 17–19, 2022. Torino, Italy

