A policy compliance detection architecture for Digital Data Marketplaces (DDM)

Lu Zhang, Reginald Cushing, Cees de Laat, Paola Grosso
MultiScale Networked Systems Lab, Informatics Institute, University of Amsterdam

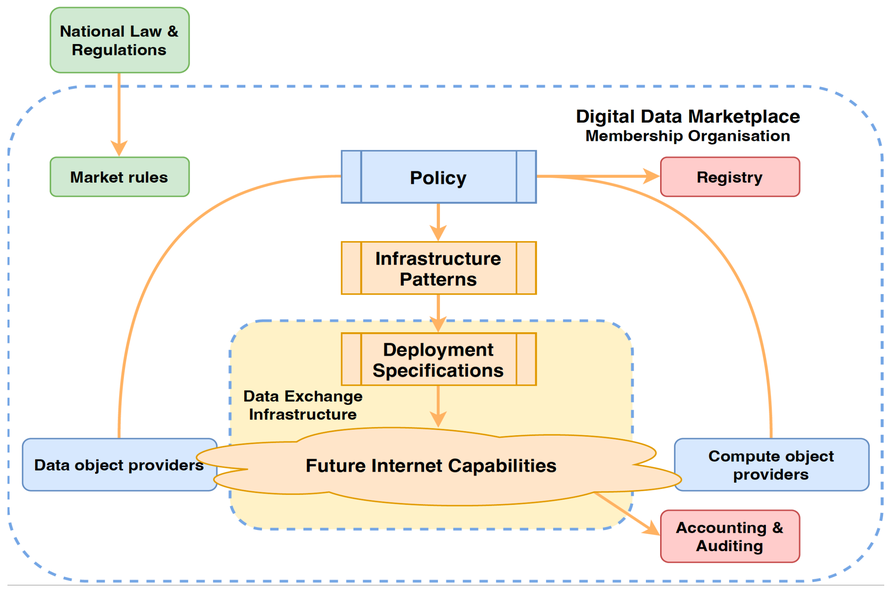
Digital Data Marketplace

A Digital Data Marketplace (DDM) is a digital infrastructure that facilitate secure and trustworthy data sharing

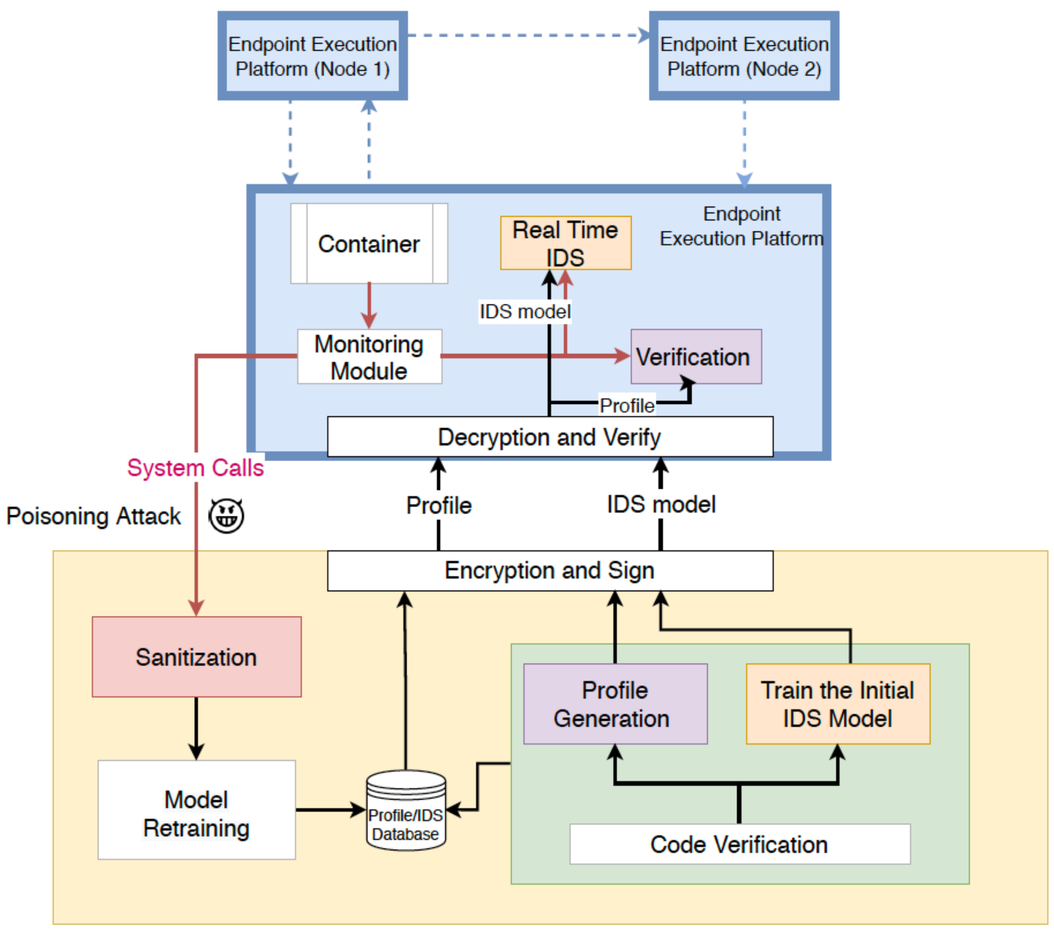
Airline Use Case: Multiple airline companies aggregate data to train a ML model to predict the necessity of aircraft maintenance

Policy Examples

- The outsourced aircraft data can only be used to train the prediction model but not the others
- The aircraft data can not be leaked to any unauthorized parties



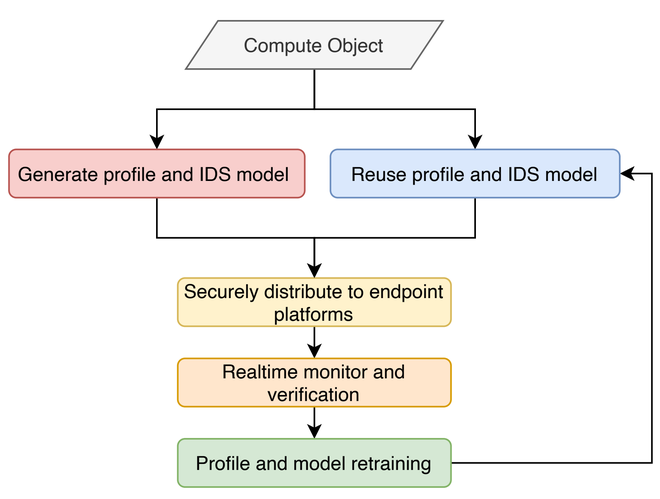
Modules of the policy compliance detection architecture



- Monitor and analyse **Linux system calls** during the execution stage to detect policy breach
- **Profile generation and validation**
  - Profile with n-grams frequency distributions
  - Verify at the endpoint
- **A hybrid IDS module**
  - Use OC-SVM for anomaly detection
  - apply the signature-based methodology to reduce false alarms
- **Sanitization module**
  - Filter out malicious samples with DB-SCAN clustering algorithm
  - Defend against adversarial machine learning attacks

Procedures of the policy compliance detection architecture

- A **profile and a pre-trained IDS model** are built for every **uniquely identifiable** compute object
  - Initially trained in a secure environment and **allow reuse**
- Distribute the profile and IDS model to endpoint execution platforms **in a secure channel**
- Monitor, analyse and verity **in endpoint platforms** in real time
- Gather the new monitoring data and **periodically re-training** to increase generalization of the IDS model



Acknowledgements: This research is funded by the Dutch Organization for Scientific Research (NWO) under contracts 628.009.014 (SSPDDP project) and 628.001.001 (DL4LD project).