UPPSALA
UNIVERSITET

DATA GENERATION AND KNOWLEDGE SHARING

FOR INTRUSION DETECTION SYSTEMS IN THE INTERNET OF THINGS

Christian Rohner and Andreas Johnsson

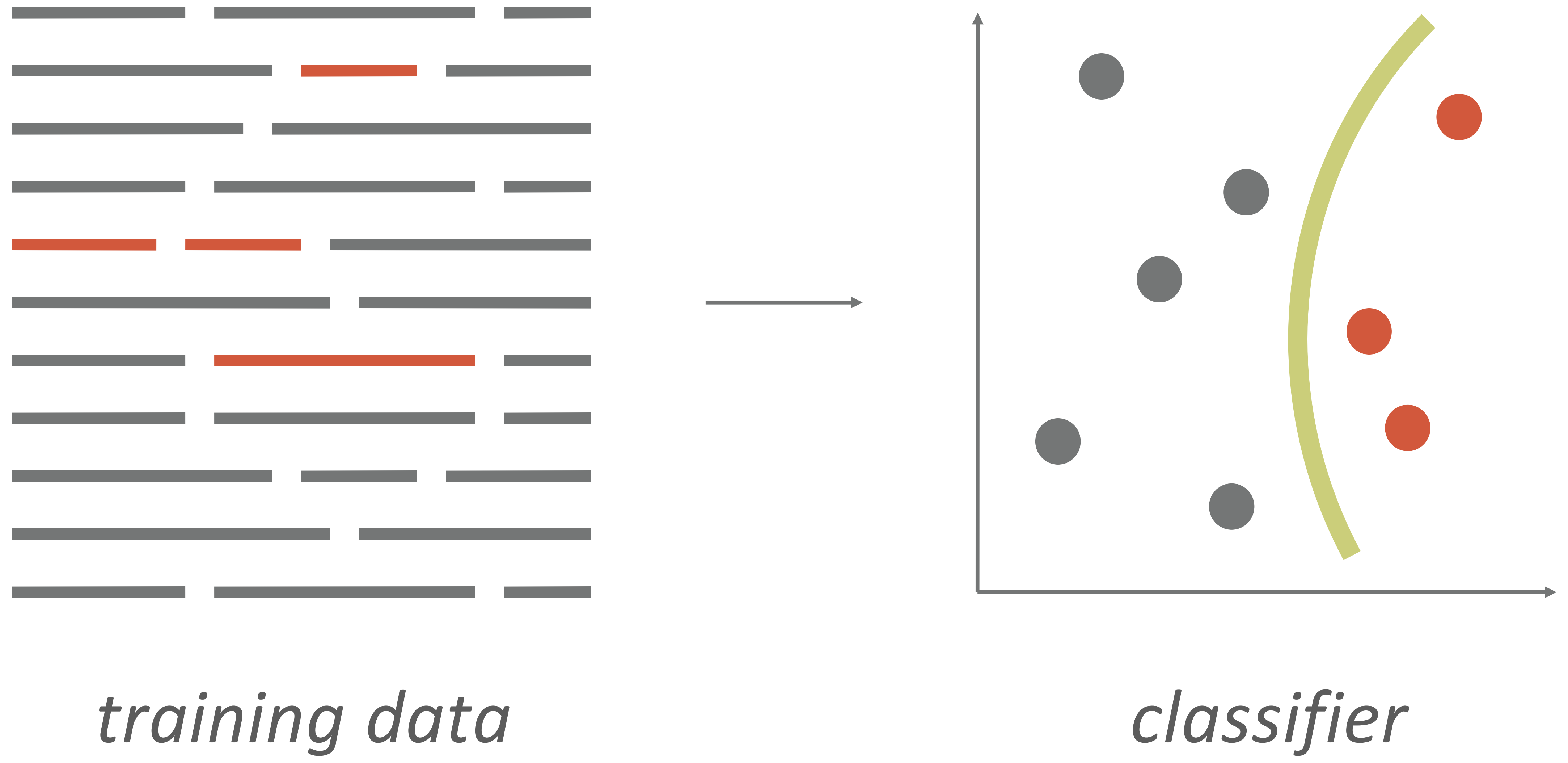
VINNOVA
Sveriges innovationsmyndighet

THE INTERNET OF THINGS

- Monitor and control and environment or process using multiple (wireless) sensors and actuators.
- Multiple possibly competing actors offering individual services.
- Often shared communication and computing infrastructures.

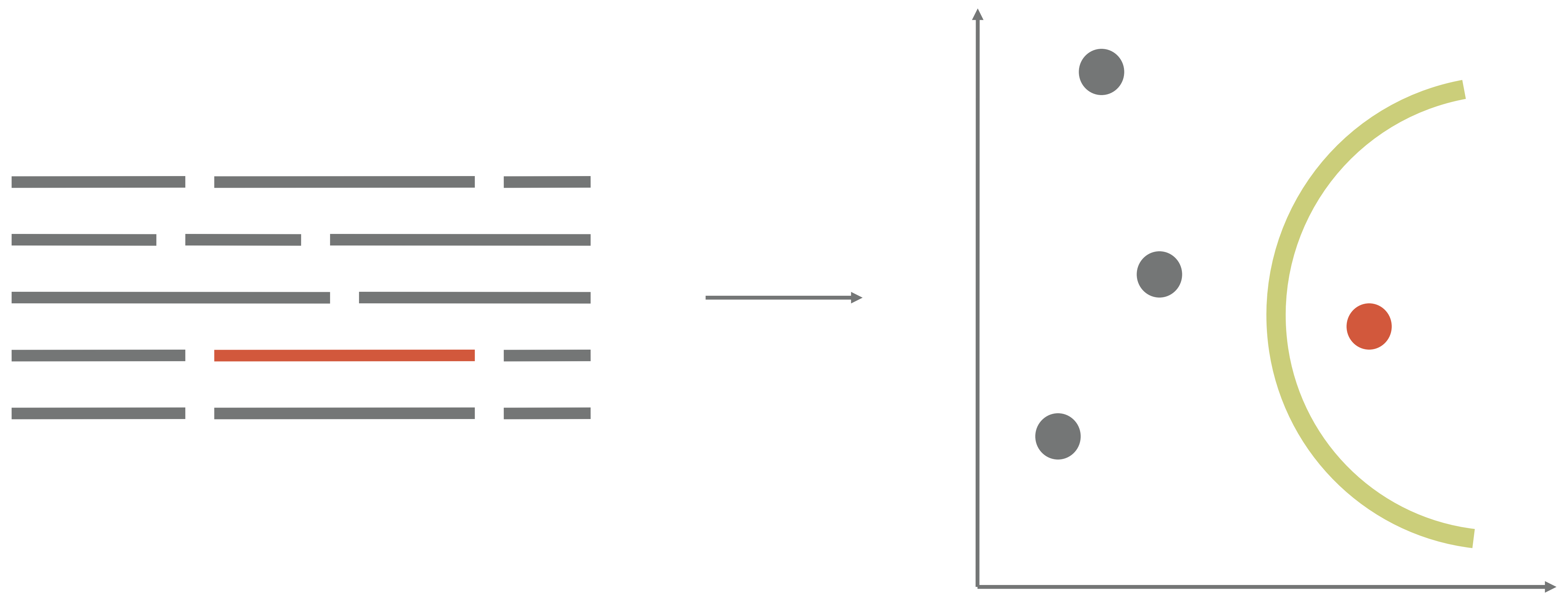
- IoT is target of attacks which severely impact privacy, robustness, performance and businesses of critical importance.
- Data-driven Intrusion Detection Systems (IDS): attacks and anomalies are detected and learned from previous examples.

DATA-DRIVEN INTRUSION DETECTION SYSTEMS



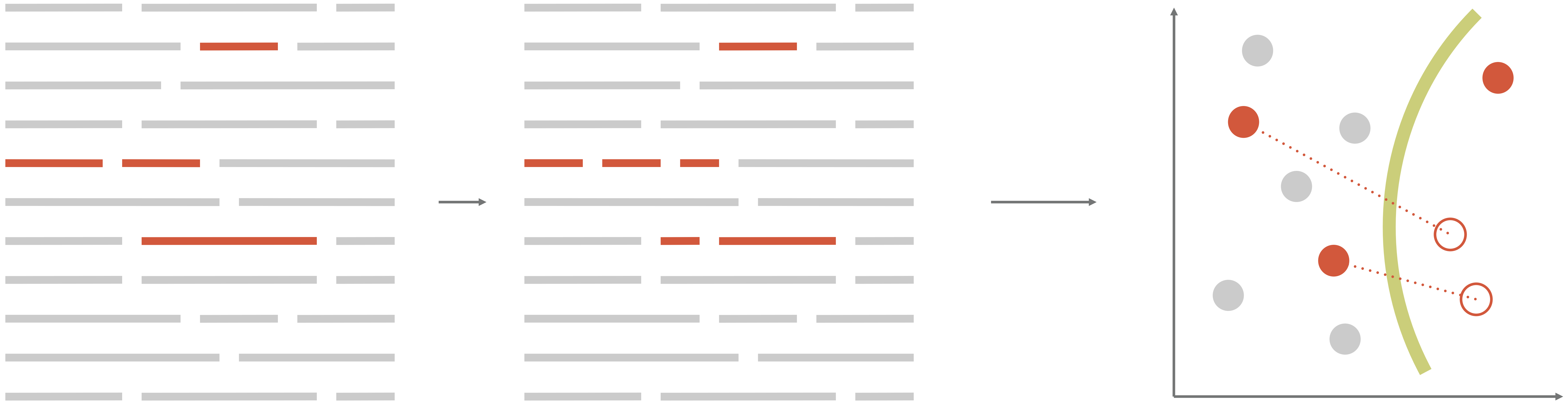
DATA-DRIVEN INTRUSION DETECTION SYSTEMS

- Data availability Challenge: classification only as good as the data used to train



ADAPTIVE ADVERSARIES

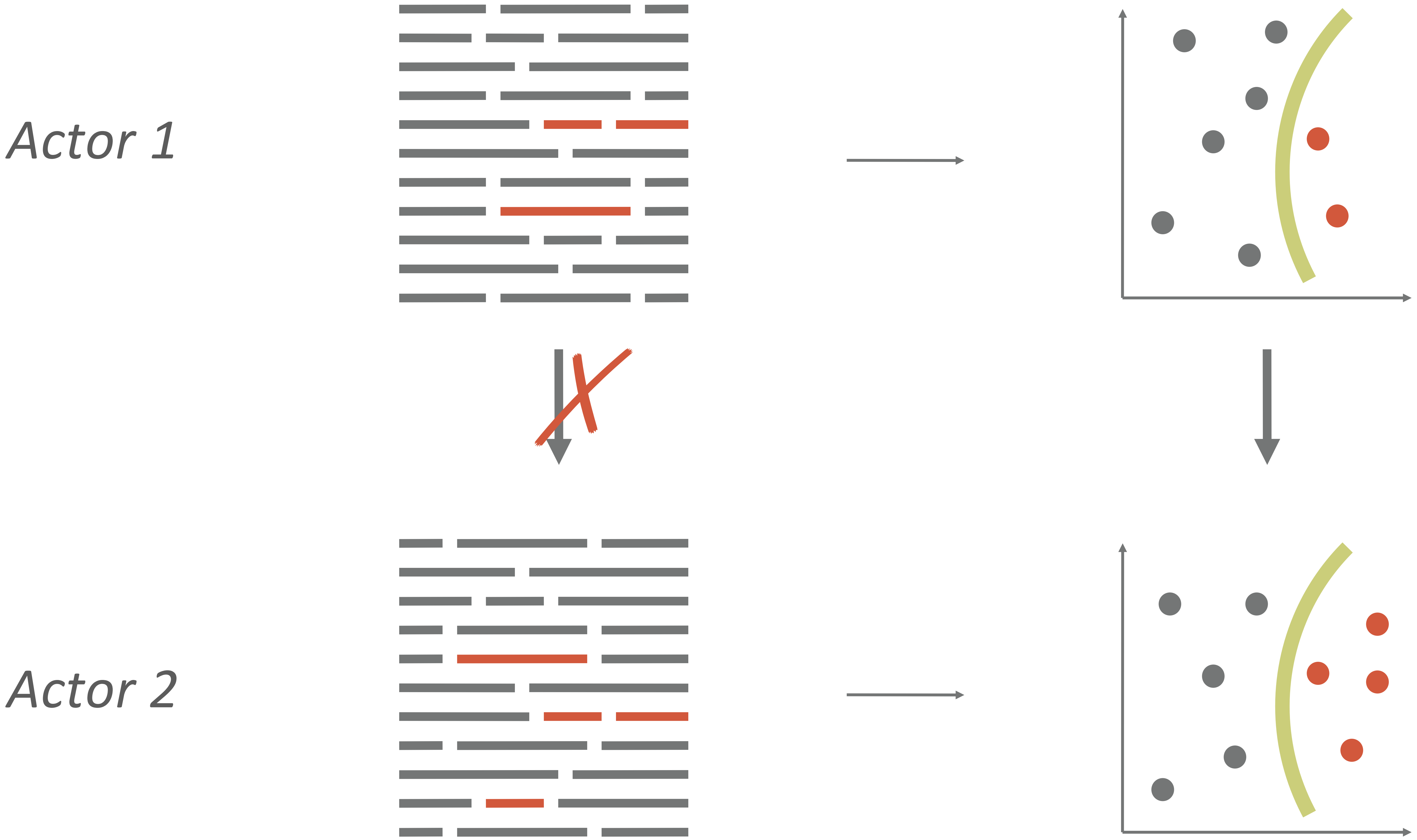
- Robustness Challenge: small variations of the attack can evade the classifier



evasion

PRIVATE KNOWLEDGE SHARING

- Privacy Challenge: don’t reveal attacks that were used in the training set



Actor 1

Actor 2

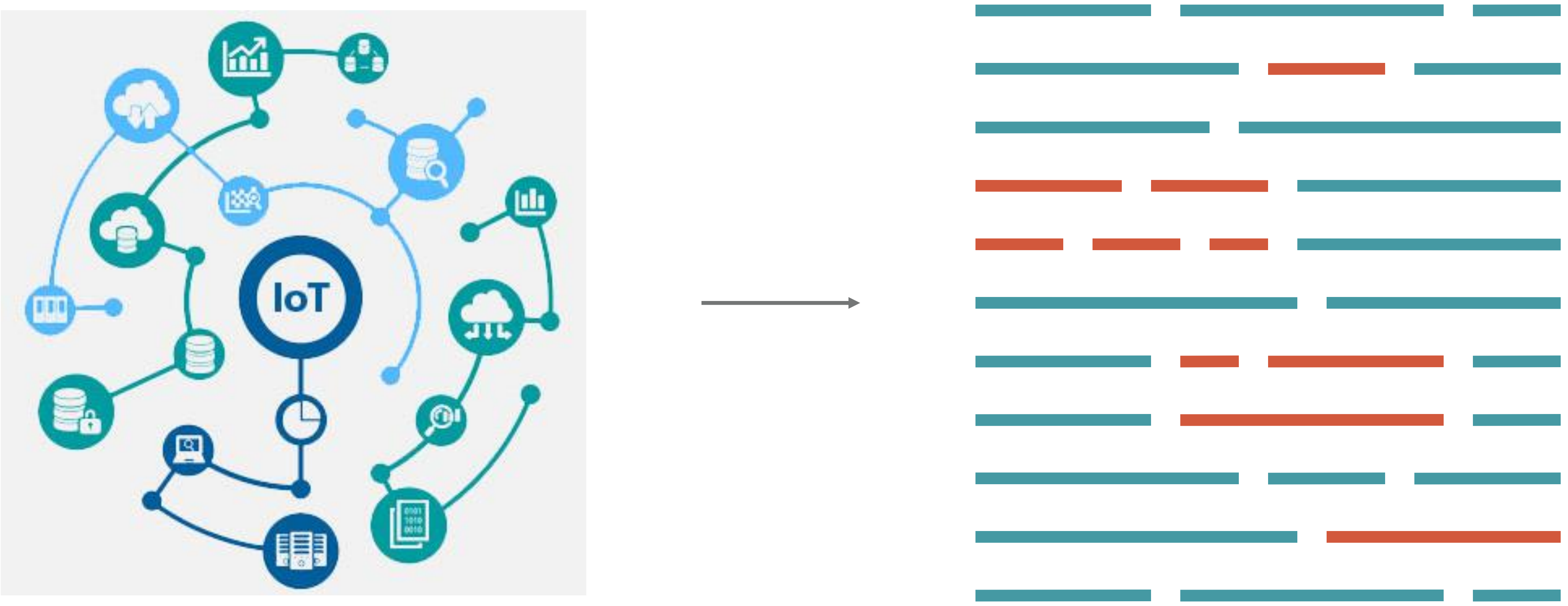
GOAL 1: DATA GENERATION

➤ Testbed and Simulation

Attack implementations

Attack variations

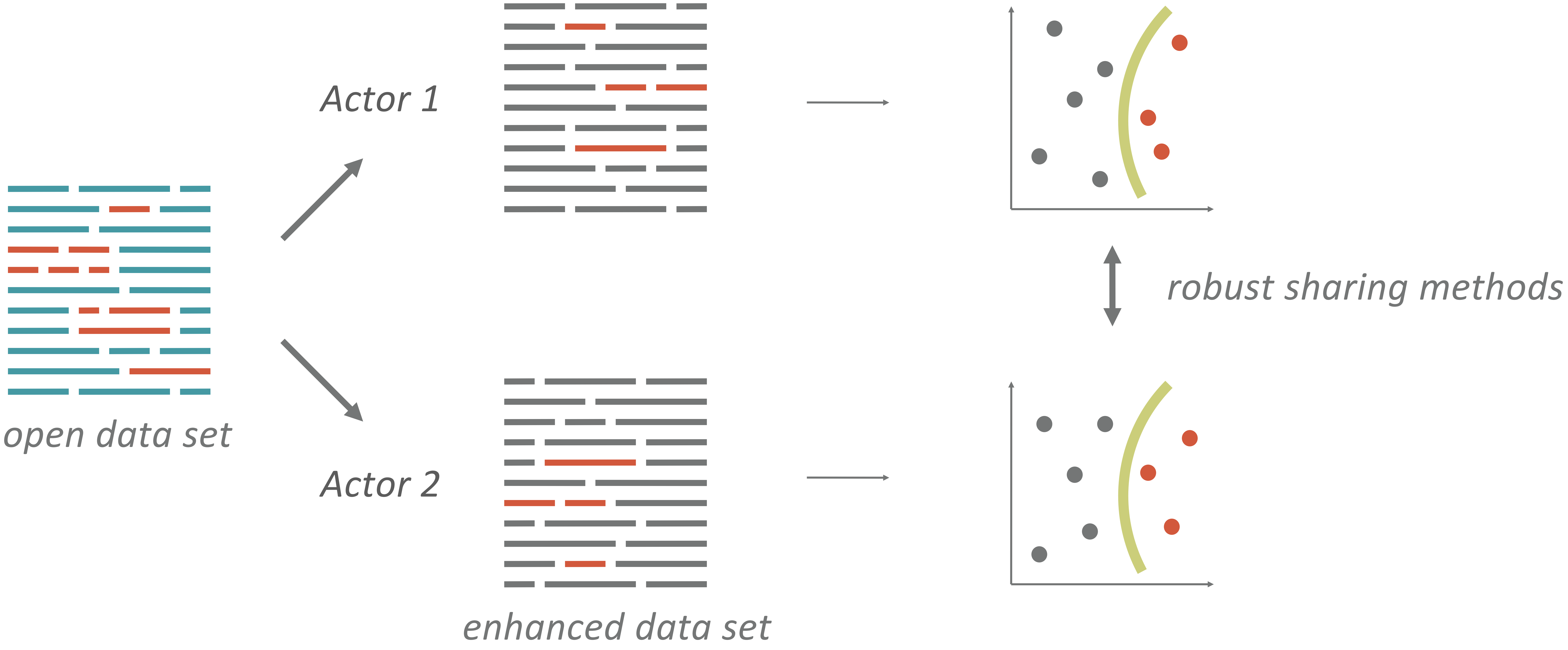
…



open data sets

GOAL 2: PRIVATE KNOWLEDGE SHARING

➤ Transfer learning and Federated learning



CONTACT

- Christian Rohner (Security and IoT expertise)
  christian.rohner@it.uu.se

- Andreas Johnsson (Network performance and ML expertise)
  andreas.johnsson@it.uu.se