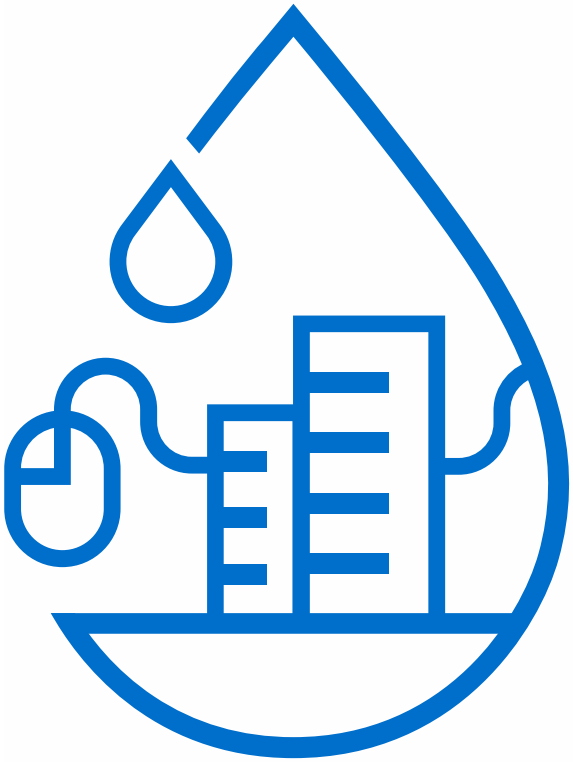


Applying ML algorithms to build anomaly-based cyber and physical detection systems

ECSCI Workshop – June 24th, 2020

Juan Caubet, PhD (EURECAT)

stop-it-project.eu

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No.740610.
The publication reflects only the authors' views and the European Union is not liable for any use that may be made of the information contained therein.

Anomaly Detection using ML – Challenges

High rate of False Positives

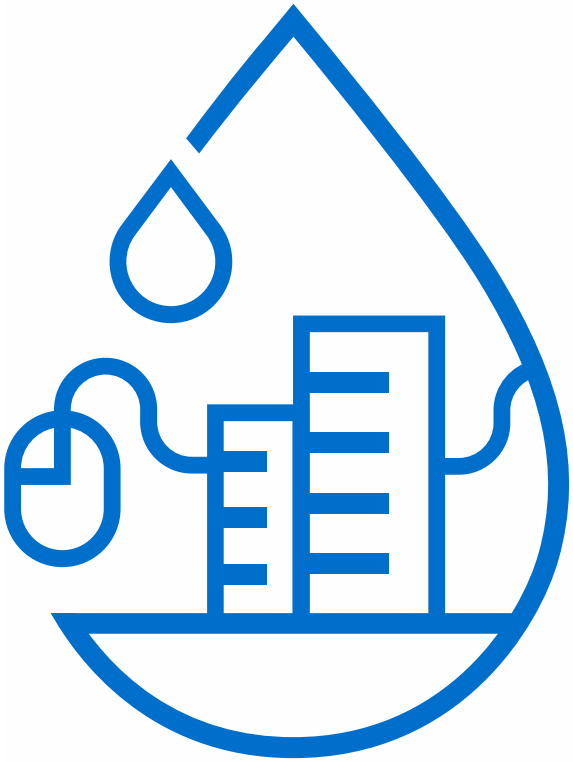
Historically, machine learning approach returns a higher amount of false positives than misuse approach.

Lack of context information

On several previous works, learns from of data.

Poor consensus on the Anomaly Detection

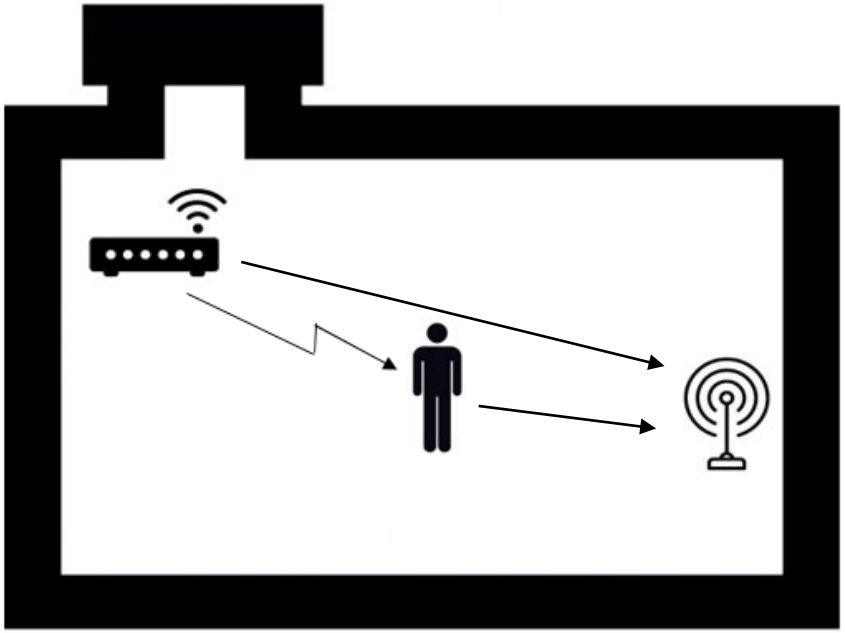
Most of the current work, try to find anomalies using a small pool of different algorithms.



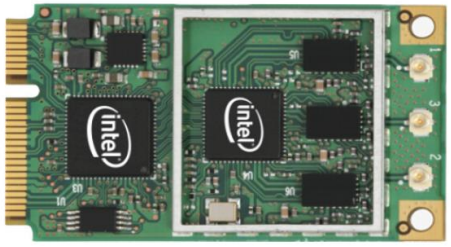
HUMAN PRESENCE DETECTOR (HPD)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No.740610.
The publication reflects only the authors' views and the European Union is not liable for any use that may be made of the information contained therein.

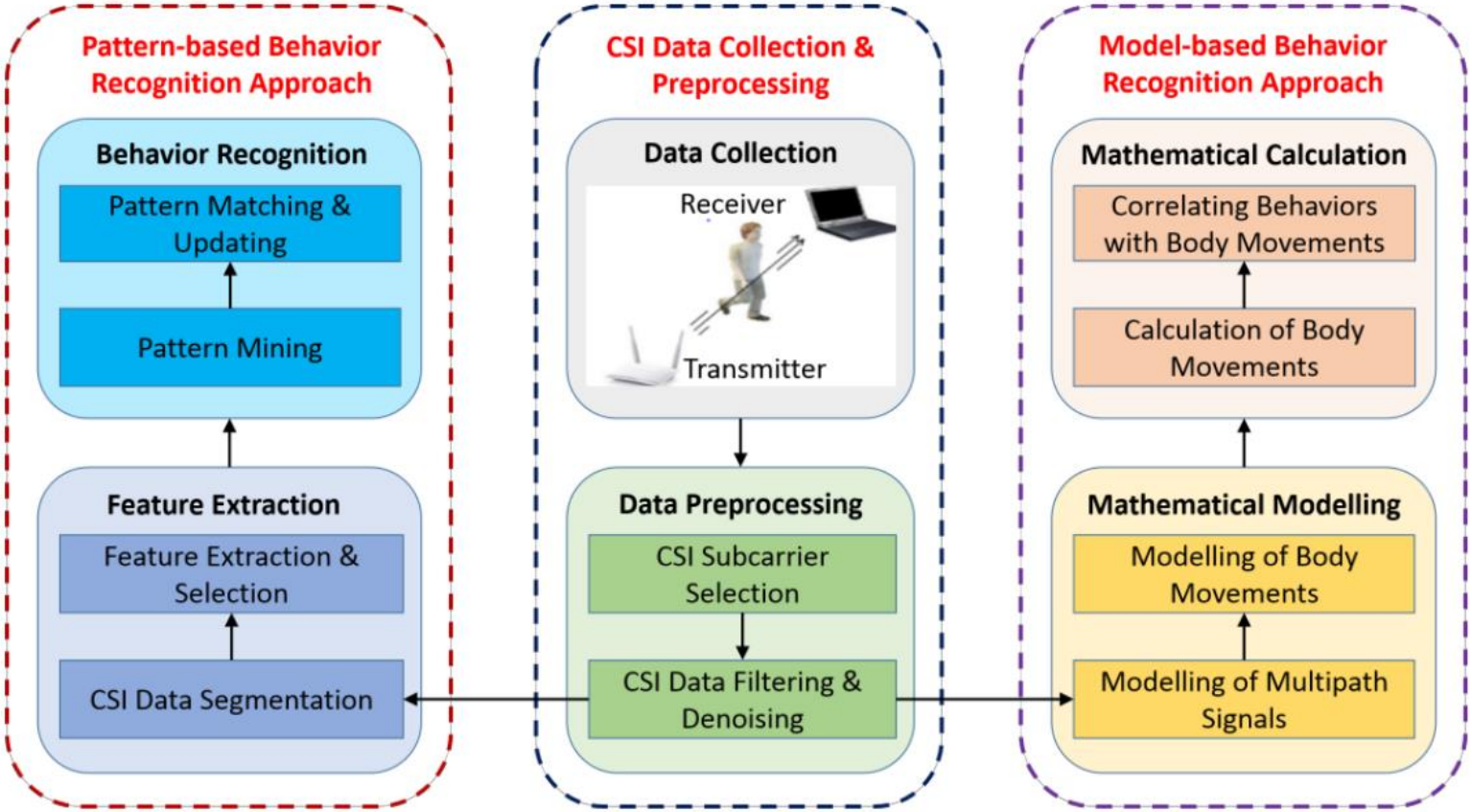
HPD – System Description



- **WiFi Signals change** due to human presence.
- The system exploits **Channel State Information (CSI)** to detect human movement.
- CSI is part of the **WiFi protocol**.
- To acquire WiFi signal reflection data are needed **two WiFi devices**.
- These devices are **WiFi Commercial Off-The-Shelf (COTS)** devices.
- It is possible to detect an intruder in a room or even **detect the intruder through the wall**.

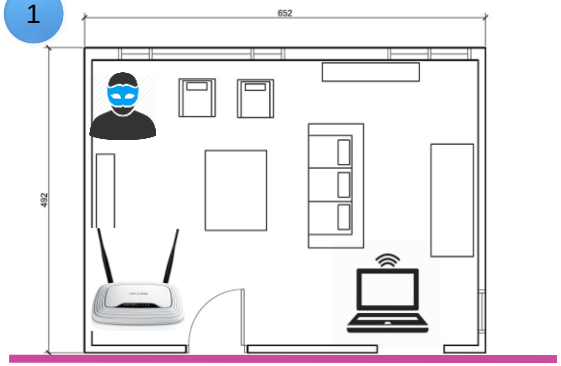


HPD – System Description



HPD – Deployment

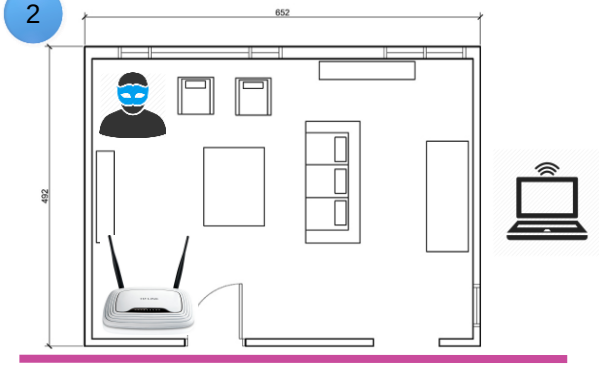
1



This method is based on CSI

Applications:
- Movement detection (intruders).
- Breathing rate analysis and identification.
- Presence detection (evacuation).
- People counting.

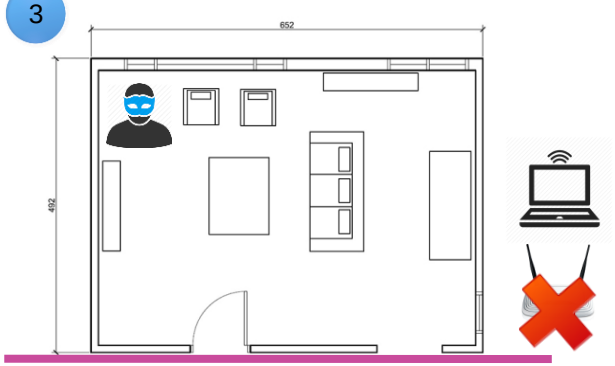
2



This method is based on CSI

Same applications but through the wall.

3

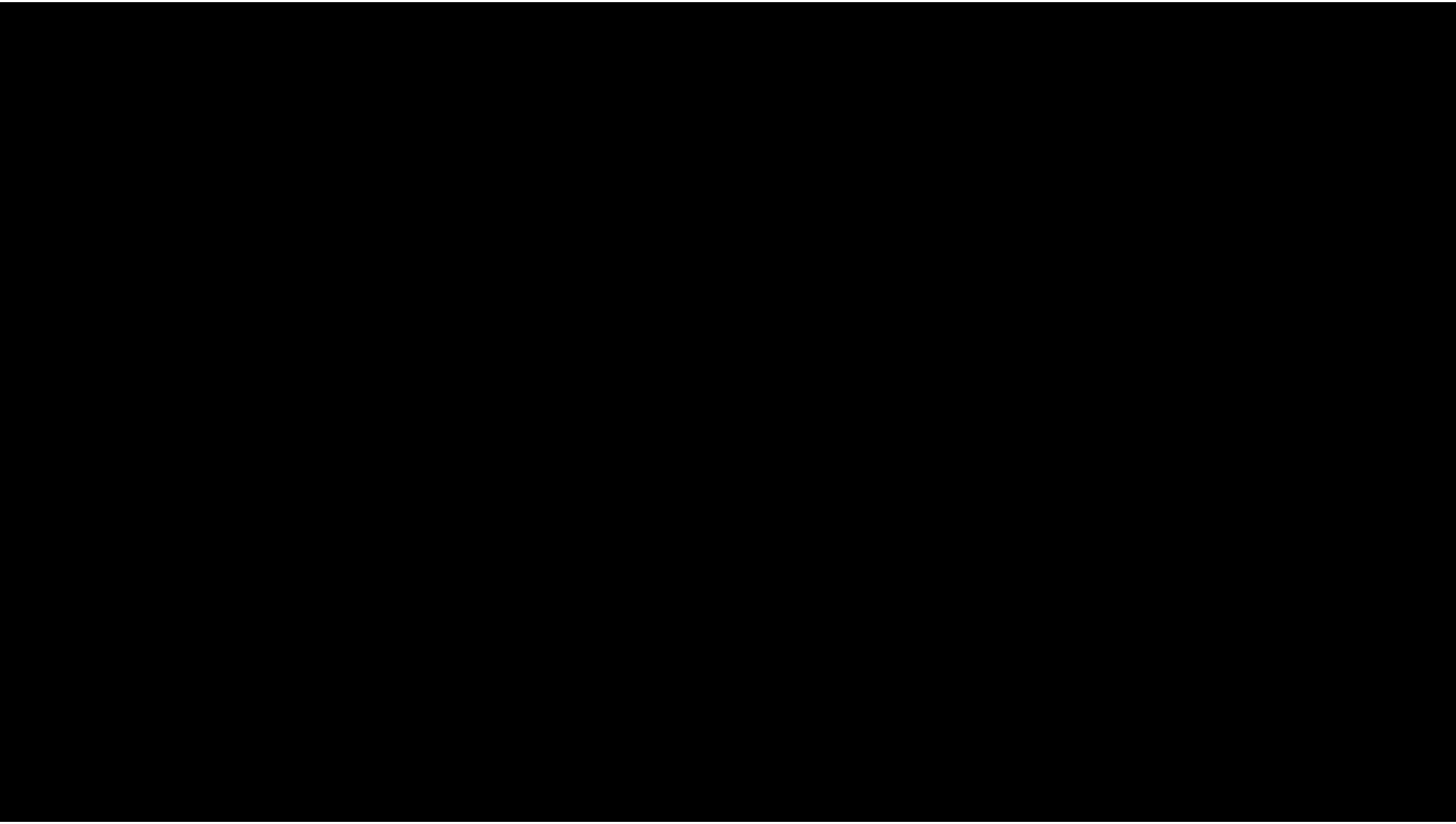


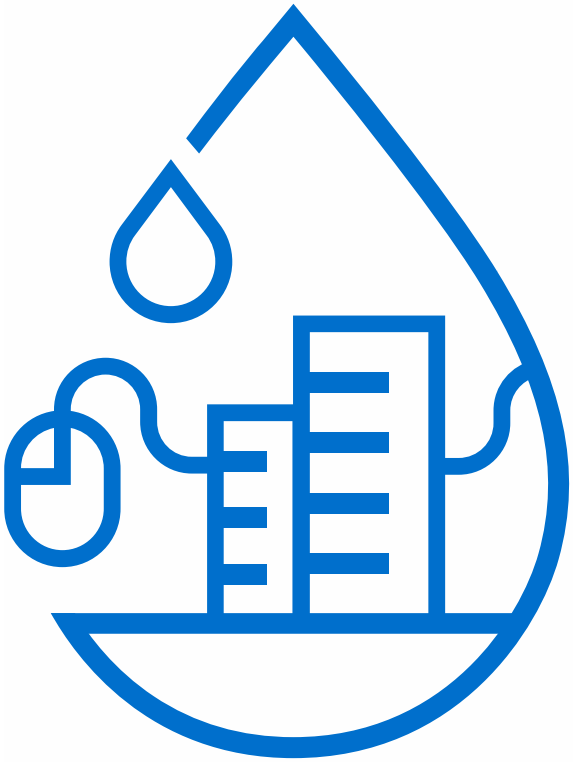
This method is not based on CSI

No studies with CSI until now. There are studies using SDR (Software Defined Radio) based on MIMO WiFi. With 90% of success.

- ❑ Limitations
  - ✓ Noise and micro-interruptions.
  - ✓ Jamming (Wi-Fi Spectrum attack).
  - ✓ CSI attacks (CSISec).
  - ✓ Range and sensitivity (antenna directivity, training and networks of routers/AP).
  - ✓ Fresnel zones.

HPD – Demo





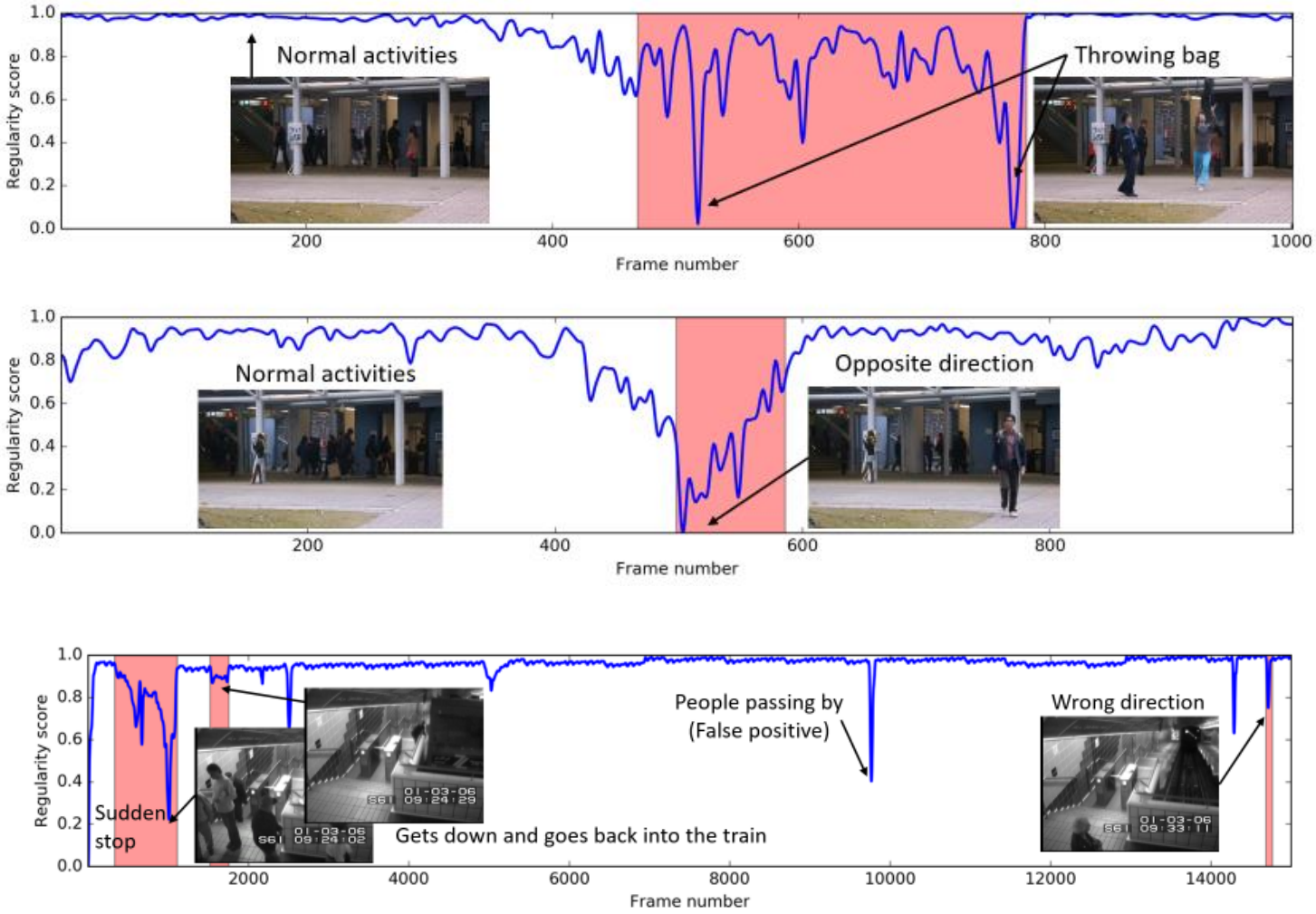
Computer Vision Tools (CVT)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No.740610.
The publication reflects only the authors' views and the European Union is not liable for any use that may be made of the information contained therein.

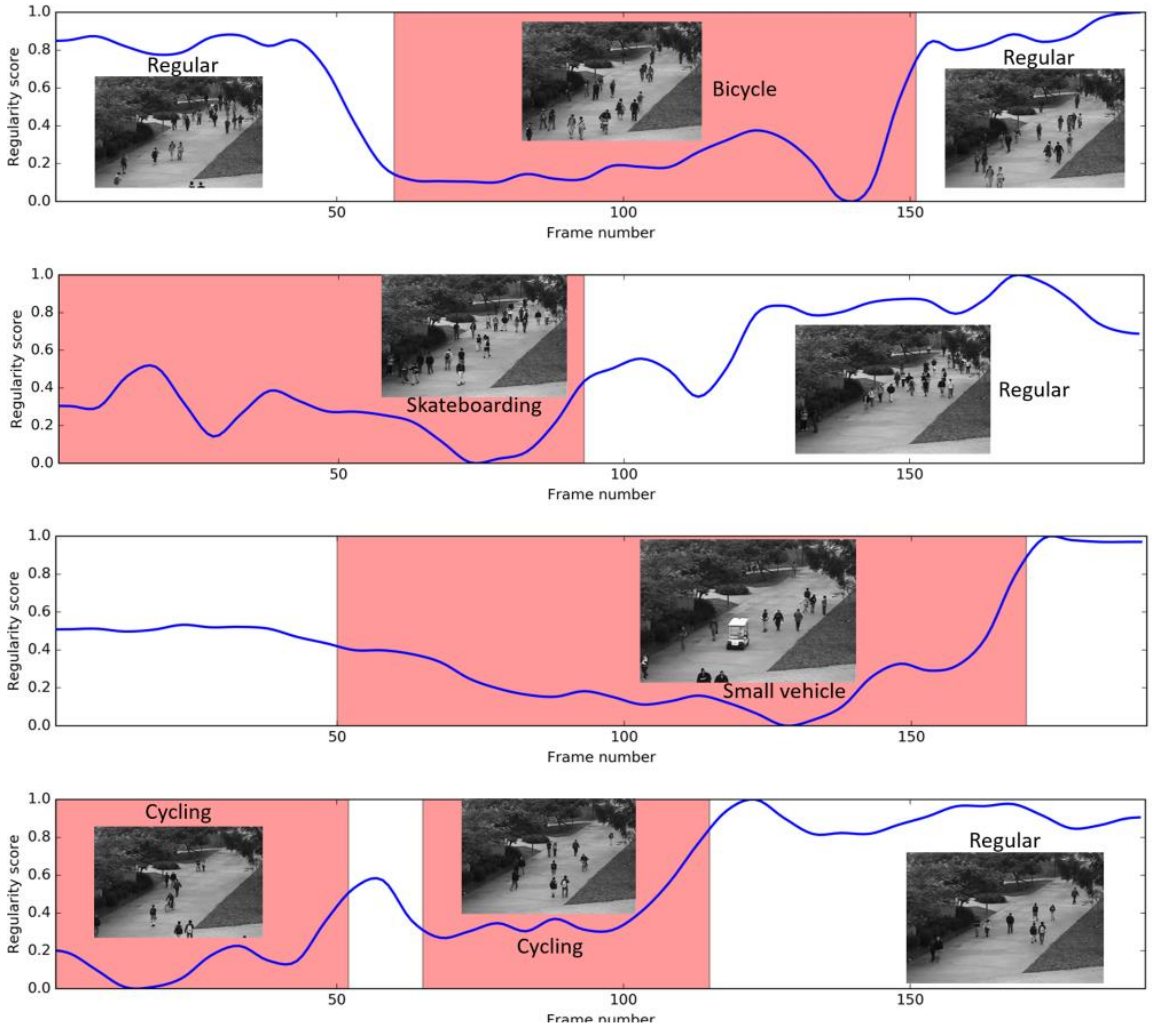
CVT – System Description

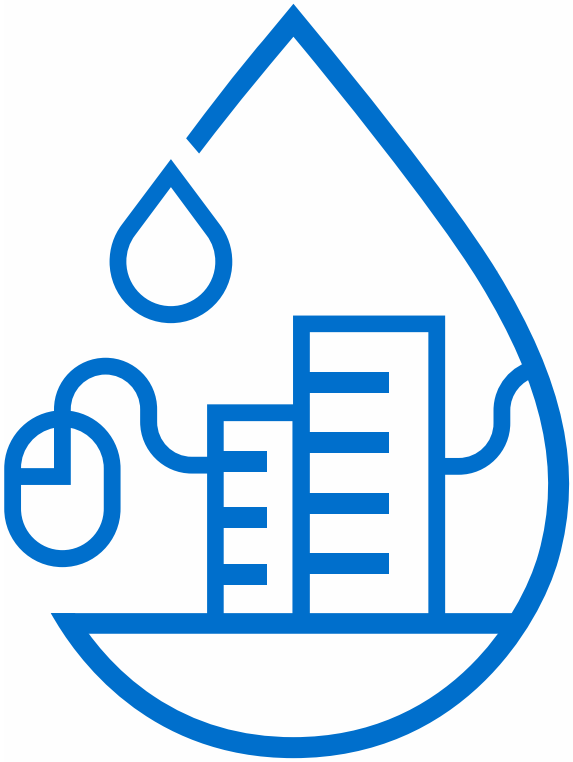
- The goal of the CVT is to **survey large-scale utility areas** using an existing network of cameras **detecting any suspicious behaviour** using a computer vision algorithm.
- **The system attempts to “predict” the next frame** based on the current input and the training set.
- When the **differences between the prediction and the ”true” frame** is beyond a threshold, the situation is considered suspicious.
- One instance of the CVT runs per video stream.
- To balance the computational cost and the real time aspect, the predictions are minimized to 5 frames per second.
- All parameters (threshold, number of predictions) can be adjusted to optimize performance in each scenario.

CVT – Results


Regularity score
Frame number
Normal activities
Throwing bag
Normal activities
Opposite direction
Sudden stop
Gets down and goes back into the train
People passing by
(False positive)
Wrong direction

CVT – Results


Regularity score
Frame number
Regular
Bicycle
Regular
Skateboarding
Regular
Small vehicle
Cycling
Cycling
Regular

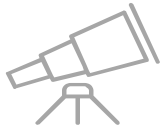


REAL-TIME ANOMALY DETECTOR (RTAD)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No.740610.
The publication reflects only the authors' views and the European Union is not liable for any use that may be made of the information contained therein.

RTAD – Objectives

We have designed a system seeking to improve the performance of existing solutions and the experience of users who interact with this type of tools:



Use and explore data from many fields.

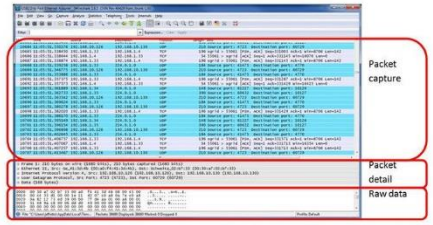
Minimise the amount of false positives.

Improve the performance involving an analyst.

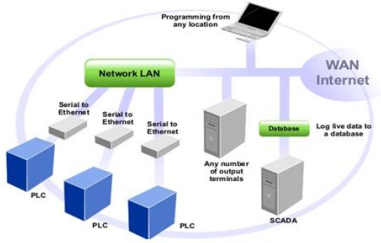
Combine different types of algorithms which have different ways to find anomalies (supervised, no supervised…).

RTAD – System Description

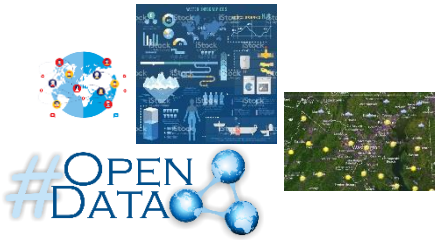
Cyber



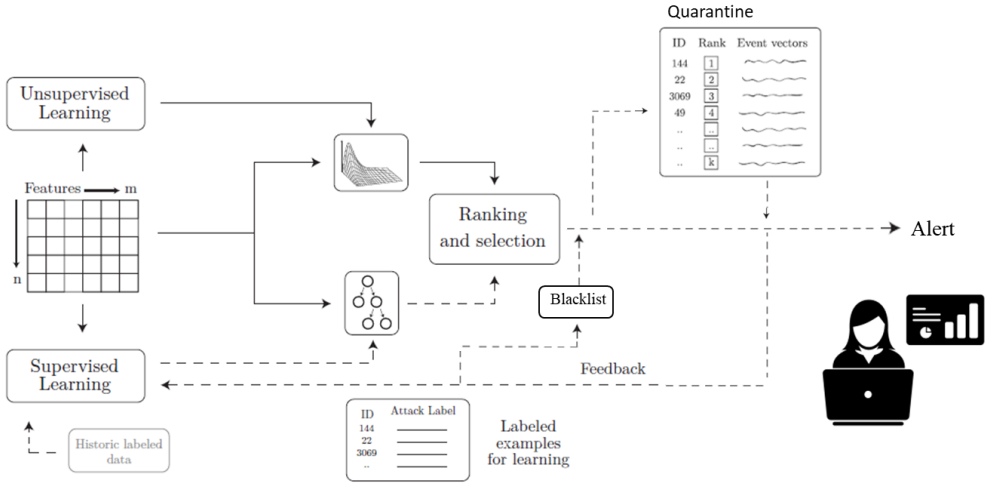
Physical



Context



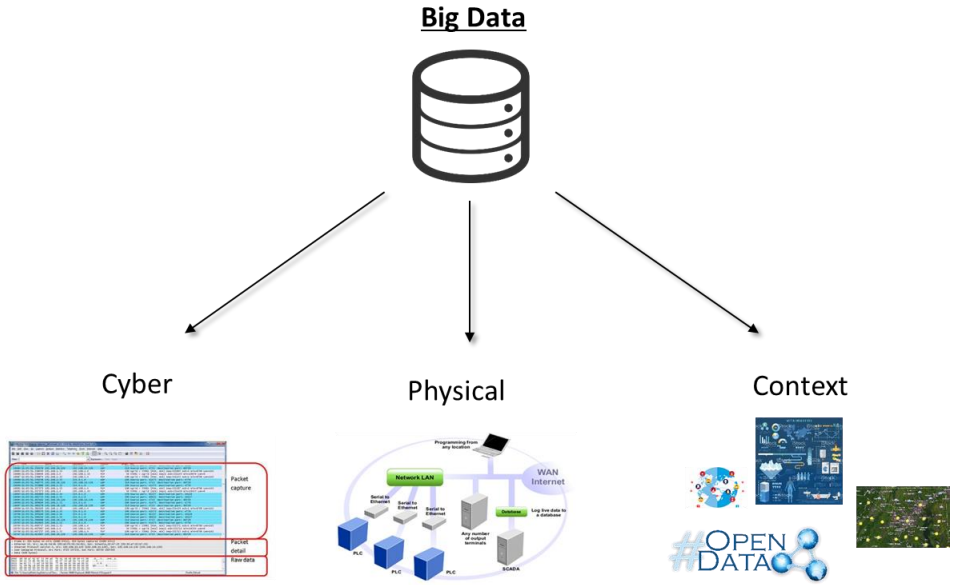
REAL-TIME BIG DATA SECURITY



K. Veeramachaneni, I. Arnaldo, V. Korrapati, C. Bassias and K. Li, "AI^2: Training a Big Data Machine to Defend," 2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS), New York, NY, 2016, pp. 49-54

RTAD – System Description

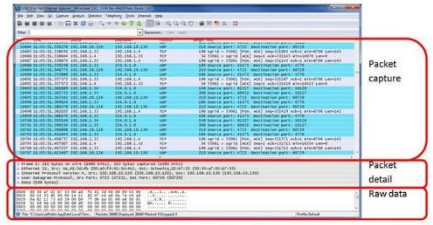
- Detect and alert attacker behaviour:
  - *Known Attacks (Signature based)*
    - Protocols: BCAnet, DNP3, ENIP, FOX, MODBUS, MODICON, OMRON, S7.
  - *Known Tactics (Behaviour):*
    - Exfiltrate Over Alternate Protocol, Data Hiding, Message Spoofing, etc.
  - *Abnormal and suspicious situations.*



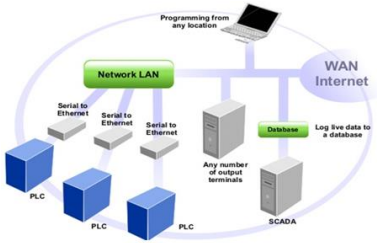
- Possible inputs:
  - ✓ **PCAPs**. These files have to contain packets from/to all devices/systems of the infrastructure that has to be monitored.
  - ✓ **Netflow data**. It could be captured using the open source tool nfdump (http://nfdump.sourceforge.net/).
  - ✓ **Logs** of hosts, PLCs, HMIs, Gateways, PCs, etc. (Syslog or other log system).
  - ✓ **Logs of IDS** (Intrusion Detection Systems) like Zeek, Snort, Suricata...
  - ✓ **Logs from tools that use DPI** (Deep Packet Inspection).
  - ✓ **Devices values** over time (actions, status, etc.).
  - ✓ **Sensor values** over time.

RTAD – STOP-IT tools connection

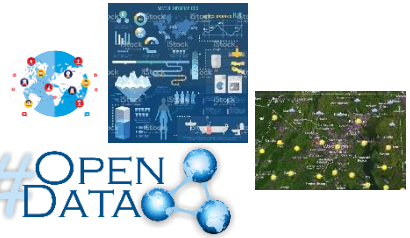
Cyber



Physical

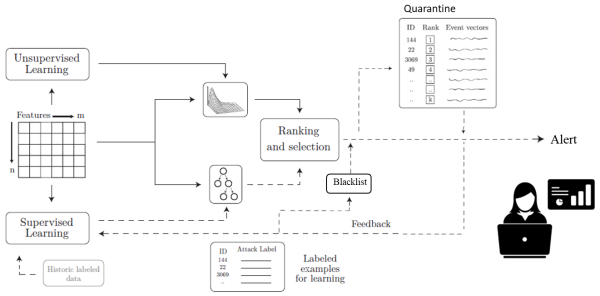


Context



REAL-TIME BIG DATA SECURITY

APACHE METRON



Jammer Detector

HPD

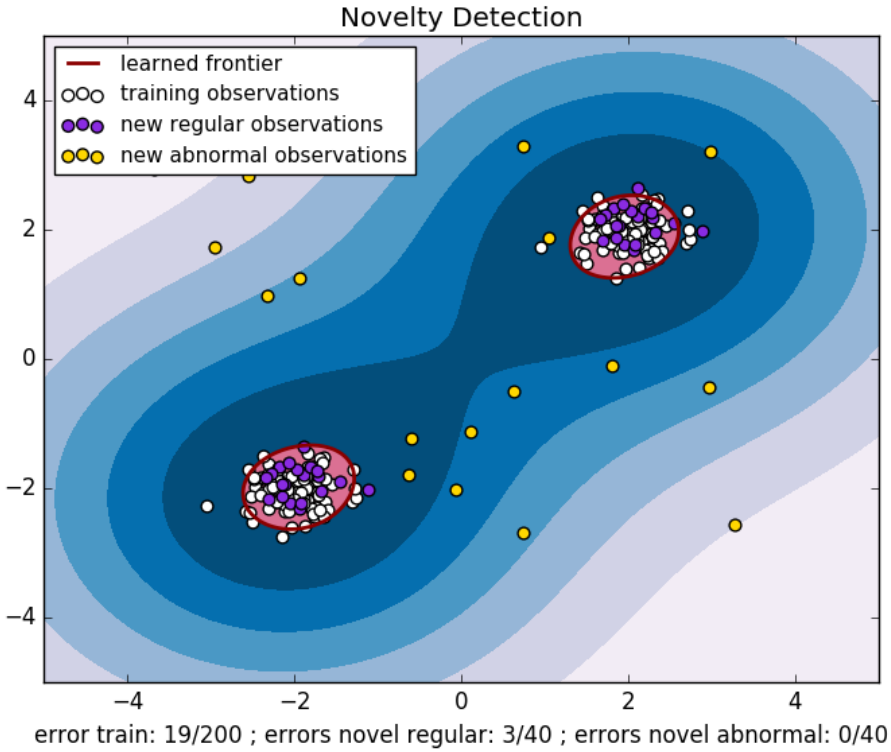
CVT

RSDP

NTSA

NTSA – System Description

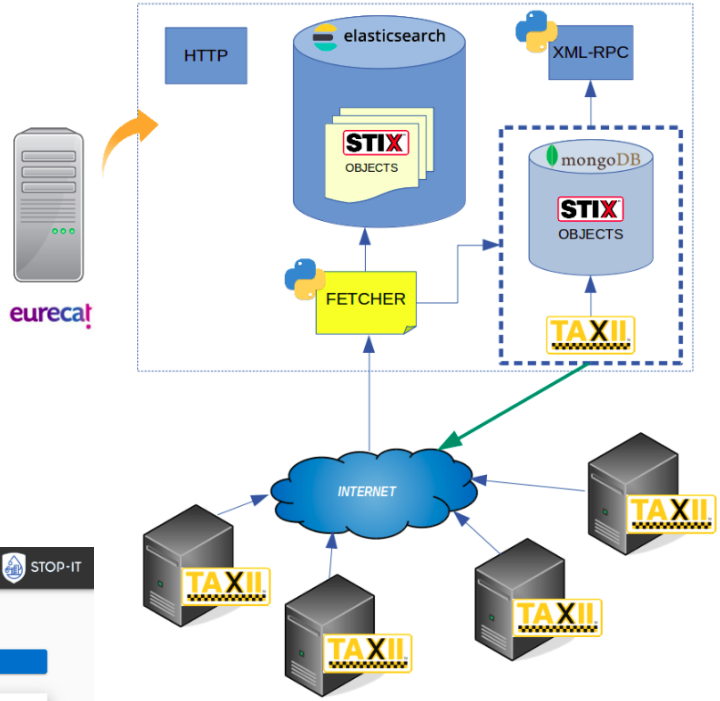
- **NetFlow-based (v5 & v9) approach**: widely used to collect aggregated data about traffic.
- Uses **unsupervised ML** (One-class SVM) to model patterns of normal traffic and identify abnormal network behaviour of devices based on the deviation from the normal operation model.
- Tested with real legitimate datasets.
- Results show a promising approach using multiple features, future work will include research to **reduce false positives by incorporating more complex features**.

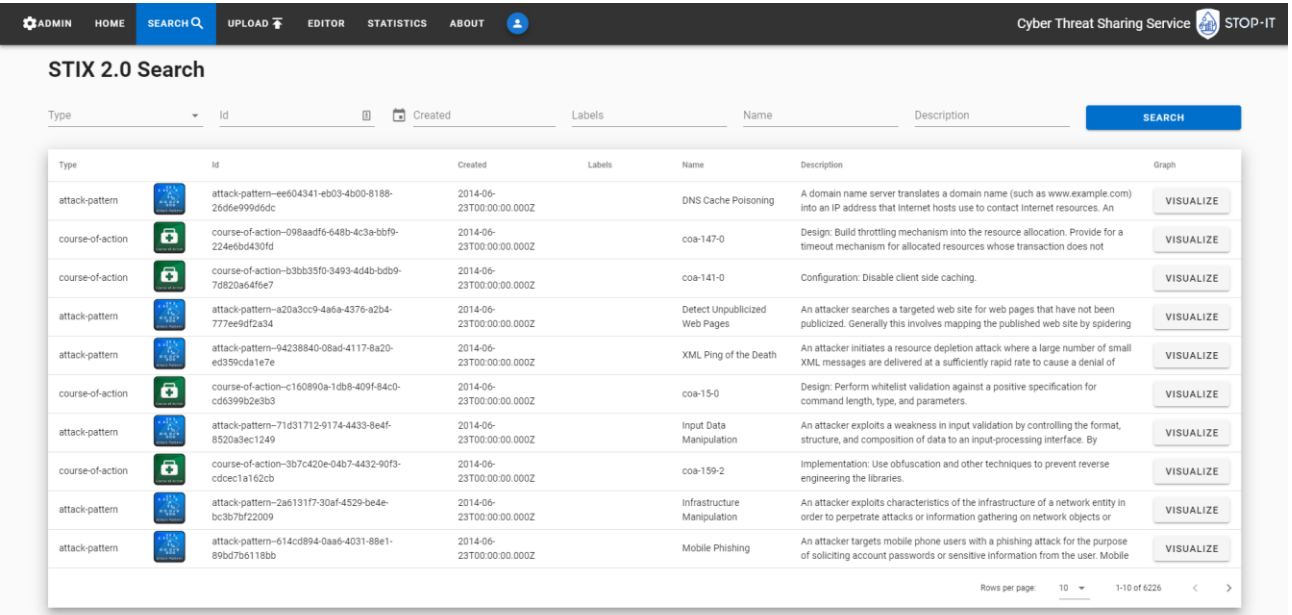


B. Schölkopf, J. C. Platt, J. Shawe-Taylor, A. J. Smola and R. C. Williamson, "Estimating the support of a high-dimensional distribution," *Journal of Neural computation,* vol. 13, pp. 1443-1471, 2001.

CTSS – System Description

- This services **collects existing threats** from relevant internal and external sources.
- It also **distribute threat information** to other feeds, systems or infrastructures.
- All information is **formatted using standards** (STIX-TAXII v2).



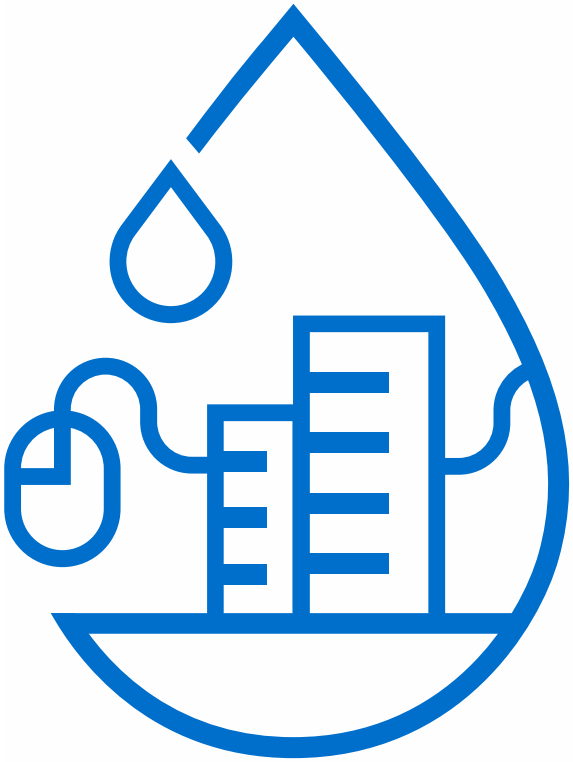


- The system provides both a **visualization environment** and a **RESTful API** to consult threats.

RTAD – Mapping Attacks to MITRE ATT&CK for ICS matrix

Initial Access	Execution	Persistence	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Data Historian Compromise	Change Program State	Hooking	Exploitation for Evasion	Control Device Identification	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Drive-by Compromise	Command-Line Interface	Module Firmware	Indicator Removal on Host	I/O Module Discovery	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Change Program State	Denial of Control
Engineering Workstation Compromise	Execution through API	Program Download	Masquerading	Network Connection Enumeration	External Remote Services	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Masquerading	Denial of View
Exploit Public-Facing Application	Graphical User Interface	Project File Infection	Rogue Master Device	Network Service Scanning	Program Organization Units	Detect Program State		Block Reporting Message	Modify Control Logic	Loss of Availability
External Remote Services	Man in the Middle	System Firmware	Rootkit	Network Sniffing	Remote File Copy	I/O Image		Block Serial COM	Modify Parameter	Loss of Control
Internet Accessible Device	Program Organization Units	Valid Accounts	Spoof Reporting Message	Remote System Discovery	Valid Accounts	Location Identification		Data Destruction	Module Firmware	Loss of Productivity and Revenue
Replication Through Removable Media	Project File Infection		Utilize/Change Operating Mode	Serial Connection Enumeration		Monitor Process State		Denial of Service	Program Download	Loss of Safety
Spearphishing Attachment	Scripting					Point & Tag Identification		Device Restart/Shutdown	Rogue Master Device	Loss of View
Supply Chain Compromise	User Execution					Program Upload		Manipulate I/O Image	Service Stop	Manipulation of Control
Wireless Compromise						Role Identification		Modify Alarm Settings	Spoof Reporting Message	Manipulation of View
						Screen Capture		Modify Control Logic	Unauthorized Command Message	Theft of Operational Information
								Program Download		
								Rootkit		
								System Firmware		
								Utilize/Change Operating Mode		

STUXNET Mapped to ATT&CK for ICS matrix



THANK YOU FOR YOUR ATTENTION

stop-it-project.eu

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No.740610.
The publication reflects only the authors' views and the European Union is not liable for any use that may be made of the information contained therein.