Intrusion Detection System based on physical data for Internet of Things devices

Rémi GASCOU, Jérôme MAMPIANINAZAKASON[1], Eric ALATA,
Romain CAYRE, Vincent MIGLIORE, Vincent NICOMETTE[1,2]

[1] : INSA Toulouse - [2] : LAAS - CNRS

Context

The massive and rapid development of Internet Of Things (IoT) devices raises numerous security issues as security is often ignored during their design. Therefore, there is a growing need for auditing devices able to detect modifications in the physical and network environment that might be caused by attacks on the analysed object. Currently, only systems using network data or systems using physical data but focusing on specific types of connected objects are implemented to identify attacks.

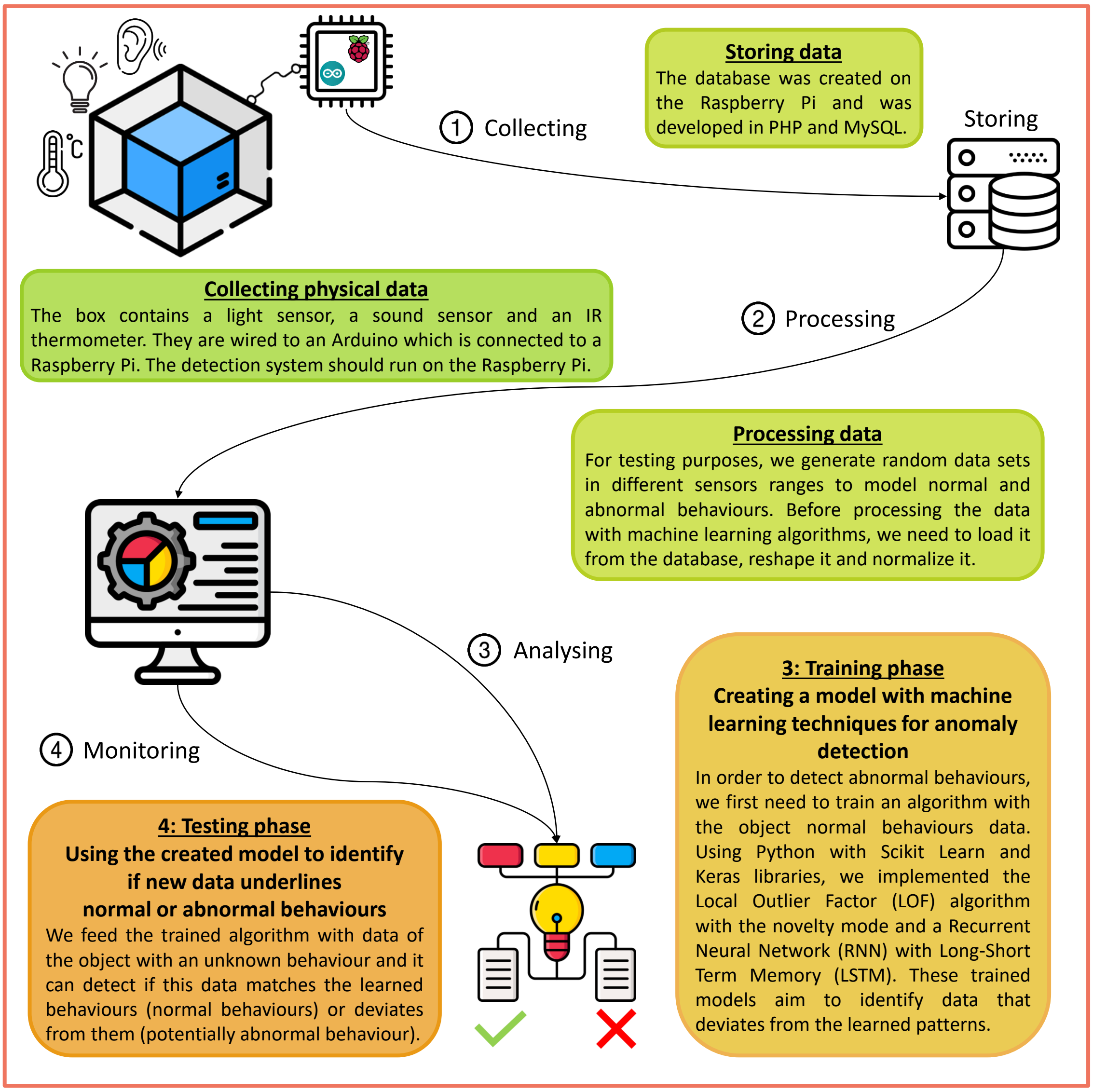
Objectives

The aim of this project was to develop a non-intrusive Intrusion Detection System (IDS) with a view to testing IoT devices reactions to known attacks. This device would be based on the collection of physical information using a variety of sensors and would use machine learning algorithms for anomaly detection.

Main IoT vulnerabilities

1. Default credentials or weak to dictionary attacks
2. Lack of encryption
3. Lack of update
4. Insecure conception
5. Insecure network service
6. Insecure management interface

Architecture of our Intrusion detection system



Storing data
The database was created on the Raspberry Pi and was developed in PHP and MySQL.

Collecting physical data
The box contains a light sensor, a sound sensor and an IR thermometer. They are wired to an Arduino which is connected to a Raspberry Pi. The detection system should run on the Raspberry Pi.

Processing data
For testing purposes, we generate random data sets in different sensors ranges to model normal and abnormal behaviours. Before processing the data with machine learning algorithms, we need to load it from the database, reshape it and normalize it.

3: Training phase
Creating a model with machine learning techniques for anomaly detection
In order to detect abnormal behaviours, we first need to train an algorithm with the object normal behaviours data. Using Python with Scikit Learn and Keras libraries, we implemented the Local Outlier Factor (LOF) algorithm with the novelty mode and a Recurrent Neural Network (RNN) with Long-Short Term Memory (LSTM). These trained models aim to identify data that deviates from the learned patterns.

4: Testing phase
Using the created model to identify if new data underlines normal or abnormal behaviours
We feed the trained algorithm with data of the object with an unknown behaviour and it can detect if this data matches the learned behaviours (normal behaviours) or deviates from them (potentially abnormal behaviour).

Implemented exploits

- WIFI de-authentication
- MiTM (ARP cache poisoning)
- Eavesdropping HTTP
- Default credentials
- Telnet dictionary attack

Conclusion

Goals achieved:
Collecting data, storing data in a database, detecting abnormal behaviours on randomly generated data with the LOF algorithm with the novelty mode.

Next step:
Integrating the different components of the system together to test it with vulnerable IoT devices.

Perspectives:
- Extending the system by adding network communication traces to the data used for anomaly detection.
- Developing a standalone system for real-time intrusion detection.