[Status Report] Privacy concerns in IoT systems with the use of AI techniques

Fabio Palomba
fpalomba@unisa.it
Universitá degli studi di Salerno
Salerno, Italy

Giammaria Giordano
ggiordano@unisa.it
Universitá degli studi di Salerno
Salerno, Italy

Biagio Boi
Gigi Jr Del Monaco
b.boi@studenti.unisa.it
g.delmonaco1@studenti.unisa.it
Universitá degli studi di Salerno
Salerno, Italy

1 INTRODUCTION

The evolution of smart devices over last years has increased exponentially and the introduction of these devices in the house is progressively growing. The major problem related to these devices is that usually the privacy is not considered, although there are a lot of regulations (just see the GDPR) that describe how the user data have to be stored and who can access to these data. Starting from these two points We've decided to understand what happens within the context of smart assistance. The final idea is to develop a tool able to preserve the privacy of the users.

2 OBJECTIVE

The goal of the project is to develop a tool based on a ML model able to preserve privacy during the information exchange in the IoT context, by analyzing the packets sent over the network.

3 METHODOLOGY

In order to implement the tool, we've decided to follow each of these steps:

(1) Consider the current state of art in order to retrieve useful informations. This step is important to produce knowledge to better perform the next steps;
(2) Analyze the existing datasets to achieve feature engineering;
(3) Apply normalization techniques (data cleaning, data balancing);
(4) Implementation and training of a ML model by considering different approaches to find the best fit model for our problem. Looking to the context related projects is most likely that we're going to focus on a Neural Network by using Keras;
(5) Analyze, monitor and compare the results of each model by using ML Flow tool;
(6) Develop a real time tool based on this model.

Clearly, all these steps will be conducted using a MLOps approach.

4 PERFORMED ACTIVITIES

We've started to consider all the related works for the domain of the problem; we're currently analyzing the existing dataset.

5 PLANNED ACTIVITIES - MILESTONES

- May 24 - Analyze the existing dataset;
- May 28 - Feature engineering process;
- May 31 - Data cleaning and balancing;
- June 5 - Implementation, training and analysis of each approach;
- June 9 - Develop a tool based on the best fit model.