Enhancing Security and Visibility Through IoT Vendor and Function Labeling

Bar Meyuhas[1], Anat Bremler-Barr[2], Tal Shapira[3]
[1]Reichman University, [2]Tel-Aviv University, [3]Hebrew University

Research Goal

Label vendor and function of IoT device that has never-seen before

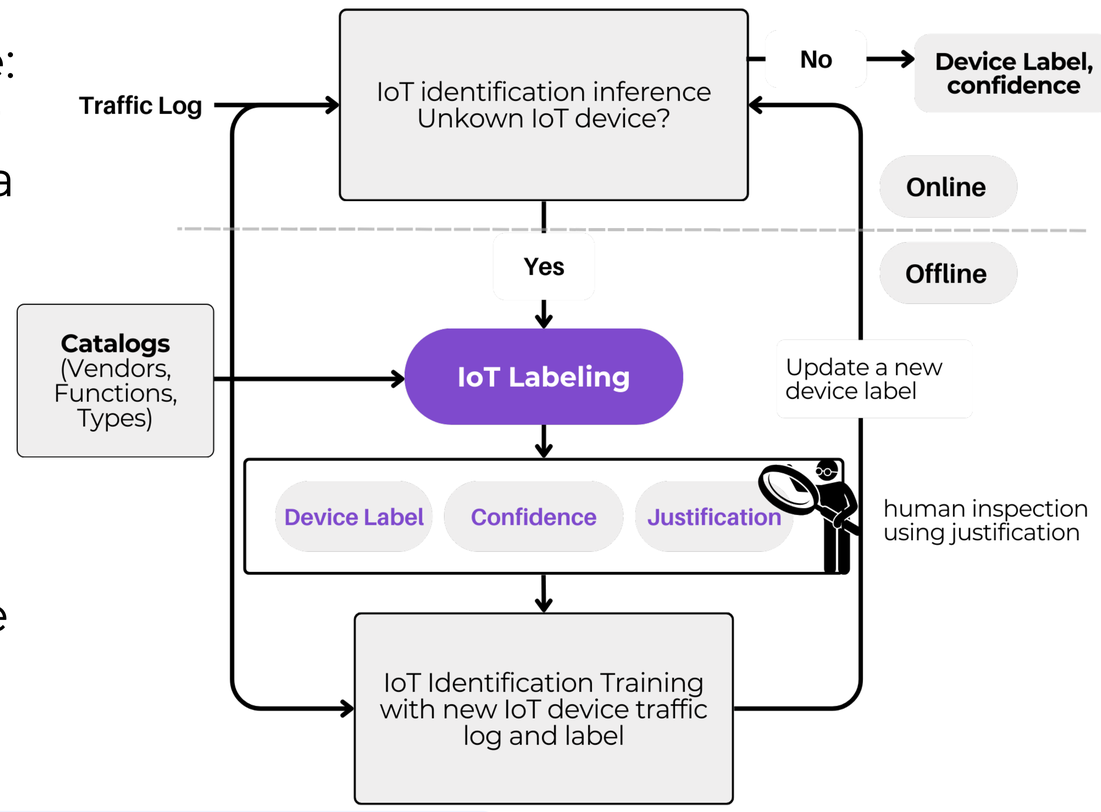
1 IoT identification systems identify the device type: type=<vendor, function>, i.e., < SmartThings,Hub>

- IoT Identification models require labeled data
- These models learn specific traffic characteristics per labeled device

2 Challenge: there are tens of thousands of different device types

3 **IoT Labeling Task:** label the type of unseen device

- Offline task, may receive long traffic log



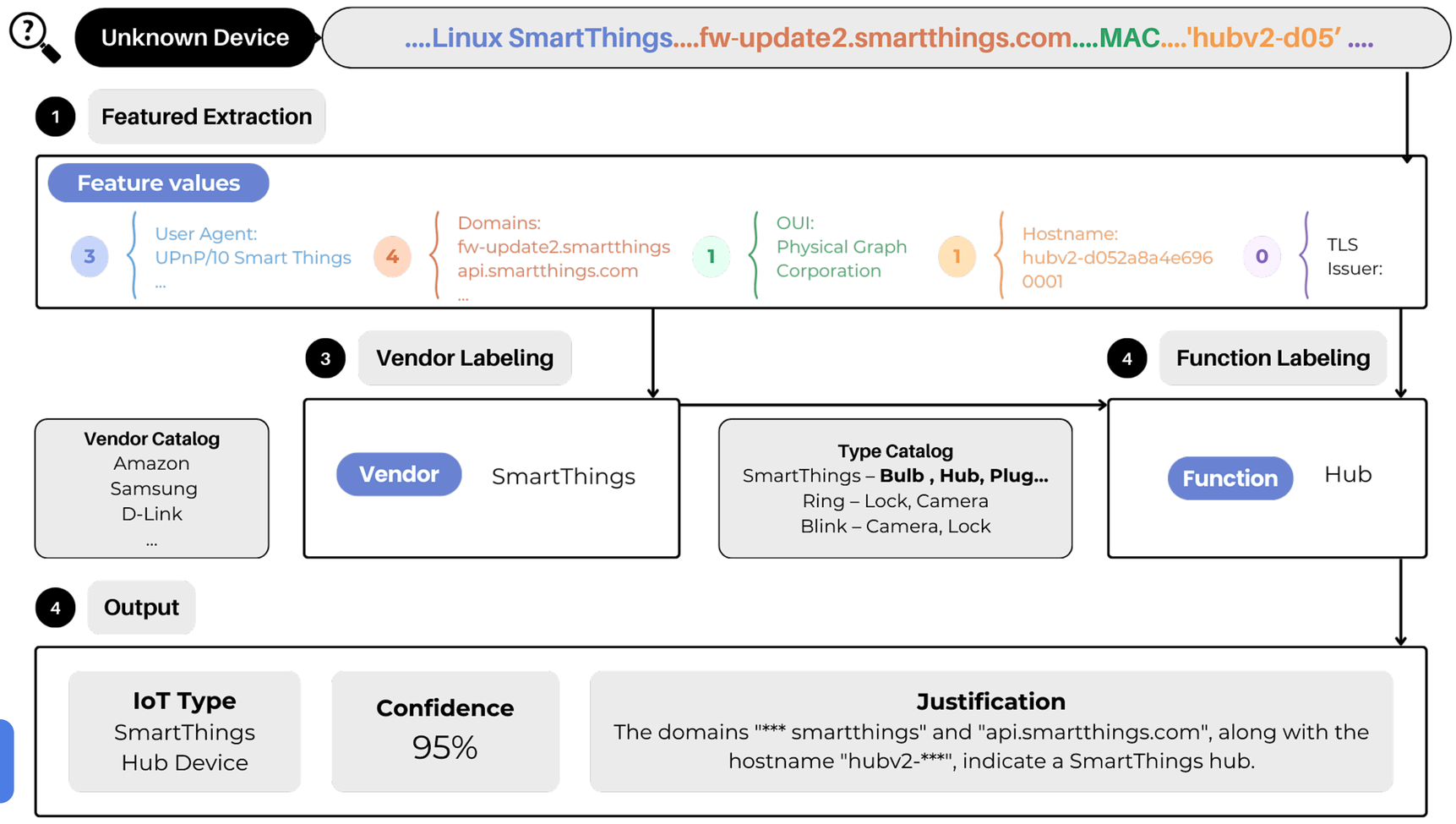
Labeling approach

never-seen device labeling using LLM

Features Extraction (1):
User-agent, Domain, OUI, hostname, TLS issuer.

LLM Utilization:
Specific prompts guide the LLM to analyze and label vendor **(2)** and then label function **(3)**

Output (4):
IoT type label, confidence, justification (for human verification)



Experimental results

Dataset details:
97 device:
55 vendors, 23 functions

Accuracy results:

- vendor labeling: **80%**
- function labeling: **69%**

Given the information provided by the user and extracted info from the internet, please classify the following IoT devices into {label}. Please provide a confidence score for every result. If there are several options provide only the first three with the highest confidence level. When classifying {labels} please use label from the list of {labels} provided by the user. A confidence score is a number between 0% - 100%.
Please add Explainability (max. 50 words) for your choice.

GPT - 4

Intuition

How LLM labeling work ?

- The features directly include vendor or function (i.e: Domains: api.xiaomi.com)
- The model knowledge, i.e., Hostname: HS100, the hostname corresponds to a model of smart plugs by TP-Link. There is an internet web page with information about HS100 TP-Link smart plug model.

Part of this work has been supported by Israel Innovation Authority within the ENTM consortium

For more INFO, DEEPNES Lab
bar.meyuhas@gmail.com