PRISM: Privacy Preserving IoT Security Management

Yuting Zhan
Anna Maria Mandalari
Hamed Haddadi
Imperial College London

PROJECT TIMELINE

Start date: 1 April 2022
Finish date: 31 August 2022

INTRODUCTION

With an increasing number of IoT devices being presented in our homes, information leakage channels rise, resulting in a growing range of security threats and privacy risks. PRISM aims to translate the lab-based platform into a home gateway setting, ready for real-world trials. We propose to adopt lightweight ML models from our advanced IoT labs, and enable privacy-preserving crowdsourcing IoT behavioural insights.

AIM

1. Port and evaluate the latest security threat analysis, and privacy features, on a real industrial gateway.
2. Implementation and evaluation of the feasibility of crowdsourcing IoT behavioural insights.
3. Conduct a demonstrator use case with UK Dementia Research Institute (DRI) volunteers.

WHY

The security threats and privacy risks are growing with emerging IoT devices. Current large-scale experiments and emulated scenarios are limited to specific testbeds and do not represent the average daily usage patterns.

METHODOLOGY

1. Evaluating activity inference on DRI data individually
2. Implement API for features extraction
3. Introducing local Differential Privacy (DP)

EXPECTED IMPACT

1. Translate lab-based platform into a real-world home gateway setting
2. Implement the edge inference network on a real industrial gateway
3. Enable multiple edge devices collaboratively to train personal models

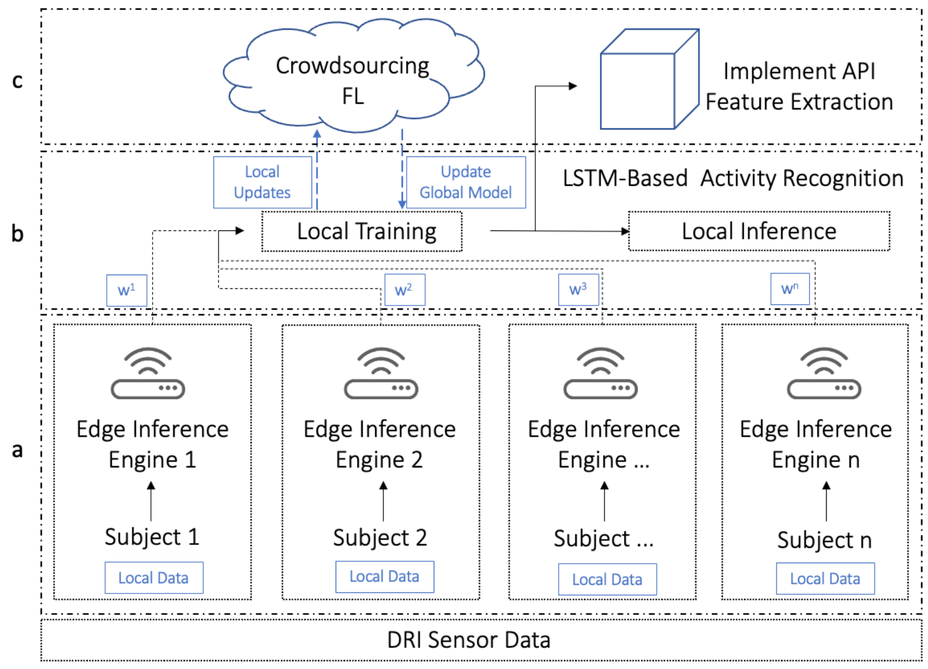

Figure 1

Figure 2

KEY OUTCOMES

We infer the activities of some patients at the edge, in real-time and demonstrate the advantage/disadvantage of our methodology in this context.

We then find the trade-off between DP level and local inference performance.

MAJOR FINDINGS

1. The individual-level performance of inferring activity at the edge
2. The trade-off between inference time and accuracy of local inference
3. Cost of privacy-preserving at the edge

USER PARTNERS

NHS
UK DRI

ACKNOWLEDGEMENTS

This work has been supported by the PETRAS National Centre of Excellence for IoT Systems Cybersecurity.