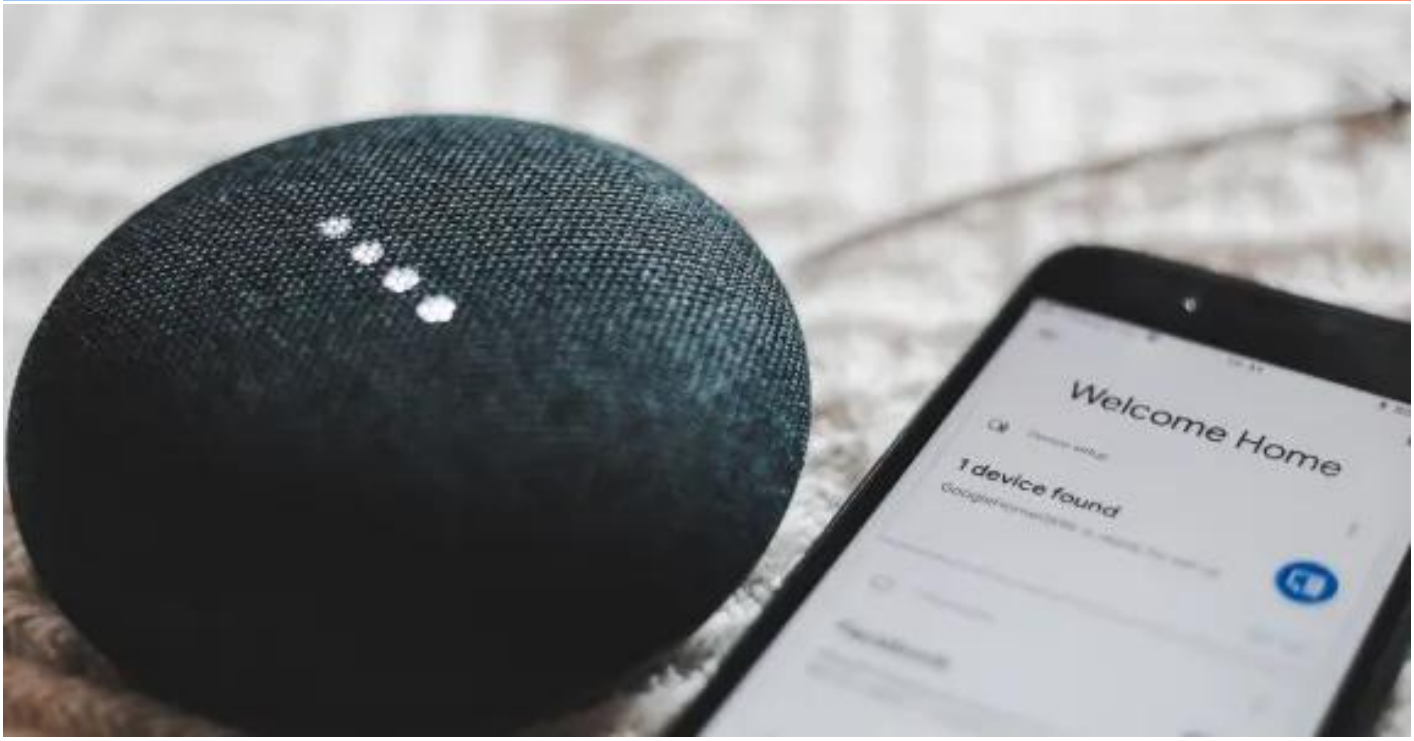

SunRISE project on shared IoT security wins Penta Innovation Award 2022

06 December 2022, 10:00

Penta, a Eureka cluster on electronic components and systems, has awarded the R&D project SunRISE (Shared IoT Security) with this year's Innovation Award and by that highlighted the importance of security and privacy ensuring machine learning technologies. The Belgian consortium consisting of Engie Laborelec, NXP and Sirris focused on a privacy-preserving federated solution for detecting malfunctioning home appliances from smart meter data.

In a wide range of domains systems can benefit from the use of machine learning (ML) approaches. However, ML performs well only if meaningful and qualitative data is used. Unfortunately, in many scenarios the data of interest is privacy-sensitive, as it refers to the users' situations, habits, preferences, etc. The R&D project SunRISE aimed to enable ML solutions under privacy-preserving circumstances and make cyber-physical systems resilient against cyberattacks.

Use case on energy consumption and production

In the context of the energy communities use case that the Belgian consortium focused on, smart meters can provide near real-time information about energy consumption and production in private households, as well as in industrial or public environments. This information can lead to a reduction in electricity demand, as energy wastage can be identified and prevented. In addition, it can enable smarter orchestration of renewable energy sources.

At the same time, the processing of highly granular consumption data can lead to critical privacy risks, as the socio-economic situation of the households can be inferred with high accuracy. In order to prevent or lower this risk, it is desirable that the processing of the data is performed direct g transferred. Furth tanding global energ

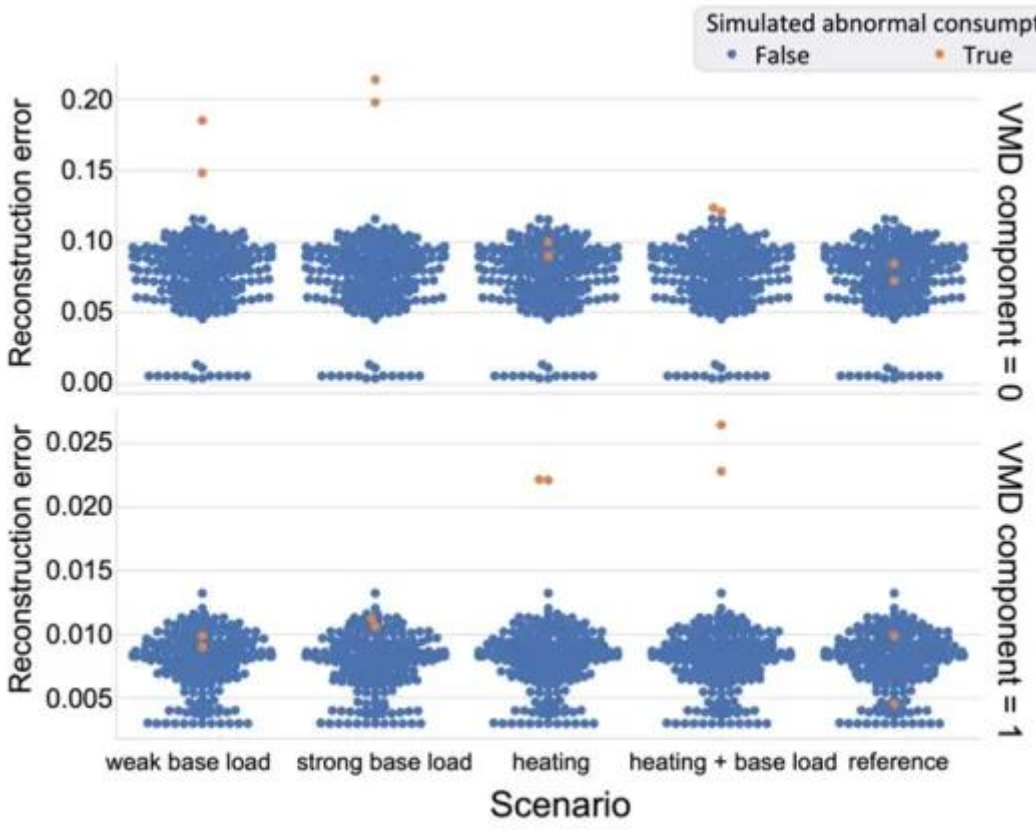

Figure 1: Reconstruction error obtained by the federated approach for identifying malfunctioning home appliances. By decomposing the signal (top and bottom), it is possible to identify different scenarios of malfunctioning devices.

Federated Learning approach

In order to address this challenge, Sirris researched a federated learning approach that can identify malfunctioning home appliances in a privacy-preserving fashion. For this, Engie Laborelec provided real-world data from their Home Lab. In our approach, instead of sharing consumption data with a central device such as a cloud service, a lean deep-learning model is trained at the edge, the smart meter. A centralized model is then trained in a federated fashion across different households by only sharing the model weights. Additionally, using a signal decomposition technique, it is possible to identify different types of malfunctioning home appliances, e.g. from a malfunctioning heating or from a constant loss. The results in figure 1 show how for the days with simulated malfunctioning of devices (orange dots) the reconstruction error significantly increases in the two decomposed components (top, bottom) for the different scenarios. Since the model weights can still leak private information, a privacy-friendly aggregation algorithm was developed by NXP such that the privacy-sensitive information remains private. These results are described in the article Unsupervised, Federated and Privacy-Preserving Detection of Anomalous Electricity Consumption in Real-World Scenarios, presented at IEEE Sustainable Power and Energy Conference (iSPEC) on 6 December 2022.

“Working together with Engie Laborelec and Sirris in the SunRISE project brought together all the right competences to create this impressive result ensuring that privacy-sensitive IoT data remains protected at all times” - Joppe Bos, Senior Principal Cryptographer at NXP

“I would like to thank Sirris and NXP for their work and efforts put in this collaborative project. This joint effort has led to the development of secure technologies for Engie and the energy world of tomorrow” - Charles Faes, Project Engineer Cybersecurity at ENGIE Laborelec

The SunRISE project on shared IoT security in the framework of Penta has been funded by VLAIO.

Authors