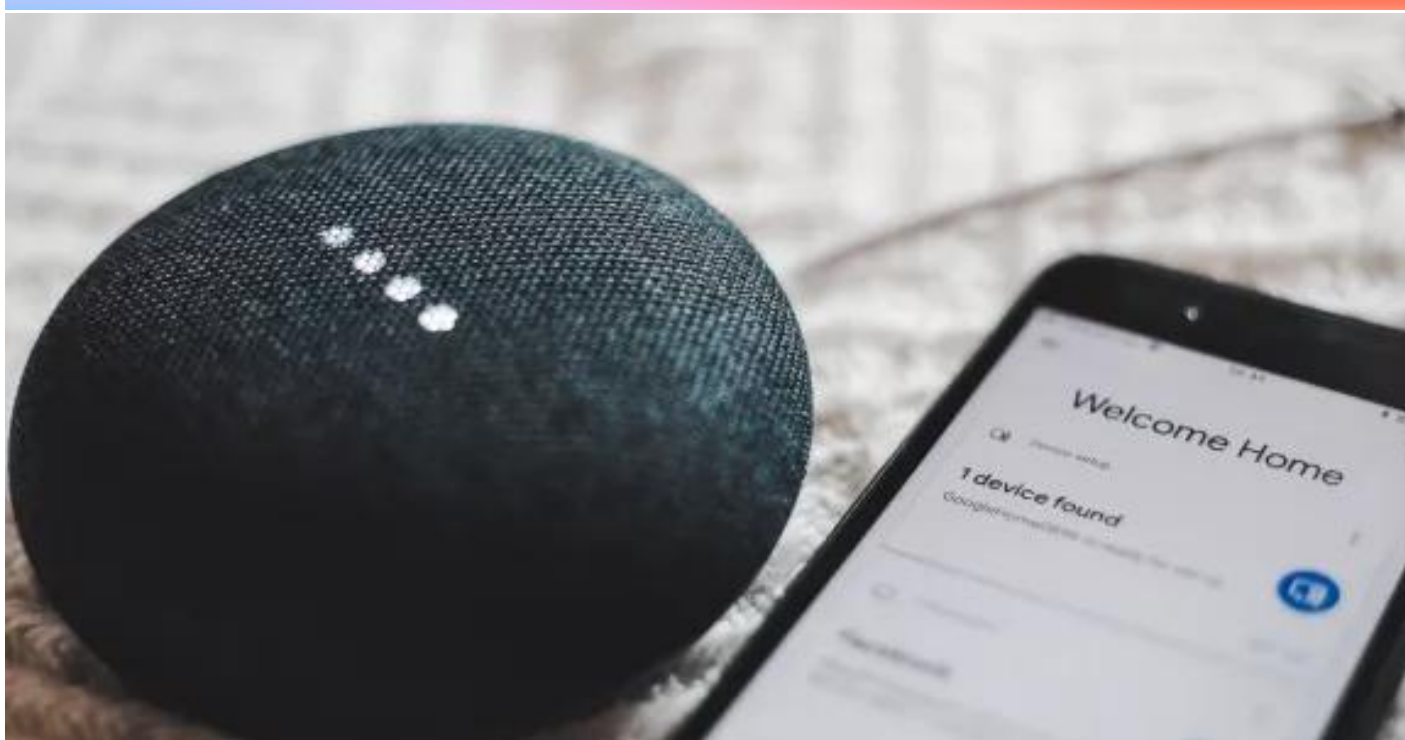




Le projet SunRISE sur la sécurité IoT partagée remporte le Penta Innovation Award 2022

08 décembre 2022, 16:20

[Penta](#), un cluster Eureka sur les composants et systèmes électroniques, a décerné l'Innovation Award de cette année au projet R&D [SunRISE](#) (sécurité IoT partagée), soulignant ainsi l'importance des technologies d'apprentissage automatique assurant la sécurité et la confidentialité. Le consortium belge composé d'Engie Laborelec, NXP et Sirris s'est penché sur une solution fédérée préservant la confidentialité pour la détection des appareils domestiques défectueux sur la base des données des compteurs intelligents.

Dans de nombreux domaines, les systèmes peuvent bénéficier d'approches reposant sur l'apprentissage automatique. Cependant, l'apprentissage automatique ne peut donner de bons résultats que si on utilise des données significatives et qualitatives. Malheureusement, dans de nombreux scénarios, les données utiles sont de nature confidentielle, car elles touchent à la situation, aux habitudes, aux préférences et autres des utilisateurs. Le projet R&D [SunRISE](#) entendait définir des solutions d'apprentissage automatique dans un cadre préservant la confidentialité et renforcer les systèmes cyberphysiques contre les cyberattaques.

Cas d'utilisation sur la consommation et la production d'énergie

Le consortium belge s'est penché sur le cas des communautés d'énergie. Dans ce contexte, les compteurs intelligents peuvent fournir des informations en temps quasi réel sur la consommation et la production d'énergie dans les ménages, ainsi que dans les environnements industriels ou

publics. Ces informations peuvent aboutir à une réduction de la demande d'électricité, car il est possible d'identifier et d'éviter le gaspillage d'énergie. En outre, elles permettent de mieux penser l'orchestration des sources d'énergie renouvelables.

En même temps, le traitement de données de consommation très granulaires peut entraîner des risques critiques pour la confidentialité, car on peut déduire avec une grande précision la situation socio-économique des ménages. Pour prévenir ou réduire ce risque, il est souhaitable que le traitement des données se fasse directement au niveau du compteur intelligent, ce qui limite la

quant
conn
énerg

les
la demande

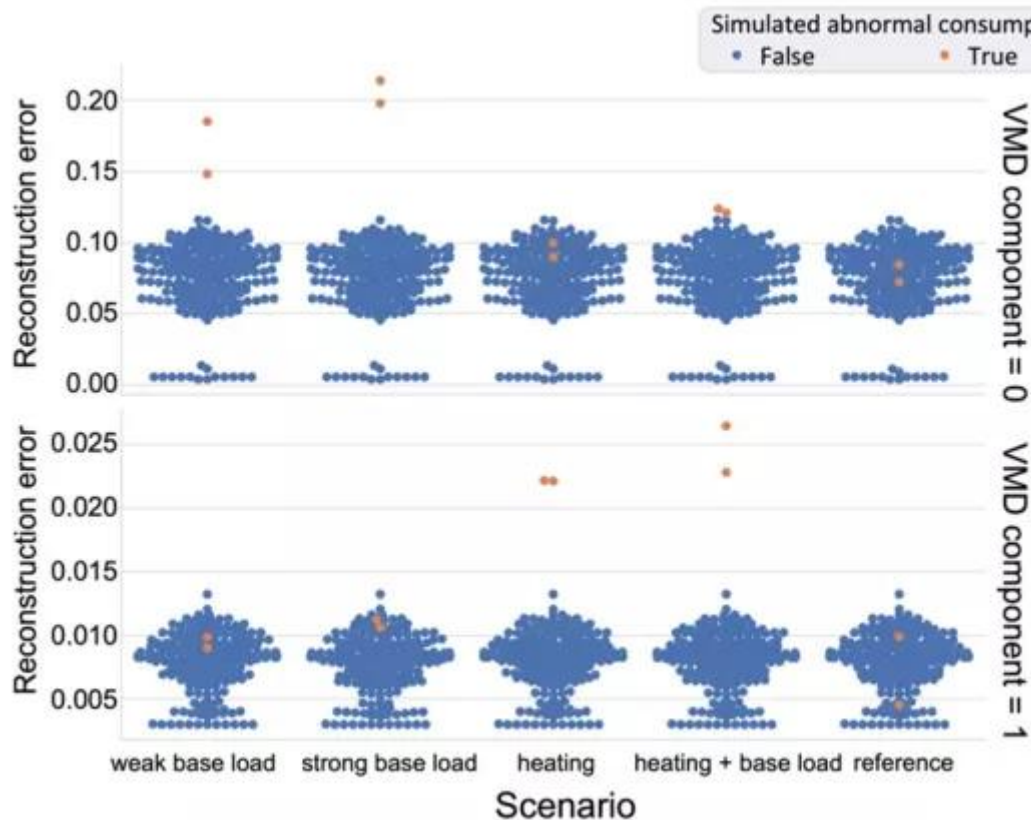


Figure 1 : Erreur de reconstruction obtenue par l'approche fédérée pour l'identification des appareils domestiques défectueux. En décomposant le signal (haut et bas), il est possible d'identifier différents scénarios de dysfonctionnement des appareils.

Approche d'apprentissage fédéré

Pour relever ce défi, Sirris a étudié une approche d'apprentissage fédéré qui permet d'identifier les appareils domestiques défectueux tout en préservant la confidentialité. À cette fin, Engie Laborelec a fourni des données réelles provenant de son Home Lab. Dans notre approche, au lieu de partager les données de consommation avec un système central tel qu'un service de cloud, un modèle d'apprentissage profond allégé est formé en périphérie, au niveau du compteur intelligent. Un modèle centralisé est ensuite entraîné de manière fédérée dans différents ménages en partageant uniquement les pondérations du modèle. En outre, en utilisant une technique de décomposition du signal, il est possible d'identifier différents types de dysfonctionnements des appareils domestiques, par exemple un mauvais fonctionnement du chauffage ou une perte constante. Les résultats de la figure 1 montrent comment, pour les jours avec dysfonctionnement

simulé des appareils (points orange), l'erreur de reconstruction augmente de manière significative dans les deux composantes décomposées (haut, bas) pour les différents scénarios. Étant donné que les pondérations du modèle peuvent encore laisser échapper des informations confidentielles, NXP a développé un algorithme d'agrégation qui protège la confidentialité, de sorte que les informations confidentielles le restent. Ces résultats sont décrits dans l'article *Unsupervised*,



ption in Real-World
(EC) le 6 décembre

« La collaboration d'Engie Laborelec et Sirris dans le cadre du projet SunRISE a permis de réunir toutes les compétences nécessaires pour obtenir ce résultat impressionnant. Les données IoT confidentielles restent ainsi toujours protégées. » – Joppe Bos, Senior Principal Cryptographer chez NXP

« Je tiens à remercier Sirris et NXP pour leur travail et leurs efforts dans ce projet collaboratif. Cet effort conjoint a mené au développement de technologies sécurisées pour Engie et le monde de l'énergie de demain. » – Charles Faes, Project Engineer Cybersecurity chez ENGIE Laborelec

Le projet [SunRISE](#) sur la sécurité IoT partagée dans le cadre de Penta a été financé par VLAIO.

Auteurs