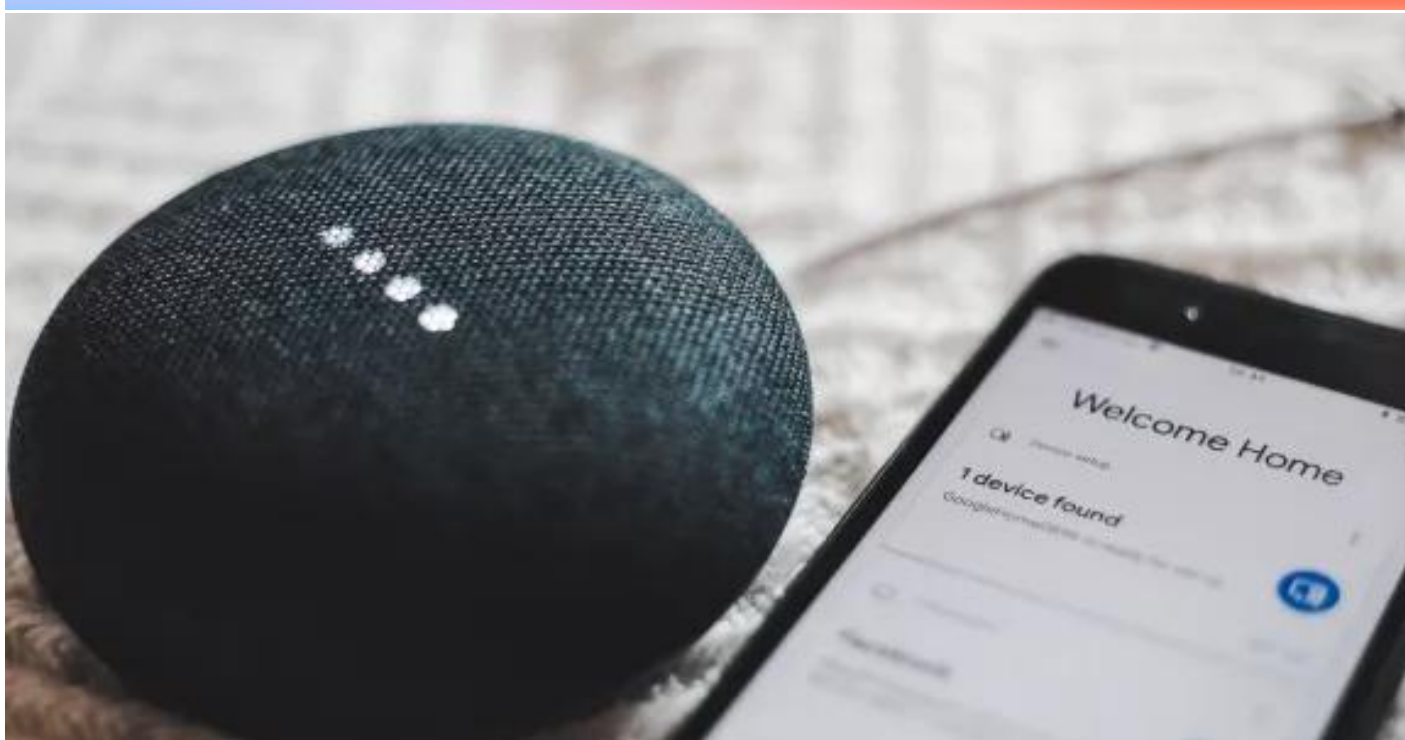




SunRISE-project rond gedeelde IoT-beveiliging wint Penta Innovation Award 2022

08 december 2022, 16:27

[Penta](#), een Eureka-cluster rond elektronische componenten en systemen, heeft dit jaar de Innovation Award toegekend aan het R&D-project [SunRISE](#) (Shared IoT Security) en benadrukt zo het belang van machinelearning-technologieën die de beveiliging en de privacy vrijwaren. Het Belgische consortium van projectpartners Engie Laborelec, NXP en Sirris spitsten zich toe op een gefedereerde oplossing mét behoud van privacy voor het detecteren van slecht werkende huishoudapparaten op basis van gegevens van slimme meters.

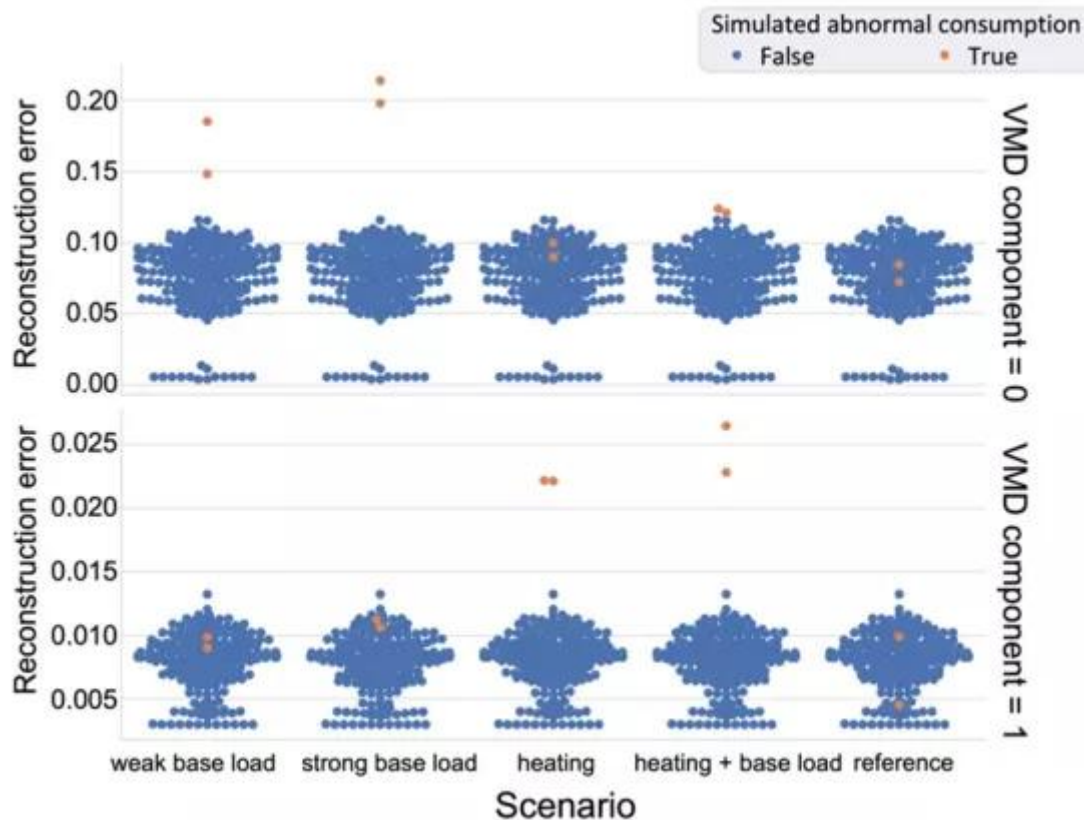
Systemen kunnen in tal van domeinen gebaat zijn bij machinelearning (ML). Echter, machinelere werkt alleen goed als zinvolle en kwalitatieve data worden gebruikt. Jammer genoeg zijn de data die van belang zijn in veel scenario's privacygevoelig, aangezien ze betrekking hebben op situaties, gewoonten of voorkeuren van de gebruikers. Doel van het R&D-project [SunRISE](#) was het ontwikkelen van ML-oplossingen onder omstandigheden die de privacy beschermen en het weerbaar maken van cyberfysische systemen tegen cyberaanvallen.

Use case rond energieverbruik en -productie

Het Belgische consortium spitste zich toe op de use case van de energiegemeenschappen. In deze context kunnen slimme meters bijna-realtime informatie verstrekken over energieverbruik en -productie bij particuliere huishoudens én in industriële of openbare omgevingen. Deze informatie

kan een vermindering van de vraag naar elektriciteit opleveren, aangezien men energieverpilling kan opsporen en voorkomen. Daarnaast maakt ze ook een betere afstemming van de hernieuwbare energiebronnen mogelijk.

Tegelijk kan de verwerking van zeer gedetailleerde verbruiksgegevens leiden tot kritieke privacyrisico's, omdat de socio-economische situatie van de particuliere huishoudens met grote nauwkeurigheid kan worden afgeleid. Om dit risico te voorkomen of te beperken is het wenselijk dat de gegevensverwerking rechtstreeks bij de slimme meter plaatsvindt, met de hoeveelheid privacyrisico's die voortvloeit uit het gebruik van meerdere slimme meters in een huishouden.



Figuur 1: Reconstructiefout verkregen door de gefedereerde aanpak voor de identificatie van slecht werkende huishoudapparaten. Door het signaal te ontleden (hoog en laag) kan men verschillende scenario's van slecht werkende apparaten identificeren.

Federated learning-aanpak

Om deze uitdaging aan te gaan, onderzocht Sirris een federated learning-aanpak die slecht werkende huishoudapparaten kan identificeren mét bescherming van de privacy. Hiertoe verstrekte Engie Laborelec concrete praktijkgegevens afkomstig van zijn Home Lab. In onze aanpak worden verbruiksgegevens niet gedeeld met een centraal apparaat, zoals een clouddienst, maar wordt een lichter deep learning-model getraind aan de rand, bij de slimme meter. Vervolgens wordt een gecentraliseerd model op een gefedereerde manier over verschillende huishoudens getraind door alleen de wegingen van het model te delen. Bovendien laat een signaalontledingstechniek het toe verschillende soorten storingen in huishoudapparaten te identificeren, bijvoorbeeld een slecht werkende verwarming of een constant verlies. De resultaten in figuur 1 geven aan hoe voor de

dagen met gesimuleerde storingen van apparaten (oranje stippen) de reconstructiefout in de twee ontlede componenten (hoog, laag) voor de verschillende scenario's aanzienlijk toeneemt. Aangezien de wegingen van het model nog steeds privé-informatie kunnen lekken, ontwikkelde NXP een privacyvriendelijk aggregatiealgoritme om de privacygevoelige informatie privé te houden.



and Privacy-Preserving
op de IEEE
d voorgesteld.

"De samenwerking met Engie Laborelec en Sirris in het SunRISE-project bracht alle nodige competenties samen om tot dit indrukwekkende resultaat te komen en ervoor te zorgen dat privacygevoelige IoT-gegevens te allen tijde beschermd blijven", aldus Joppe Bos, Senior Principal Cryptographer bij NXP.

"Ik wil Sirris en NXP bedanken voor hun werk en inzet in dit samenwerkingsproject. Deze gezamenlijke inspanning heeft het mogelijk gemaakt veilige technologieën voor Engie en de energiewereld van morgen te ontwikkelen", aldus Charles Faes, Project Engineer Cybersecurity bij ENGIE Laborelec.

Het [SunRISE](#) project rond gedeelde IoT-beveiliging in het kader van Penta wordt gefinancierd door VLAIO.

Auteurs