FedXI-IDS: AN EXPLAINABLE FEDERATED INCREMENTAL LEARNING APPROACH FOR INTRUSION DETECTION SYSTEM

Nguyen Huu Quyen[1,2]

[1] Information Security Laboratory, University of Information Technology, Ho Chi Minh city, Vietnam

[2] Vietnam National University, Ho Chi Minh city, Vietnam

What ?

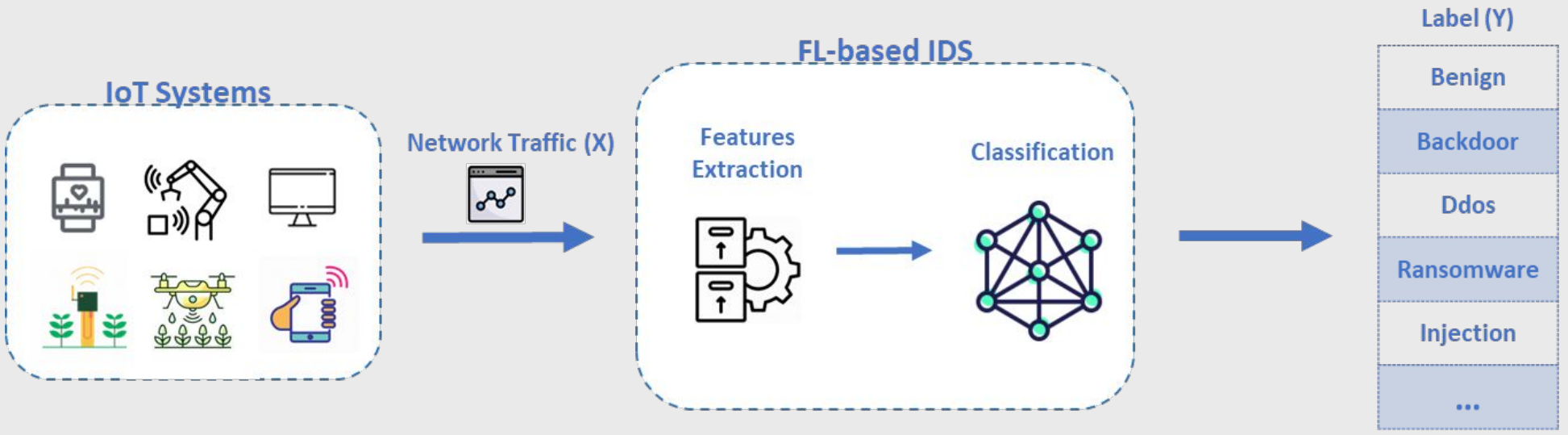
We introduce an explainable federated incremental learning approach for intrusion detection system FedXI-IDS, in which we have:

- Proposed a robust federated incremental training method to detect zero-day attacks in the context of cybersecurity.
- Compared with several incremental training methods and also several ML-based IDSes.

Why ?

- ***Non-id data*** and ***new classes*** are always the biggest problem in building and applying ML model in real world application. Especially, with recent federated IDS, zero-day attacks and label-skew in client have a high effect to the performance of global model.
- Machines participates in federated training often have ***limited*** storage ***resources***.
- Most ML model unable to ***explain*** their ***decisions*** to humans users.

Overview



Description

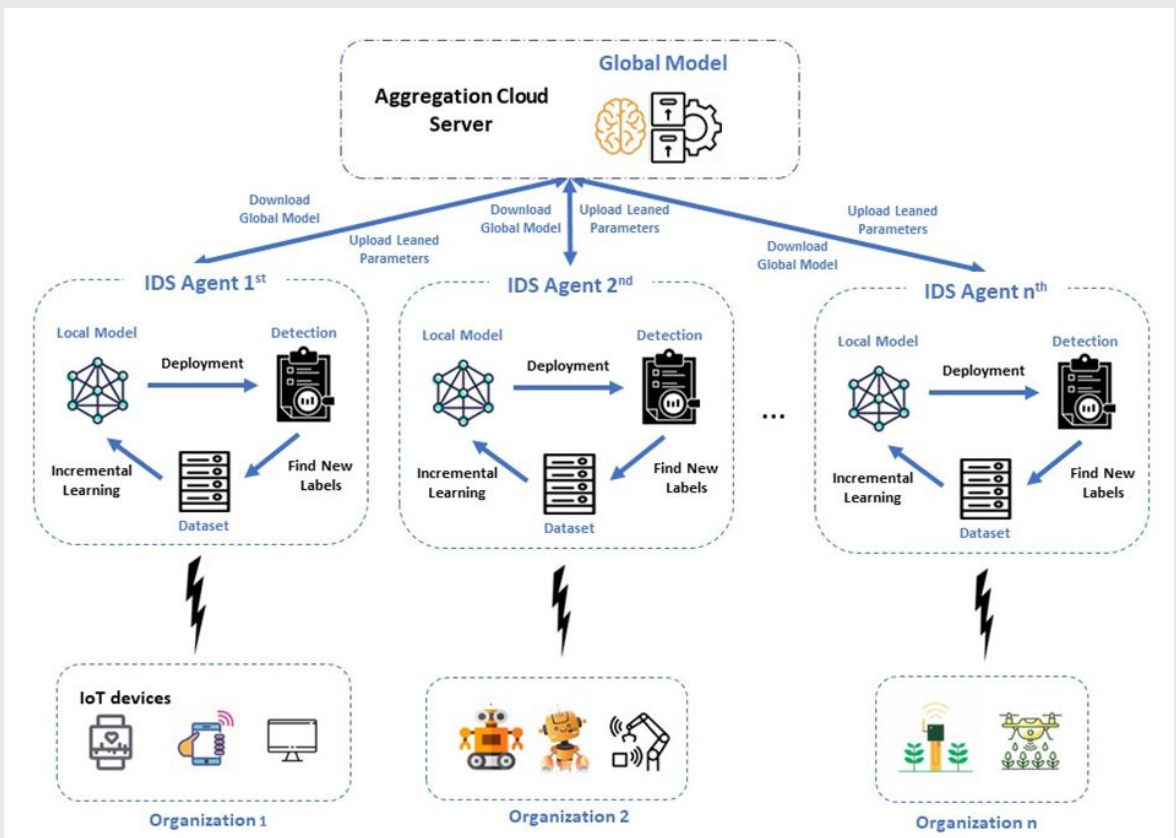


Figure 1. FedXI-IDS architecture.

1. XAI-based IDS

- XAI-based IDS helps to interpret the influence of data features on the model's predictions.

2. XAI-based FedIDS

- The weights of the global model are aggregated from the weights of the all IDS agents based on the FedAVG formula.
- XAI-based FedIDS model is trained with decentralized dataset to reduce training costs and protect data privacy of participants.

3. FedXI-IDS

- We propose an explainable federated incremental learning approach for intrusion detection system (FedXI-IDS) based on deep learning methods.
- FedXI-IDS helps to improve the performance of the model in detecting "new attack classes".
- Moreover, this proposed will deal with the effect of NonIID data and large amounts of data when constantly updating new data, without increasing storage and computational costs during retraining.

NII

Nguyễn Hữu Quyền – Trường Đại học Công nghệ Thông tin

TEL : 0336310354 Email : Huuquyen2606@gmail.com