NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

School of Computer Science and Engineering
College of Engineering

Privacy-Preserving Federated Learning(I)

For Botnet Detection on Home Network IoT Devices

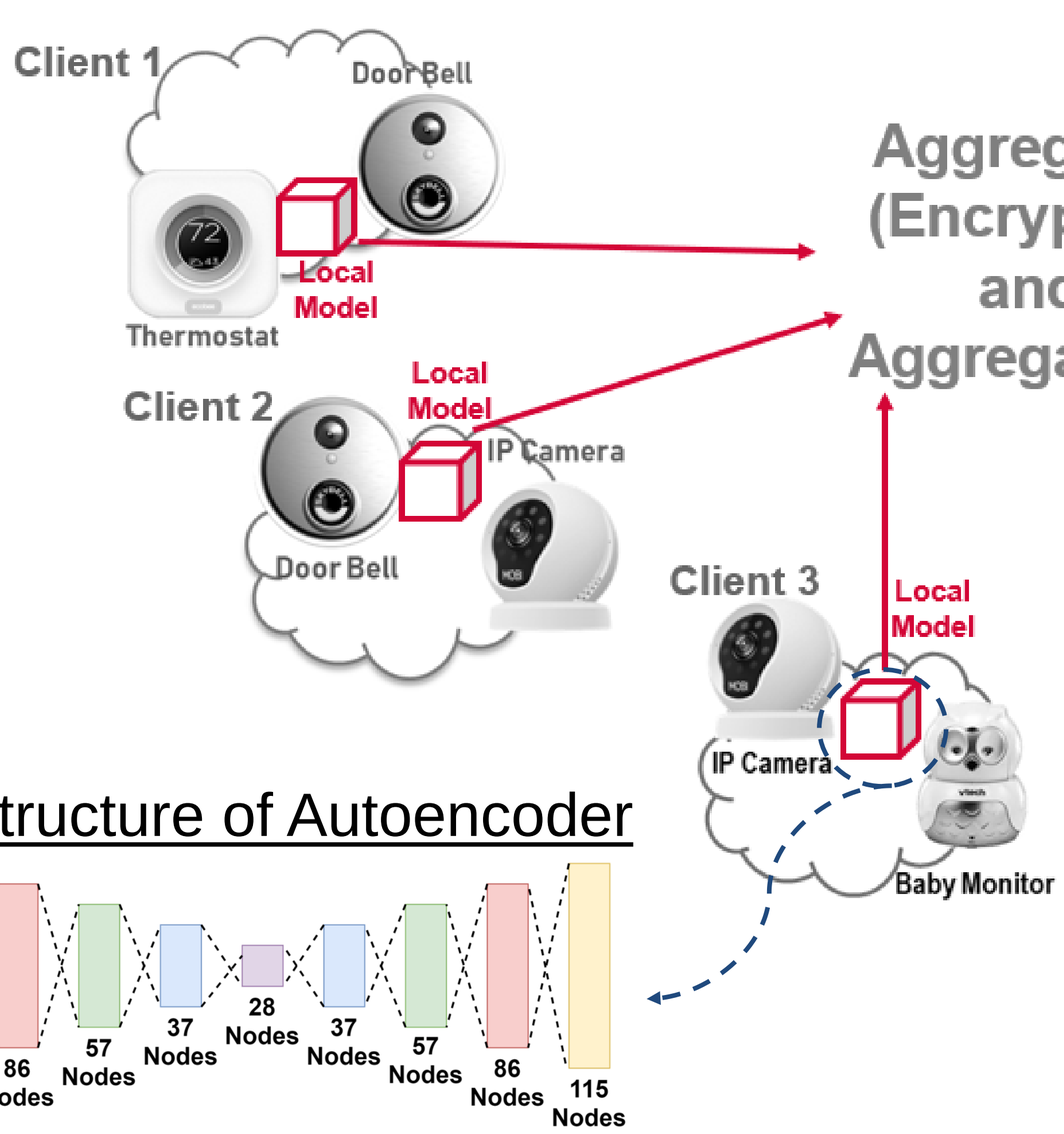
Student: Wang Ying Supervisor: Dr Sourav Sen Gupta

Objectives:

- Developing a Federated Learning model with Autoencoder for Anomaly Detection to solve botnet detection problem in home network IoT devices without exchanging sensitive data.
- Integrating the Federated Learning model with a Secure Aggregation platform for further privacy protection of local data at the IoT endpoints.

Implementation:

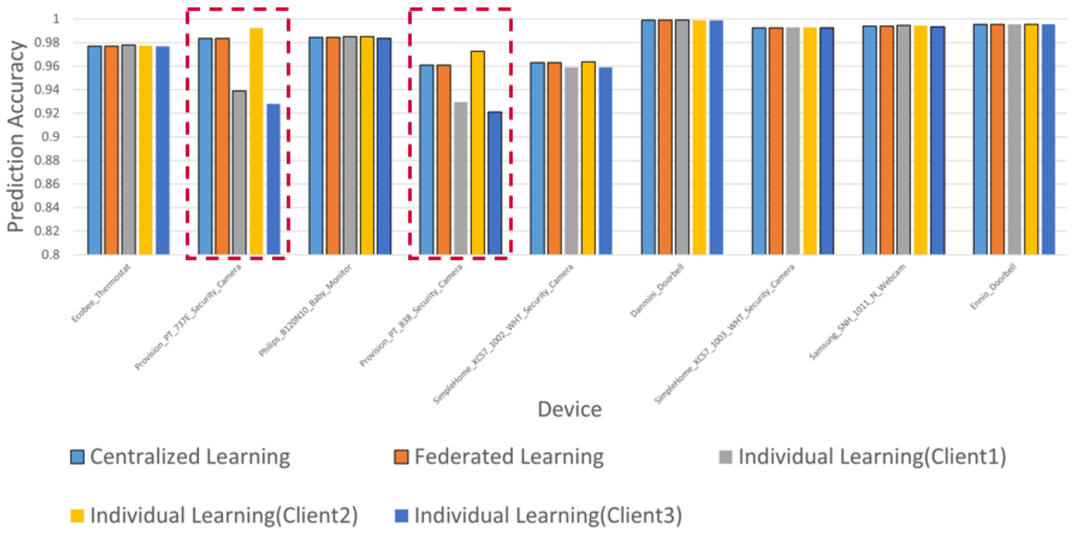
Structure of Federated Learning on Secure Aggregation Platform



Structure of Autoencoder

- Allocate IoT devices to 3 clients to simulate 3 different home networks.
- Each client trains and sends local Autoencoder model to Aggregator to generate encrypted model.
- Server performs decryption to get the global model.

Experiment Result:



Federated Learning shows a significant improvement on botnet detection ability.