Coastal Virginia

Securing IoT Devices through Power Side Channel Auditing and Privacy Preserved Convolutional Neural Networks

Gang Zhou: CS, William & Mary

Chunsheng Xin: ECE, Old Dominion University

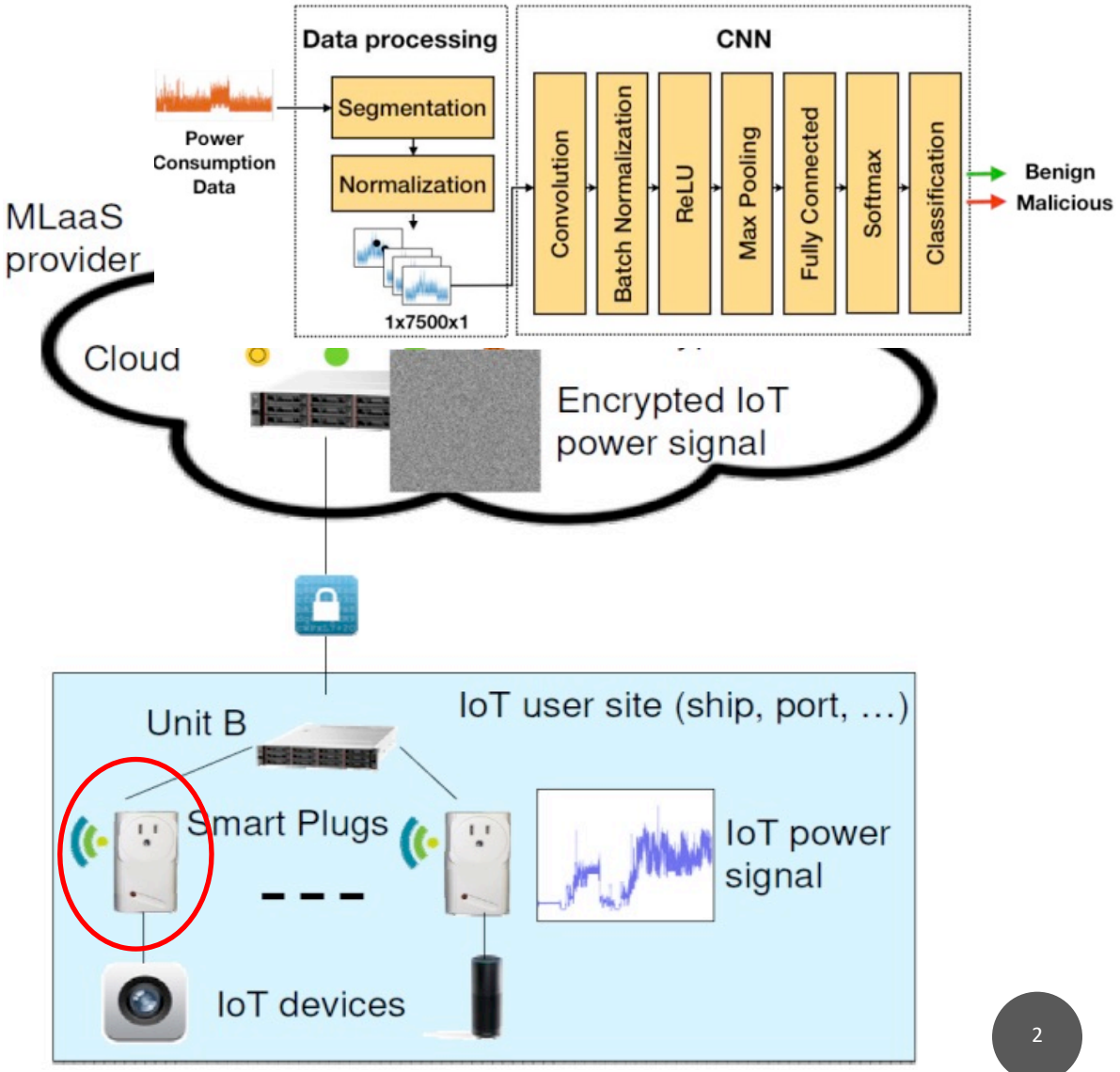
Danella Zhao: CS, Old Dominion University

Coastal Virginia

Research Problem & Approach

- The objective of this project is to secure IoT devices through power side channel auditing and privacy preserved Convolutional Neural Networks.

- Task 1: IoT Bot Detection via Power Consumption Modeling
  - Data Processing and Modeling
  - Smart Plug Design
- Task 2: Privacy Preserved Cloud based IoT Bot Detection
  - NN Computation Optimization
  - Communication-Computation Co-design



Coastal Virginia

Achievements so far

- Task 1: IoT Bot Detection via Power Consumption Modeling
  - Data Processing and Modeling
    - Achievement 1: Data processing and CNN models were developed and evaluated with existing and newly collected data, showing high accuracy and low delay.
  - Smart Plug Design
    - Achievement 2: A prototype Smart Plug platform was designed, which can power an external IoT device and also measure the IoT device's real-time power consumption for processing by the aforementioned data processing and CNN models.
- Task 2: Privacy Preserved Cloud based IoT Botnet Detection
  - NN Computation Optimization
    - Achievement 3: A scheme based on the Homomorphic Encryption has been implemented for privacy preserved IoT botnet detection using CNN models. Running time has been optimized to be sub-second.
    - Achievement 4: A highly efficient scheme using secret sharing has been designed and implemented for privacy preserved IoT botnet detection. The running time is in the order of millisecond.
- Related Publication
  - "IoT Botnet Detection via Power Consumption Modeling," Woosub Jung, Hongyang Zhao, Minglong Sun, Gang Zhou, in Elsevier Smart Health, 2019. Also presented at ACM/IEEE Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE), Washington, D.C., 2019