(Thesis: Improving Electricity Theft Detection for Smart Homes: Insights from Real and Synthetic Attack Scenarios)

Name: Abraham Olufemi Abiodun

Laboratory' s　Laboratory for Cyber Resilience

Supervisor' s　Professor Youki Kadobayashi

Abstract:
Electricity theft detection (ETD) in smart homes is challenging because smart meter data aggregates legitimate and malicious usage patterns. Traditionally, theft detection has depended on manual inspections and meter failures. However, with the advancement of machine learning (ML), it is now possible to automatically detect theft based on meter reading patterns. The proposed framework utilizes ML knowledge-based synthetic attack data (KBSAD) to train an attack classifier. These data consist of benign and attack patterns, that serve as the foundation for generating synthetic and simulated attacks that closely mirror real-world scenarios. The framework was validated using the Almanac of Minutely Power dataset version 2 (AMPds2), which contains fine-grained time-series data from a smart home. We preprocessed the data for binary classification to evaluate our synthetic attack model using real attack data. The Extreme Gradient Boosting algorithm performed best with an average area under curve (AUC) score of 98.74% and 98.69% for detecting and classifying anomalies in real and simulated attacks, respectively. These methods outperformed legacy unsupervised methods (LUM). By integrating the KBSAD, our approach eliminates the need for extensive data collection for real attacks and seamlessly combines synthetic attacks with genuine consumption readings, representing a significant advancement in the field of smart-home electricity theft detection.