MANIPAL
ACADEMY of HIGHER EDUCATION
(Institution of Eminence Deemed to be University)

kaspersky x acm mit bengaluru

HackSky 2025

Round 1

Team Name: 0verr1de

MANIPAL ACADEMY of HIGHER EDUCATION
(Institution of Eminence Deemed to be University)

Team Members

kaspersky x acm mit bengaluru

Paranjay Chaudhary

9686358882

paranjay.mitblr2023@learner.manipal.edu

Harthik MV

7676452975

harthik.mitblr2023@learner.manipal.edu

MANIPAL ACADEMY of HIGHER EDUCATION
(Institution of Eminence Deemed to be University)

Previous Experience of Hackathon

kaspersky x acm mit bengaluru

This team has participated in the online evaluation round of the Manipal Hackathon (Tech Tatva 2024)

MANIPAL ACADEMY of HIGHER EDUCATION
(Institution of Eminence Deemed to be University)

Track

kaspersky x acm mit bengaluru

The Transformation of ICS and Cyber Threats

Introduction

Motivation

- Industrial Control Systems (ICS) are the backbone of critical infrastructure—power grids, water treatment plants, and manufacturing lines.
- These systems face growing threats, such as sophisticated cyber-physical attacks and Limited visibility due to air-gapping, legacy devices, and lack of modern monitoring.

Challenge

How do we detect attacks without disrupting operations or installing intrusive sensors?

Introduction

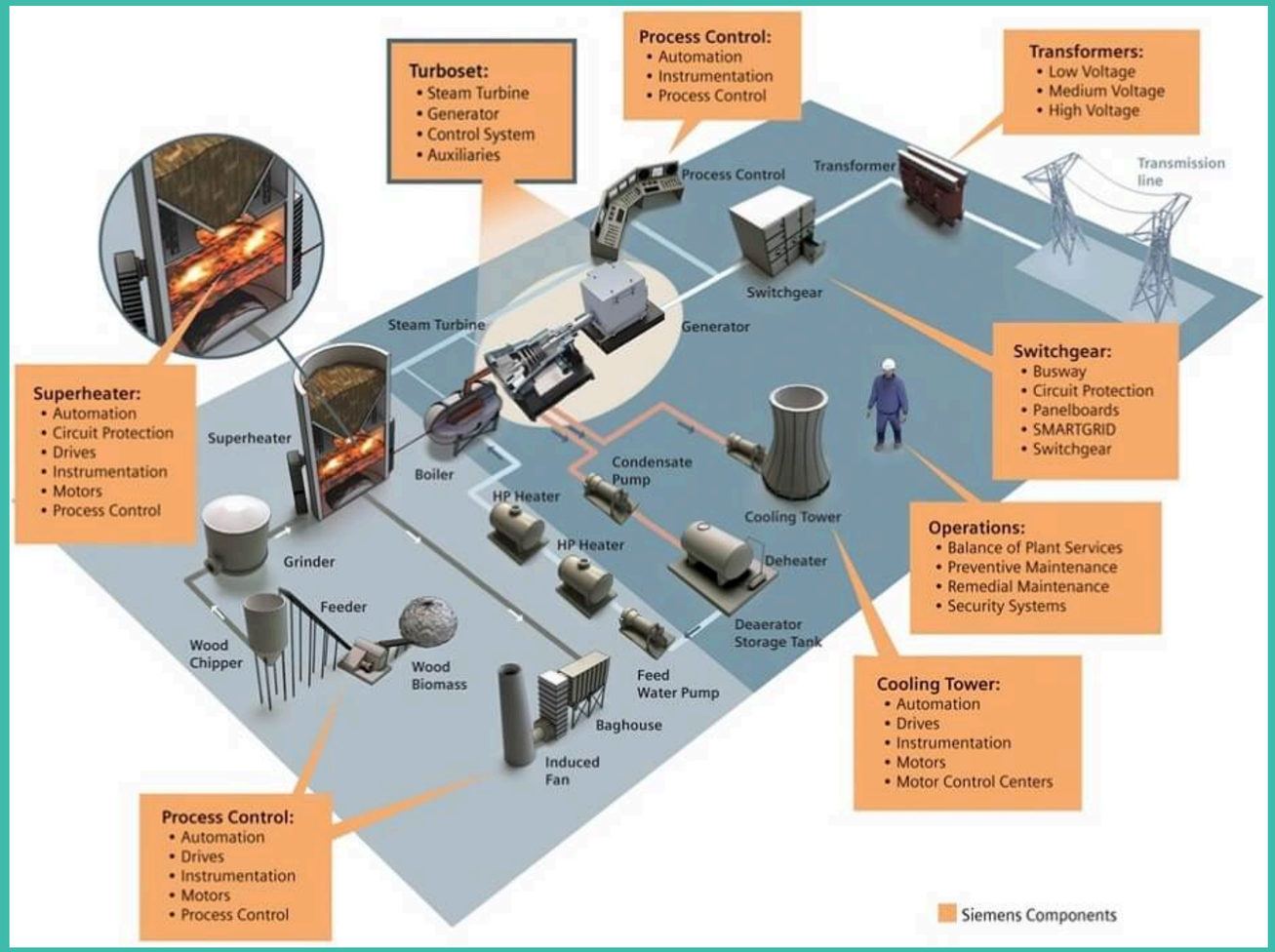

Fig. This illustration of a power plant shows the critical role of ICSs in energy infrastructure, where computer systems are situated in process control sections of the plant.

Solution Overview

Our Idea

- Non-Intrusive Load Monitoring (NILM): Originally for smart homes, it can infer appliance-level behavior from total energy use.
- In ICS: Can we apply NILM-like techniques to detect malicious activity via indirect signals, without modifying existing infrastructure?
- Only access to the power supply via traces or a meter would be required to monitor multiple ICSs.

Train deep learning models on proxy data to detect anomalies and possible attacks

Solution Overview

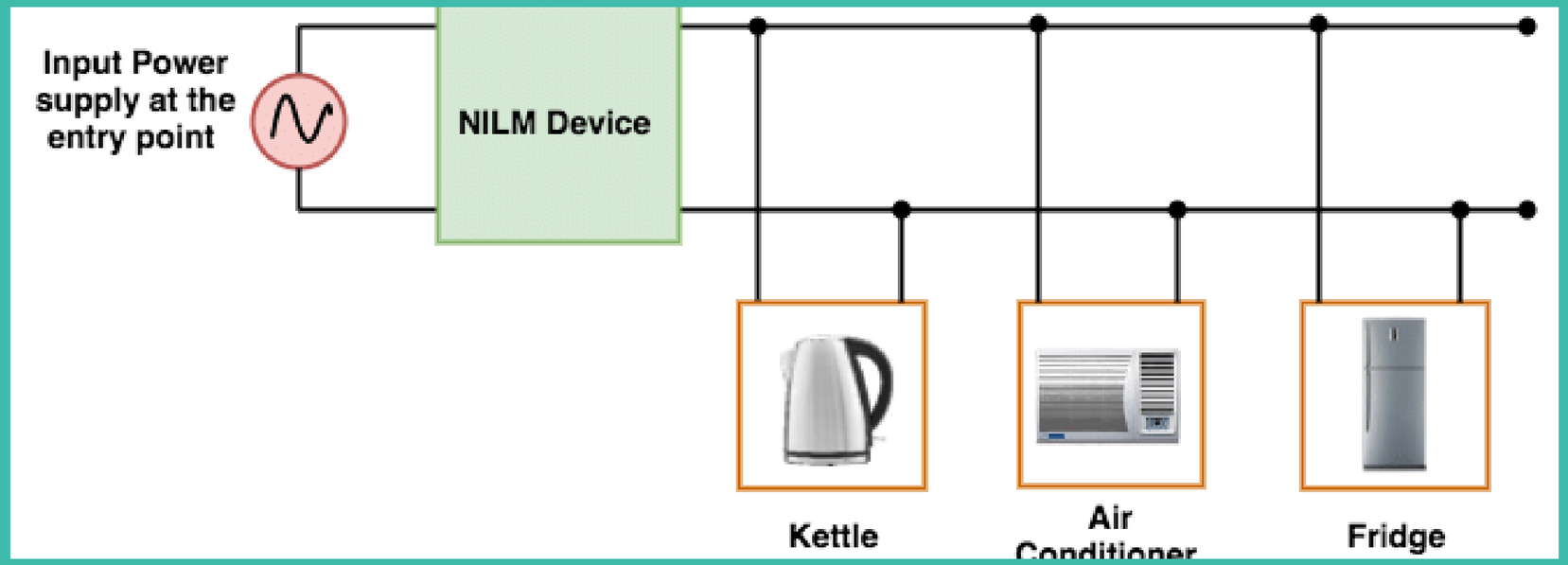

Fig: A typical NILM deployment in a home

MANIPAL ACADEMY of HIGHER EDUCATION
(Institution of Eminence Deemed to be University)

Solution Overview

kaspersky x acm mit bengaluru

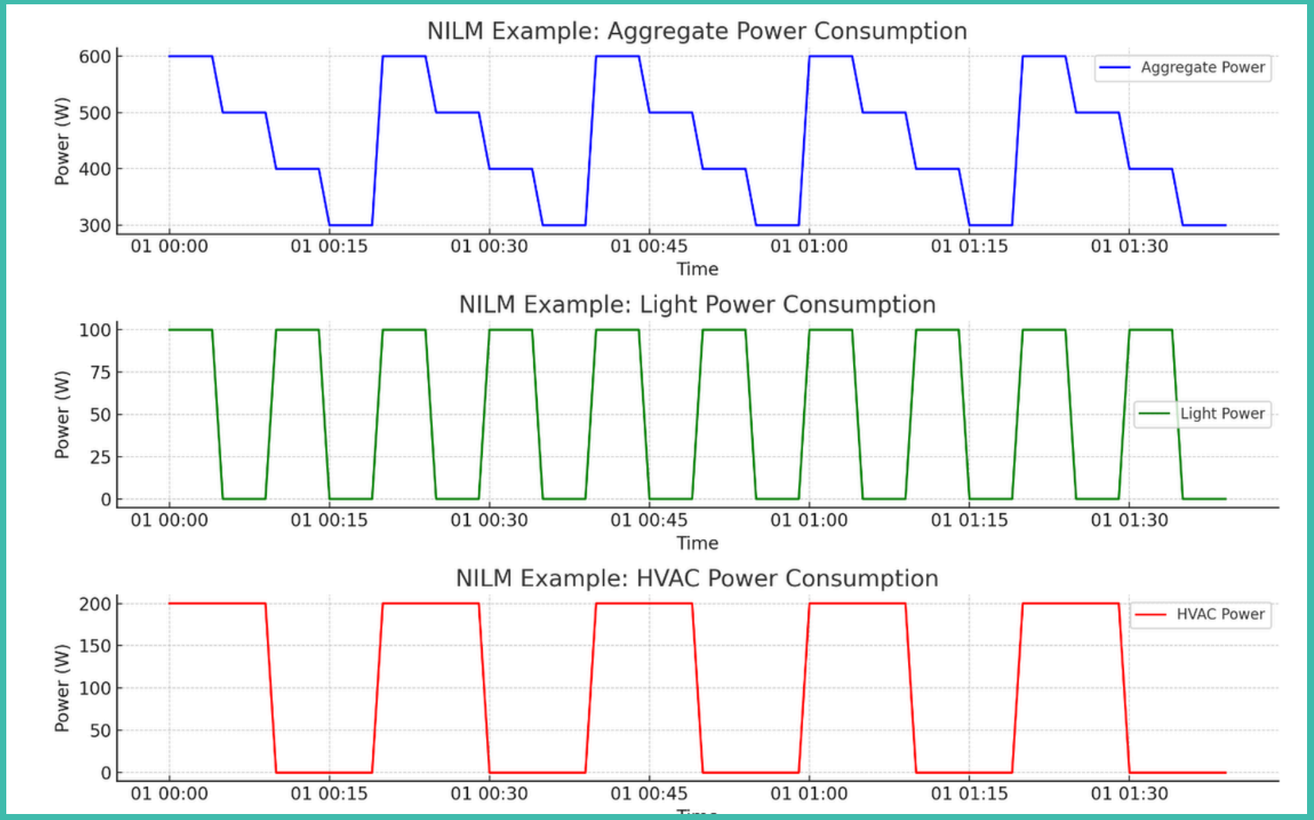

Fig: Time Series data showing NILM in action

Implementation

- Collect appliance-level power data from ICS environment (or simulated)
- Use it as a proxy to learn system behavior patterns
- Apply deep learning models, ie, 1D CNNs
- Train on normal & attack scenarios (or unsupervised for anomaly detection)
- Output: detect deviations and flag as potential cyber-physical attacks

Plan

- Simulated ICS + appliance-level power traces
- Preprocessing
- Normalize, window, label proxy signals
- Model Development and decide on architecture
- Train deep learning models (1D CNN or LSTM)
- Evaluation of models
- Test in a closed-loop ICS environment

Challenges

- Proxy Gap: Appliance behavior may not always reflect internal ICS state
- Data Scarcity: Real ICS attack datasets are rare or classified, and using proxy data could pose a formidable challenge
- Noise & Variability: Electrical signals are noisy & environment-dependent
- Generalization: Models trained on one setup may not transfer easily
- Explainability: Black-box DL models makes it hard to interpret for operators

MANIPAL ACADEMY of HIGHER EDUCATION
(Institution of Eminence Deemed to be University)

Technical Approach and Tech Stack

kaspersky x acm mit bengaluru

Data Simulation & Preprocessing

- Python, NumPy, Pandas, SciPy
- Optionally: OpenDSS, GridLAB-D (for ICS load sim)

Deep Learning Models

- PyTorch
- Scikit-learn for ML baseline
- TorchTS / PyTorch Forecasting for time seires

Visualization & Evaluation

- Matplotlib, Seaborn
- TensorBoard / Weights & Biases (optional)

Deployment/Prototyping

- Jupyter for experiments
- Docker (if containerizing)
- Raspberry Pi / low-power edge device (future deployment)

Technical Approach and Tech Stack

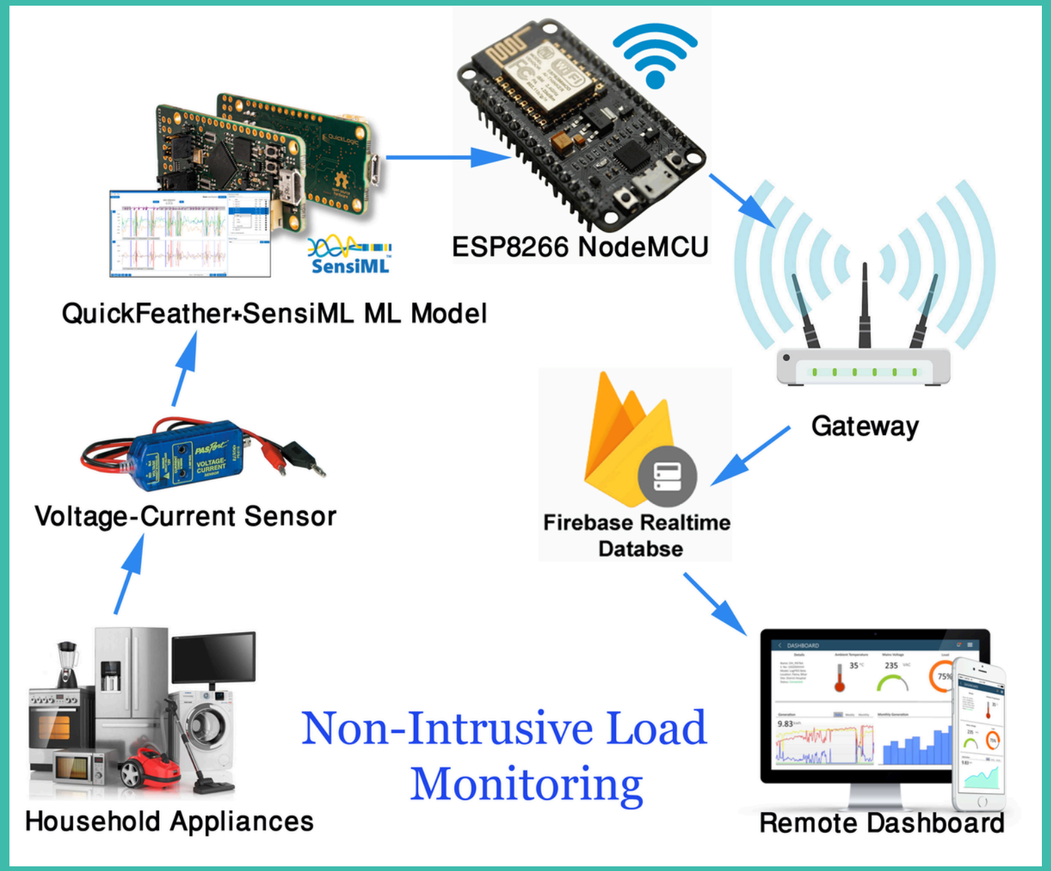

Fig: An ideal NILM deployment with an edge device. For our use case, we would monitor ICSs instead of applicances.

Future Scope

Multi-modal Proxy Signals

- Combine power data with other signals (e.g., EM emissions, timing patterns, network activity)

Real-world ICS Integration

- Deploy in real ICS testbeds with live industrial workloads

Self-supervised & Continual Learning

- Adapt models to new devices and unseen attack patterns over time

Edge Deployment

- Run lightweight models on embedded devices for on-site anomaly detection

Explainability & Operator Trust

- Add interpretability tools using xAI to help ICS operators understand alerts