Funded by:

SOLAR ENERGY
TECHNOLOGIES OFFICE
U.S. Department Of Energy

# AI for Cybersecurity in Photovoltaic Systems

Presenter: Qinghua Li

Associate Professor and the 21st Century Research Leadership Chair

Dept. of Electrical Engineering and Computer Science

University of Arkansas

**Project:** Multilevel Cybersecurity for Photovoltaic Systems (DE-EE0009026)

**Principal Investigator:** H. Alan Mantooth, University of Arkansas, mantooth@uark.edu

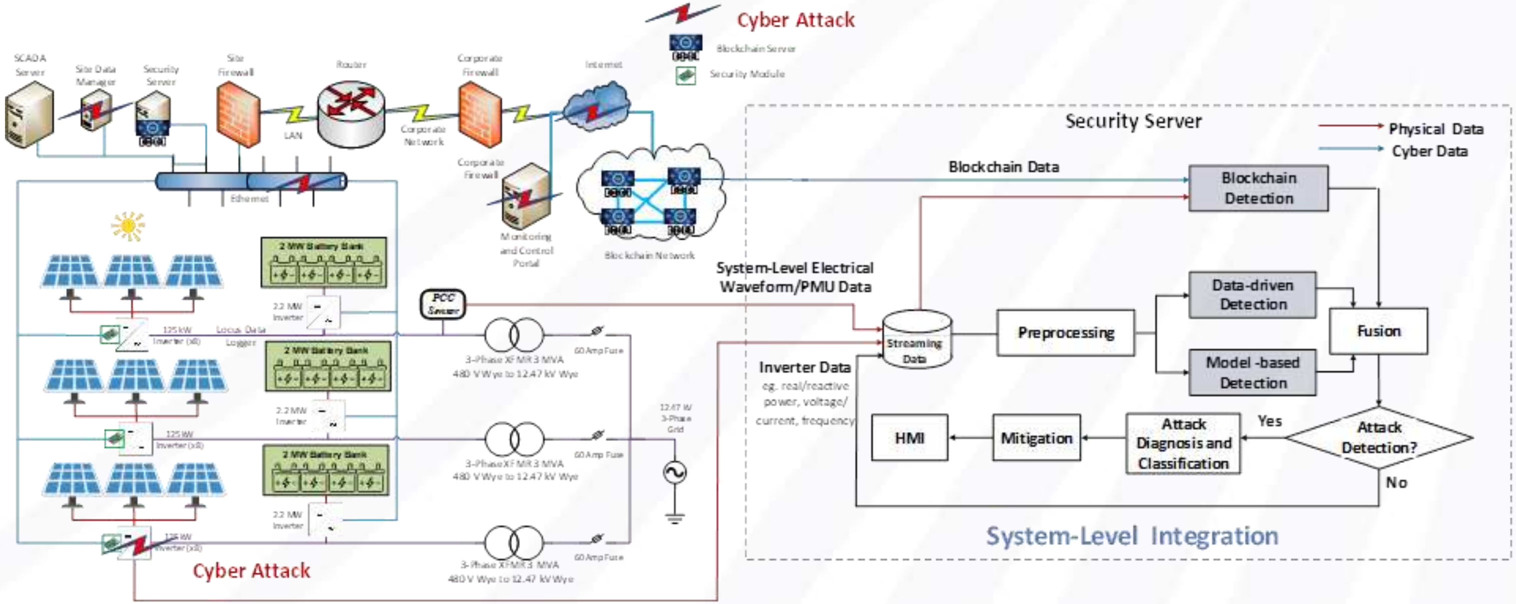
**Subawardees:** NREL, UGA, UIC, TAMUK, TPI, Ozarks Electric, GE Research, ANL

Funded by: SOLAR ENERGY TECHNOLOGIES OFFICE U.S. Department Of Energy



# Project Overview

- Inverter-level security
  - Digital twin and hot patching
  - Vulnerability mitigation
  - Attack detection
  - Supply chain security
- System-level security
  - Model- and ML-based attack detection
  - Blockchain-based security

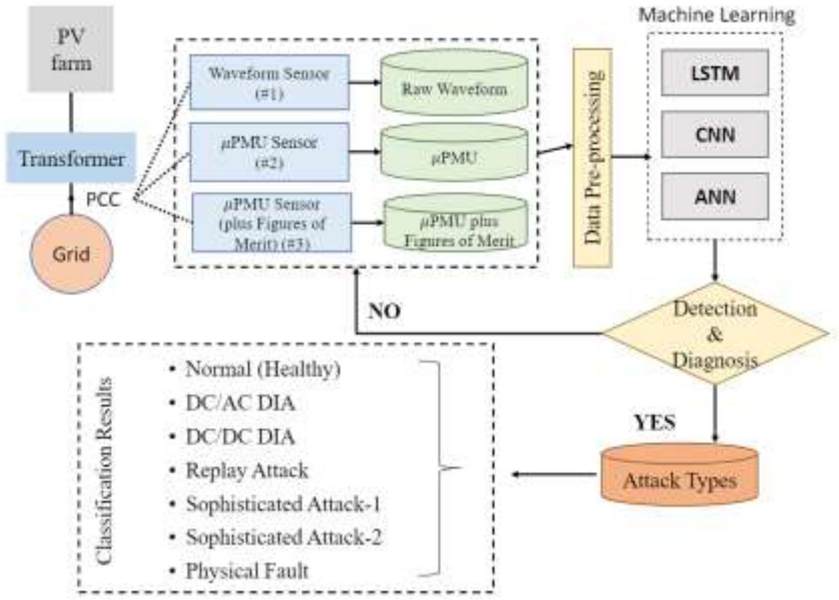


Funded by:
SOLAR ENERGY TECHNOLOGIES OFFICE
U.S. Department Of Energy

# AI in the Project

## Data-driven Cyberattack Detection

- **A comprehensive comparison of data-driven cyber-attack detection methods**




Neural Network
- Artificial Neural Network (ANN)
- Convolution Neural Network (CNN)
- Long Short-Term Memory (LSTM)

Input Data
- Type 1: Waveform
- Type 2: μPMU
- Type 3: figure of merit, such as μPMU, THD, unbalanced degree

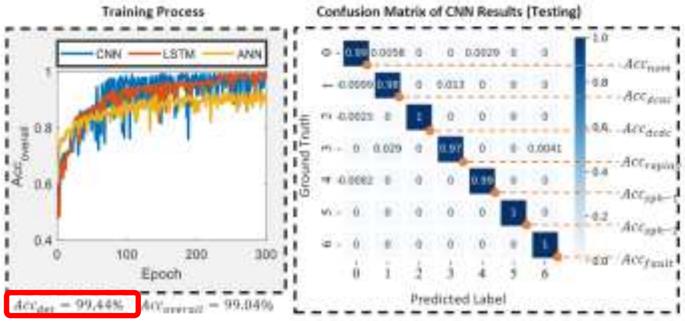
J. Zhang, L. Guo, J. Ye, A. Giani, A. Elasser, W. Song, J. Liu, B. Chen, and H. A. Mantooth, "Machine Learning-based Cyber-attack Detection in Photovoltaic Farms", in *IEEE Open Journal of Power Electronics*, 2023.

Funded by:
SOLAR ENERGY TECHNOLOGIES OFFICE
U.S. Department Of Energy

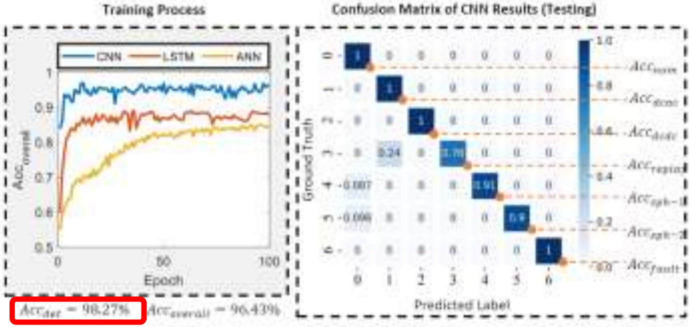
# AI in the Project

## Data-driven Cyberattack Detection

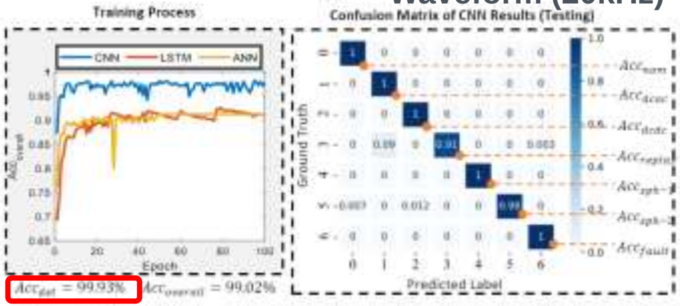
- A comprehensive comparison of data-driven cyber-attack detection methods



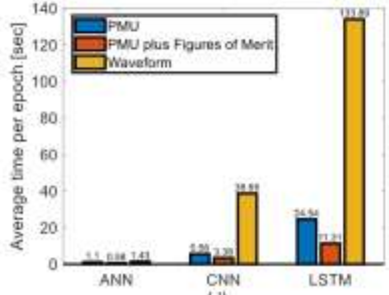

(a) **Waveform (20kHz)**




(b) **PMU (120Hz)**




(c) **Figures of Merit (120Hz)**




(d)

**Conclusion**:

- Well-designed Figures of Merit outperform the Waveform and PMU data in terms of efficiency and accuracy.
- CNN shows superior performance surpassing ANN and LSTM.
- This method cannot detect novel attacks that are not included in the training set.

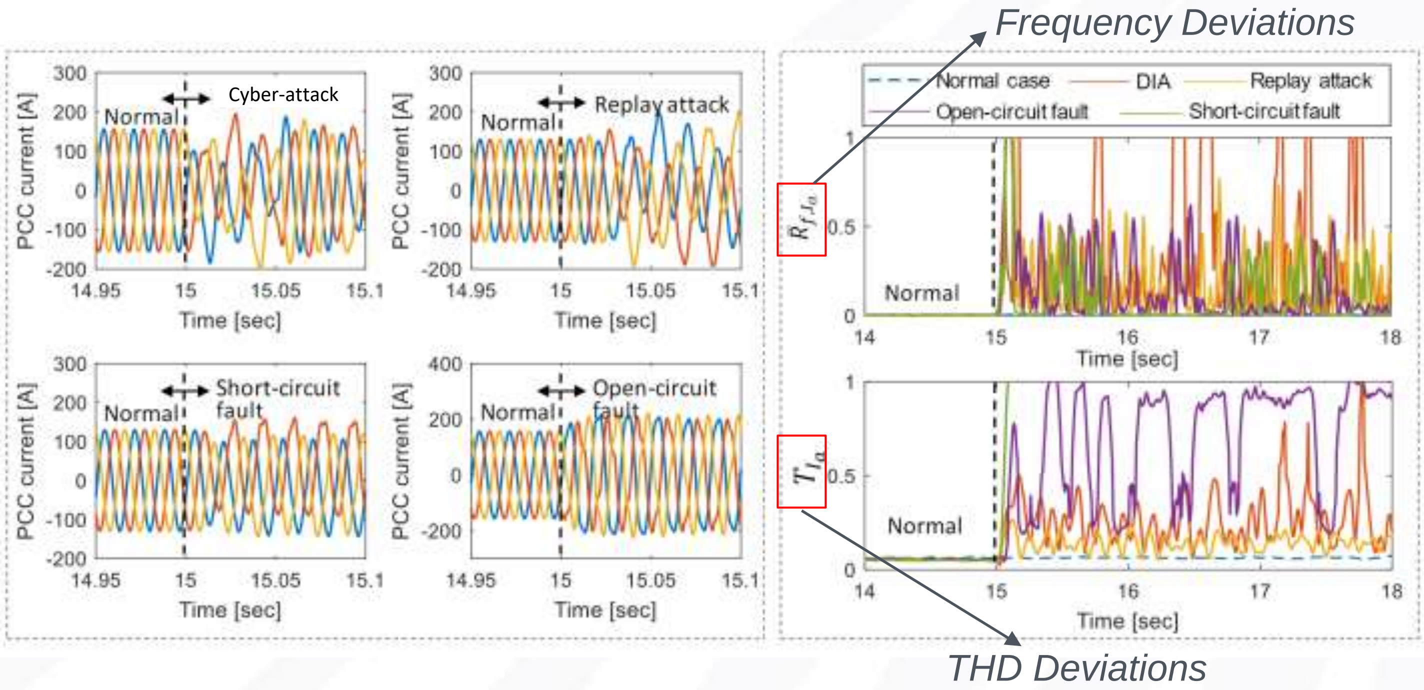
J. Zhang, L. Guo, J. Ye, A. Giani, A. Elasser, W. Song, J. Liu, B. Chen, and H. A. Mantooth, "Machine Learning-based Cyber-attack Detection in Photovoltaic Farms", in *IEEE Open Journal of Power Electronics*, 2023.

Funded by: SOLAR ENERGY TECHNOLOGIES OFFICE U.S. Department Of Energy

# AI in the Project

## Data-driven Cyberattack Detection

- **Data-driven cyber-attack detection using physics-guided time-frequency features**




L. Guo, J. Zhang, J. Ye, S. J. Coshatt. and W. Song, "Data-driven cyber-attack detection for PV farms via time-frequency domain features," *IEEE Transactions on Smart Grid*, 2021.

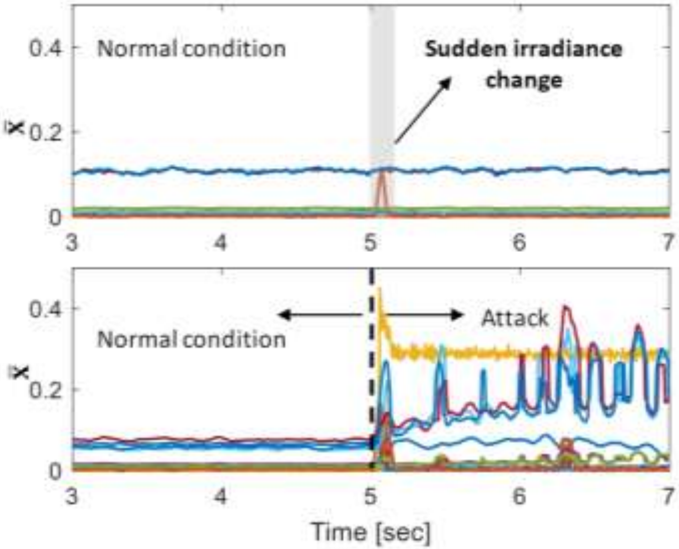
# AI in the Project

## Data-driven Cyberattack Detection

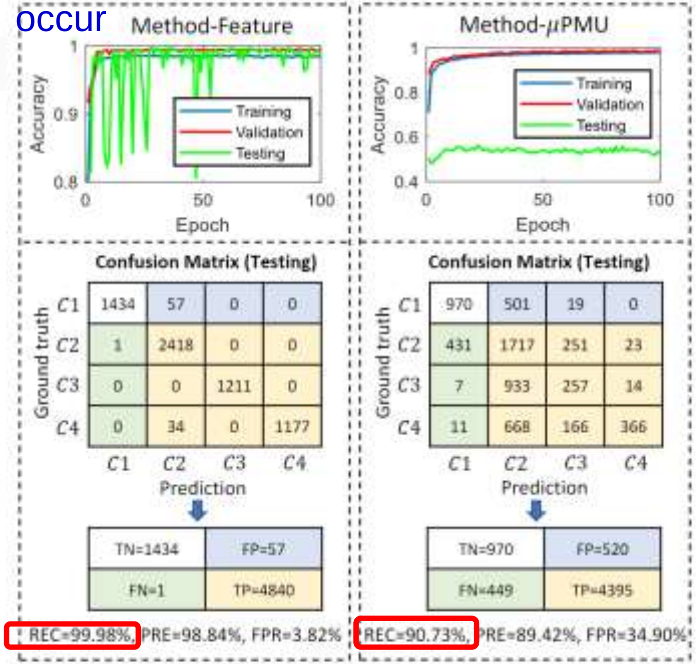
- Data-driven cyber-attack detection using physics-guided time-frequency features

**Innovative Features to Address New Attacks**

Irradiance Impacts




Testing Results when **New Attacks** occur

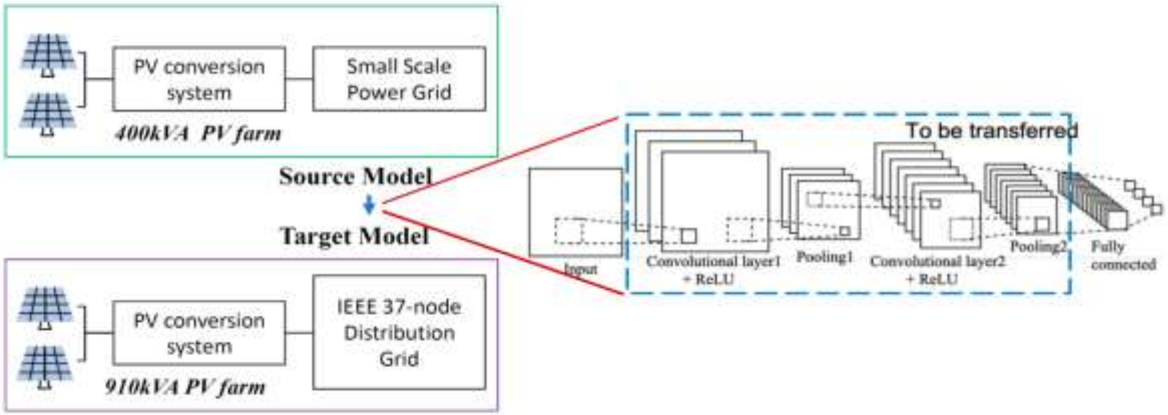



L. Guo, J. Zhang, J. Ye, S. J. Coshatt. and W. Song, “Data-driven cyber-attack detection for PV farms via time-frequency domain features,” *IEEE Transactions on Smart Grid*, 2021.

# AI in the Project

## Data-driven Cyberattack Detection

- **A transfer learning technique for cyber-attack detection in PV farms**




- Research problem- how to reduce the data needs and time of training machine learning models for a new solar farm?
- Two solar farm attack models are built to generate the dataset
  - Solar farm #1: 400 kVA in a small-scale power grid.
  - Solar farm #2: 910 kVA connected to the IEEE 37-node distributed grid.
- Transfer learning is used

Q. Li, J. Zhang, J. Ye and W. Song, "Data-driven cyber-attack detection for photovoltaic systems: A transfer learning approach," *2022 IEEE Applied Power Electronics Conference and Exposition (APEC)*.

Funded by:
SOLAR ENERGY TECHNOLOGIES OFFICE
U.S. Department Of Energy

# AI in the Project

## Data-driven Cyberattack Detection

- **A transfer learning technique for cyber-attack detection in PV farms**

Performance comparison between transferred model and the newly trained model

| Training samples | F1 (transfered model) | F1 (newly trained model) |
|---|---|---|
| 10% | **0.757** | 0.673 |
| 20% | **0.805** | 0.698 |
| 40% | **0.912** | 0.822 |
| 60% | **0.952** | 0.894 |
| 80% | 0.979 | **0.982** |
| 100% | 0.978 | **0.989** |

**Transferred model achieves 95.2% accuracy (F1 score) using 60% training dataset.**

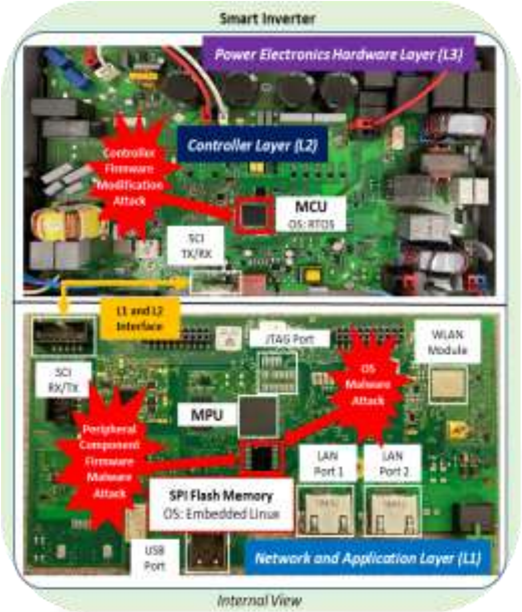
- Transfer learning requires much lower amount of dataset and training time compared with newly-trained model.

Q. Li, J. Zhang, J. Ye and W. Song, "Data-driven cyber-attack detection for photovoltaic systems: A transfer learning approach," *2022 IEEE Applied Power Electronics Conference and Exposition (APEC)*.

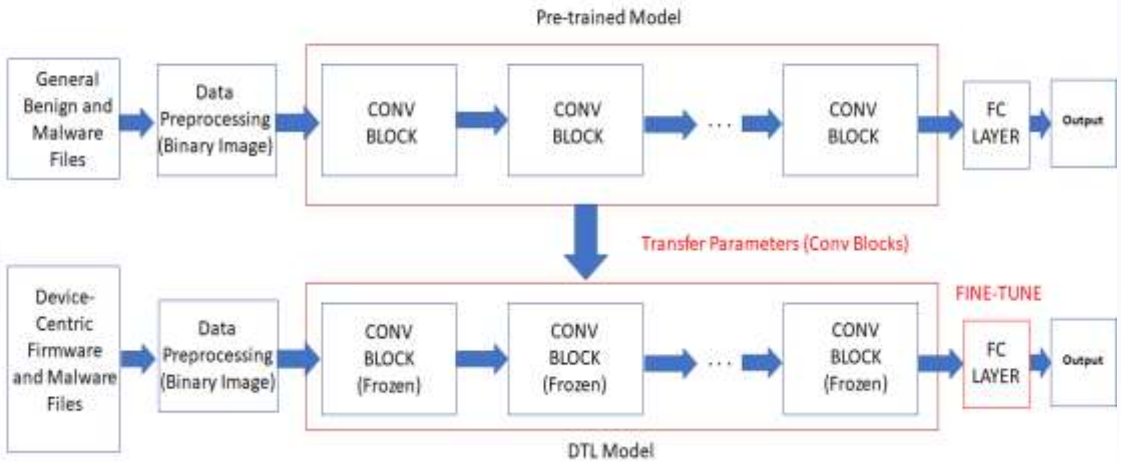
# AI in the Project

## Firmware Malware Detection for Smart Inverters

- The DTL method takes a pre-trained model from a type of image dataset, freeze a portion of the layers, and then fine-tune the last few layers on the newly obtained dataset




*A commercial smart inverter architecture*




*The proposed DTL model*

S. Alvee, B. Ahn, S. Ahmad, K. Kim, T. Kim, J. Zeng, "Device-Centric Firmware Malware Detection for Smart Inverters using Deep Transfer Learning," IEEE Design Methodologies Conference (DMC), 2022

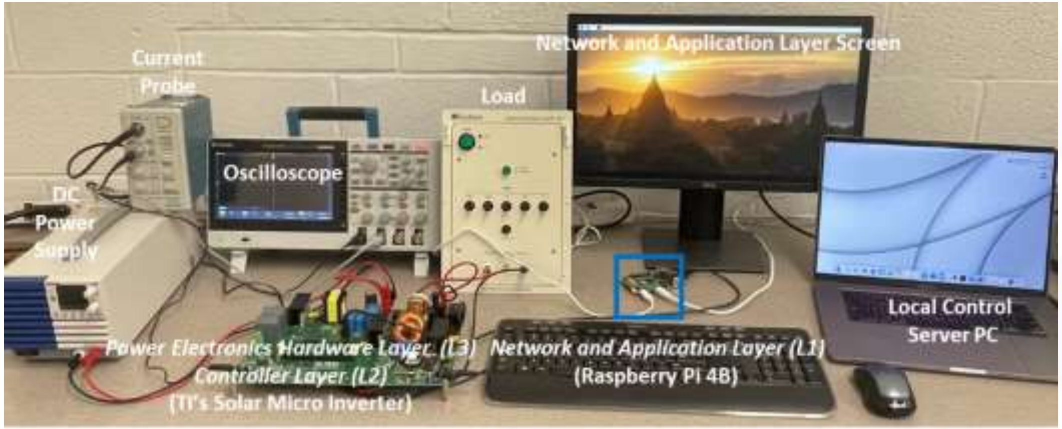
Funded by:
SOLAR ENERGY TECHNOLOGIES OFFICE
U.S. Department Of Energy


# AI in the Project

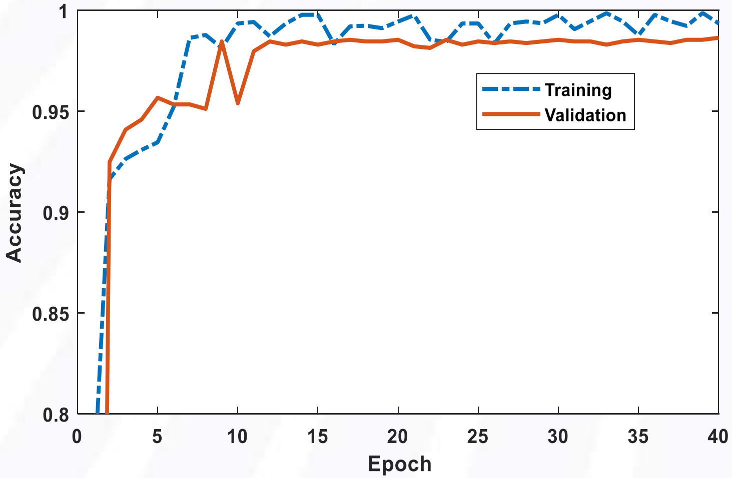
## Firmware Malware Detection for Smart Inverters

- The basis DL model experiment
  - 100 benign files and 100 malware

- The proposed DTL model experiment
  - IoT device (Raspberry Pi 4B)
  - 1 benign file and 5 malware




*Experiment setup on an emulated smart inverter security testbed*




*Training and validation accuracy of the DTL model*

S. Alvee, B. Ahn, S. Ahmad, K. Kim, T. Kim, J. Zeng, "Device-Centric Firmware Malware Detection for Smart Inverters using Deep Transfer Learning," IEEE Design Methodologies Conference (DMC), 2022

# What We Learned

- ML is a promising technique in PV system cybersecurity
- No ML model works for all
- Lack of data – transfer learning might help
  - Transfer across domains
  - Transfer within PV systems
- Physics-informed feature selection could be leveraged
- Cyber attacks and physical faults should be considered together

# Acknowledgment

- This material is based upon work supported by the Department of Energy under Award No. DE-EE0009026.
- Some content in the slides is shared from Drs. Alan Mantooth, Jin Ye, Taesic Kim, and Chris Farnell.