# Effect of Check Meter Quantity on Theft Detection in Distribution Networks with Rooftop PV and Net Metering

Kaira Maxine V. Gonzales | Carlos Demetri S. Vicencio
Adviser: Adonis Emmanuel D.C. Tio, Ph. D.

# Table of contents

01

# Introduction

# Introduction

## Philippine Energy Plan

Aims to strengthen the use of clean energy sources

## Rooftop Photovoltaic (PV) and Net Metering (NM)

Program that would allow consumers generate their own electricity and sell excess electricity

# Introduction

## Challenge

PV and NM introduce a new form of electricity theft which may affect the performance of current theft detection methods

02

# Related Work

# System Loss

Difference between energy delivered and energy consumed

Causes financial loss that are passed on consumers.

- Private utilities: 8.5% of consumption
- Electric Cooperatives: 13% of consumption

## Administrative

Energy used by the distribution utility

## Technical

Power dissipation during transmission and distribution

## Non-technical

Energy losses not controlled by the distribution utility
→ Electricity Theft

# Electricity Theft Attacks

### Interruption of Measurement

Physically disconnects or reset the meters

### Store demand tampering

Meter readings are manipulated

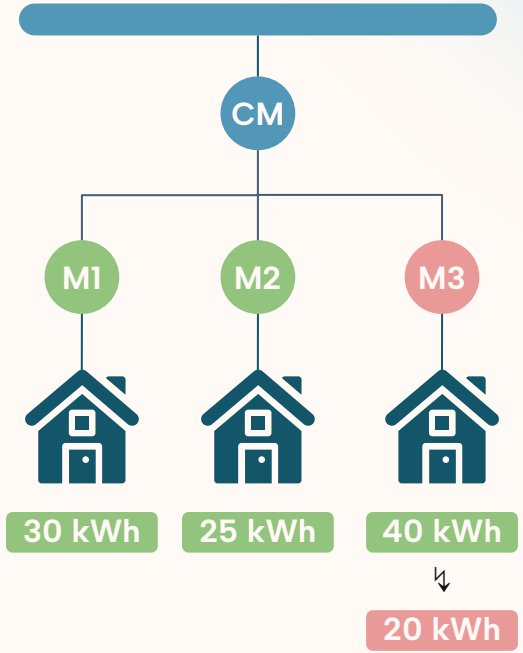
### Network Modification

Hijacking of meters to deliver forged data

# Electricity Theft Detection

## Check Meters

- Devices that measure the supplied electricity to downstream consumers
- Readings do not change even with meter tampering
- Check meter readings can be compared to the total readings of the downstream households
- Difference must be significant



# Electricity Theft Detection Approaches

## Data-oriented

Use of consumer related information

## Network-oriented

Uses data about the network including topology and measurements

## Hybrid

Utilizes both data-oriented and network-oriented approach

# Electricity Theft Detection Machine Learning

## Support Vector Machine (SVM)

Determines optimal hyperplane that categorized samples

## Artificial Neural Networks (ANN)

Computational network that maximizes the use of multiple layers of interconnected nodes

## Decision Tree (DT)

Tree-like structure of several decisions and consequences

## Random Forest (RF)

Combination of multiple DTs

# Related Work

## PV & NM on System Losses

- Reverse power flow increases transmission line losses and 3-phase equipment malfunction [1]

## ETD on Network with PV & NM

- Different theft representations [2]
- NM affects ETD more than PV [3]
- Explored different features and algorithms [4]

## Role of Check Meters

- Compared single CM and individual household readings [5]
- Used multiple CMs to lessen downstream households [3][4][6]


[1] R. A. Walling, R. Saint, R. C. Dugan, J. Burke and L. A. Kojovic, "Summary of Distributed Resources Impact on Power Delivery Systems," in IEEE Transactions on Power Delivery, vol. 23, no.3, pp. 1636-1644, July 2008
[2] . M. Badr, M. I. Ibrahem, M. Baza, M. Mahmoud and W. Alasmary, "Detecting Electricity Fraud in the Net-Metering System Using Deep Learning," 2021 International Symposium on Networks, Computers and Communications (ISNCC), Dubai, United Arab Emirates, 2021.
[3] C. Lavilla, M. Osorio, and Z. Restituto, "Effect of Net Metering and Rooftop Photovoltaics on Electricity Theft Detection," Capstone Project, EEEI, University of the Philippines, Diliman, 2021.
[4] R. M. P. Maala, A. M. B. Rebamba and A. E. D. Tio, "Classification-Based Electricity Theft Detection on Households with Photovoltaic Generation and Net Metering," TENCON 2023 - 2023 IEEE Region 10 Conference (TENCON), Chiang Mai, Thailand, 2023, pp. 1094-1099
[5]. Huang, S. Liu and K. Davis, "Energy Theft Detection Via Artificial Neural Networks," 2018 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe), Sarajevo, Bosnia and Herzegovina, 2018, pp. 1-6
[6] . Ismail, M. F. Shaaban, M. Naidu and E. Serpedin, "Deep Learning Detection of Electricity Theft Cyber-Attacks in Renewable Distributed Generation," in IEEE Transactions on Smart Grid, vol. 11, no. 4, pp. 3428-3437, July 2020.

# Summary

- Machine learning algorithms are effective in detecting electricity theft.
- Few studies considered networks with PV and NM
- Most research used historical time-series data of individual household readings
- No studies have explored the effect of the quantity of check meters on electricity theft detection.

03

# Problem Statement & Objectives

# Problem Statement

## Problem

Widespread electricity theft harms the power industry

## Challenge

More consumers are availing PV and NM which affects performance of electricity theft detection

## Existing Work

Limited studies on electricity theft detection on networks with PV and NM

Use of impractical and costly models with several check meters

## Problem Statement

There are currently no studies that have explored the effect of check meter quantity on theft detection in networks with PV and NM.

# Objectives

## Primary Objective

Study the effect of check meter quantity in electricity theft detection methods

## Specific Objectives

- Create training datasets with varying check meter quantities
- Compare the performance of electricity theft detection algorithms under different PV and NM penetration and check meter quantity

# Scope and Limitations

## Machine Learning Algorithms

Support Vector Machine (SVM)

Artificial Neural Network(ANN)

Decision Tree(DT)

Random Forest (RF)

## Network

Varying PV and NM penetration

Varying check meter quantity

Check meters will be placed evenly throughout the network.

## Limitations

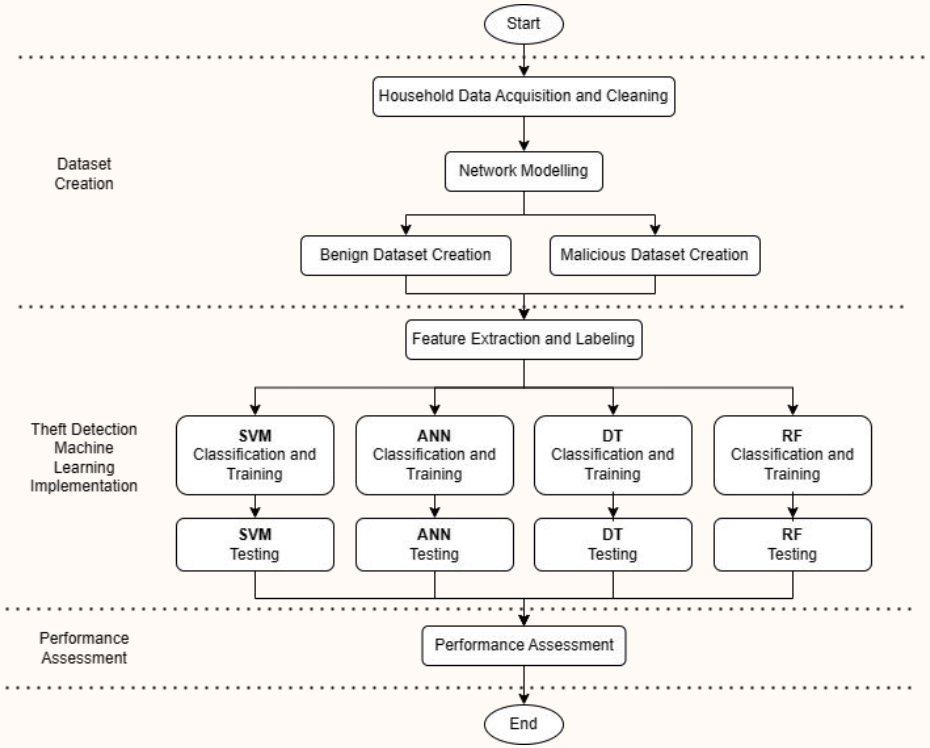
One pilferer tampers with meter readings

Optimal placement of check meters will not be studied

# 04

# Methodology

# Process Flowchart



# Dataset Creation

# Household Data Acquisition and Cleaning

## Ausgrid Dataset

- 300 customers
- Households with Rooftop PV
- Half-hour interval readings
- Meter reading categories
  - Gross Generation (GG)
  - Gross Consumption (GC)
  - Controllable Load (CL)

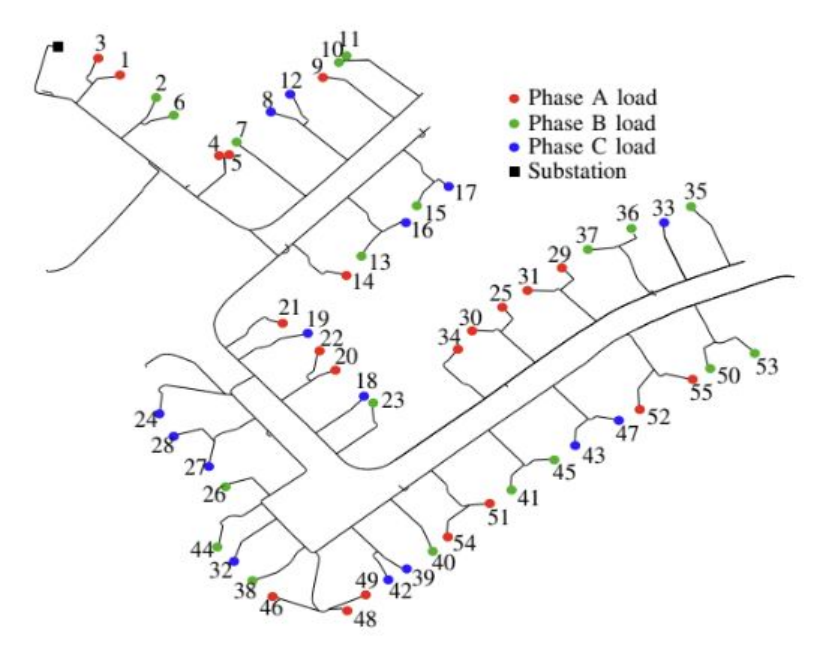
## Data Cleaning

- Narrow to 2010–2011 data
- Filter out households with CL
- Use data points from period with similar weather forecast as the Philippines

# Network Modeling

## IEEE European LV Test Feeder

- Open source base test feeder with minimal alterations
- 55 PQ loads and 1 Distribution Transformer
- Simulate in OpenDSS



# Network Modeling

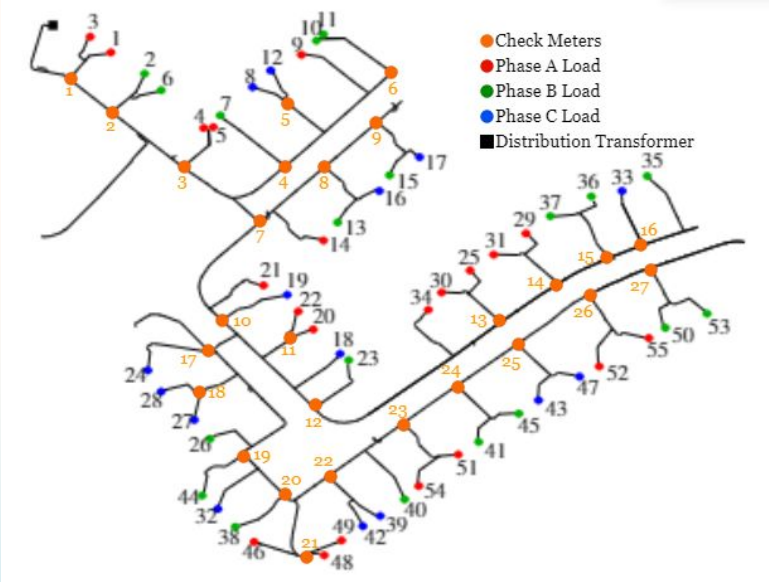
## Test Network Cases - Check Meter (CM) Configuration

| CM Configuration | CM Qty | Households per CM |
|---|---|---|
| C1 | 27 | 2-3 |
| C2 | 10 | 5-6 |
| C3 | 5 | 10-12 |
| C4 | 1 | 55 |

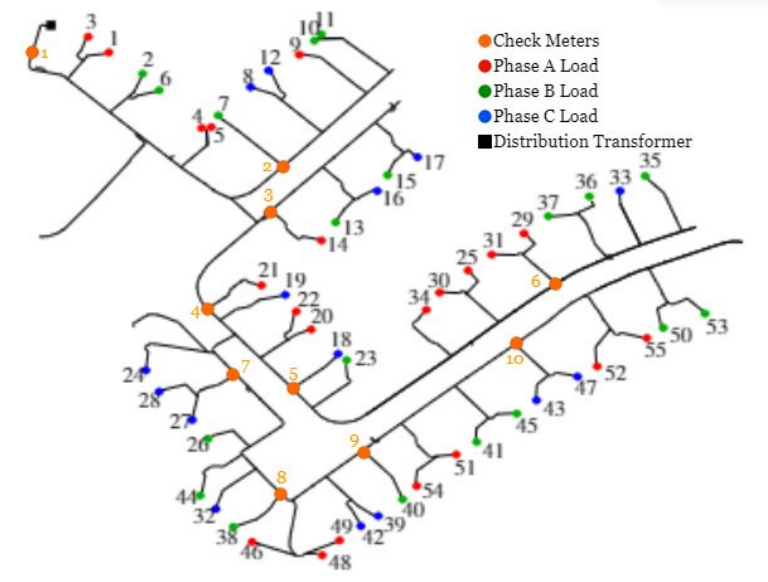
# Network Modeling

## Check Meter (CM) Placement

### C1:



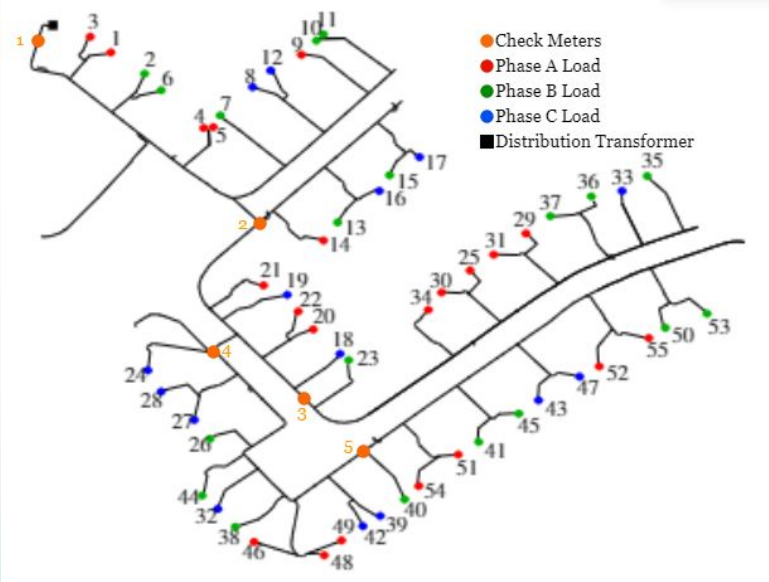

### C2:



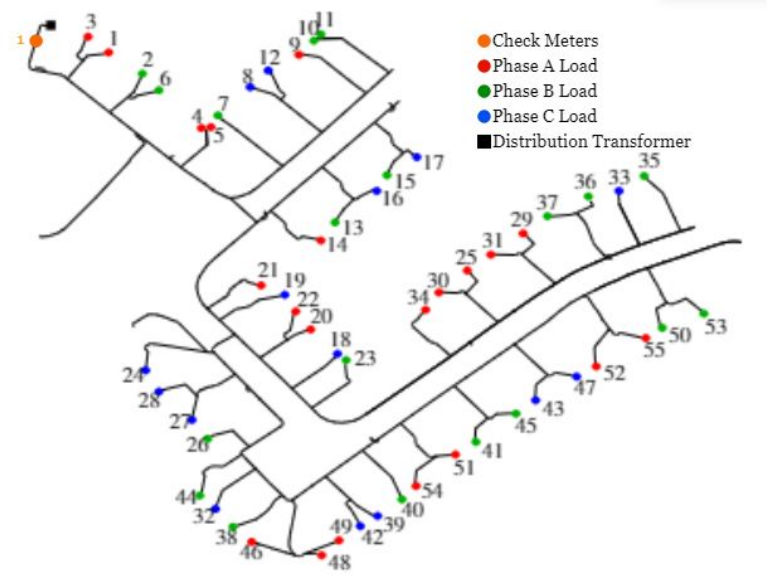
# Network Modeling

## Check Meter (CM) Placement

### C3:




### C4:



# Network Modeling

## Test Network Cases - PV and NM Penetration Levels

| PV + NM Config. | PV Pen. (%) | PV Houses Qty | NM Pen. (%) | NM Houses Qty |
|---|---|---|---|---|
| P0 | 0 | 0 | 0 | 0 |
| P1 | 50 | 27 | 33 | 9 |
| P2 | 100 | 55 | 33 | 18 |
| P3 | 50 | 27 | 66 | 18 |
| P4 | 100 | 55 | 66 | 36 |
| P5 | 50 | 27 | 100 | 27 |
| P6 | 100 | 55 | 100 | 55 |

# Dataset Creation

## Benign Dataset

- 55 randomly selected household per simulation
- Half-hour meter readings will be summed to be converted into daily readings
- Each simulation will have 7 data points – one per day

| Dataset | Sim # | CM | PV + NM |
|---|---|---|---|
| D1 | 1-110 | C1 | P0 |
| … | … | … | … |
| D7 | 661-770 | C1 | P6 |
| … | … | … | … |
| D28 | 2971-3080 | C4 | P6 |

# Dataset Creation

## Malicious Dataset

- Theft multiplier
  - Mean = 0.5
  - Standard deviation = 0.05
  - 3 Standard deviations from mean
    - 35% to 65%
- Pilferer's NM reading
  - + : Reduced consumption
  - – : Increase in sold energy

$$X = \begin{cases} X * k & \text{if } x > 0 \\ X - (|X| * k) & \text{if } x < 0 \end{cases}$$

# Dataset Creation

## Malicious Dataset

- Two theft frequencies
  - Full day: Steals for 24 hours
  - Half day: Steals from 6AM to 6PM
- Each dataset will be divided into two
  - 55 simulations for each theft frequency

| Dataset | Sim # | Theft Frequency |
|---|---|---|
| D1_mal | 1-55 | Full Day |
| | 56-110 | Half Day |
| ... | ... | ... |
| D28_mal | 2971 - 3025 | Full Day |
| | 3026 - 3080 | Half Day |

# Theft Detection Implementation

# Feature Extraction and Labeling

## Gamma Deviance, Log Cosh Loss, and % Loss Error

$$Gamma\ Deviance = 2(log(\frac{\sum_{n=1}^{k} M_n}{CM}) + \frac{CM}{\sum_{n=1}^{k} M_n} - 1)$$

$$Logcosh = log(cosh(\sum_{n=1}^{k} M_n - CM))$$

$$\%\ Loss\ Error = \frac{|\sum_{n=1}^{k} M_n - CM|}{CM}$$

- CM – Daily Check Meter Reading
- ΣMn – Sum of daily meter readings of households under a certain check meter

# Theft Detection Algorithm Implementation

## Classifiers

- Support Vector Machine (SVM)
- Artificial Neural Network (ANN)
- Decision Tree (DT)
- Random Forest (RF)

- 336 classifiers

## Train-Test Split

- 80% of data for training
- 20% of data for testing

## Resources

- Google Colab
- Scikit-learn

# Theft Detection Algorithm Implementation

## SVM

- Radial-Basis Function (RBF) kernel to handle non-linear features
- 10-fold cross validation to split training set
- Support Vector Classifier (SVC) library from Scikit-learn

## ANN

- Optimizers
  - Stochastic Gradient Descent (SGD)
  - Adaptive Moment Estimation (ADAM)
- Activation Functions
  - Sigmoid, Hyperbolic Tan, Rectified Linear Unit
- 5-fold hyperparameter optimization
- Keras and MinMaxScaler libraries in Colab

# Theft Detection Algorithm Implementation

## DT

- No overlaps between training and testing data
- DecisionTreeRegressor library from Scikit-learn

## RF

- Hyperparameters
  - Number of DTs
  - Max Depth
- Hyperparameter optimization
- RandomForestClassifier library from Scikit-learn

# Performance Assessment

# Performance Metrics

$$Accuracy = \frac{TP + TN}{TP + FP + TN + FN}$$

- True Positive (TP) – correctly identified theft
- True Negative (TF) – correctly identified non-theft
- False Positive (FP) – wrongly accused theft
- False Negative (FN) – undetected theft

# Preliminary Work

# Preliminary Work

01

Ausgrid Dataset

02

European IEEE LV Test Feeder

03

File Repository of Previous Work

05

# Project Schedule & Deliverables

# Gantt Chart

| Task Name | Week | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| **Pre-Work** | | | | | | | | | | | | | | | | |
| Familiarization with Machine Learning Algorithms | | | | | | | | | | | | | | | | |
| Familiarization with Power Flow Simulations | | | | | | | | | | | | | | | | |
| **Household Data Acquisition and Cleaning** | | | | | | | | | | | | | | | | |
| **Network Modelling** | | | | | | | | | | | | | | | | |
| **Benign and Malcious Dataset Creation** | | | | | | | | | | | | | | | | |
| Network C1 | | | | | | | | | | | | | | | | |
| Network C2 | | | | | | | | | | | | | | | | |
| Network C3 | | | | | | | | | | | | | | | | |
| Network C4 | | | | | | | | | | | | | | | | |
| **Theft Detection Machine Learning Implementation** | | | | | | | | | | | | | | | | |
| Feature Extraction and Labeling | | | | | | | | | | | | | | | | |
| Network C1 (SVM, ANN, DT and RF) | | | | | | | | | | | | | | | | |
| Network C2 (SVM, ANN, DT and RF) | | | | | | | | | | | | | | | | |
| Network C3 (SVM, ANN, DT and RF) | | | | | | | | | | | | | | | | |
| Network C4 (SVM, ANN, DT and RF) | | | | | | | | | | | | | | | | |
| **Performance Assessment** | | | | | | | | | | | | | | | | |
| **Documentation** | | | | | | | | | | | | | | | | |

Legend: **Gray** - *All* , **Green** - *Gonzales* , **Blue** - *Vicencio*

# Halfway Deliverables

01

## Libraries for ML implementation

SVM, ANN, DT, RF

02

## File Repository

Python scripts for data cleaning

OpenDSS file of test network

Raw and processed power flow datasets

03

## Documentation

Output of each task

# Final Deliverables

01

## ML Prediction Results

SVM, ANN, DT, RF

02

## Theft detection performance metrics

Accuracy

03

## File Repository

Datasets, test network, scripts, and other related files

04

## Documentation

Final Manuscript

05

## IEEE Format Article

Condensed version of study

# Effect of Check Meter Quantity on Theft Detection in Distribution Networks with Rooftop PV and Net Metering

Kaira Maxine V. Gonzales | Carlos Demetri S. Vicencio
Adviser: Adonis Emmanuel D.C. Tio, Ph. D.

# References


[1] R. A. Walling, R. Saint, R. C. Dugan, J. Burke and L. A. Kojovic, ”Summary of Distributed Resources Impact on Power Delivery Systems,” in IEEE Transactions on Power Delivery, vol. 23, no.3, pp. 1636-1644, July 2008

[2] . M. Badr, M. I. Ibrahem, M. Baza, M. Mahmoud and W. Alasmary, ”Detecting Electricity Fraud in the Net-Metering System Using Deep Learning,” 2021 International Symposium on Networks, Computers and Communications (ISNCC), Dubai, United Arab Emirates, 2021.

[3] C. Lavilla, M. Osorio, and Z. Restituto, "Effect of Net Metering and Rooftop Photovoltaics on Electricity Theft Detection," Capstone Project, EEEI, University of the Philippines, Diliman, 2021.

[4] R. M. P. Maala, A. M. B. Rebamba and A. E. D. Tio, ”Classification-Based Electricity Theft Detection on Households with Photovoltaic Generation and Net Metering,” TENCON 2023 - 2023 IEEE Region 10 Conference (TENCON), Chiang Mai, Thailand, 2023, pp. 1094-1099

[5]. Huang, S. Liu and K. Davis, ”Energy Theft Detection Via Artificial Neural Networks,” 2018 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe), Sarajevo, Bosnia and Herzegovina, 2018, pp. 1-6

[6] . Ismail, M. F. Shaaban, M. Naidu and E. Serpedin, ”Deep Learning Detection of Electricity Theft Cyber-Attacks in Renewable Distributed Generation,” in IEEE Transactions on Smart Grid, vol. 11, no. 4, pp. 3428-3437, July 2020.