International Journal of Engineering Research Excellence and Applied Science (IJEREAS)

Volume-II (Issue 3) – September 2024 ISSN: 3048-5355

Ensuring Privacy Preservation in Advanced Energy Theft Detection Mechanisms for Smart Grid Networks

Kuldeep Kumar[1]
M.Tech Scholar

Jitendra Kumar Sharma[2]
Assistant Professor

Dr. Sanjay Kumar Mathur[3]
Principal & Professor

[1,2,3] Department of Electrical Engineering
Aryabhatta College of Engineering and Research Center, Ajmer, Rajasthan, India

Abstract- Apart from convention theft by passing the energy meter, more advanced theft are present due to vulnerability of data transmitted. In the simulation, Energy theft added in load2 and load3 at 0.5. The energy theft will happen we collect the data from that data and find when the theft is happened and data contains non-theft and ANN Technique used to detect the theft data by as well as get the theft time

A novel method for energy theft detection in AMI setup is presented by employing hybridization of distributed totalization metering, Artificial Intelligence & cryptographic techniques, which is able to detect & prevent both conventional, or data manipulation/hacking type of energy theft attempts using MATLAB Software.

Keywords-AMI (Advanced Metering Infrastructure), Distributed Totalization Metering, Artificial Intelligence, Cryptography.

I. Introduction

Energy cannot be formed or destroyed, only from one form to another can it be modified. The power to alter an entity is energy. The change could involve the movement, location or particles of an object. The quantitative property according to energy in physics has to be passed to the object in order for work to be done or the object to heat.

All human energy must come from one of the key sources of energy, there are no alternative energy sources. Primary energy is compared to end energy consumption. In order to make this primary energy supplier a power currency or a secondary fuel before it can be used, primary energy almost always has to be converted into an energy conversion technology. For example, Coal produces electricity normally in a coal-fired power station.

Until electricity can be produced, wind must be harnessed by a wind turbine. Sources of secondary energy Secondary sources of energy are obtained in a fuel or energy supply from primary sources. Technological processes in this intermediate transition are leading to a decrease in primary energy for consumers. Secondary sources of energy are also known since energy suppliers, as they transfer energy in a usable way.

II. Proposed Methodology

The System Block Diagram of Energy Theft Prevention in AMI systems is presented below. The proposed system comprises of two main blocks Data Collector and Power Operator which are connected through (TCP/IP Network). The Data Collector is responsible for communication with the metering nodes & collect energy usage data over RF/Wireless or PLCC mediums. The Power Operator is responsible for generating & maintaining Truly Random Variable Length Public Key, & Machine Addresses of Metering Nodes for generation of metering node specific Private Keys. Apart from secured communication between Metering Nodes, Addition & Deletion of Nodes, Data Collector also checks for energy theft by employing distributed totalization metering & Artificial Intelligence.

Main meter is connected between Power Distribution Transformer & Metering Devices at consumer premises to collaborate data collector and different metering nodes. Whenever any theft detection occurs, ANN analyses the energy consumption reported of the metering nodes as well as the main meter, if there is any theft detection in any metering node it is detected by the ANN & an alert is generated.

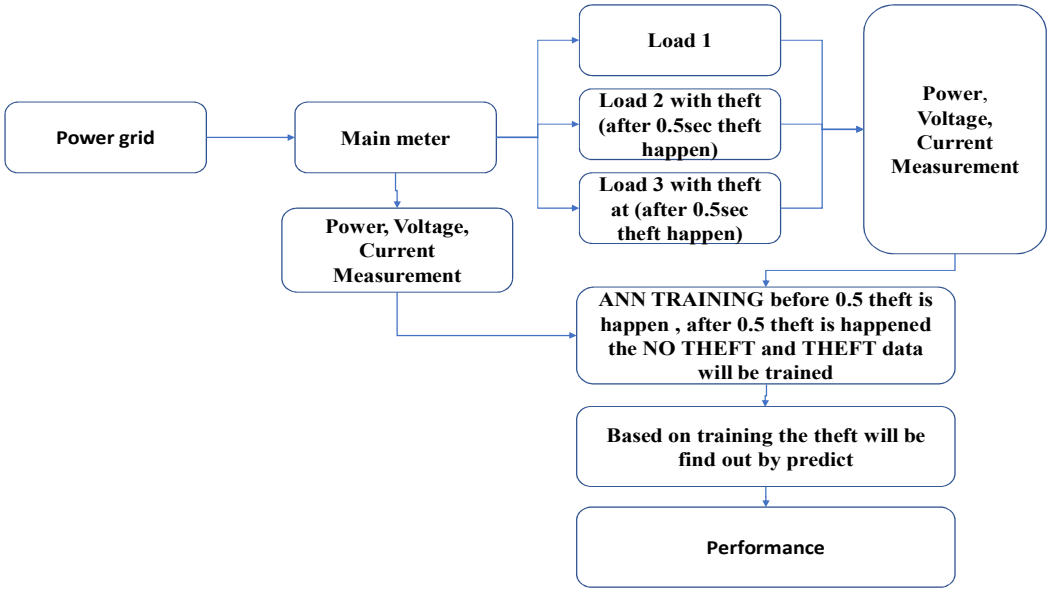

Figure: 1 Block Diagram of System

Thus as proposed Two Tier Security against Energy Theft in AMI Systems has been implemented as described below.

1. Powerful & robust encryption & decryption for communication, truly random variable length key, Real Time Clock randomize device machine adder.

2. Employment of Distributed Totalization Metering In Conjunction with Artificial Intelligence.

A. Neural Network Tool Algorithm & Employed

Neural Network Tool Box

Neural Network ToolboxTM offers functions and applications that cannot be easily modeled with a closed form equation for modeling complex non-linear systems. The Neural Network Toolbox supports regulated education with feed, radio and dynamic networks. It also facilitates uncontrolled learning with independent maps and competitive layers. The toolbox enables neural networks to be designed, trained, visualized and simulated. For applications like data accuracy, pattern recognition, clustering, time-series prediction, and dynamic system modeling and control you can use Neural Network Toolbox. You can spread computation and

data through multi-core processors, GPUs and computer clusters using Parallel Computing ToolboxTM to accelerate the training and manage massive data sets.

Key Features

• Supervised, multi-layered networking networks, radial base, LVQ learning, time delay, autoregressive nonlinear (NARX) and layer-recurrent networking.

Networks that are unsupervised, like autonomous maps and competitive layers.

• Data fitting, pattern recognition and clustering applications · · Parallel processing and GPU support for training acceleration (using Parallel Computing Toolbox)

Pre-processing and post-processing for network education improvement and network performance evaluation − Modular network representation for arbitrary network management and visualisation¨ Simulink ® blocks for neural network construction and evaluation, and control system applications

B. Neural Network Tool Box Function Application

Speech Recognition

Speech plays a significant role in the relationship between human beings. Consequently, it is common to assume programming language interfaces. In the current period, people also need complex languages that are hard to understand and use when they communicate with machines. A easy alternative may be communicating in a speech language that the computer would understand, to ease this communication barrier.

Character Recognition

The general field of Pattern Recognition is a fascinating challenge. For the automatic identification of hand-written characters, letter and number, many neural networks have been created. Following are some ANNs which have been used for character recognition −

- "Multilayer neural networks such as Back propagation neural networks."
- "Neocognitron"

International Journal of Engineering Research Excellence and Applied Science (IJEREAS)
Volume-II (Issue 3) – September 2024 ISSN: 3048-5355

Table: 1 Neural Network Tool Box Function

Sr.No.	FUNCTION NAME	SYNTAX	NARRATION
1.	fitnet	`net = fitnet(hiddenSizes)` `net = fitnet(hiddenSizes,trainFcn)`	"`net = fitnet(hiddenSizes)` returns a function fitting neural network with a hidden layer size of `hiddenSizes`"
2.	train	`trainedNet = train(net,X,T,Xi,Ai,EW)` `[trainedNet,tr] = train(net,X,T,Xi,Ai,EW)`	"This function trains a shallow neural network. For deep learning with convolutional or LSTM neural networks, see train Network"
3.	perform	perform(net,t,y,ew)	"`perform(net,t,y,ew)` takes these arguments, `Net`Neural network"
4.	view	view(az,el) view([az,el])	"The position of the viewer (the viewpoint) determines the orientation of the axes"
5.	plotperform	plotperform(TR)	"`plotperform(TR)` plots error vs. epoch for the training, validation, and test performances of the training record `TR` returned by the function `train`"
6.	plotregression	plotregression(targets,outputs) plotregression(targs1,outs1,'name1',targs2,outs2,'name2',...)	"`plotregression(targets,outputs)` plots the linear regression of `targets` relative to `outputs`"
7.	ploterrhist	ploterrhist(e) ploterrhist(e1,'name1',e2,'name2',...)	"`ploterrhist(e)` plots a histogram of error values `e`. `ploterrhist(e1,'name1',e2,'name2',...)` takes any number of errors and names and plots each pair"

International Journal of Engineering Research Excellence and Applied Science (IJEREAS)

Volume-II (Issue 3) – September 2024 ISSN: 3048-5355

III. Results

Three-phase circuit breaker

Implements a three-phase circuit breaker. When the external switching time mode is selected, a Simulink logical signal is used to control the breaker operation.

- Breaker resistance Ron (Ohm): 0.01
- Snubber resistance Rs (Ohm): 1e6
- Snubber capacitance Cs (F)- inf

Simulink Execution

In this figure we can see our Simulink model during compiling condition.

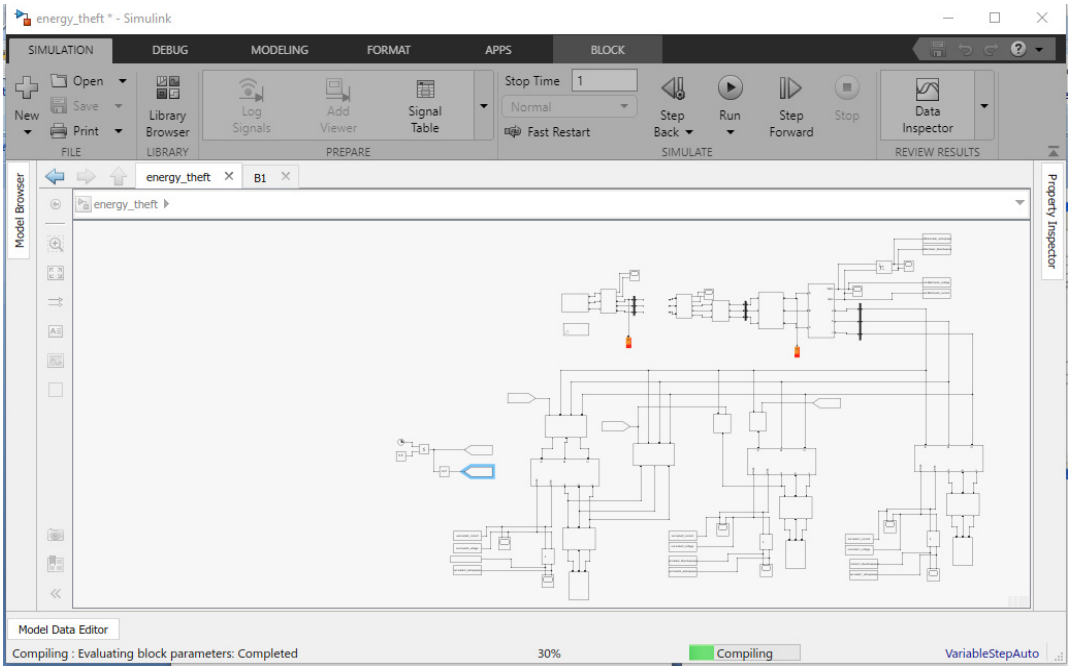

Figure: 2 Start simulation of Simulink model

In this figure we can see our obtained graph of active and reactive power of main meter.

International Journal of Engineering Research Excellence and Applied Science (IJEREAS)

Volume-II (Issue 3) – September 2024 ISSN: 3048-5355

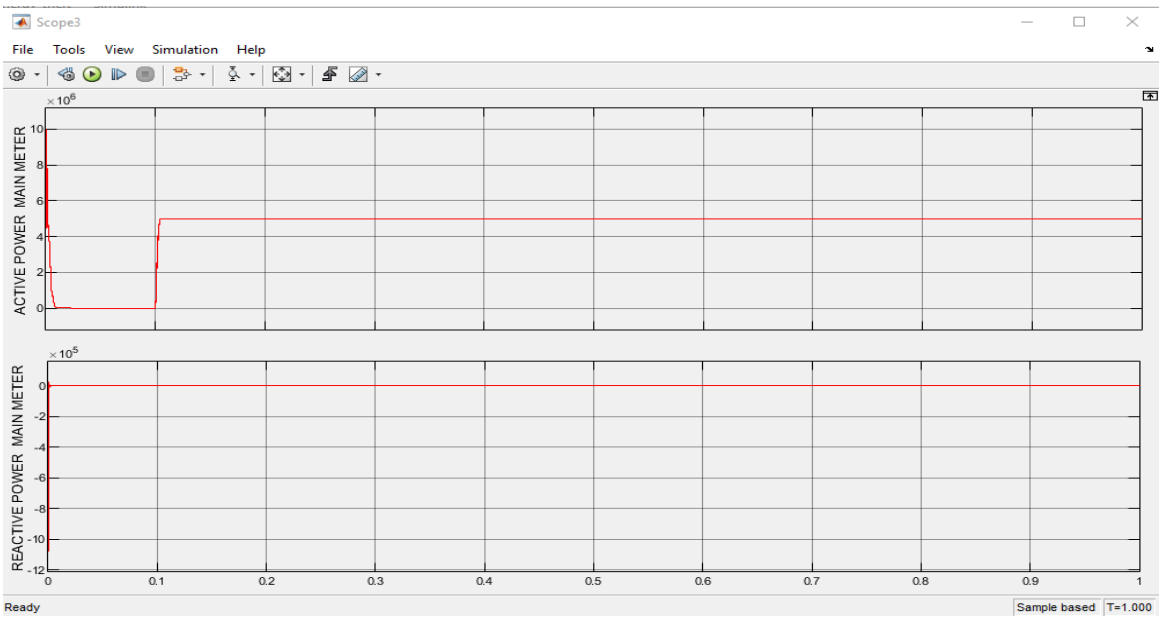

Figure: 3 Active power and reactive power of main meter

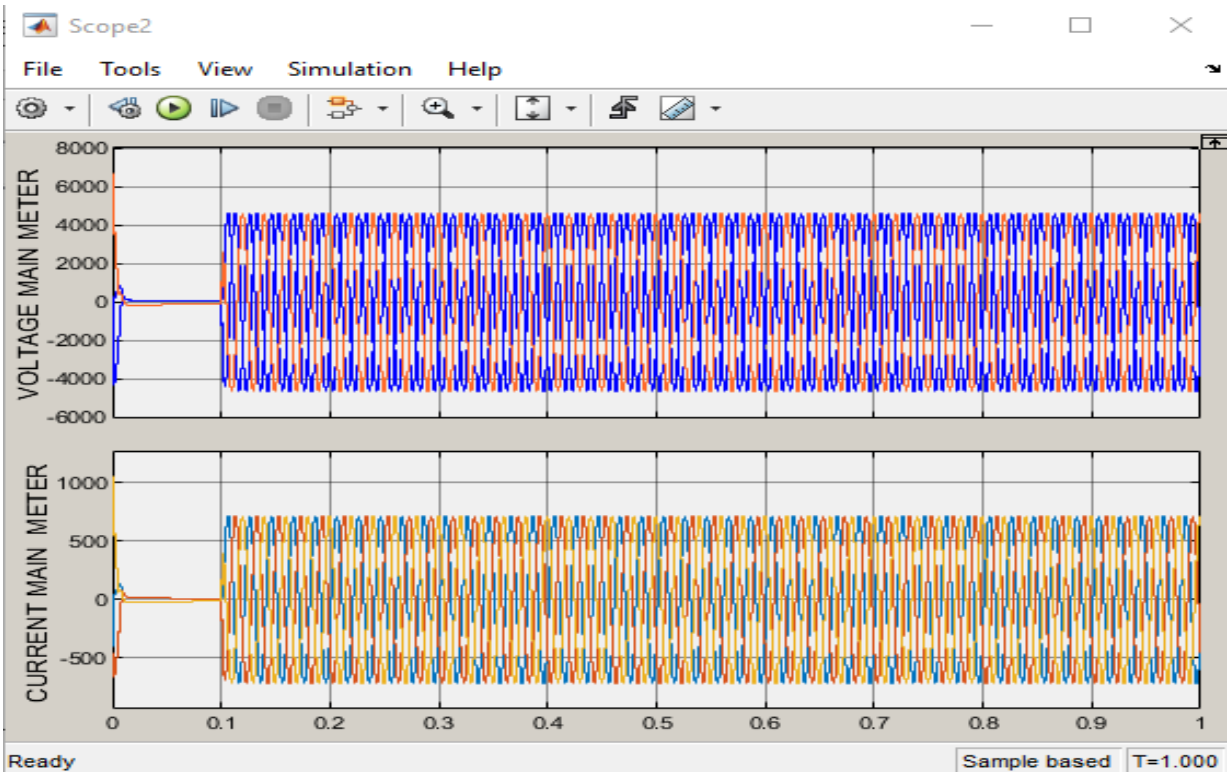

Figure: 4 Current and voltage of main meter

International Journal of Engineering Research Excellence and Applied Science (IJEREAS)

Volume-II (Issue 3) – September 2024 ISSN: 3048-5355

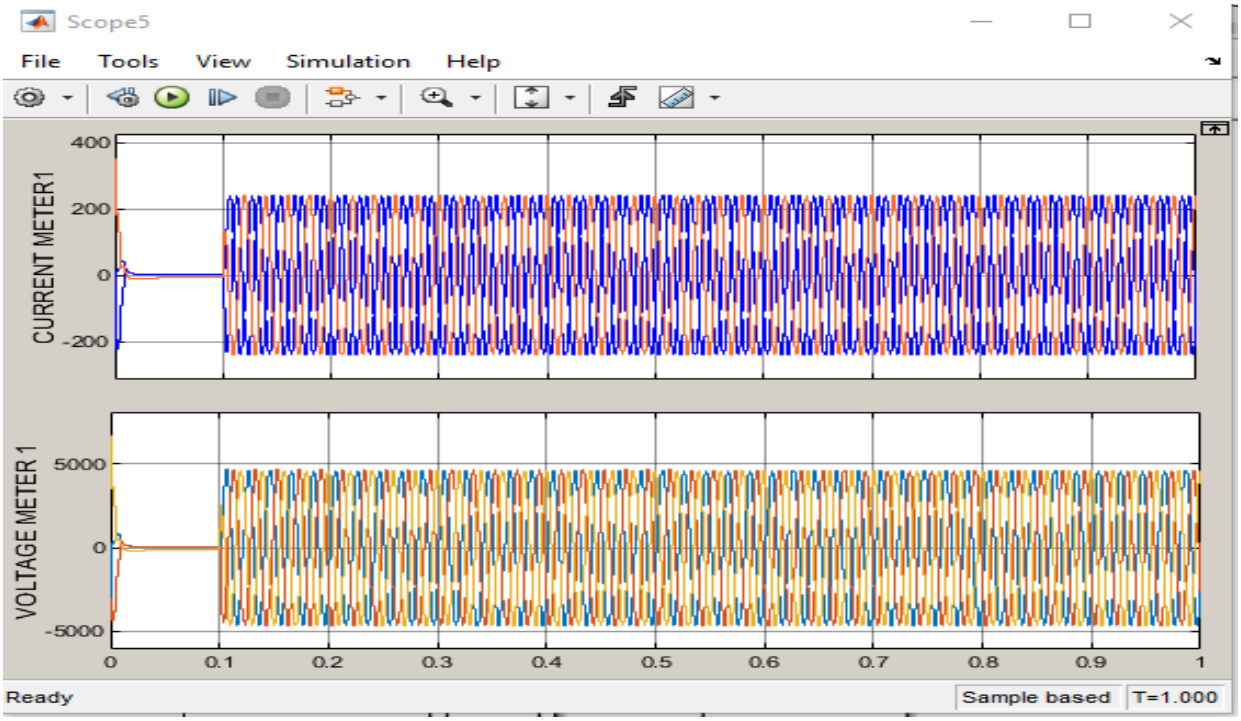

Figure: 5Current andvoltage of meter 1

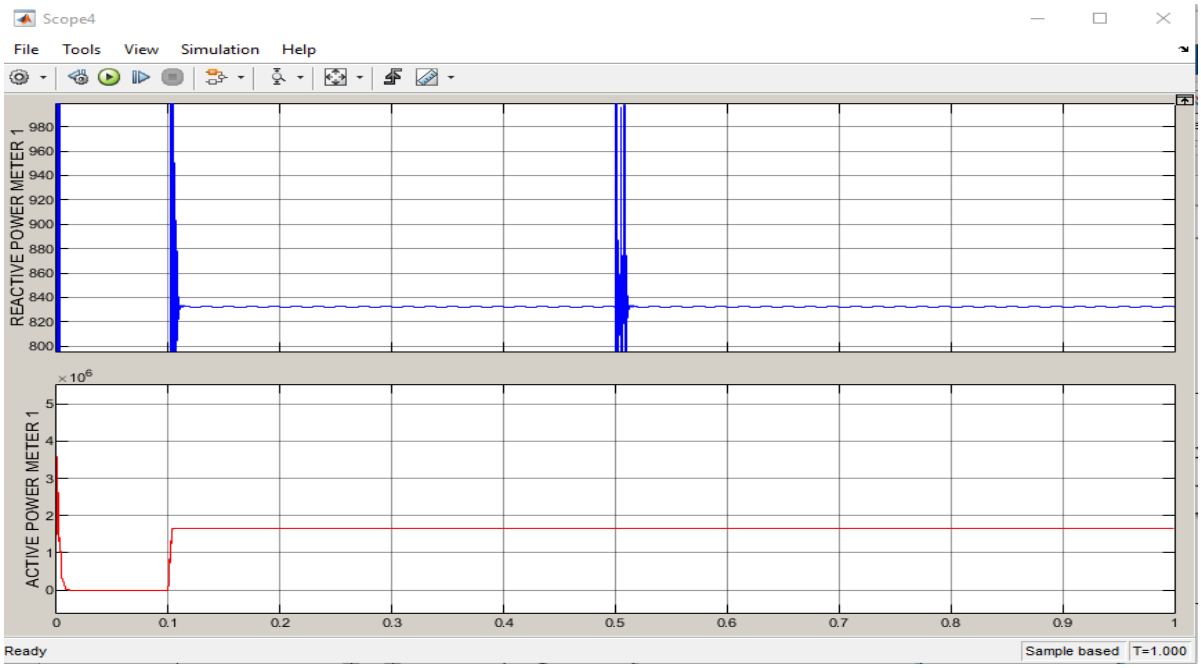

Figure: 6 Active power and reactive power of meter 1

International Journal of Engineering Research Excellence and Applied Science (IJEREAS)

Volume-II (Issue 3) – September 2024 ISSN: 3048-5355

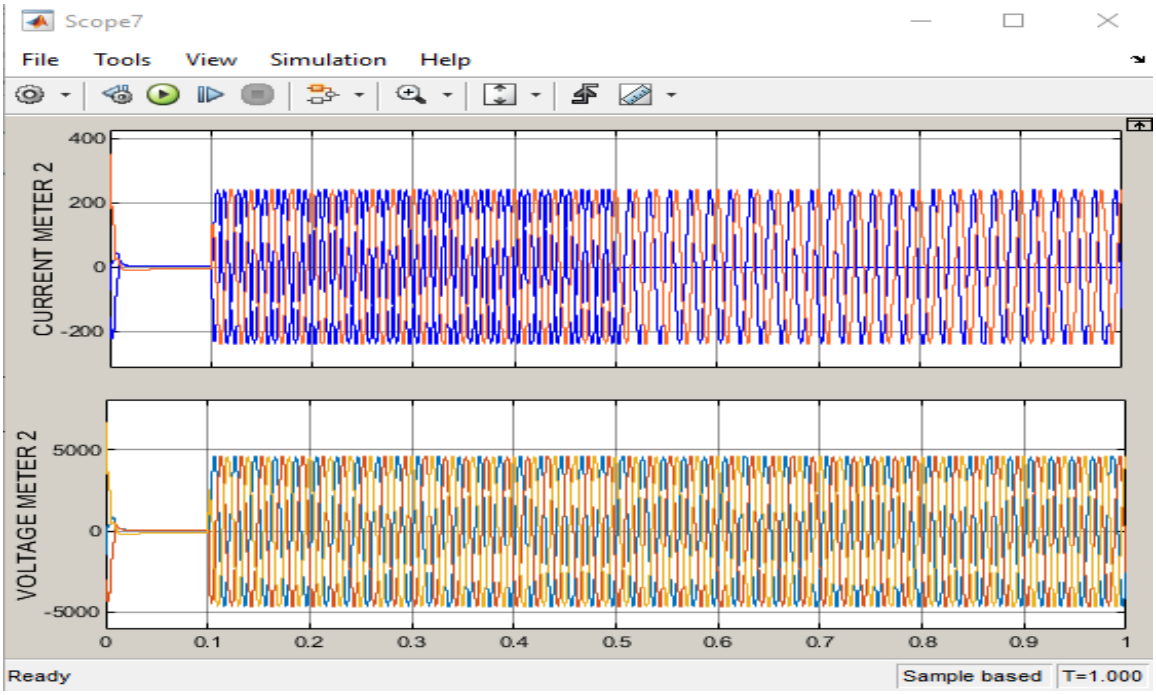

Figure: 7 Current and voltage of meter 2

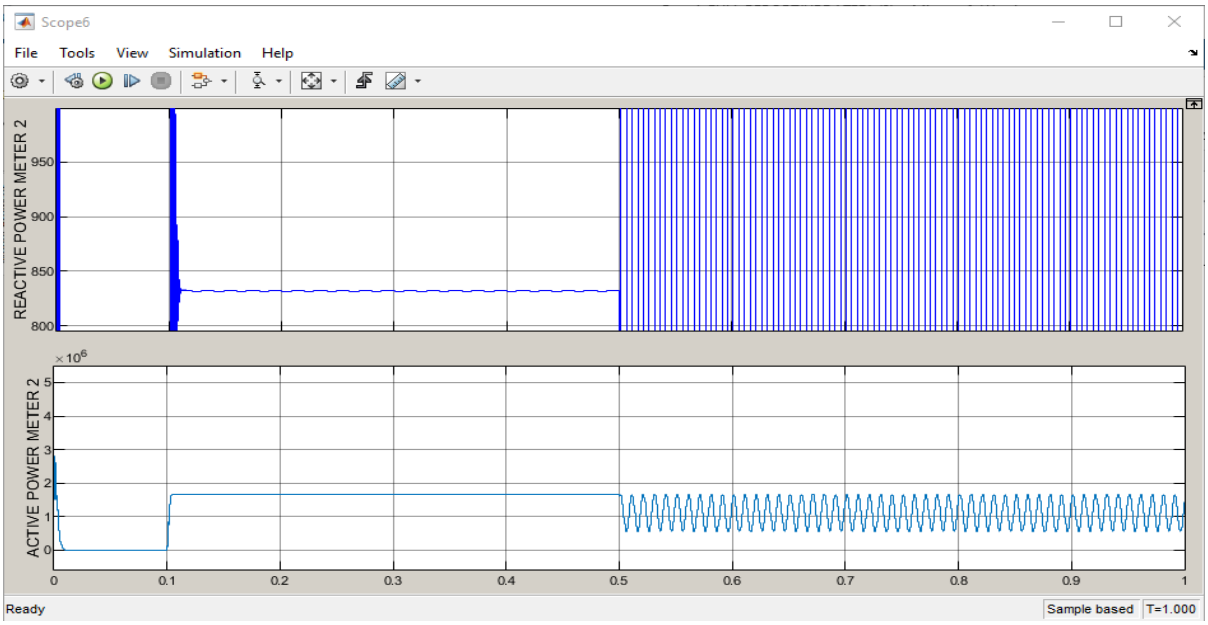

Figure: 8 Active power and reactive power of meter 3

International Journal of Engineering Research Excellence and Applied Science (IJEREAS)

Volume-II (Issue 3) – September 2024 ISSN: 3048-5355

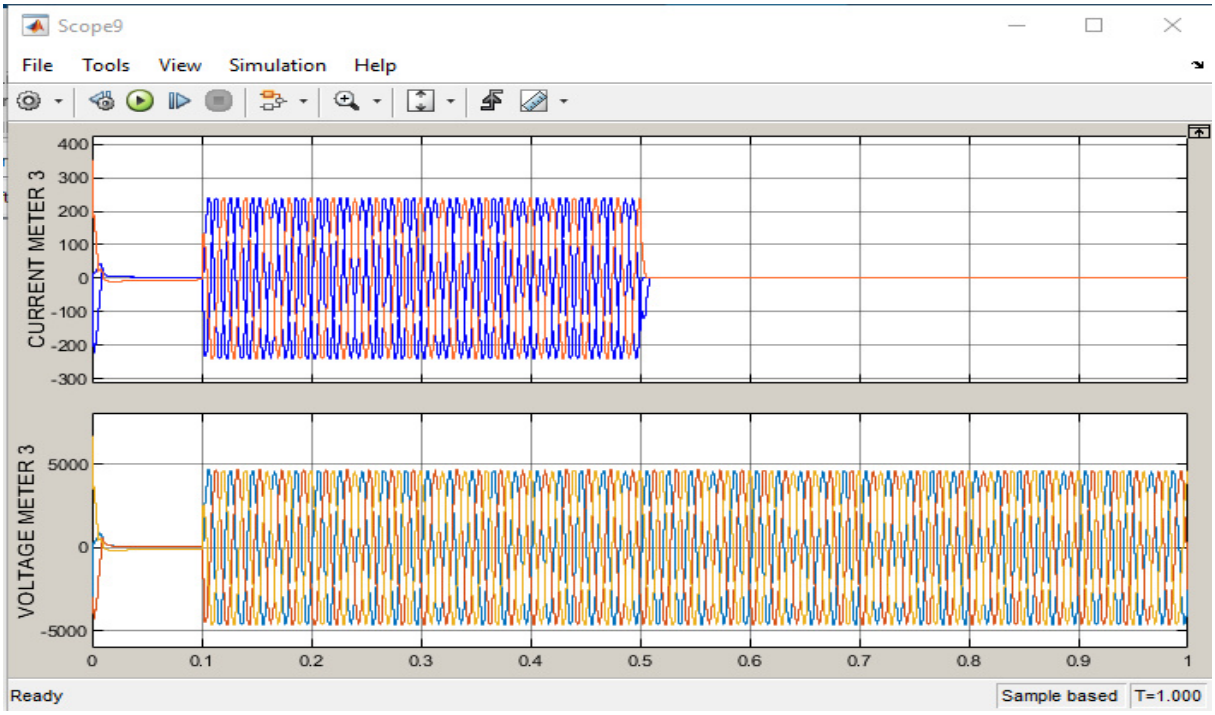

Figure: 9 Current and voltage of meter 3

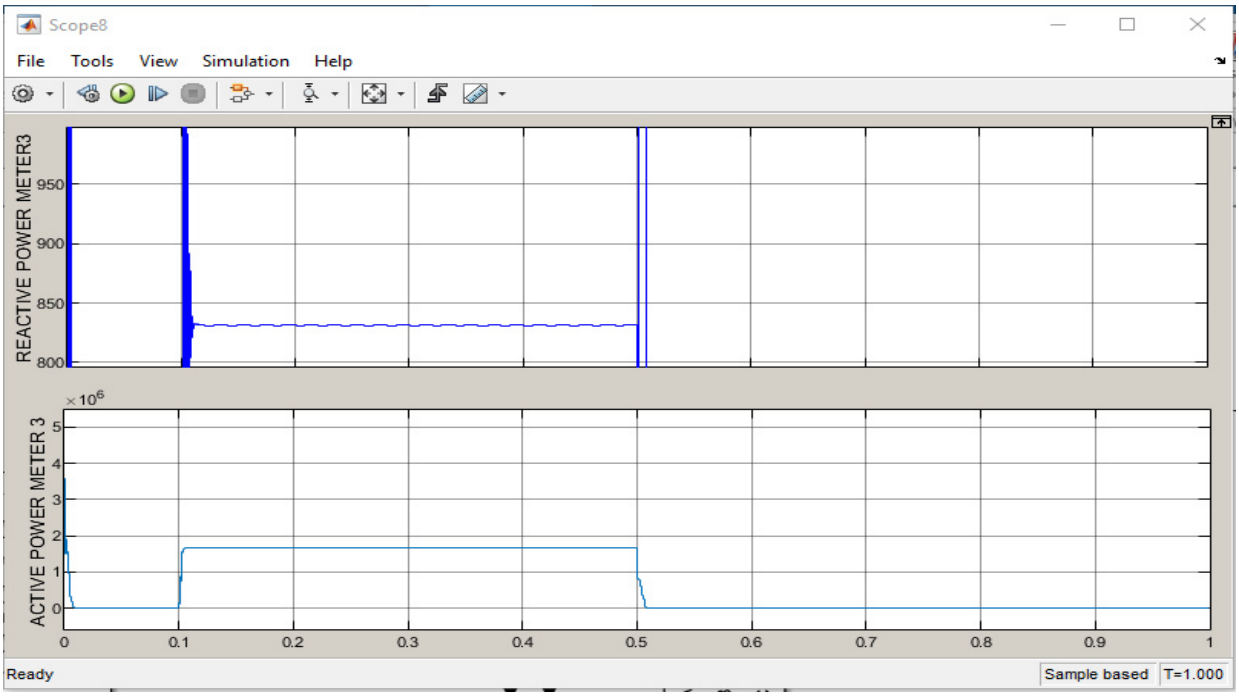

Figure:10 Active power and reactive power of main meter 3

International Journal of Engineering Research Excellence and Applied Science (IJEREAS)

Volume-II (Issue 3) – September 2024 ISSN: 3048-5355

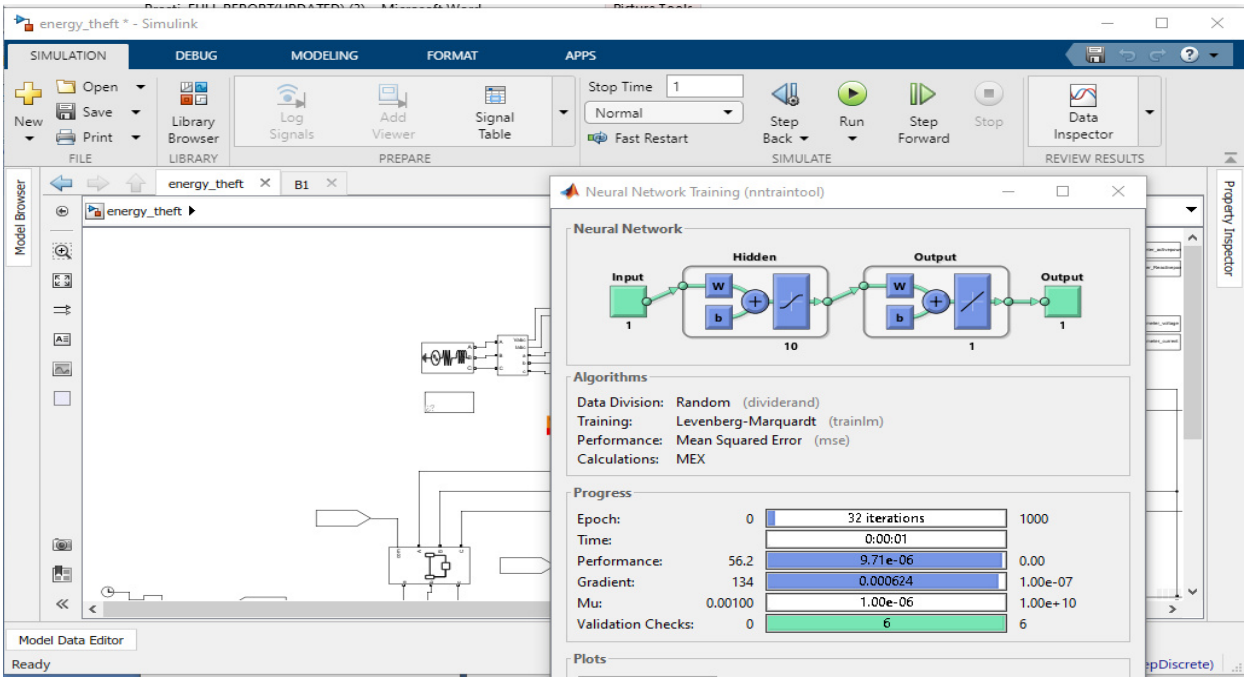

Figure:11 ANN Apply for theft detection

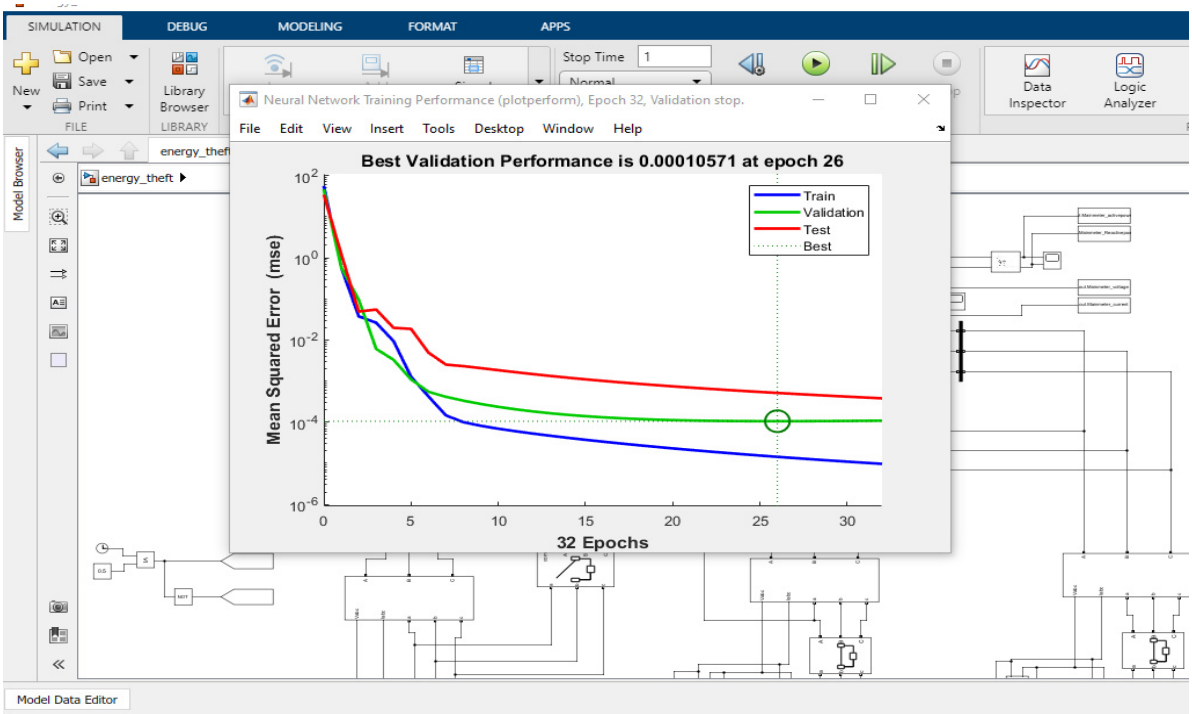

Figure:12 Validation performance of ANN

International Journal of Engineering Research Excellence and Applied Science (IJEREAS)

Volume-II (Issue 3) – September 2024 ISSN: 3048-5355

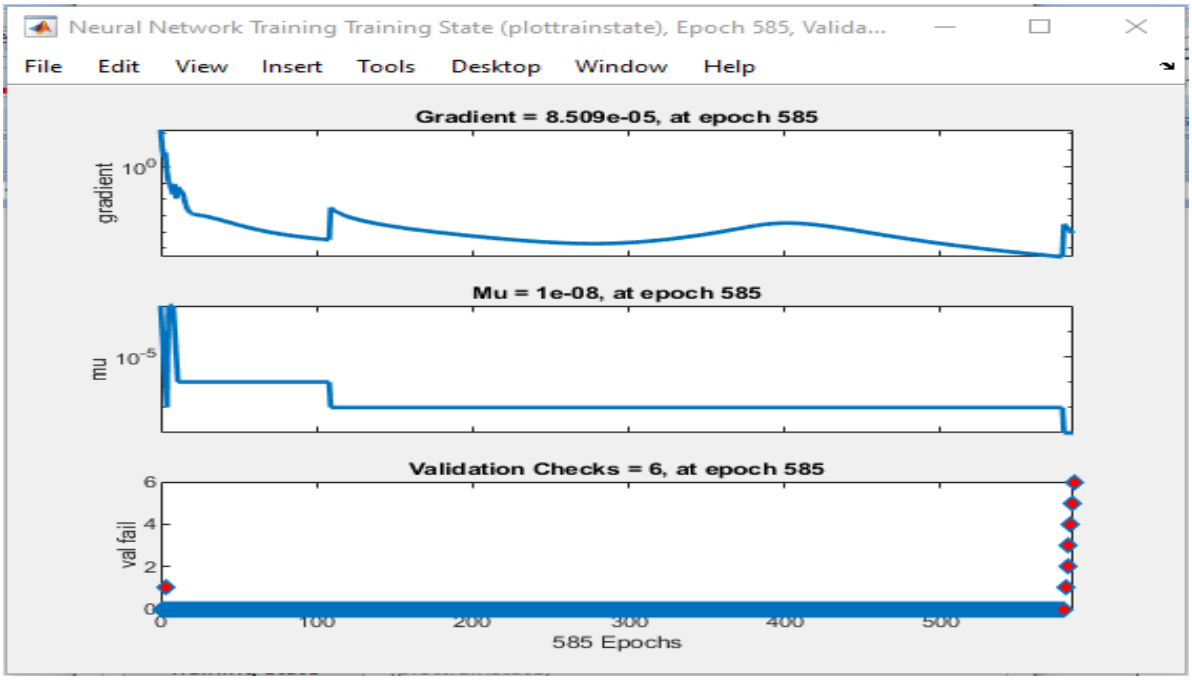

Figure:13 Gradient, Mu,validationcheck, performance of ANN

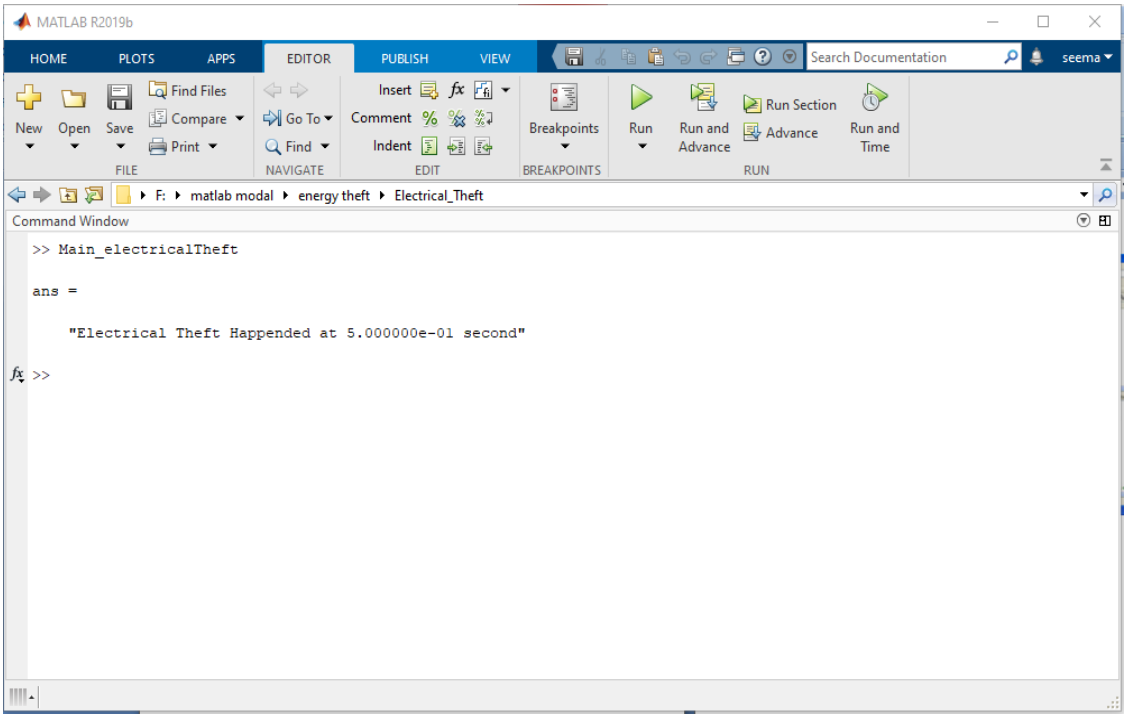

Figure:14 Energy theft detection

These figures showing the results under normal conditions and electrical energy theft conditions in the form of voltage, current, active and reactive power. The meter 3 indicates the electrical energy theft at a time of 0.5 seconds. It means that if there is any electrical theft for more than 0.5 seconds, the proposed system will activate and find the condition of energy theft; if there is energy theft for less than 0.5 seconds, the system will not be activated.

References

1. Jaime Yeckle,Bo Tang " Detection of Electricity Theft in Customer Consumption using Outlier Detection Algorithms " 2018 1st International Conference on Data Intelligence and Security.
2. Rajiv Punmiya and SanghoChoe "Energy theft detection using gradient boosting theft detector with feature engineering-based preprocessing" 2019
3. AbdulrahamanOkino Otuoze1,2 , Mohd Wazir Mustafa1, OlatunjiObalowu Mohammed1,2, Muhammad Salman Saeed1, NazmatToyin Surajudeen-Bakinde2, Sani Salisu1,3 "Electricity theft detection by sources of threats for smart city planning"2019
4. Muhammad Ismail1 , Mostafa Shahin1 , Mostafa F. Shaaban2 , Erchin Serpedin3 , and Khalid Qaraqe1 "Efficient Detection of Electricity Theft Cyber Attacks in AMI Networks" 2018
5. Mahmoud Nabil∗, Muhammad Ismail†, Mohamed Mahmoud∗ , Mostafa Shahin† , Khalid Qaraqe† , and ErchinSerpedin† " Deep Recurrent Electricity Theft Detection in AMI Networks with Random Tuning of Hyper-parameters" 2018.
6. Sandeep Kumar Singh, Ranjan Bose, "Minimizing Energy Theft by Statistical Distance based Theft Detector in AMI" 2018.
7. Sandeep Kumar Singh, Ranjan Bose, AnupamJoshi "Energy Theft Detection in Advanced Metering Infrastructure" 2018.
8. Sandeep Kumar Singh1 , Ranjan Bose2, Anupam Joshi3, "Energy theft detection for AMI using principal component analysis based reconstructed data"2018.
9. Kedi Zheng, QixinChen,Yi Wang, " A Novel Combined Data-Driven Approach for Electricity Theft Detection"2018.

10. Hao Huang, Shan Liu, Katherine Davis, ""Energy Theft Detection Via Artificial Neural Networks" 2018.
11. A.N. Akpolat1*, E. Dursun1, "Advanced Metering Infrastructure (AMI): Smart Meters and New Technologies" 2017.
12. Shan Zhou, Daniel C. Matisoff"Advanced Metering Infrastructure Deployment in theUnited States: The Impact of Polycentric Governanceand Contextual Changes" 2016.
13. Mahshid Delavar1, Sattar Mirzakuchaki2, Mohammad Hassan Ameri3, Javad Mohajeri4, "PUF-based solutions for secure communication in Advanced Metering Infrastructure (AMI)"2016.
14. TawfeeqShawly, Jun Liu, Nathan Burow, Saurabh Bagchi,Robin Berthier, Rakesh B. Bobba "A Risk Assessment Tool for Advanced Metering Infrastructures"2014.
15. I S Jha,SubirSen,Vineeta Agarwal "Advanced Metering Infrastructure Analytics -A Case Study" 2014.
16. A. Bouallaga1,2,3, R. Kadri1,4, V. Albinet1,3, A. Davigny1,3, F. Colas1,4, V. Courtecuisse5, A. Merdassi6, X. Guillaud1,7, B. Robyns1,3, "advanced metering infrastructure for real-time coordination of renewable energy and electric vehicles charging in distribution grid" 2014.
17. Robin Berthier and William H. Sanders, "Monitoring Advanced Metering Infrastructures with Amilyzer"2013.