International Journal for Rapid Research in Engineering Technology & Applied Science
Vol IX Issue I January 2023
ISSN Online: - (2455-4723)

Artificial Neural Network Techniques for Energy Theft Detection in AMI

Diwakar Agrawal, Asst. Prof. Mamta Devi Sharma, Associate Prof. Ravi Kumar Hada
Dept.of Electrical Engineering, Global Institute Of Technology , Jaipur
Diwakaragrawal750@Gmail.Com, Mamta.Sharma@Gitjaipur.Com, Ravi.Hada@Gitjaipur.Com

Abstract: The success of using renewable energy sources is driving the biggest change to the power grid in a long time. This change is happening from centralised control of the electricity supply to an infrastructure that is smart and not centralised. On the other hand, when different parts of a power grid become more connected to each other, these parts become more vulnerable to cyber attacks, fraud, and software problems. In recent years, a lot of progress has been made in cyber-physical security, like the ability to detect physical tampering, as well as more traditional information security solutions, like encryption. Traditional information security solutions, on the other hand, can't handle all of the problems that cyber threats pose, because digital electricity meters can have software bugs and hardware problems. As a result of making electricity meters digital, many security problems that had been solved in the past, such as electricity theft, have come back as IT problems. For these new problems, we need new ways to find out about them that are based on data analysis, machine learning, and making predictions. Rapid changes in statistical methods, which are similar to techniques used in machine learning, have led to a rise in interest in ideas that can model, predict, or extract load information, such as that provided by a smart meter, to spot early signs of tampering. Anomaly Detection Systems can find tampering techniques by looking at statistical deviations from a normal behaviour that has already been set. This method is widely accepted as a good way to find abuse patterns that were not known before. This study gives a number of anomaly detection algorithms that use power measurements to make it easier to find tampered electricity meters early on. Time series prediction and probabilistic models have been used to create and test algorithms with detection rates of more than 90%. Several things were taken into account in this process. One of the things that was added was the study of complex threads, such as behaviors that are similar to each other. Other contributions include an analysis of the different kinds of data that are already available, the creation of metrics and methods of aggregation that make it easier to find specific patterns, and so on. This work helps us learn more about the important features and typical behaviour of electric load data, as well as find evidence of tampering and, more specifically, energy theft.

Keywords: **(Advanced Metering Infrastructure), Distributed Totalization Metering, Artificial Intelligence, Cryptography**

I Introduction

The internet of things (IoT) and artificial intelligence (AI) are two cornerstone technologies enabling smart cities, and have been interacting with each other into an organic ecosystem. In the smart grid, smart meters and various sensors are widely used to increase the two-way communication capability. Combined with the advanced metering infrastructure (AMI), they enable energy companies to obtain real-time voltage, current, active power, reactive power, energy usage and other measurements from the smart meters deployed at user homes [1],[2]. Recently, smart meters are shown to be vulnerable to cyber physical attacks in the smart grid due to their insecure and distributed network and physical environment [3]–[5]. One serious threat is energy theft attacks, which cost more than 25 billion dollars every year to the energy companies [6]. Such an attack aims to pay less by attacking user meters to tamper with the energy usage sent to energy company. Another severe threat is privacy violation. As smart meters collect real-time energy usage that may reveal user's habits and behavior at home, the user privacy concern will be raised if the collected data is not well protected [7]. For example, if the user's daily energy consumption is low, it may imply that the user is not at home [8]. Thus, such privacysensitive information must be protected from unauthorized access. To disclose the usage for theft detection and to hide the usage for privacy preservation are conflicting goals. We aim to address both theft detection and privacy preservation in this work. A number of works have been conducted for energy theft detection in the smart grid. Some used the classificationbased support vector machine (SVM) technique to classify the normal and attack samples from the energy usage database [9]–[11]. In addition, matrix decomposition [12], linear regression [13] and state estimation [14] can be used to analyze the data for energy theft detection. However, these approaches cannot be applied to cases with massive amounts of data. [15] proposed a wide and deep convolutional neural network model to analyze energy theft behavior of individual users. In our paper, we additionally study the energy theft

behavior from a user group perspective, i.e., a group of users may exhibit similar energy consumption patterns due to local activities for a certain period of time. We plan to exploit this behavior characteristic to more accurately detect the sophisticated attacker. Most theft detection schemes require the access of the original smart meter data that are highly user privacy-sensitive. Although privacy-preserving techniques have been introduced in the smart grid communication [16]–[18], they are rarely proposed in the context of theft detection. One work is developed under an assumption that the normal energy output of a photovoltaic device is similar to that from a geographical region [19]. With the homomorphic encryption technique, the calculation of the distance of two vectors is conducted while the vectors (energy data) are not disclosed to unauthorized entities. However, the proposed work detects energy theft from the perspective of generators; it cannot solve the diversity of theft. For example, if a user's meter is tampered with usage by external illegal attack, it cannot be detect. In addition, [20] proposed a privacy-preserving state estimation scheme based on two loosely coupled filters to detect energy theft attacks and achieve privacy preservation. But it is not conformed the actual grid operation, because it protects privacy by sending residual rather than user usage, so the smart grid cannot be dispatched and paid for bills.

II RELATED WORK

The Advanced Metering Infrastructure, also known as AMI, is a crucial part of the smart grid that is responsible fOr measuring and analyzing data on customers' energy consumption. The development of new information and communication technologies made it feasible to construct this network, which ultimately led to the network's expansion. However, the use of these technologies resulted in the emergence of brand new challenges at the AMI. One of these is something known as "electric robbery," which has emerged as a big issue for traditional energy networks all across the world. In order to find a solution to these problems, a thorough examination of data sets concerning the consumption of power is being carried out. The use of machine learning and data mining technologies is one of the more traditional strategies for identifying intruders. In this study, we investigate whether or not it would be possible to use outliers to improve AMI protection by detecting illegal use of electricity. On real data, we evaluate the results produced by a variety of various external detection techniques (consumer energy usage). The findings demonstrate how practicable it is to employ outliers algorithms in the protection of AMI and how effective it is to apply these strategies in robbery data sets. [Citation needed] [1].This letter provides a predictor of the Smart Grids energy theft based on the three newest GBCs: extreme grade boosts, categorical boosts (CatBoost), and light gradient boosts. The following gradient is used for the smart grid energy theft recognition (LightGBM). Most current ML algorithms concentrate on the finest tuning of the hyper parameters in the classification system. Our ML algorithm, GBTD, is designed to improve detection efficiency and time complexity through the use of feature engineering preprocessing. By generating storage features such as standard deviation, mean, minimal, and maximum value of daily electricity use, the GBTD increases both the detection rate (DR) and false positive rate (FPR). GBTD also reduces the complexity of the classifier using weighted feature-import extraction techniques (WFI). The realistic implementation of the proposed ML for robbery detection was emphasized by reducing FPRs and data storage and improving the complexity of GBTD classification times. This letter also proposes the imitation of the real world theft patterns and to use the dataset for an assessment of the number of the algorithm proposed to update the current robbery in six cases. [2]

The worldwide focus of smart city implementation and deployment is obviously energy efficiencies but the preparation of smart grid vulnerability threatens to undermine smart grids (SGs). Adversaries launch attacks for different reasons; however, SG installations and thus energy conservation are seriously concerned with the rising threat of electricity theft. Intelligent electricity meter installations across advanced electricity metering infrastructure provide exciting solutions and greater potential as they provide sufficient data for analytical lessons to achieve constructive action against different cyber attacks. The first phase in such preventive steps to curb electrical stealing, this study indicates the origins of risks. It offers a mechanism to track, recognize and curb risks based on electricity theft factors in a clever utilities network. These symptoms are mainly concentrated in the proposed system on the risks listed that indicate the potential incidence of electric theft to prevent robbery. This study offers smart city planners a useful background in developing a more dependable, robust and safe energy management system that a sustainable city needs. [3]

III PROPOSED SYSTEM

Modern power grids are able to enable two-way communication between utilities and their customers for matters pertaining to the generation and consumption of electricity thanks to the use of advanced metering infrastructure (AMI) and an effective communication network. This function gives utilities a better perspective of their customers' electricity use, which in turn helps

utilities better schedule the power generation at the appropriate times to avoid wasting resources. Additionally, the two-way communication is an essential component of the business relationship that exists between the utilities and their respective clients. By doing so, the utilities can encourage their customers to use electricity in a more cost-effective manner by providing them with a real-time electricity rate, which has the potential to bring the overall price of electricity down. However, this application faces a significant challenge in the form of energy theft. This problem arises from the fact that energy theft can lead to erroneous meter readings, which in turn can result in financial loss for utility providers and their customers. Because of it, each year several millions of dollars are thrown away. In addition to this, the theft of electricity can also result in concerns with the stability and safety of power grids. As a result, rectifying the issue of energy theft in power systems is both extremely vital and necessary. Because of AMI, utility companies now have significantly more data than in the past on the energy usage of their end users. This presents a difficulty for the utility companies in managing the vast number of data, but it also presents chances for the detection of energy theft. The purpose of this thesis is to offer an approach to the detection of energy theft using artificial neural networks (ANNs). In order to train ANNs with this approach, a significant amount of historical data is utilized. The trained ANNs are able to identify instances of energy theft using the data that is received.

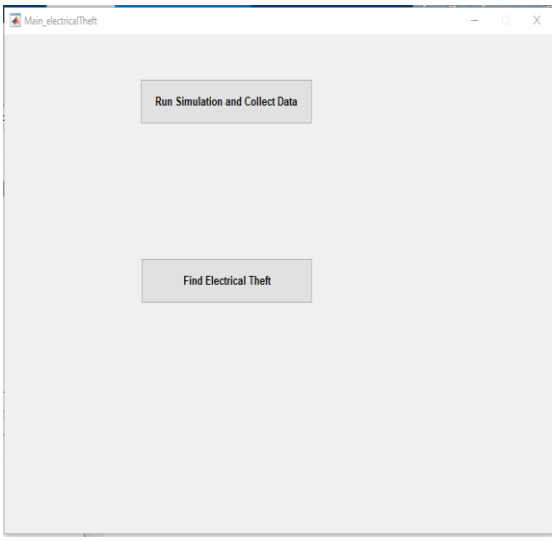

Fig 1 simulation GUI window.

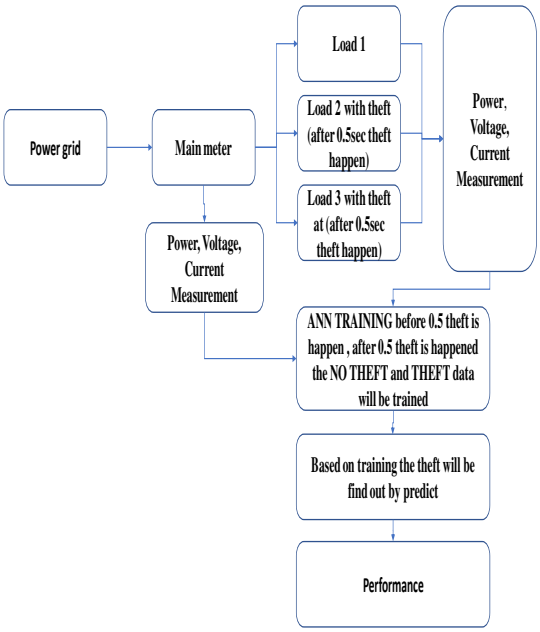

Figure: 2 Block Diagram of System

System Block Diagram:

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 .

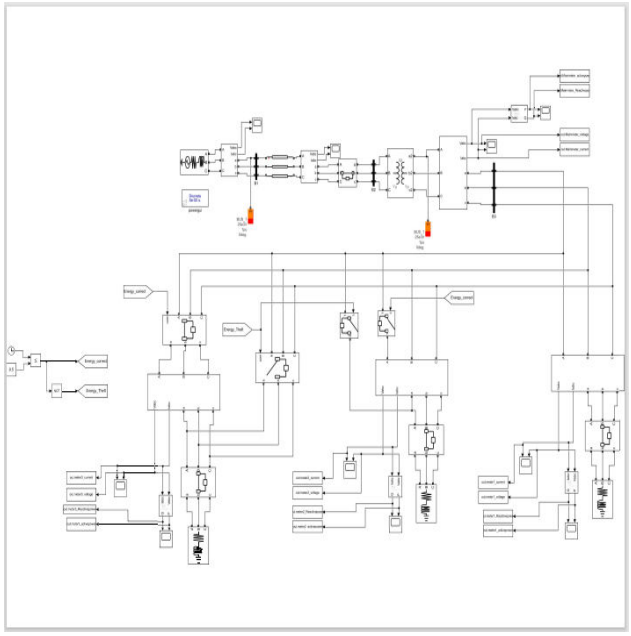

Figure 3 Simulink Model.

IV. SYSTEM PARAMETERS

Three-phase voltage source in series with RL branch.

- Phase-to-phase voltage (Vrms)-- 25e3
- Frequency (Hz)-50
- Source resistance (Ohms)- 0.8929
- Source inductance (H)- 16.58e-3
- Base voltage (Vrms ph-ph)-- 25e3

Three-phase transformer model

This model of a three-phase transformer demonstrates how windings on distinct phases of a three-limb or five-limb core can be inductively coupled together to make a connection with one another. In addition to that, it enables you to model a three-phase transformer by breaking it down into its component single-phase transformers (no coupling between phases). The R L parameters of a transformer can be determined by conducting tests in positive and zero order with no load and short circuits, respectively. The model of the transformer consists of six connected windings regardless of whether the "Three-limb or five-limb" core type is selected. In every other case, it is represented by three sets of two connected windings (Z0=Z1)

- Pnom (VA) and Fnom (Hz) stand for nominal power and frequency. — [100e3, 50]
- Nominal line-line voltages [V1, V2] (Vrms)— [2400, 600]
- Winding resistances [R1 and R2] (pu): [0.01, 0 .01]
- Positive-sequence no-load losses (W)- 1000
- Positive-sequence short-circuit reactance X12 (pu) = 0.06. Zero-sequence no-load excitation current with Delta windings open (% of Inom) = 100.
- Zero-sequence no-load losses with Delta windings open (W)
- Zero-sequence short-circuit reactance X12 (pu)- 0.03

2.Circuit breaker –

Circuit breaker A circuit breaker is a mechanical switch that trips in the event that a fault current flows through it. This protects the circuit from the potential harm that the fault current could do. As soon as it detects a significant increase in the amount of current being drawn, whether from overloading or a short circuit, it immediately breaks the circuit. In addition to this, it has the ability to manually break the circuit open in order to perform maintenance or clear a fault. It is able to securely seal and open a circuit in order to prevent damage to it.

Three-phase circuit breaker

- Utilizes a breaker capable of interrupting all three phases of electricity. The breaker is managed via a Simulink logical signal in external switching time mode.
- Breaker resistance Ron (Ohm): 0.01
- Snubber resistance Rs (Ohm): 1e6
- Snubber capacitance Cs (F)- inf

3. Simulink Execution

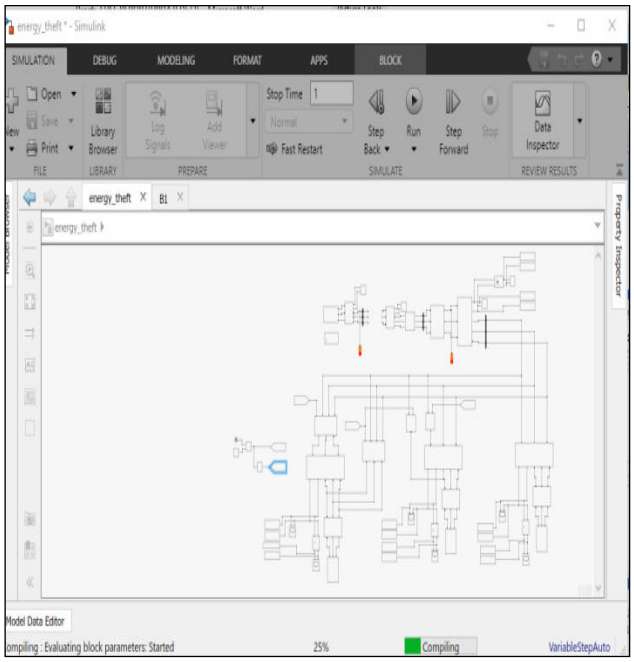

Figure 4.Simulink Model Opened.

In this figure we can see our simulink model

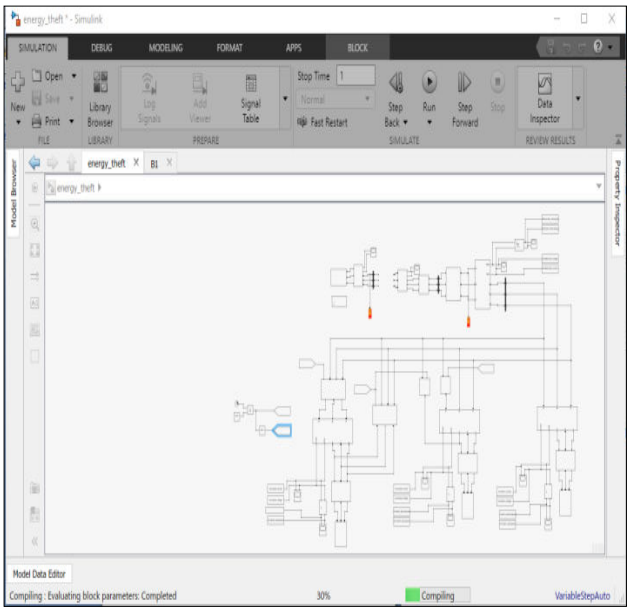

Figure 5 Start Simulation of Simulink Model

In this figure we can see our simulation of simulink model is start.

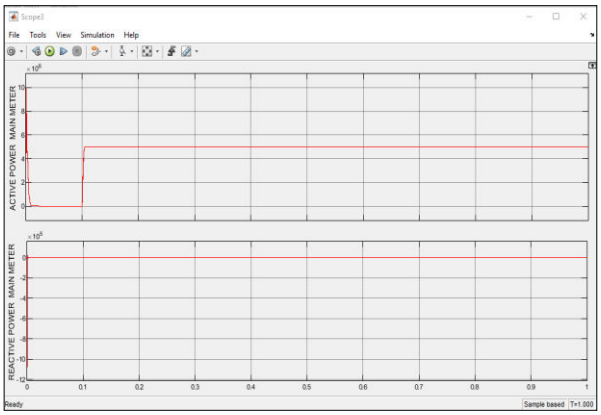

Fig 6 active power and reactive power of main meter

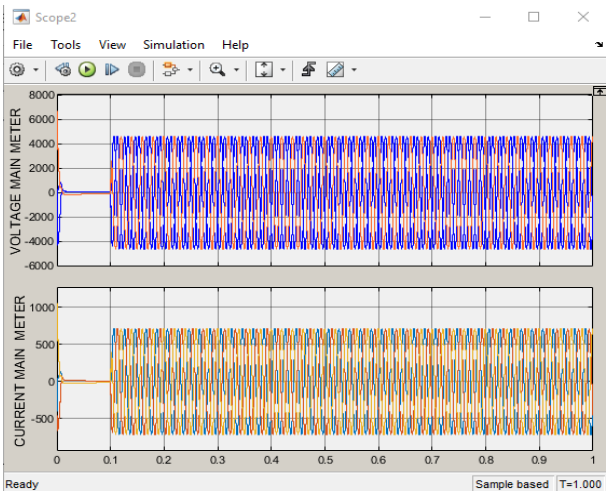

Fig 7.current and voltage of main meter

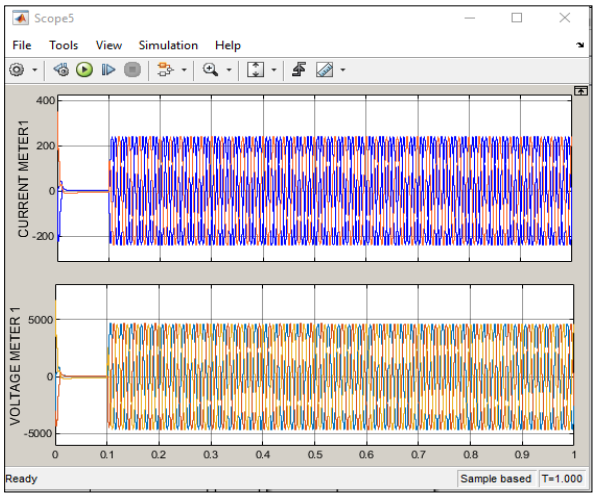

Fig 8 current and voltage of meter 1.

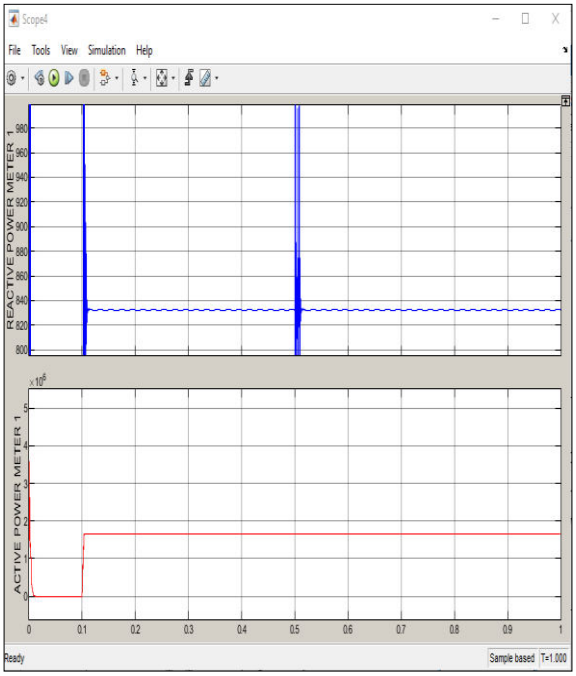

Fig 9 active power and reactive power of meter 1

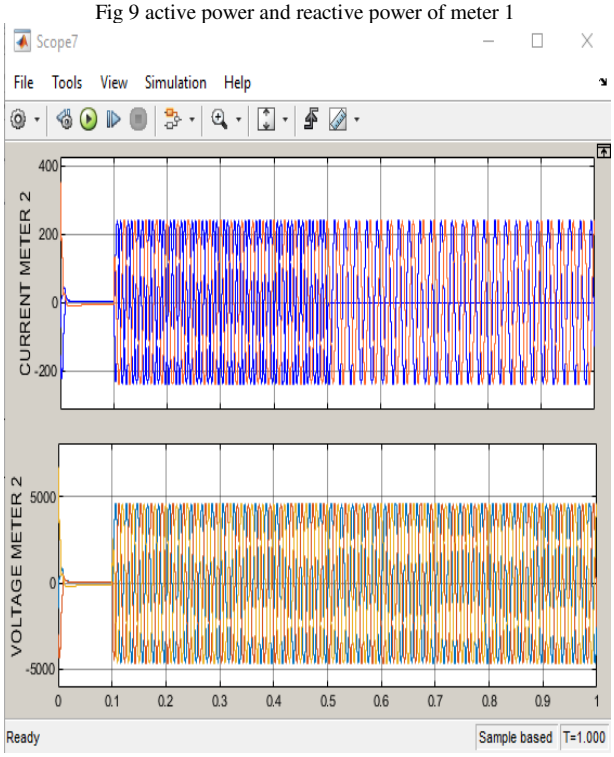

Fig 10.current and voltage of meter 2

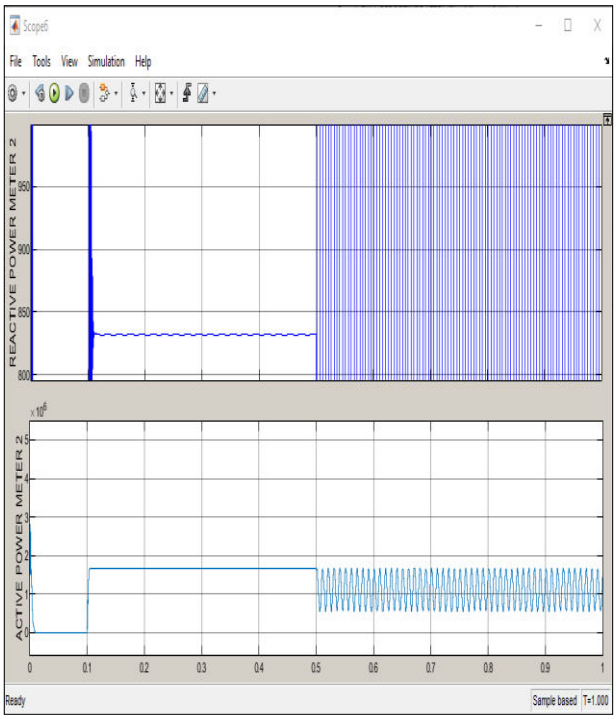

Fig 11 active power and reactive power of meter 3

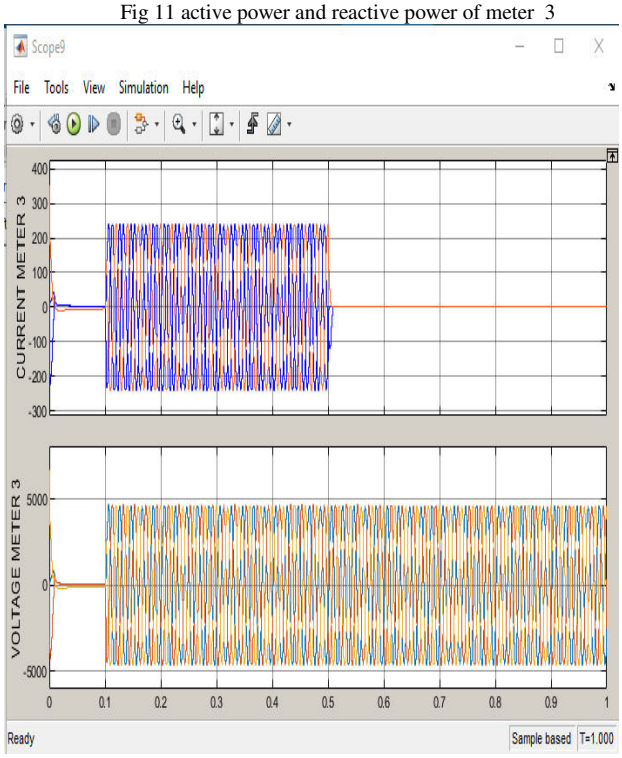

Fig 12.current and voltage of meter 3

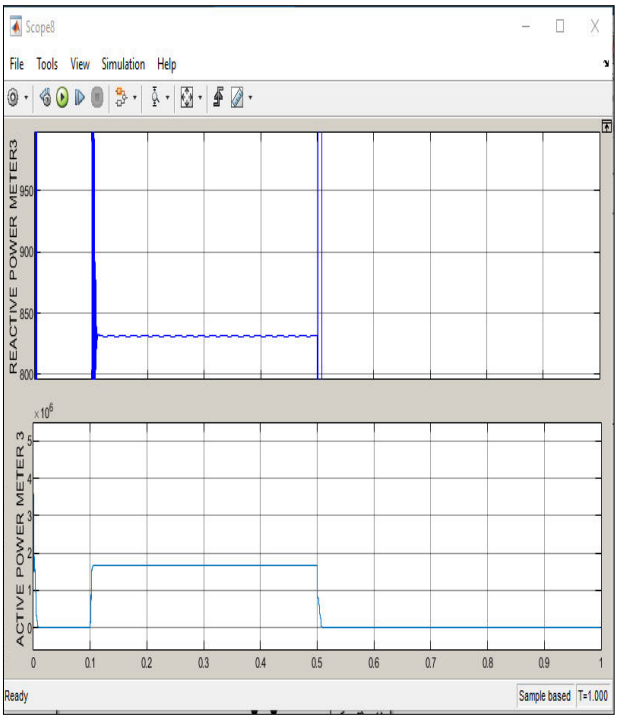

Fig 13 active power and reactive power of main meter 3.

Artificial Neural Networks (Anns) -The ANNs can be thought of as a hierarchical network of interconnected "basic neurons" whose topologies are derived from biological systems. It is not necessary to have a knowledge base to train an artificial neural network (ANN) because ANNs can learn to reason on their own from a given dataset [15]. On the other hand, feedback architecture is feasible as well. The topology of a two-layer feed-forward network is shown in Figure 2. There are clearly three distinct layers: the input layer, the hidden layer, and the output layer, albeit there may be more than one hidden layer depending on the circumstances.

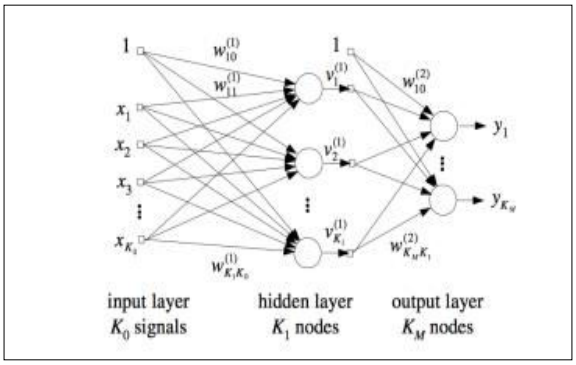

Fig 14 artificial neural networks (anns).

Ann Layer Input

- active_pow1(1) = output.Mainmeter_activepower;
- active_pow1(2) = output.meter1_activepowe
- active_pow1(3) = output.meter2_activepower
- active_pow1(4) = output.meter3_activepower
- reactive_pow1(1) = output.Mainmeter_Reactivepower;
- reactive_pow1(2) = output.meter1_Reactivepower;
- reactive_pow1(3) = output.meter2_Reactivepower;
- reactive_pow1(4) = output.meter3_Reactivepower;
- active_pow = active_pow1(:,1) - (active_pow1(:,2)+active_pow1(:,3)+active_pow1(:,4))
- reactive_pow = reactive_pow1(:,1) - (reactive_pow1(:,2)+reactive_pow1(:,3)+reactive_pow 1(:,4))
- [active_pow1,t] = simplefit_dataset
- net1 = feedforwardnet(10)
- [net1,tr1] = train(net1,active_pow1,t)
- if (mean(active_pow)>0)
- time_out1= (find(active_pow <3000));
- sprintf("Electrical Theft Happended at %s second",time_out(time_out1(end)))
- end

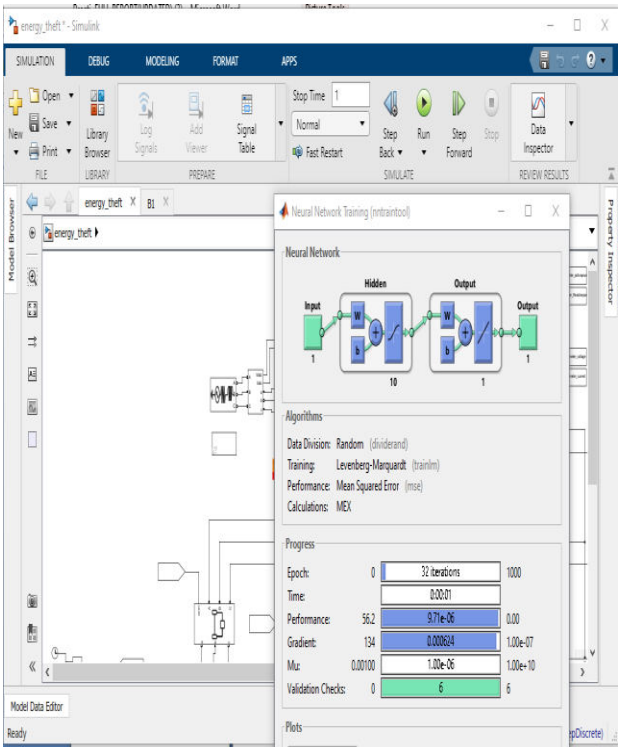

Figure: 15 ANN Apply for theft detection

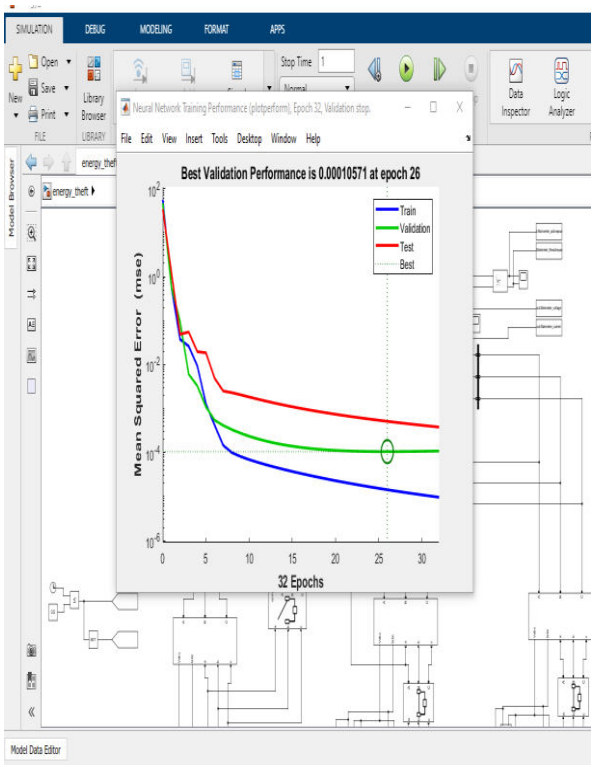

Figure: 16 validation performance of ANN

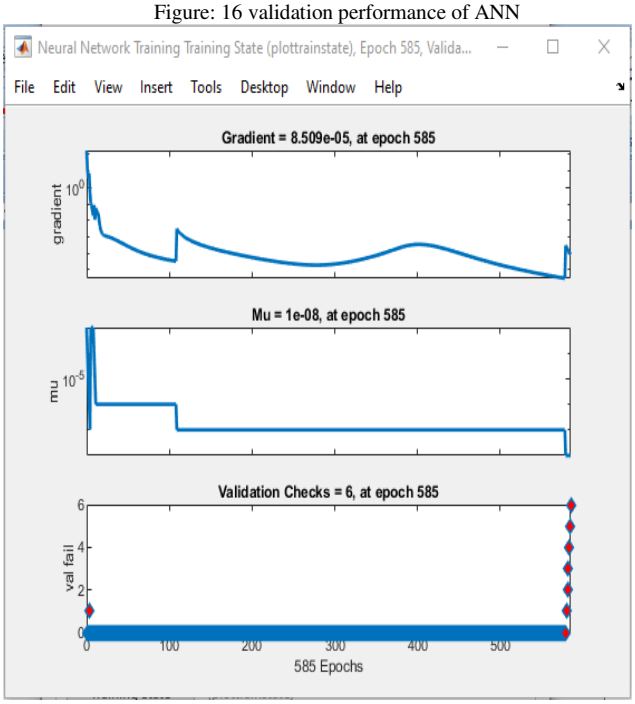

Figure: 17 gradiant,Mu,validationcheck , performance of ANN

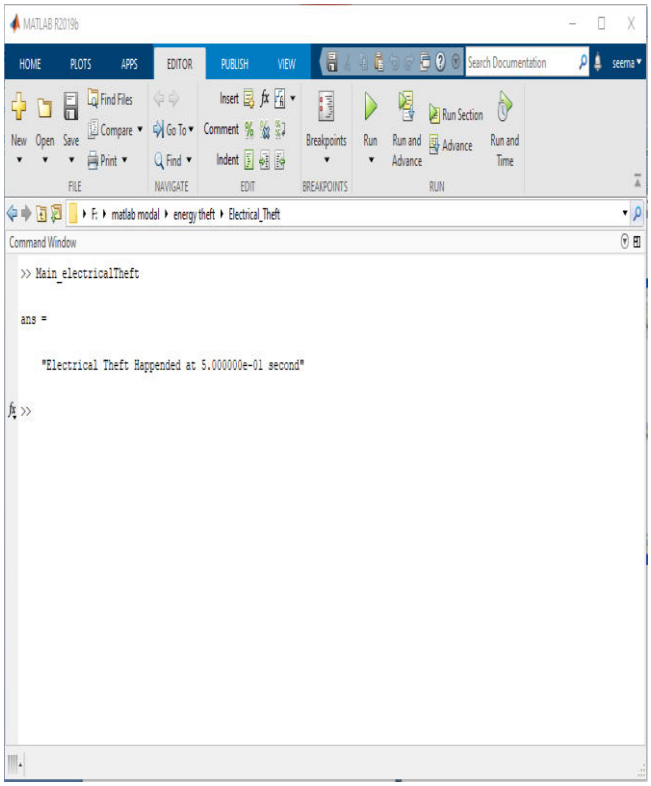

Fig.18 energy theft detection

IV Conclusions

To detect any kind of theft whether conventional or data attack, distributed totalization metering is employed in conjunction with artificial intelligence. In distributed totalization metering is employed in conjunction with Artificial Intelligence. In distributed totalization metering, a energy company owned main meter is placed at distribution end (feeder/distribution transformer) before preventing electricity at consumers premises. In theory, the sum of all the meters at consumer premises fed by that particular distribution and should be equal to the reading of main meter. However practically, there may be some difference due to T&D (Transmission & Distribution) losses, load fluctuations, power factor issues, calibration issues etc. Here artificial intelligence comes into play, which monitors the reading of the main meter as well as the consumer meters, & gets trained during normal operation, whenever energy theft occurs, & accumulates, artificial intelligence detects the anomaly & raises on alert for energy theft , so that consumer premises, feed by that distribution end can be inspected.

Energy is the life line of modern world, no industries or household is independent of electrical energy. This work has successfully demonstrated a novel technique for prevention & detection of energy theft in AMI (Advanced Metering Infrastructure) or smart meters. As usage penetration of smart grids & AMI / smart metering devices is set to rise with IOT revolution, there is a need for constant evolvement & up-gradation to counter present & future energy theft threats.

One of the desired evolutions can be employment of self learning neural networks, so they can automatically adapt to changing consumption & load patterns & reduce false alarms. Also AMI/ smart meters may be incorporated with GPS to enhance cryptographic security by employing satellite time stamp or auto activation of high surveillance metering in case of geographic location marked for previous energy theft history. Also, the system can employ to disconnect power to a section of consumers in case of large differential theft detected.

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 Sangho Choe "Energy theft detection using gradient boosting theft detector with feature engineering-based preprocessing" 2019
3. Abdulrahaman Okino Otuoze1,2 , Mohd Wazir Mustafa1, Olatunji Obalowu Mohammed1,2, Muhammad Salman Saeed1, Nazmat Toyin 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 Erchin Serpedin† " 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, Anupam Joshi "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, Qixin Chen,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 the United States: The Impact of Polycentric Governance and Contextual Changes" 2016.
13. Bouché, J., Hock, D., & Kappes, M. (2016). On the perfor- mance of anomaly detection systems uncovering traffic mim- icking covert channels. In Proceedings of the 11th international network conference (inc) (pp. 19-24).
14. Toulouse, M., Le, H., Phung, C. V., & Hock, D. (2016). Ro- bust consensus-based network intrusion detection in presence of Byzantine attacks. In Proceedings of the 7th symposium on information and communication technology (soict) (pp. 278- 285).,
15. Hock, D., Kappes, M., & Ghita, B. V. (2016). A pre- clustering method to improve anomaly detection. In Proceedings of the 13th international joint conference on e-business and telecommunications (secrypt) (pp. 391-396).
16. Hock, D., & Kappes, M. (2018). Using the entropy for typi- cal load curve classification. In Proceedings of the 7th interna- tional conference on smart grid and clean energy technologies (icsgce) (pp. 58-64). Hock, D., & Kappes, M. (2018).
17. Hock, D., & Kappes, M. (2020). A survey on the applica- tions of energy demand. (Submitted to Elsevier RSER). Hock, D., & Kappes, M. (2020).
18. Hock, D., Kappes, M., & Ghita, B (2020). Entropy-based metrics for occupancy detection using energy demand.Entropy, 22(7), 731.
19. Hock, D., Kappes, M., & Ghita, B. (2020).Using multiple data sources to detect manipulated electricity meter by an entropy-inspired metric. Sustainable Energy, Grids and Net- works, 21, 100290.