American Journal of Engineering Research (AJER)
e-ISSN: 2320-0847 p-ISSN: 2320-0936
Volume-14, Issue-9, pp-51-58
www.ajer.org
Research Paper Open Access

Design of Intelligent Detection of Energy Theft Using Iot-Based Monitoring.

Amadi Wisdom C.
(Elect/Elect Dept., University of Port-Harcourt Nigeria.)

Nosiri Amaeze C.
(Elect/Elect Dept., University of Port-Harcourt Nigeria.)

ABSTRACT
As a case study, the Power Distribution Companies (DisCos) in Nigeria lose a huge amount of energy, worth billions of Naira to Energy Theft every month. Several steps have been taken to curb the menace of theft and this paper tends to extensively deal with the theft issues as it projects a Supplementary Sensor System (SSS), integrated with IoT devices for extensive monitoring. This project is aimed at first monitoring the energy flowing through a particular service line from the pole to the point of use using a miniaturized and low-cost Current Transformer (CT). the current transformer is linked with the IoT devices which communicate the ThingsSpeak, accessed by the DisCos. The ThingSpeak analyzes the hourly update by the microcontrollers, which is used for the monthly bill preparation, for the metered customers, the data received is juxtaposed with the smart meter reading of the system linked Id. Any disparity suggests of a possible bypass of the meter, and then investigations should then follow within a particular detected id. This is also done at the transformer point to collate all the individual consumption and the transformer energy dissipation. Finally from the transformer point, it is connected by each upriser for a faster analysis and resolution.

Key-words: Energy Theft, Smart Meter, Microcontroller (Matlab Function Block), ThinkSpeak

----

Date of Submission: 11-09-2025 Date of acceptance: 22-09-2025

I. INTRODUCTION

"Energy is neither created nor destroyed", Electrical energy is a form of it. Everyone uses energy in one way or the other at home, office space, open space etc. The primary motivation to drive the proposed research work is to minimize the NTLs in the distribution power network structure by detecting the most compromised areas of supply [11]. To this effect, some scrupulous elements use the power supplied in illicit ways. Some use and do not pay their bills, the metered homes tend to bypass the meter in several means. Faulty meters also contribute to the losses experienced by the Utility suppliers [10]. This design compares energy flow through the service line and the meter reading. It is good to note that energy loss is experienced in two divisions namely: Technical Loss (TL) and Non-Technical Loss (NTL). These losses occur in the process of Generation, Transmission, and Distribution of energy. Energy loss is defined as the difference between energy generated and consumption.

i. **Technical losses** are losses that arise from the characteristics of the materials used in transmission and distribution systems. For instance, the resistance of the conductor used in transmission lines.

ii. **Non-Technical Losses:** include all energy use that is not billed, are a serious issue that affects all industries and has a particularly detrimental effect on some regions.

1.1 **Energy Meter:** The Energy Meter is a device that measures the quantity or amount of electrons that flow through it and in this case to the residences, commercial buildings, and any electrically powered equipment, according to [7]. Energy Meters are graduated in units used in billing and the most generally accepted unit is the watt-hour. The kilowatt hour is referred to as the unit of energy consumed by a unit load of a unit kilowatt in one

hour, or 3,600,000 joules or 3,600 kilo-joules. Electricity meters operate in the manner of a continuous measurement of the instantaneous voltage (volts) and current (amperes) flowing within the system.
In the course of advancement, energy meters have advanced from the very old-fashioned to the most advanced;

- Analog/Electromechanical energy meter is the most common and age-old type of watt-hour meter.
- Digital/Electronic energy meters are more accurate, highly precise, and reliable than the mechanical meter.
- Smart energy meter, which can communicate with the utility company and provide real-time data on energy consumption and cost.

1.2 Energy Theft: Any intentional act by a customer to lower the total amount of tariff payable on power consumed, resulting in a whole or partial loss of income owed to the utility provider, is considered energy theft. Energy theft includes the following:

- **Meter Bypass:** A connection that supplies power directly to devices or appliances in a house without passing through the meter.
- Meter Tampering: Any action that can negatively impact the efficiency of the meter by manipulating or adjusting its settings, or by introducing foreign objects or substances into the meter.
- **Illegal Connection:** A customer is considered to be illegally connected to the network when they tap into the supply from neighbors, particularly those who do not have meters, or when they use concealed paths to gain access. This situation occurs without any evidence of having gone through the approved connection process, indicating that the customer is not listed in the PHED billing or customer database.
- **Illegal Reconnection:** This is when a customer who had been disconnected for either non-payment of outstanding bills or for any of the energy loss offenses goes ahead to reconnect without paying the charges for which he/she was disconnected.
- **Billing Fraud:** This is Internal collusion and manipulation of the billing in favor of consumers

II. REVIEWED WORKS AND GAP

The Bypass of an Energy Meter within the sphere of the utility suppliers in Nigeria is becoming more proliferated by the day hence there is a need to be more technical and scientific. [2] pin-pointed several kinds of bypasses which include current and voltage bypass, a reverse connection between main and load lines, and high-intensity magnetic interference, etc, the paper however focused on dealing with current bypass.[4] identified the need to develop a system to detect power thefts and monitor individual consumer utilization. In this regard, the paper presented an IoT-based power theft detection using a linear regression-based approach for detection and monitoring. Considering the more affected and investigated areas which are terminal cover opening, smart meter frame opening, and electrical lines bypassing, [3] proposed incorporation of a face detection system that will capture the culprit who stands in front of an Advanced Metering Infrastructure (AMI) smart meter. This action is performed by a separate camera controller unit inside the smart meter and could be fixated in diversified angles. The challenge with this system is that there may not be a steady supply to keep the camera running. To detect any unauthorized changes to the metering framework, a latent infrared sensor is integrated with the system. The suggested architecture improves smart home security and can accurately identify the energy used [5]. [6] observed how vulnerable the smart meters could be to energy pilferers, hence proposed the intermediate monitor meter (IMM)-based power model which entails dividing the network of smallest and independent networks to analyze the power flow in detail and effectively within a town. Energy meters would have been able to communicate better to the backend if made smarter so the official could follow through it's operations [8].

III. METHODOLOGY

Energy meters have been made smart with IoT devices. The tamper sensors have been helpful but it appears that consumers have found a way of maneuvering the tamper feature by generating a token that interrupts the accurate reading of the meter and manipulation. This system also tackles the case of some customers diverting some of their loads from the meter
To provide Electricity Board (DisCo) officials with theft detection information, this proposed solution conceptualizes the Internet of Things and the Linear Regression means.

A. Intelligent Energy-Based Detection System:

This system harvests it's data from the current Transformer attached to the service line and the distribution lines as the case may be. The sensors communicate the data to the microcontroller and through the Raspberry to the

ThingSpeak of the same data for further processing. The ThingSpeak Processes and stores the data for use. The figure 1, below portrays the typical idea.

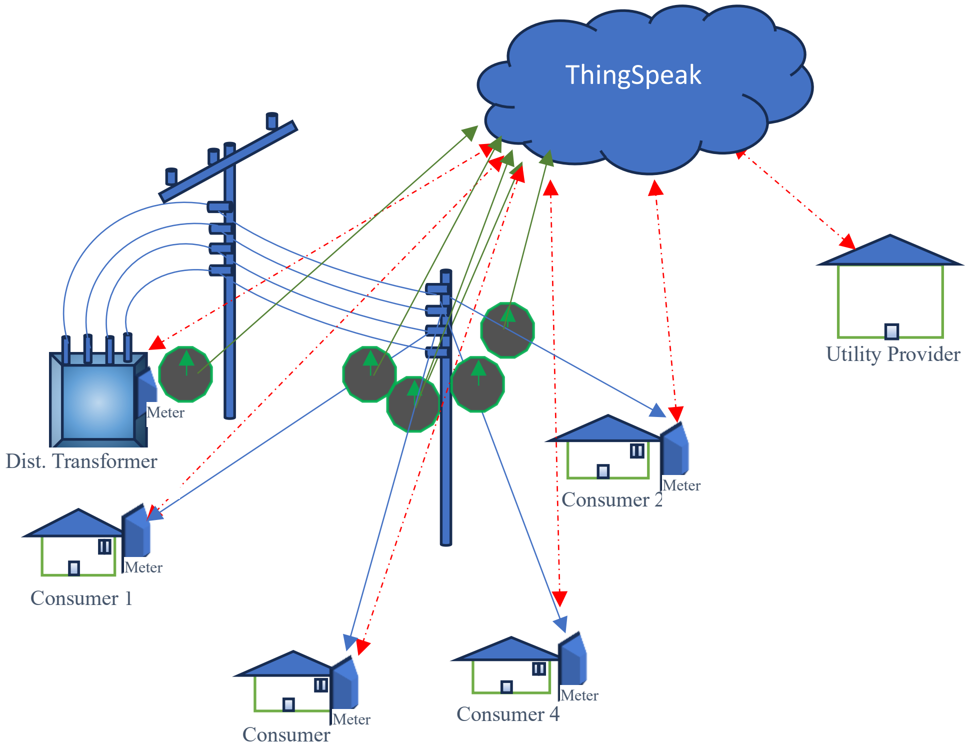


Figure 1Typicsl Representation of the system network

The figure 2, below is a matlab simulated blocks, the constant block generates the voltage signal as seen, which passes through a load, the signal got to the load component first to enable the Matlab Function block (Meter and the proposed system) read the consumption. The data is then transmitted to the ThingSpeak through the Raspberry Pi. Introducing a delay or an interruption in the meter which produces a difference between the smart meter and the proposed system, at this point, the ThingSpeak triggers a theft alert. This is also done at the Transformer base for same purpose.

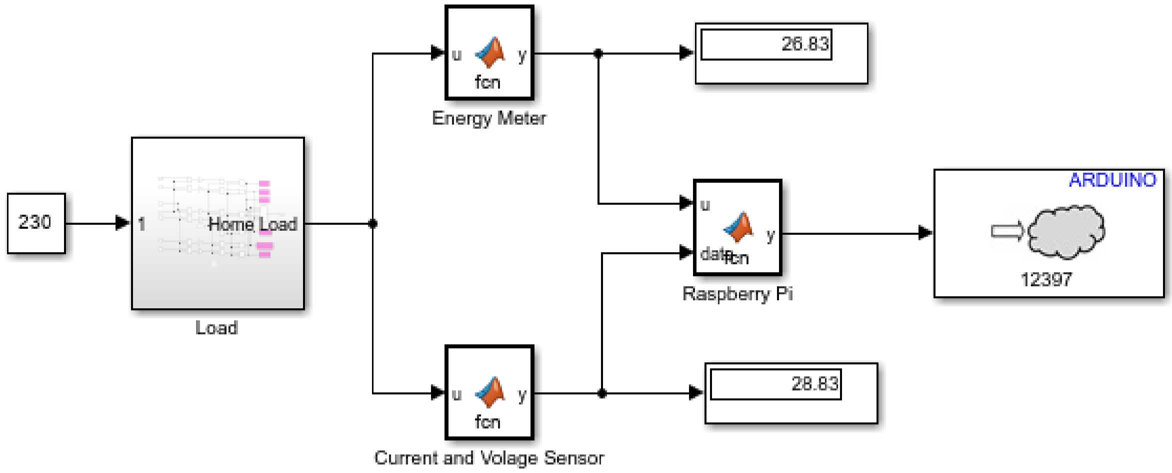


Figure 2. Matlab simulated representation of the system

Power Supply: It is a device (Electrical) that provides electrical power to a load. A power supply's primary system converts electric current from an input to the proper frequency, current, and voltage. In this context is referred to as the means of supply to a load and voltage taken to be 230v from the distribution line.

Current transformers: These are current-sensing units of the power system and are used at generating stations, electrical substations, and in industrial and commercial electric power distribution.

Microcontroller: An Integrated Circuit Unit (ICU) computer is commonly referred to as a Microcontroller Unit (MCU) or Microcontroller (MC, UC, or μC). It contains memory, programmable input/output peripherals, and one or more CPUs (processor cores).

Raspberrry Pi: The Raspberry Pi is a line of microcomputer models that may be connected to common peripherals and monitors for a variety of uses. The hardware components of RP models, which are somewhat larger than credit cards, enable standard PC functions including file creation, storage, and internet streaming.
Wi-Fi Module: A part of the Internet of Things transmission layer, the Wi-Fi module is also known as a serial to Wi-Fi module.

The Loads (Monitoring Energy Consumption): In this design, some selected home gadgets are used to run the simulation as shown below. The connection was based on the rating of the gadgets which translates to the power consumption.
The system monitors the energy combined by measuring the power consumed by each load. The power in kilowatt (kw), consumed by a unit load is determined by multiplying the voltage (volts) across the load with the current (amps) flowing through it. It is mathematically expressed as follows:

$$P_{load} = V_{load} \times I_{load} \qquad (3.1)$$

The total power consumption of the building hence becomes the sum of the individual power consumed by all loads, expressed mathematically as follows:

$$P_{total} = \sum_{i=1}^{N} P_{load_i} \qquad (3.2)$$

The energy consumption (KWH) is expressed as follows:

$$E_{total} = P_{total} \times t \qquad (3.5)$$

Where
V = Voltage from supply in Volts (V)
I = Current in Amps (A)
t = Time (hrs)
P_{load} = Individual loads

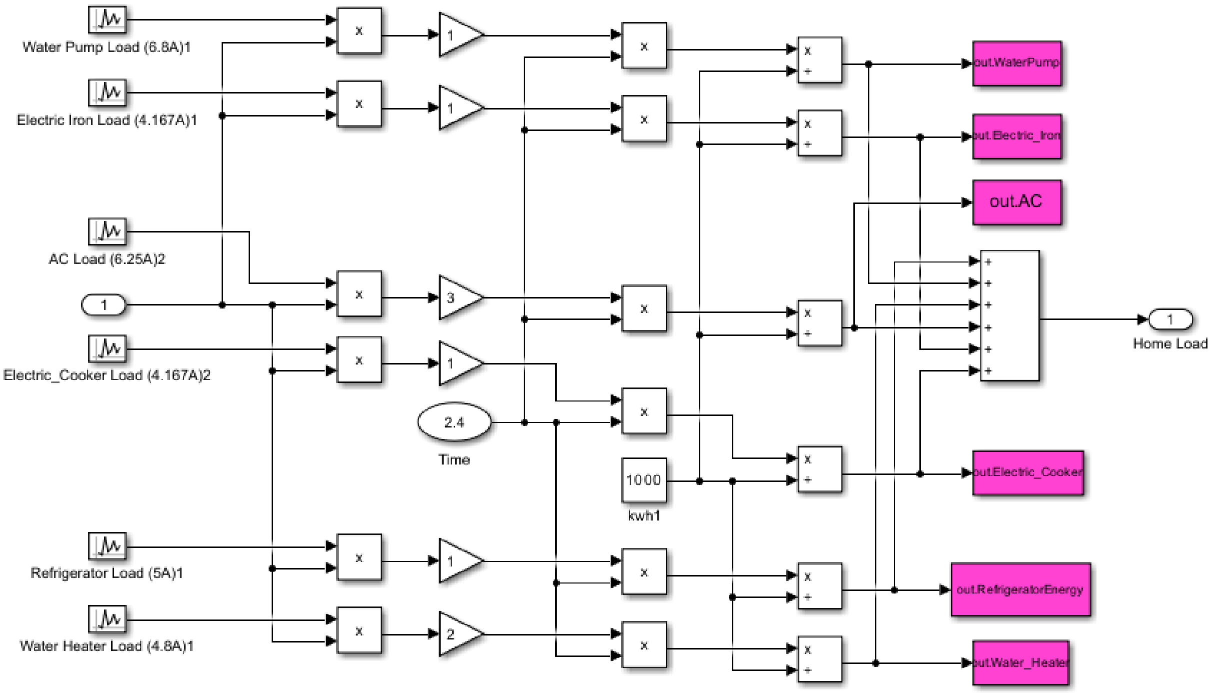


Figure 3: Selected Heavy Home Loads

B. Detection of Energy Theft By Linear Regression:

Consider a Distribution Transformer (DTR) servicing “n” homes, as shown in Fig. 1. Each consumer has a smart meter for individual monitoring of consumed energy. Also, a smart meter is installed at the transformer point, which takes a cumulative measurement of Energy dissipated by the transformer.

Let;
n → Number of consumers/customers
E(n) → Energy consumed by each home
TL → Technical losses in the distribution network
ER → Measurement errors in meters
ETh → Losses due to Energy Theft
E(DT)t → Energy Dissipated by a Distribution Transformer
The Energy consumed by the Distribution Transformer over a time “t” is given by

$$E(DT)t = E(1) + E(2) + \cdots + E(n) + TL + ER + ETh \ldots\ldots\ldots.(1)$$

$$E(DT) = \sum_{t=0}^{n} E(\mathrm{n})t + TL + ER + ETh \ldots\ldots\ldots.(2)$$

If TL and ER are negligible, the Energy Theft is given as

$$ETh = E(DT)t - \sum_{i=0}^{n} E(\mathrm{n})\,t \ldots\ldots\ldots.(3)$$

Where ETh > 0, then there is a theft.

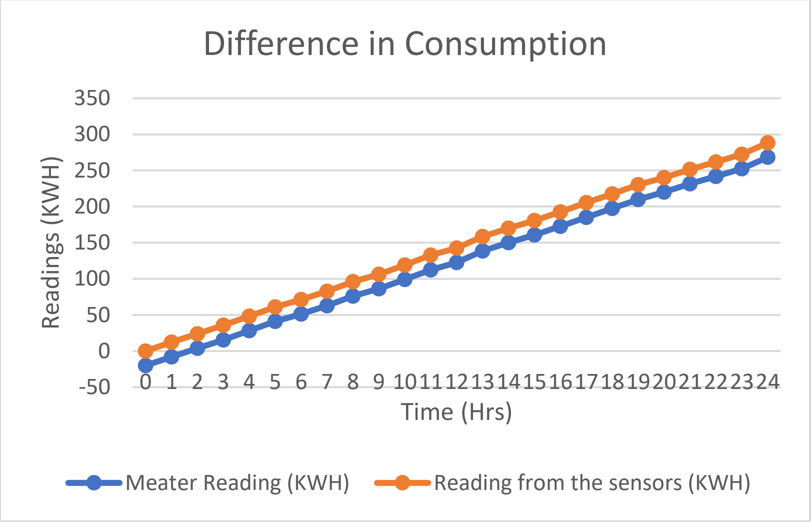
In the practical sense where the TL is considered, the ETh will be above a certain threshold value set in consideration of the system ratings and quantity of energy flow

IV. Simulated Results and Discussion

From the simulation in Figure 2, one can observe that the smart meter can be hacked, but the proposed system still delivers the real consumption automatically and transmits it to the ThingSpeak. It is observed that the meter was giving a different reading from the system with the same signal and consumption depicting that there could be an interruption in the meter deliberately or otherwise.. In this work, a fault was introduced into the meter by coding which makes it gave a lower reading. Sometimes the meter could be faulty on it’s own without any one

tampering it, this system serves as a monitor. It is also used as a meter to the direct customers which are on the postpaid billing system.
Analyzing the readings below as gotten from a 24hrs simulation of the load,

Time (hrs)	**Meater Reading (KWH)**	**Reading Fom The Sensors (KWH)**
0	-20	0
1	-7.952108533	12.04789147
2	3.976777399	23.9767774
3	15.55111666	35.55111666
4	28.1335968	48.1335968
5	40.91170812	60.91170812
6	51.17008498	71.17008498
7	62.88843339	82.88843339
8	75.98864958	95.98864958
9	86.35458525	106.3545852
10	99.02857278	119.0285728
11	112.59147	132.59147
12	122.5279694	142.5279694
13	138.4308713	158.4308713
14	150.1931919	170.1931919
15	160.4863894	180.4863894
16	172.6413097	192.6413097
17	185.2538043	205.2538043
18	197.5197669	217.5197669
19	210.0641708	230.0641708
20	219.8804865	239.8804865
21	231.5981851	251.5981851
22	241.6383092	261.6383092
23	252.4475819	272.4475819
24	268.2783594	288.2783594



The above information portrays that the smart meter could be hacked, or manipulated in a way that may not trigger the tamper effect yet the reading is reduced as seen. This system will provide the actual reading.
Again with the data provided by the system detection of theft is made easier too using the Linear regression method.

V. Conclusion

When the Non-Technical Losses are mitigated, this will yield the following benefits

- Increase in revenue.
- There would be Available funds to purchase necessary machinery like meters, transformers, poles, etc. As well as maintain our networks.
- Estimated billing will drop to near zero and customers can manage their energy usage.
- The possibility of wheeling in more energy from private generators abounds
- There would be reduced outages and improved daily hours of supply to all customers
- More enabling environment would be created for business to boom, and more profit for business outfits, companies, and industries
- A safe and friendly environment devoid of crime occasioned by lack of supply/darkness. As the saying goes “Light is life”
- May gradually have a downward drive on goods/services whose prices are influenced by high running and maintenance cost of generating sets

References

[1]. A. K. Gupta, A. Mukherjee, A. Routray and R. Biswas, "A novel power theft detection algorithm for low voltage distribution network," IECON 2017 - 43rd Annual Conference of the IEEE Industrial Electronics Society, Beijing, China, 2017, pp. 3603-3608.

[2]. N. Tangsunantham, S. Ngamchuen, V. Nontaboot, S. Thepphaeng and C. Pirak, "Experimental performance analysis of current bypass anti-tampering in smart energy meters," 2013 Australasian Telecommunication Networks and Applications Conference (ATNAC), Christchurch, New Zealand, 2013, pp. 124-129.

[3]. M. Rattanasuttikan, S. Thepphaeng and C. Pirak, "Image Centric Anti-Tampering Technique for AMI Smart Meter," 2018 International Electrical Engineering Congress (iEECON), Krabi, Thailand, 2018, pp. 1-4.

[4]. M. J. Jeffin, G. M. Madhu, A. Rao, G. Singh and C. Vyjayanthi, "Internet of Things Enabled Power Theft Detection and Smart Meter Monitoring System," 2020 International Conference on Communication and Signal Processing (ICCSP), Chennai, India, 2020, pp. 0262-0267.

[5]. A. R. and K. V., "IoT Based Smart Energy Theft Detection and Monitoring System for Smart Home," 2020 International Conference on System, Computation, Automation and Networking (ICSCAN), Pondicherry, India, 2020, pp. 1-6.

[6]. J. Y. Kim, Y. M. Hwang, Y. G. Sun, I. Sim, D. I. Kim and X. Wang, "Detection for Non-Technical Loss by Smart Energy Theft With Intermediate Monitor Meter in Smart Grid," in IEEE Access, vol. 7, pp. 129043-129053, 2019.

[7]. Bourdillon.O.Omijeh and Godwin.I.Ighalo [2013], Innovative Systems Design and Engineering ,www.iiste.org ISSN 2222-1727 (Paper) ISSN 2222-2871 (Online) Vol.4, No.1, 2013

[8]. M. Singh and E. V. Sanduja, “Minimizing Electricity Theft by Internet-of-Things,” International Journal of Advanced Research in Computer and Communication Engineering, Vol. 4(8), pp.326-329, 2015.

[9]. Jeffin, M & G M, Madhu & Rao, Akshayata & Singh, Gurpreet & Vyjayanthi, C.. (2020). Internet of Things Enabled Power Theft Detection and Smart Meter Monitoring System. 0262-0267.

[10]. Ajit Muzumdar, Chirag Modi, and C. Vyjayanthi (2022), "Designing a Blockchain-enabled Privacy-Preserving Energy Theft Detection System for Smart Grid Neighborhood Area Network". Electric Power System Research 207 (2022) 107884. Elsevier

[11]. Muhammad Umair, Zafar Saeed, Faisal Saeed, Hiba Ishtiaq, Muhammad Zubair1 and Hala Abdel Hameed (2023), CMC, 2023, vol.74, no.3 Elsevier Daad,mcxz