Energy Theft Detector (ETD): A Salvage Module from Meter Bypassing and Illegal Tapping of Electricity

OLADOSU, D. A
Department of Computer Engineering Technology, The polytechnic, Ibadan, Oyo State, Nigeria

Abstract- Energy management and optimisation are part of the key performance indicators of good governance, in which the country has failed largely. Billions of naira has been expended on generation, transmission and distribution which yield little or no result. However, merely generating more power is not enough to meet present day requirements; power consumption and losses have to be closely monitored so that the generated power is utilized in an efficient manner. Illegal electricity usage is indirectly affecting the economic status of the country and the planning of national energy becomes difficult because of unrecorded energy usage. This proposed Energy Theft Detector (ETD) consists of PZEM Energy Meter with current transformer to monitor energy consumption, detect meter bypassing and illegal tapping. For effective access of utility provider to energy consumption data that is running on a remote server, ESP-32 was employed. The data sent through this GPRS Interface was hosted on hosting platform called 00webhost. The method of weight function-based control was used to determine current imbalances between node at distribution pole and consumer's smart meter. In order to set threshold watt values for anomalies of energy consumption, consumer consumption behaviour was studied and piloted. This makes this method perform more effectively and accurately with low false-positive rate. If implemented, it would be a potential test case that can reduce energy theft in the country.

Index Terms- Bypassing, Distribution, Current, Energy, Threshold.

I. INTRODUCTION

The efficient and reliable information exchange has been grossly improved due to massive deployment of Advanced Metering Infrastructures (AMI), which includes smart meters and Internet of Things (IoT) monitoring devices to collect data in large volumes with fast speed. Smart home aapplication today focuses on system development, system architecture, communication protocols as well as forecasting tools [1], purposely to provide home consumers with a better technology in terms of energy monitoring, control, and reliability. According to Weixian Lee et al [2], Demand Side Management System (DSMS) was introduced to better manage and control power consumption for smart homes [3], which later expanded to include load-shifting, dynamic price management, forecasting demand, and demand response systems through the use of machine learning and statistical modelling.

However, with all these advancements and deployed technologies, there are still vulnerabilities to energy losses, both Technical Losses (TLs)- power dissipated in power systems' components (e.g. Non Technical Losses (NTLs)- losses not traceable to any technical components mainly referred to as energy theft [3]. Unlike TLs that occur naturally and are often calculated based on the systems' components and network parameters, energy thefts are fuelled by psycho-social/socio-economic factors, poor government policies and implementation [4].

In Nigeria, energy theft has generated tremendous concerns; the problem is as old as the power sector which constitutes over 80% of the energy losses. Average Nigerians find a way to bypass their meters. Research has shown that the moneybags are not left out, from Ikeja GRA in Lagos, home of very rich Nigerians, to Asokoro in Abuja, to a place called Bompai in Kano, to highbrow areas in Jos; the story is the same [5]. It was reported that DisCos lose about ₦30 billion monthly owing to electricity theft [6]. The same thing is applicable to Ikeja Electricity Distribution Company (Plc.) report on high incidence of electricity theft through meter bypass and illegal connections while disconnection orders are often being subverted by illegal re-connections. On the side of Eko Electricity Distribution Company (Plc.), it was discovered that no fewer than 43,000 prepaid meters were tampered with out of 134,000 installed by the company in the last five years. This accrued to almost 32 per cent of the total number of prepaid meters in use across the area covered by the company [7].

Consequently energy theft has resulted into huge revenue losses, while generation units are sometimes overloaded to meet load demand by installed capacity. This always leads to reduced reliability in grid operations and damage to infrastructure. Also, unfavourable load shedding, as utility, tends to favour the areas where increased revenue is realised, however with higher tariff. There are high subsidy payments by government to make the tariffs affordable and discouragement of private sectors' involvements because huge tasks and high expenses involved in the attempt to curb the menace especially, in conventional power systems.

Several efforts have been taken for many years with power companies and the Nigerian government in order to curb these financial losses. The Central Bank of Nigeria (CBN) in collaboration with relevant agencies came up with policies such as the National Mass Metering Programme (NMMP), an initiative for customers to pay for electricity in advance and reduce the incentive for electricity theft. In 2013, Nigerian Electricity Regulatory Commission (NERC) formulated the electricity theft and other related offences regulations to curb electricity theft and vandalisation of electricity supply infrastructure [7]. Efforts are also on going to increase public awareness and education about the impacts of electricity theft on the power sector and accompanying consequences that will deter prospective offenders.

This work proposes another technical approach to curb this menace with the development of a new device, Energy Theft Detector (ETD) that can easily be installed and integrated with node on a distribution pole in the low voltage segment to calculate energy consumed and detect the abnormalities with good precision

II. LITERATURE REVIEW AND THEORETICAL BACKGROUND

Transmission and Distribution Losses (TD Losses) constitute entire losses by the power sector. It comprises an aggregate of Technical Losses (TL) and Non-Technical Losses (NTL). TD losses represent the difference between the electricity generated and the electricity consumed [8]. On the other hand, NTL constitutes losses arising from defective meters, errors in billing, and flaws in supply, unmetered connections, as well as malicious activities by the consumer, such as tampering of meter and illegal connections. The Non-Technical Losses (NTL) in relation to TD and TL is given as:

$$NTL = \text{Total Energy Losses (TD)} - TL \quad (1)$$

$$\text{Total Energy Losses} = \text{Energy Supplied} - \text{Bills paid} \quad (2)$$

According to [8], Transmission and Distribution (TD) losses were further classified as Aggregate Technical and Commercial losses (AT&C).

$$AT\ \&\ C\ \text{Losses} = \{1 - (BE \times CE)\} \times 100 \quad (3)$$

$$T\ \&\ D\ \text{Losses} = \{1 - (BE)\} \times 100 \quad (4)$$

Where Billing Efficiency (BE) = Total Unit Billed/Total Unit Inputs

Collection Efficiency (CE) = Revenue Collected/Amount Billed

- TD loss is the difference in input energy and energy billed.
- AT&C loss is the difference in input energy and energy for which revenue has been collected.

Summarily [8], $AT\ \&\ C\ \text{Losses} = TL + CL \quad (5)$

Technical losses (TL) are those losses which are internal to the system such as energy dissipation (conduction and convention) by the electrical equipments used in distribution which is roughly propounded as [9]

$$TL = \frac{T_c - T_e}{\frac{1}{2 \cdot \pi \cdot r \cdot L \cdot h_{ar}}} = I^2.R \quad (6)$$

where:

T_c is the temperature of the bare conductor;

T_e is the environment temperature in the surroundings of the conductor;

L is the distance between two temperature sensors measuring the temperature of the conductor; h_{ar} is the convection coefficient for air, in $W{:}m^{-2}{:}C^{-1}$;

$r = R_1$ is the radius of the inner cylinder (conductor radius)

R is the resistance of the conductor of length L;

I is the current flowing through the conductor.

and that of overhead insulated conductors (conductive and convective) thermal resistances can be calculated as [9]

$$R_{12} = \frac{\Delta T_{12}}{q_{cond}} = \frac{\ln(r_{outer}/r_{inner})}{2 \cdot \pi \cdot k_{ins} \cdot L} \tag{7}$$

$$R_{23} = \frac{\Delta T_{23}}{q_{conv}} = \frac{1}{2 \cdot \pi \cdot r_{ins} \cdot L \cdot h_{ar}} \tag{8}$$

Then, TL can be deducted as

$$TL = \frac{T_c - T_e}{\frac{\ln(\frac{r_2}{r_1})}{2 \cdot \pi \cdot K_{ins}} + \frac{1}{2 \cdot \pi \cdot r_2 \cdot L \cdot h_{ar}}} \tag{9}$$

Where:

T_1 represents the conductor's temperature

T_2 represents the temperature at the insulation

T_3 represents the temperature of the environment

Te is air temperature

R_{12} and R_{23} are the thermal resistances representing conductive heat loss and convective heat loss, respectively

q_{cond} and q_{conv} are the conductive heat flux and convective heat flux, respectively.

NTL is mostly CL that occurs at low segment voltage, considering Energy balance formula

$$NTL_k = TE_k - \sum_{j=1}^{n} (CE_{kj}) - TL_k \tag{10}$$

NTL_k are the Non-Technical Losses in the low voltage network supplied by the kth transformer;

TE_k is the total energy measured in the kth transformer;

CE_{kj} is the energy supplied to the j consumer by the kth transformer;

TL_k are the technical losses in the low voltage segment supplied by the kth transformer.

TE_k and CE_{kj} values are obtainable from the Smart Energy Meter (SEM).

A critical look showed that energy thefts constitute most of NTLs, such as unauthorised line tampering and diversions, meter bypass (partial or complete), billing irregularities, ineffective governance or accountability by the power sector, political instability and high levels of corruption. In Advance Metering Infrastructure (AMI), NTLs are caused by false data injection via smart meters and unlawful tapping from the distribution networks, cyber-related attacks which may affect the networks, buying and selling of illegal prepaid vouchers, and questionable employees' integrity etc. Energy Thefts have a severe implication on the country's economic growth due to the cascading problems caused, which also result in load shedding that is, however, not peculiar to Nigeria alone. Recent researches showed approximately US$89.3 billion were lost annually in the world [12]. In the USA alone, the cost of nationwide electricity power theft is about $1.6 billion yearly and at least one house in every seven houses in the Nelson Mandela Bay Metro (South Africa) has its electric meter tampered with [12]. This electricity theft is the main reason why most Electrical Departments in municipalities went into oblivion

Several Techniques have been developed, as propounded by [13] on redevelopment of the Automated Meter Reading (AMR) that enables 'bidirectional' data exchange between consumer meters and the utility company using wireless communication systems and devices such as ZigBee module, wireless local area network (WLAN), broadband power line communication (PLC) etc, to obtain the total aggregated electricity consumption and detect meter tampering unnoticed. It also efficiently computes the electricity bill for each customer through dynamic pricing for load monitoring and energy management. However, it could not detect illegal connections.

Muhammad et al developed a smart prepaid energy metering system to control electricity theft by monitoring consumer's power usage through the linkage of the server and the consumer energy meter with a network. This was explored with GSM technologies; the prototype consumer energy meter was designed with ATMega32 microcontroller, energy measuring chip (ADE7751), GSM module (Siemens A62 mobile phone), MAX232, potential transformers, current transformers, a relay, and LCD

Shinde et al developed an Internet of Things (IoT)-based power theft detection using a 32-bit RISC ARM processor core licensed by AMR holdings to capture power usage. The ARM microprocessor receives captured electric data from the measuring device and sends the data to LCD for display so that the consumer is able to see how much is being consumed by the load with the aid of Micro-controller and ADC that link micro grid and the smart metering. Other related systems include a monitoring system that utilizes an electro-optical sensor incorporated into a smart energy meter to detect when the meter is covered and when it is opened [26]; or a Light Dependent Resistor (LDR), and a comparator [16]. Most IoT-based smart meters are designed to transmit the recorded energy usage data through network channels such as radio frequency (RF), broadband over power lines (BPL), and public networks. This recorded data is transferred to the utility central meter data management system (MDMS) for data analysis [17].

Olusegun & Kingsley (2022) modelled an energy theft system with typical parameters and consumer loads. They developed a program which was first initialized under conditions of no theft, using the section line parameters and the actual voltage/current used at each consumer as reported by a smart tariff meter and the result of the initialization step as a matrix of consumer branch resistances to energy theft detection. This was achieved by comparing the actual voltages at each pole computed by propagation from all connected consumer nodes using the stored branch resistances. Differences were identified as indicators of theft and were further processed to estimate the power consumed. The result showed a dependence of detection accuracy on location of theft, relative magnitude of theft and network conditions. However, minimum power theft that could be detected was between 10 W to 260 W [18]

[19]The research focused on recommending the best prediction model using Machine Learning in electrical energy theft. The source of the information on the electricity consumption of 42372 consumers was a dataset published in the State Grid Corporation of China. The method used was data imputation, data balancing (oversampling and under sampling), and feature extraction to improve energy theft detection. Five Machine Learning models were tested. As a result, the accuracy indicator of the SVM model was 81%, Nearest Neighbours 79%, Random Forest 80%, Logistic Regression 69%, and Naive Bayes 68%. It is concluded that the best performance, with an accuracy of 81%, is obtained by using the SVM model. Another [20] system involved the integration of various machine learning methods with a statistical model in three stages. In the first stage, two deep learning models- dense network and long short-term memory- are integrated for predicting the electricity consumption pattern of a consumer and the performance from a house in Pakistan.The second stage was a statistical model. The Exponential Moving Average (EMA) was used to filter the abnormal consumption in 24 hours. The last stage filtered abnormalities with respect to maximum consumption in the history.

II. PROPOSED SYSTEM METHODOLOGY

This work intended to develop Energy Theft Detector (ETD) that can be easily installed on a node point of distribution pole, neutral line or other facilities, in the low voltage segment to calculate the energy usage and detect illegal connection and meter bypassing with good precision and low cost. The novelties of the proposed system as a solution to electricity theft detection encompassed in the respective work-flow (Fig 1) are basically made up of five parts:

ETD consists of PZEM Energy and Current Transformer to monitor eenergy consumption by the utility users (Fig 2). PZEM-004(V3.0) of electrical parameter measurement with overload alarm function that stores and displays data when power off was employed. It works with Serial Communication Interface and Working voltage of 80 ~ 260VAC, Test voltage: 80 ~ 260VAC, Rated power: 100A/22000W, Operating frequency: 45-65Hz 5 and Measurement accuracy: 1.0 grad [21].

3.1 Hardware Interface

The Current Transformer was of maximum rating capacity 100/5 A ampere with work temperature of -25^{o}C to +70^{0}C.

3.2 GPRS Technology Communication Protocol/Interface

The ETD module employed ESP-32 (Fig 2) to send energy consumption remotely to utility provider and report illegal connection/bypassing. Chipset ESPRESSIF-ESP32 is a 240MHz single-/dualcore 32-bit LX6 microprocessor of 520kB SRAM. It has working voltage and current of 2.7V-3.6V and about 70mA respectively, Working temperature range -40℃ ~ +85℃, Protection interval Frequency range 2.4GHz~2.5GHz (2400M~2483.5M). It works with networking protocol IPv4, IPv6 and SSL. [22]

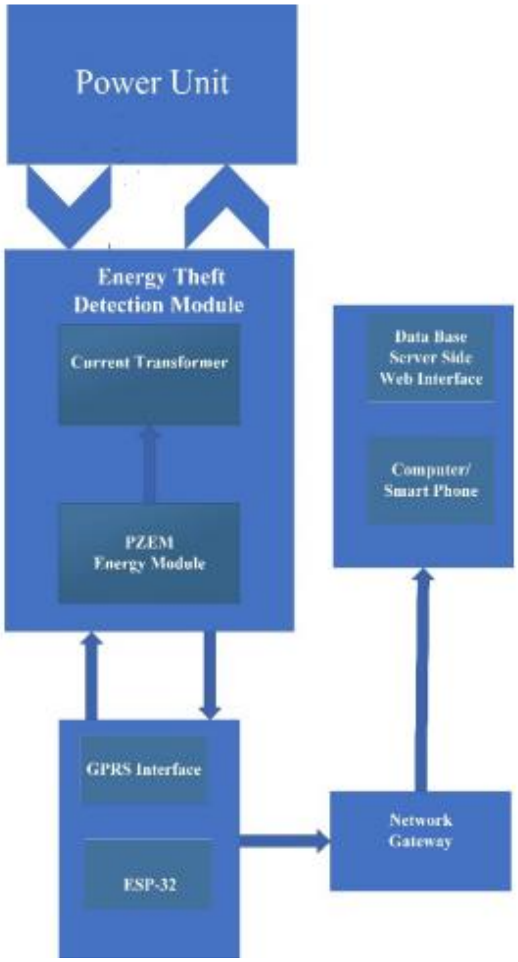

Fig 1: Block Diagram of ETD

3.3 Web Technology Interface and Back End

For effective access of utility provider to interact with Energy Consumption Data, running on a remote server for a Real Time Theft Detection; HTML, CSS and JAVA Scripts were needed to be employed in order to navigate the internet and structure the website, as well as to add stylistic elements to the web page with dynamics and interactivity of the website. Also, in order to generate dynamic page contents of energy consumption data, control the use-access and encrypt energy consumption data, PHP apps and MYSQL had to be utilised for storing and tabulating energy consumption for different subscribers. However, we hosted the website on platform called 00webhost

3.4 Power Unit

The accrued current value for the ETD design was 700mA, while 3.3volt Lithium battery of ampere rating 2.5amps was used as backup for the system. This battery was charged with 5/3.7 volt DC to Dc step down converter (Fig 2).

The ETD module constructed was integrated with the node of the pole at neutral line and the result was monitored with smart phone/computer system through GPRS (General Packet Radio Service)

3.5 ETD Techniques for Smart Theft Detection

Smart Theft Detection was modelled mathematically using weight function-based control algorithm [23]

$$I_{th} = I_p - I_m \quad (11)$$

I_p and I_m are currents at the line of the pole linked with the distribution and sensed current at the smart meter of consumer respectively. I_{th} is the difference in the pole and sensed current of smart meter (I_{theft}). To validate the system application, the following conditions were propounded for electricity theft Detection in the distribution lines so as to be monitored in real-time via the web dashboard

Condition 1: The system was designed to measure and monitor watt-hour in every 1000ms, (duration of surge current t)

Condition 2 : When the line is under normal condition

For $t \leq t_1$, $I_p = I_m$ $I_{th} = 0$. (12)

t_1 is the duration of surge current = 1000ms

Condition 3: When the line is under theft condition (illegal connection)

For $t > t_1$, $I_p > I_m$, $I_{th} > 0$ (13)

Condition 4: When the line is under theft condition (bypassing)

For $t > t_2$, $I_p < I_m$, $I_{th} < 0$ (14)

t_2 is the duration of surge current = 1000ms

These conditions were coded and stored in the PZEM energy meter through current transformer in form of watt-hour. Since energy consumed (E) in watt-hour is given as

$$E = IVt = Wt \quad (15)$$

Threshold powers were set for normal condition, metre bypassing and illegal connection. They were represented as $W_n t$, W_b t and $W_l t$ respectively, where t is response time selected (1000ms). The system detected load connected and communicated amount of watt-hour with the ESP-32.

The results of the model were validated through Test Bed in the laboratory and field survey. For Test bed the threshold values chosen were:

Normal Condition: $16 \leq W_n t \leq 79$ (16)

Illegal Connection $W_l t \geq 80$ (17)

Metre Bypassing $W_b t \leq 15$ (18)

For field Survey, Oremeji-Agugu, Ibadan, Oyo State, Nigeria was the study setting for likert survey. It is a Service Band D with maximum of 8hrs per/day as categorised by Ibadan Electricity Distribution Company (IBEDC) and it is one of the areas where electricity theft is rampart. Thirty (30) houses were selected at random with Energy Theft Modules installed at different times to the node at the distribution pole in other to ascertain average utilities consumed per day. The same houses were subsequently used to validate energy theft detection.

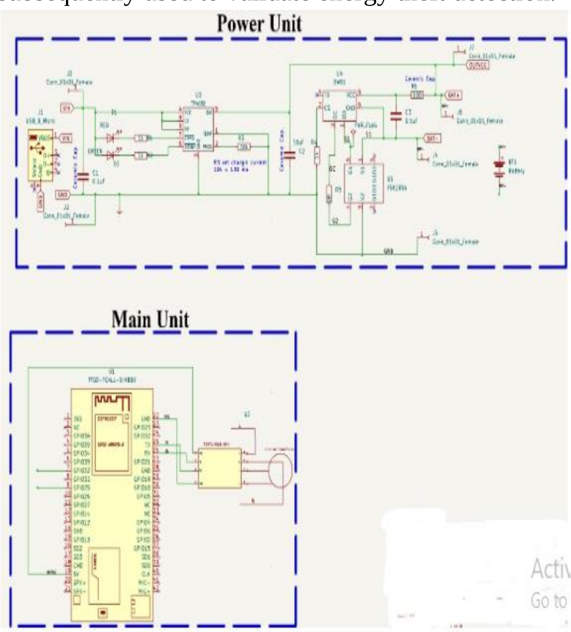

Fig 2: Complete Circuit Diagram of ETD

The average consumption was found to be around 600 to 800watt per day with 75% of the consumption during the night. In respect to that, the threshold values chosen were:

Normal Condition: $450 \leq W_n t \leq 799$ (19)

Illegal Connection $W_l t \geq 800$ (20)

Metre Bypassing $W_b t \leq 200$ (2)

This mathematical model was coded and embedded into the module to enable the detection of multiple energy thefts occurring in the electricity network under No Load and Normal Load, Bypassing and Illegal Connection.

IV. ETD RESULT ANALYSIS AND DISCUSSION

ETD utilizes current readings to produce the power readings in every second, measured from the distribution pole grids/nodes and energy consumption measured in consumer houses. During the test bed, the prototype displayed readings used under load Condition (Fig 3) and Power of 0 watt on the GUI status of the system (Fig 4)

Condition 2: Normal Load Condition- the status was "No Theft detected" (Fig 5). It means that a current flow from distribution node is of the same value with smart meter current. Hence, network was intact. .

Condition 3: Illegal Connection- the status was "Theft Detected". It means that current flows from distribution node are of higher value than that of Smart meter current. The power consumption displayed was at high side, illegal connection suspected (Fig 6).

Condition 3: Bypassing- the status was "Theft Detected". It means that current flows from distribution node are of lower value than that of smart meter current. The Power consumption displayed was very low, evidently meter has been bypassed (Fig 7)

The result from field survey was in tandem with the test bed. consumer houses H3, H13, H17and H24 bypassed the mater smart meter to steal electricity, and powers displayed by the module for consumed energy were far from the actual power consumed, compared to threshold value. Specifically, supplying currents of those houses from the pole will be lower than their Smart meter. as calculated energy used was high. It means that the compared currents were otherwise.

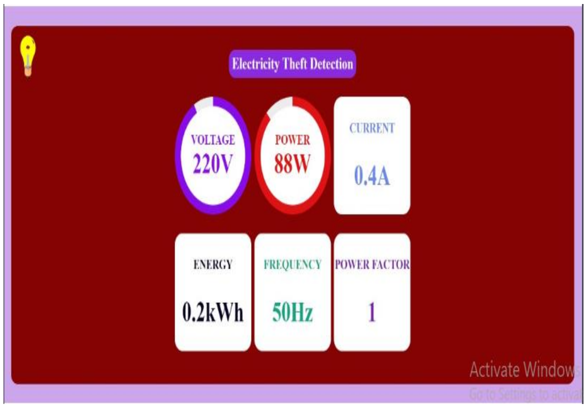

Fig 3 : Readings on Prototype Interface when loaded

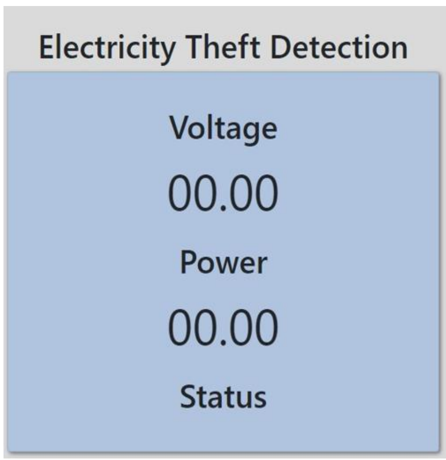

Fig 4: Power of 0 watt on the GUI status of the System Web Interface

Application of the technique used here in design and model a theft detecting device showed accuracy of theft location above 84% with the maximum detectable theft power at a node being in the range of 10 W to 1kW for both Meter bypassing and illegal Electricity tapping. The result of this study implements a potential test case that can reduce energy theft because of thorough survey of Consumer behaviour on energy usage was done before setting threshold watt values for the design. This method performed more effectively and was accurate with low false-positive rate. However, there might be unusual customers' behaviour based on their short-term usage

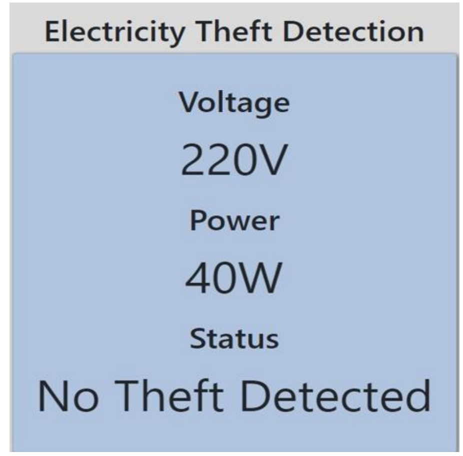

Fig 5: Display on GUI status of the System Web Interface under No Theft Condition

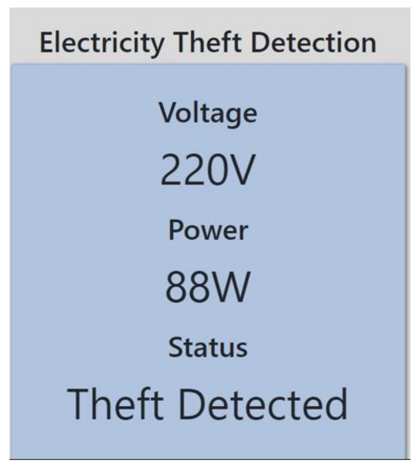

Fig 6: Display on GUI status of the System Web Interface during Illegal Taping

Fig 7: Display on GUI status of the System Web Interface during Meter Bypassing

V.

CONCLUSIONS AND RECOMMENDATIONS

Electric energy theft is a global problem, combating it should be a critical task especially for a developing country like Nigeria that generates less than required demand and yet more than 50% of the paltry sum is lost. In this paper, we have described a technique for energy theft detection using data obtained from the utility subscribers to set the threshold for modelling and designing ETD. Although the implementation of this system by any power utility may be costly, cost recovery is possible within five years because there will be drastic reduction in power theft. Besides, the proposed system can be easily developed into complete modules with at least ten (10) connection nodes on distribution pole based on expected number of consumers allocated to tap from the pole. This will serve as total enclosure and illegal tapping/connection will be totally eradicated

ACKNOWLEDGEMENT

I immensely grateful and acknowledge Nigeria Tertiary Education Trust Fund (tetfund) and The Polytechnic, Ibadan for the Internal Based Research (IBR) grant for the research

REFERENCES

[1] W. Li, T. Logenthiran, V.-T. Phan, and W. L. Woo, (2016) “Intelligent multiagent system for power grid communication,” Region 10 Conference (TENCON), 2016 IEEE. IEEE, 2016, pp. 3386–3389.

[2] Li Weixian, Logenthiran Thillainathan, Phan Van Tung and Woo, Wai Lok (2019) “ A Novel Smart Energy Theft System (SETS) for IoT based Smart Home”. IEEE, Internet of Things Journal, 6 (3). pp. 5531-5539. ISSN 2327-4662 Northumbria Research, Link:http://nrl.northumbria.ac.uk/id/eprint/38304/

[3] Abdulrahaman Okino Otuoze., Mohd Wazir Mustafa., Olatunji Obalowu Mohammed., Muhammad Salman Saeed., Nazmat Toyin Surajudeen-Bakinde., Sani Salisu.(2019)“Electricity theft detection by sources of threats for smart city planning”, IET Smart Cities, 2019, Vol. 1 Iss. 2, pp. 52-60

[4] Ahmad, T., Ul Hasan, Q.: (2016) ‘Detection of frauds and other non-technical losses in power utilities using smart meters: a review’, Int. J. Emerg. Electr. Power Syst., 2016, 17, (3), pp. 217–234

[5] https://thenextier.com/the-impacts-of-electricity-theft-on-the-power-sector/

[6] N. O. Shokoya , & A. K. Raji, (2019) “Electricity theft mitigation in the Nigerian power sector” International Journal of Engineering &Technology, 8 (4) (2019) 467-472.

[7] M. O. Obafemi, E. A. Oluwole, T.E. Omoniyi, P.N Meduna, A.S. Alaye (2021) “Prevalence Of Electricity Theft Among Households In Lagos State, Nigeria” Journal of Technology (NIJOTECH) Vol. 40, No. 5, September 2021. 2.2.3.5

[8] Divam Lehri and Arjun Choudhar (2019) “A Survey of Energy Theft Detection Approaches in Smart Meters”, In book: Intelligent Energy Management Technologies ICAEM 2019 (pp.9-24), Publisher: Springer

[9] H.O. Henriques, R.L.S. Corrêa, M.Z. Fortes ⇑ , B.S.M.C. Borba, V.H. Ferreira (2020) “Monitoring technical losses to improve non-technical losses estimation and detection in LV distribution systems” https://doi.org/10.1016/j.measurement.2020.107840

[10] Abdulrahaman Okino Otuoze, Mohd Wazir Mustafa1, Olatunji Obalowu Mohammed, Muhammad Salman Saeed1, Nazmat Toyin Surajudeen-Bakind, Sani Salisu (2019) “Electricity theft detection by sources of threats for smart city planning” IET Smart Cities, 2019, Vol. 1 Iss. 2, pp. 52-60

[11] Celimpilo Lindani Zulu, Oliver Dzobo “Real-time power theft monitoring and detection system with double connected data capture system” Electrical Engineering (2023) 105:3065–3083 https://doi.org/10.1007/s00202-023-01825-3

[12] Nicholas N (2017) Analysis: Electricity theft in South Africa, June 27, 2017. [Online]. Available:

https://www.smart-energy. Com/features-analysis/electricity-theft-south-africa/

[13] Foudeh, H. A and Mokhtar, A. S (2015) Automated meter reading and Advanced metering infrastructure projects, In: 9th Jordanian international electrical and electronics engineering conference (JIEEEC), pp. 1–6, 12–14

[14] Mohammad N, Barua A, Arafat MA (2013) A smart prepaid energy metering system to control electricity theft, Proc. 2013 Int. Conf. Power, Energy Control. ICPEC 2013, pp. 562–565 15. Kumar R, Arora S, Singh S, Tomar A (2017) Design of intelligen

[15] Shinde P S, Maskar S, Pise A, Salunkh S (2019) IoT based Power Theft Detection. J Opt Commun Electron 5(1):19–23

[16] Asogwa TC, Isizoh AN, Nwobodo HN, Okide SO (2014) Automatic power theft locator. Int J Innov Sci Eng Technol. 1:375–

[17] Ogu RE, Chukwudebe GA, Ezenugu IA (2016) An IoT based tamper prevention system for electricity meter. Am J Eng Res - AJER 5:347–353

[18] Olusegun Mayowa Komolafe & Kingsley Monday Udofia (2022) “A Technique for Electrical Energy Theft Detection and Location in Low Voltage Power Distribution Systems” Engineering and Applied Sciences 2020; 5(2): 41-49

[19] Ivan Petrlik, Pedro Lezama, Ciro Rodriguez, Ricardo Inquilla, Julissa Elizabeth Reyna-González, Roberto Esparza. (2022) “Electricity Theft Detection using Machine Learning” (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 13, No. 12, 2022

[20] Afrah Naeem & Nadeem Javaid,” A Practical Electricity Theft Detection-Smart System (ETD-SS) for Smart Homes” https://www.researchgate.net

[21] PZEM-004T-V3.0-Datasheet-User-Manual.

[22] TTGO T-Call V1.4 ESP32 Wireless Module-User-Manual

[23] Md Atiqur Rahman and Jayanti Choudhary (2023) “IoT-based compensation and control of power theft in weak distribution system” Eng. Res. Express 5 04505