American Journal of Engineering Research (AJER)
e-ISSN: 2320-0847 p-ISSN : 2320-0936
Volume-5, Issue-10, pp-347-353
www.ajer.org
Research Paper Open Access

An IoT Based Tamper Prevention System for Electricity Meter

R. E. Ogu[1], Prof. G. A. Chukwudebe[1], I. A. Ezenugu[2]
[1]*Dept. of Electrical and Electronic Engineering, Federal University of Technology, Owerri, Nigeria.*
[2]*Dept of Electrical/Electronic Engineering, Imo State University, Owerri, Nigeria.*

ABSTRACT: *This paper presents an IoT based Tamper Prevention System for Electricity Meters (IoTETPS). The power sector in Nigeria is an untapped gold mine for investors, because of the huge population without access to stable electricity. However, electricity theft is one of the challenges facing the power companies; it makes the infrastructure needed for effective operations to be unsustainable because power companies cannot make adequate profit from the electricity they generate and distribute. This work has developed an embedded system that will help in prevention of electricity theft using Internet of Things technology. The system comprises of an Arduino WiFi Shield 101 mounted on top of Arduino Mega 2560 board for the connectivity and controller functions, while a Passive Infrared Sensor and Solid State Relay were used for sensing and actuation. The result of this work is a functional Internet of Things based system that is capable of detecting tamper and disconnecting the consumer; this is in addition to sending the GPS location of the meter to the distribution company portal. The incorporation of this system will reduce electricity theft, make the Grid smart and subsequently lead to a vibrant profitable power sector.*

Keywords: *detection, electricity theft, Energy Management, Internet of Things, prevention, Smart Grid.*

I. INTRODUCTION

With over 170 million people, and an installed capacity of less than 10,500MW by mid 2016, the Nigerian power sector is an untapped gold mine [1]. The liberalization of the power and telecom sectors in Nigeria started same time in 2000; sixteen years after, the telecom sector has recorded huge successes. The tele-density of the country has become transformed from 0.3% in 1999 to 104% in 2015 [2].

The major reason for this success was the availability of prepaid payment platforms for mobile phone technology. With the tamper proof prepaid technology for mobile phone systems, investors were able to quickly recoup their investments, and make huge profits as they roll out more phone lines. Unfortunately, it is a different scenario for the Power sector; the investors were hesitant because the technology for averting electricity theft was not mature by early 2000s. This is coupled with several issues such as illegal connections, old non-functional analog meters, transformer and transmission line vandalizations, etc.

As at the time of writing this paper, the Nigerian power sector had become unbundled with private investors in the distribution and generating sectors. Unfortunately, very little improvement is observed, probably because there is presently no competition in the distribution sector; since consumers have only one operator in their zone. Hence, the issues are still persisting; some electricity consumers get inflated bills of power not consumed, some are tapping electricity directly from the distribution network while some bypass their prepaid meters, etc. All these activities constitute electricity theft.

Electricity theft, an activity done, so that the consumer of electricity will use electric power without paying, is one of the crippling factors in Electricity distribution business. It contributes to an appreciable amount of the losses classified as non-technical losses [3]. Electricity theft has several disadvantages, both for the operator and consumer. Often the operator tries to compensate for the losses by hiking the electricity tariff and causing the masses to pay more than they should [4].

Naturally, if the consumers do not pay for electricity used; the distribution companies will not be able to pay for power generated and transmitted to them, the situation creates a vicious cycle that can cripples any electricity sector.

Presently, the power grid in Nigeria is not smart and this has prevented the electricity companies (Generating, Transmission and Distribution) from the proper management of the electricity they generate, transmit and distribute respectively.

In this research, to address the issue at the Distributor/consumer interface, a tamper-proof smart meter using Internet of Things (IoT) technology is proposed. The Internet of Things, a technology that can connect

devices (sensors and actuators) to the Internet or intranets, to reduce human interference to machine operations, promises to be useful in home automation, transportation, energy management, environmental monitoring, etc.

From the study, IoT will revolutionize all aspect of human life starting from the home to the industrial activities [5]. IoT technology promises to be able to proffer solutions to the nagging energy management challenges in developing countries.

II. LITERATURE SURVEY

Electric power theft occurs in several forms and various groups of people involved in the act include: power utility staff and consumers or even an amalgamation of the two groups of people. Electricity theft is a serious problem facing utility companies in many developing countries; it is capable of destroying the entire power sector of any country [4]. In the following section, a summary of related literature on mitigation of electricity theft is presented.

In [3], an Advanced Metering Infrastructure (AMI) was proposed to help in mitigation. A ZigBee module was utilized to send the status of the meter to the utility company. They concluded that electricity theft is still possible even with the installation of smart meters and suggested that sensitization of the people is very important so that they can avoid electricity theft.

An electricity detection system that indicates when there is electricity theft was presented in [6]. This device will consider any act to bypass the meter as a means of electricity theft. In this system, one current transformer is placed at the input side of a pole while another current transformer is placed at the distribution point of the consumer. The values of the current through the current transformers are compared by a microcontroller (PIC microcontroller). If there is a sufficient difference between the two currents, an RF transmitter communicates with an RF receiver which is placed on a board, the RF receiver transfers the data to a microcontroller which in turn sends an SMS to the utility company using a GSM module [6].

A ZIGBEE based system electricity theft detection system was designed in [7]. The system uses a comparative method in its operation, a watt-second meter is used as a standard meter to test power used by a consumer, while another meter whose calibration/accuracy is well known is used to measure the power consumed over the same period of time with the same load conditions [7].

In [8], an Energy Meter Tampering Detection and Prevention is developed. In the system, there is a photodiode illuminated by an Infrared LED. In the normal operation (when the meter has is not tampered with), the photodiode is configured to send logic 0 to the microcontroller but when the meter is tampered with, the photodiode sends logic 1 to the microcontroller. The microcontroller sends a message to the utility company using a GSM module. The power can be cut off or the meter can be replaced as an action when the utility company receives a message [8].

A system which detects any type of electricity theft: power tapping and meter tampering is proposed in [9]. It uses wireless techniques to communicate the location of the theft activity to the utility company. While an IoT based system which consists of Power Line Communication (PLC) modem, a theft detection unit and a Wi-Fi unit was presented in [10]. It had two separate systems; one of the systems is installed at the point of entrance of electricity in a consumer's premises while the other unit is installed at the utility company. This system utilized three microcontrollers; two were used in the system installed at the consumers end while the third was used in the system located at the utility office [10].

A system which compares the current passing through the low voltage side of the distribution transformer and the current passing through the meter of a connected consumer was proposed in [11]. In this system, a control unit incorporated in the device so that once an electricity theft activity is detected; the unit injects frequency disturbances in the low voltage side.

This work reviewed the shortcomings of existing systems in literature and developed an IoT based electricity theft prevention system to mitigate some of the identified frequently used techniques for electricity theft in Nigeria.

III. METHODOLOGY

An IoT based Tamper Prevention System for Electricity Meters (IoTETPS) is designed and a prototype implemented in this work. It is assumed that the meter is placed in a boxlike enclosure with the display and keypad portions of the meter exposed. The IoTETPS will be inside the meter box, any attempt by anybody to open the box to tamper with the meter or bypass it will disconnect the electricity supply and a message will be seen at the distributor's office showing the time of tamper and the exact geographical location of the meter.

3.1 System Development

The proposed system is conceptualized in a way that it will suit either the Green-field approach or the Brown-field approach of incorporating the Internet of Things technology to a system. As the concept is

confirmed, meter manufacturers can start integrating it to electricity meters during manufacture to ensure a smart energy management ecosystem.

IoT technology involves the gathering of data, transmission of data to the Internet and analysis of the data. Thus, generally, an IoT system will contain sensors, processors and network interfaces as its main elements. The block diagram of IoTETPS is shown in Figure 1. It should be noted that the software part of an IoT device is responsible for the behavior of the device and it is written in the Ardiuno platform for this research.

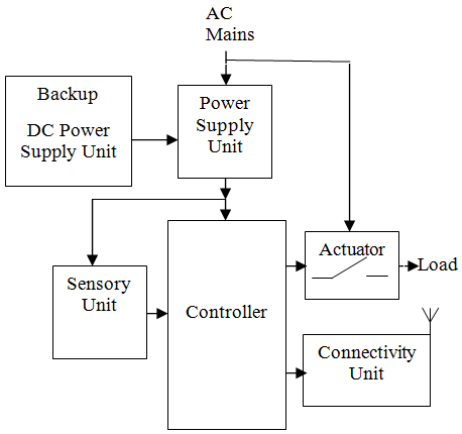

Figure 1: Block Diagram of IoT Electricity Meter Tamper Prevention System (IoTETPS).

3.1.2 The Controller

The controller is the heart or the brain of the entire system; it coordinates the functionality of other parts of the system. It can be any microcontroller, for this research, an Arduino microcontroller board was used for easy prototyping, implementation, and emulation of embedded systems.

3.1.3 The Sensory Unit

The sensory unit is responsible for detecting when the meter has been tampered with. Upon detection of any tampering activity, it sends signals to the microcontroller which in turn coordinates the proper response of other parts of the system.

In this approach, whenever the sensitive part of a meter is opened, the sensory unit will signal the controller that the meter has been tampered with. For an electromechanical meter, the sensitive part can be considered as the rotating disc or the part where connections are made to the meter, while the sensitive part of an electronic meter is considered as the terminals where connection are being made to the meter or the board where the electronic circuits are located.

For this research, the sensory unit is a Passive Infrared Sensor (PIR), located in the meter enclosure. The PIR sensor will detect the presence of anybody who opens the meter enclosure or tries to bypass the meter; and send a signal to the controller.

3.1.4 The Connectivity Unit

For any device to be able to connect to the Internet, it must first of all connect to a network that is Internet-ready. The connectivity unit of the proposed system performs the tasks of connecting the device to a network and subsequently connecting the system to the Internet. In this case, the system can connect to a Wi-Fi network and then connect to the Internet. The Arduino Wi-Fi Shield 101 which is designed for IoT technology is used for this research [12].

3.1.5 The Actuator

The actuator in this regard is responsible for either connecting the meter to the load or disconnecting the load from the meter when there is tamper activity. A solid State Relay (SSR) is used in this regard.

3.2 The IoT Electricity Tamper Prevention System Implementation

The Arduino WiFi Shield 101 was mounted on top of the Arduino Mega 2560 board (just like other shields). The output of the PIR sensor was connected to the A0 analogue input pin of the Arduino WiFi Shield 101. The input of the Solid State Relay (SSR) was connected to digital pin 5 of the Arduino WiFi Shield 101. The Power Supply Unit was constructed and connected to the other parts of the system using a power jack.

After the hardware integration the software program was uploaded to the Microcontroller using a USB cable, to form a complete system. The complete system is shown in Figure 2.

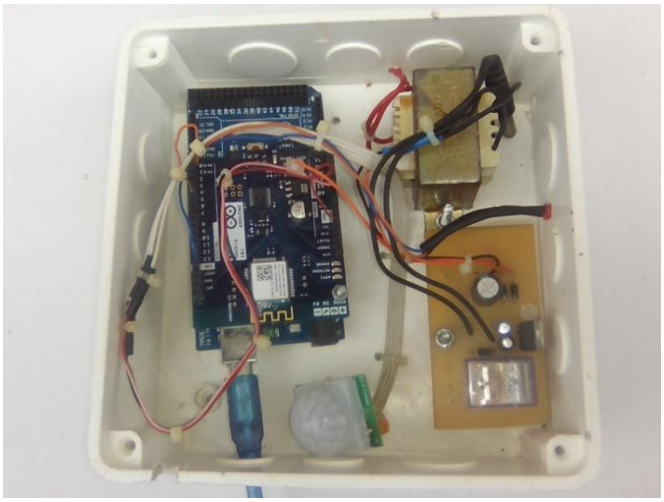

Figure 2: The IoT Electricity Tamper Prevention System.

3.3 System Operation and Simulation

The algorithm that illustrates the mode of operation of the system is represented as a flowchart in Figure 3. Once the device is powered ON, all components will be initialized. The system will check if the connectivity interface is in proper working condition. If the connectivity interface is working properly, the system constantly checks if the meter is tampered with. As soon as the meter is tampered with, the sensor will send a signal to the processor which will in turn trigger the connectivity interface to send message to the Web that the meter has been tampered with. At the same time, the load connected to the meter is disconnected from the distribution network.

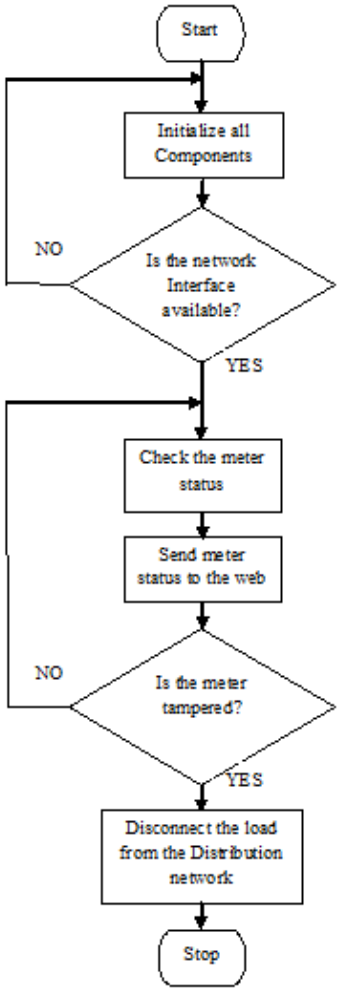

Figure 3: IoTETPS Operation Flowchart.

The system is designed in a way that the status of the device is always shown on a Web page of the Control Center of the Distribution Company. For this research, the *"Thingspeak"* platform was used for data collection and analysis [13]. An account was created with the *Thingspeak* platform and a channel named Ant-Theft. The location and status of a chosen meter can be viewed at www.thingspeak.com/channels/112443. The channel is set to private mode and cannot be viewed by the public. The IoTETPS was put in a box and tested.

IV. RESULTS AND DISCUSSION

4.1 Results

Figure 4 shows a snapshot of the Web page during the simulation process. Once the *Meter box enclosure* is opened, the graph rises and indicates the exact time of tamper on the left side, while the map on right shows the exact loction of the meter.

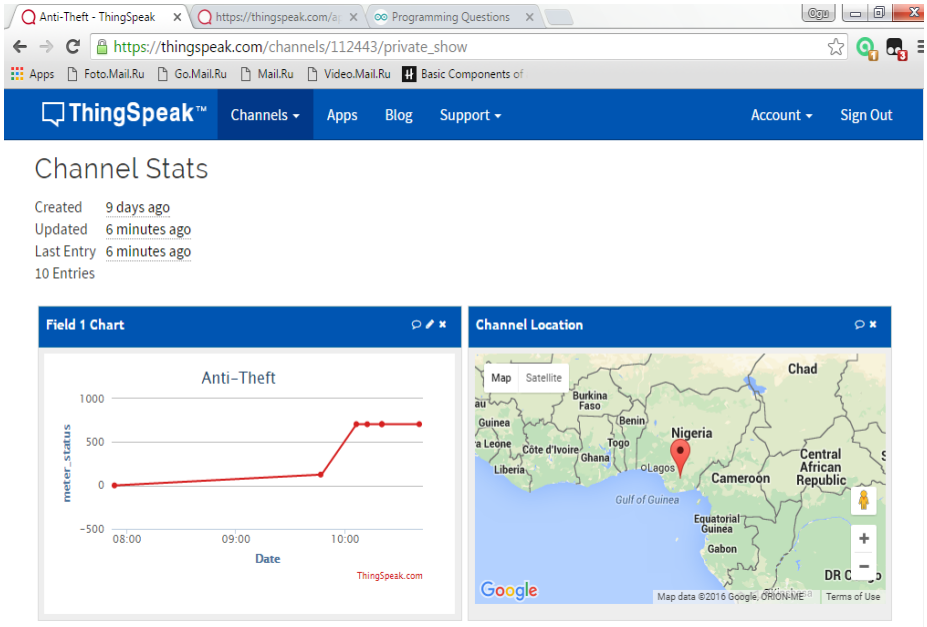

Figure 4: Web channel when Meter is tampered with.

The snapshot on opening many times and closing is show in Figure 5.

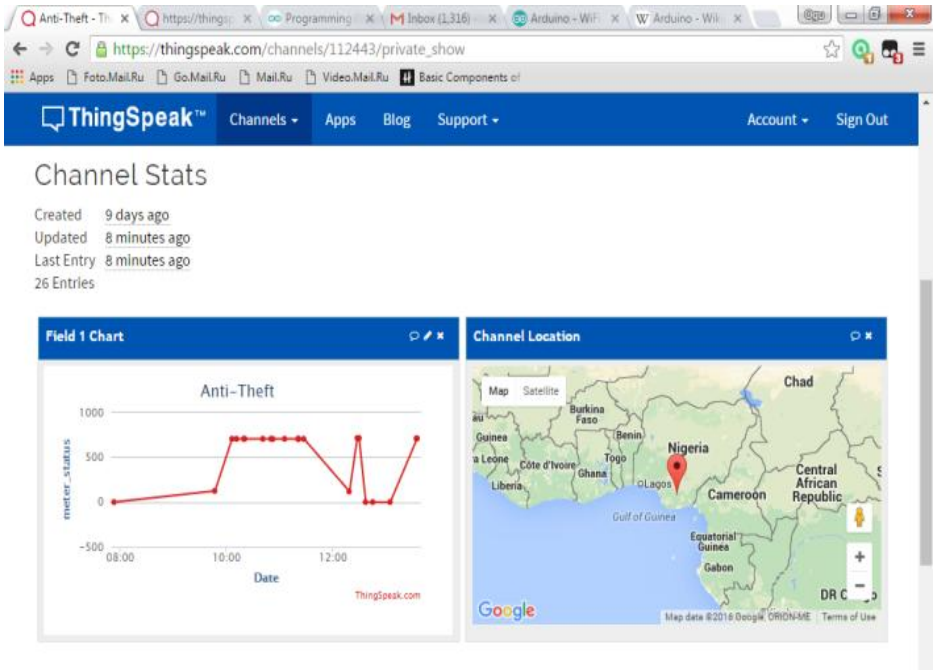

Figure 5: Snapshot of the entire simulation process.

4.2 Discussion

Figure 5 is a continuation of Figure 4, it can be observed from the snapshot that between 8am and 10am, the graph is almost a straight horizontal line indicating that the meter has not been tampered with. This means that the PIR sensor has not detected the presence of any human because the meter enclosure is still intact and thus it sent a 0V to the controller which in turn used the connectivity module to update the Internet.

As soon as the enclosure was opened at 10am, the PIR detected the presence of a human; it outputted a 3.1V to the controller which in turn updated the Internet by making the initial horizontal line to rise (Figure 5). This indicates that the meter has been tampered with. As long as the enclosure remained opened, the system periodically updated the webpage that there is a tampering activity.

In Figure 5, it can be seen that sometime before 12noon, the meter box was closed and thereafter opened again by 12noon, closed soon after and around 12:30pm it was opened. Thus the graph has the spikes; sharp transition from down to up and up to down.

The exact location of the meter is shown on the right hand of Figure 5 to enable the Distribution Company apprehend the electricity thief for necessary action.

V. CONCLUSION

Electricity theft is a great challenge for developing economies without adequate installed capacity and distribution network. For the Nigerian power sector used as a case study, although, the sector has become unbundled with private investors in the distribution and generating sectors; there is presently no competition in the Distribution sector, consequently, the issues are still persisting; some electricity consumers get inflated bills of power not consumed, some are tapping electricity directly from the distribution network, some bypass their prepaid meters, etc

Obviously, if the consumers do not pay for electricity used, the distribution companies will not be able to pay for power generated and transmitted to them; the situation creates a vicious cycle that can cripple any electricity sector.

Presently, the power grid in Nigeria is not smart and this has prevented the electricity companies (Generating, Transmission and Distribution) from the proper management of the electricity they generate, transmit and distribute respectively.

In this research, to address the issue at the distributor/consumer interface, an IoT based tamper-proof add-on to the meter enclosure is developed and implemented.

The study has been able to achieve its main objective to develop an embedded system that will help in the detection and prevention of electricity theft in order to ensure improvement in energy management.

VI. RECOMMENDATIONS

One key success factor for the power sector of developing economies like Nigeria will be introduction of resilient tamper-proof consumer electricity meters. Once there are robust platforms for payment of bills, the distribution companies can maintain existing facilities, expand the networks and be able to buy more power from generating companies. The generating companies will in turn increase power generation; the push will also motivate the transmission company to expand.

In this work, only one meter was used; it is recommended that further work should experiment with many meters. This solution works well where there is access to Internet/Intranet, for real life implementation, distribution companies need to subscribe to an Internet Service Provider or have their own intranet.

One of the factors that have delayed investment in the Nigerian power sector was unavailability of payment technology to avert electricity theft; electricity meter manufacturer's can utilize this IoTETPS concept for integration into smart meters to make them tamper-proof.

This work did not consider cases of tamper, whereby the consumer taps directly from the distribution line, though this is not common, its solution is recommended for further research.

REFERENCE

[1]. Nigeria Electricity Market, NIPP, http://www.nipptransactions.com/background/electricity-market/, accessed June 6, 2016.

[2]. Subscriber statistics, Nigerian Communications Commision, http://www.ncc.gov.ng/index.php? option=com_content& view=article &id=125&Itemid=73 , accessed June 9, 2016.

[3]. M. Anas, N. Javaid, A. Mahmood, S. M. Raza, U. Qasim, and Z. A. Khan, "Minimizing Electricity Theft using Smart Meters in AMI", arXiv:1208.2321v1 [cs.NI] (2012).

[4]. R. Kalaivani, M. Gowthami, S. Savitha, N. Karthick, and S. Mohanvel, "GSM Based Electricity Theft Identification in Distribution Systems" International Journal of Engineering Trends and Technology (IJETT), ISSN: 2231-5381, Volume 8 Number 10, pp. 512-516, http://www.ijettjournal.org,(2014).

[5]. D. Evans,"The Internet of Things: How the Next Evolution of the Internet Is Changing Everything", Cisco White Paper, http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf, accessed May 2016.

[6]. S. Anusha, M. Madhavi,and R. Hemalatha, Detection of Power Theft Using GSM, *International Journal of Advanced Research Trends in Engineering and Technology (IJARTET), Vol. 1(I3),* 2014, pp.15-17.

[7]. P. Virendra, S. G. Simrat, and S. Amit, Wireless Electricity Theft Detection System Using Zigbee Technology, *International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321 – 8169, Volume:1(4)* (2013),pp.364–367.
[8]. T. Agarwal, "Power Theft Prevention Techniques", https://www.elprocus.com/power-theft-prevention-techniques/, accessed June 9, 2016.
[9]. P. Sagar, P. Gopal, and P. Kirtikumar, Electrical Power Theft Detection and Wireless Meter Reading, *International Journal of Innovative Research in Science, Engineering and Technology, ISSN: 2319-8753, Vol. 2(4)*, 2013, pp.1114-1119.
[10]. N. Darshan, and K. A. R. Radhakrishna, IoT Based Electricity Energy Meter Reading, Theft Detection and Disconnection using PLC modem and Power Optimization, *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 4(7)*, 2015, pp.6482-6491.
[11]. S. Thangalakshmi, G. Sangeetha, and S. Muthu, Power Theft Prevention in Distribution Systems using Smart Devices, *International Journal of Applied Engineering Research ISSN 0973-4562, Vol. 10(42)*, 2015, pp.30841-30845.
[12]. WiFi 101 ThingSpeak Data Uploader Tutorial, https://www.arduino.cc/en/Guide/ArduinoWiFiShield101, accessed March 27, 2016.
[13]. ThingSpeak Community Arduino Tutorial, http://community.thingspeak.com/tutorials/arduino/send-data-to-thingspeak-with-arduino/, accessed March 27, 2016.