International Journal of Electrical and Computer Engineering (IJECE)
Vol. 9, No. 5, October 2019, pp. 4184~4191
ISSN: 2088-8708, DOI: 10.11591/ijece.v9i5.pp4184-4191

Smart prepaid energy metering system to detect energy theft with facility for real time monitoring

Somefun T.E., Awosope C.O.A, Chiagoro A.
Department of Electrical and Information Engineering, Covenant University, Ogun State

Article Info

Article history:

Received Jun 28, 2018
Revised Apr 22, 2019
Accepted Apr 30, 2019

Keywords:

Advanced meter infrastructure
Electricity theft
Energy management
Microcontroller
Smart-meter

ABSTRACT

Electricity theft remains a huge loss incurred by electricity distribution companies. This theft arises majorly because of activities carried out by consumers such as energy-meter by-passing, energy-meter tampering etc. This research study offers an approach for handling energy meter by-passing and tampering. The system design is based on the monitoring of the readings of two current sensors by a programmed microcontroller. While one of the current sensors monitors the current drawn by the user's load, the latter installed before the meter monitors current drawn by all loads. Any discrepancy between the values read, indicates theft. A momentary switch is also installed in the meter to trigger the meter once it is tampered with. Furthermore, the user is provided with a remote access to the energy meter for recharging energy units and for monitoring energy consumption. It was observed that the system accurately measured load consumption and detect any attempt to by-pass or tamper with the energy meter. Lastly, all unscrupulous attempts were reported using GSM technology.

Corresponding Author:

Somefun T.E.,
Department of Electrical and Information Engineering,
Covenant University, Canaan land, KM 10, Idiroko Rood,
P. M. B. 1023, Ota, Ogun State.
Email: tobi.shomefun@covenantuniversity.edu.ng

1. INTRODUCTION

It is impossible for an electric power system to be 100% free from theft. In 1999, Transparency International revealed that close to 15% of the generated power is lost as a result of electricity theft. For instance, between 1998 and 1999, in Bangladesh, the Bangladesh Power Development Board (BPDB), after generating about 14,600 MWhr of electricity, could only account for 11,462 MWhr of billed energy, reflecting a total loss of about 22% [1]. In developing countries like Nigeria, electricity theft remains one of the major problems being faced by the power sector of which the government has little or no control over due to lack of the required technology. While the implementation of Automatic Metering Infrastructure (AMI) has eliminated the need for meter readers, it has adversely increased non-technical losses incurred by power utility companies [2]. It is estimated that Nigeria's grid has a total transmission and distribution (T&D) losses of about 40% which is tremendously high when compared to United States whose T&D losses are at 7% [3, 4]. Electricity theft is a form of non-technical loss. According to [5], any form of interference done by complete or partial bypassing of the meter to adulterate its values is referred to as electricity theft. The Non-technical losses are caused by human error. This error is an external action that has nothing to do with the characteristics of the power system. These activities include meter tampering, bypassing of meter, billing irregularities and unpaid bills [4, 6, 7]. To respond to the electricity theft and growth trend, the country needs to take appropriate initiatives not only to boost its power generation capacity but also to make residential sector more energy smart and efficient [8].

Analogue meters which are still widely used in most parts of the nation, pose lots of challenges for monitoring the power consumed by users. In addition, with the analogue meters, operators must go to the consumer's house to disconnect his power supply if he does not pay up his bills. Even in most cases, the operators accept bribes from the consumer so that their supply will not be disconnected. Consumers also have been known to tamper with the energy meters in order to reduce or stop the meter from reading without the knowledge of the operators. With traditional analogue meters, consumers have no way of disconnecting power in their houses when they travel and forget to disconnect or turn off their appliances. This leaves the meter running, incurring more payment for the energy consumer. Prepaid meters have provided a better way of monitoring power consumption by users. The motivation of this study is based on the fact that electricity theft as a result of energy meter by-passing and energy meter tampering has constituted a major problem to the power supply stabilization and has also resulted in a huge loss of revenue to the Nigerian power sector.

This study aims at developing a system with energy meter theft and tampering detection systems that can accurately measure and monitor the supply and distribution of power. In addition, it provides a remote energy management system for the consumer to disconnect or connect his load at free will. The rest of this paper is organized as follows. Section 2 reviews the previous researches related to energy theft detection and meter tampering that have been carried out earlier. Section 3 discusses the methodology for this study. The implementation and results are presented in section 4. In section 5, recommendations for future works are given.

2. REVIEW OF RELATED WORKS

2.1. Anti-theft metering for smart electrical distribution system [5]

A conceptual approach was used to determine both the approximate location of energy theft and estimation of the energy theft at the location using power line communication as the tool of communication by AMI's. Analog signal being continuous in nature, reflects deterioration that occurs during its transmission from the sender to the receiver end. The signal's signature deterioration is utilized for diagnosis and localization of energy theft. Using Power line carrier (PLC), a carrier frequency is modulated on top of existing 50/60-Hz power line carriers. In this system, meters communicate with each other via PLC such that if meter A sends a signal to meter B, meter A acknowledges and sends to the base station. If no tapping has occurred between the meters, signal will not deteriorate. The Automatic Metering Infrastructure must be equipped with filters as the signal must be filtered before supplying power to the loads. This filtered signal is compared with the base signal or reference signal to determine if deterioration has occurred and to what level. If there is deterioration, which indicates that power has been tapped illegally between the two meters, meter B will identify this corrupt signal and will communicate it to the central station. The degree of deterioration is dependent on the power consumed at the illegal tapings between the meters. In addition, since the metering facility employed here is of Automatic Metering Infrastructure (AMI) type, and communication exists between meters and base stations, electricity theft coordinates could be located within the range of two meters where deterioration occurred. For this system to be effective, all valid meters must be equipped with PLC handshaking capability.

2.2. A smart prepaid energy metering system to control electricity theft [1]

Nabil Mohammed et al proposed a prepaid energy metering system that controls electricity theft. A single-phase smart meter is installed at the consumer's unit which communicates with a server that is run by the public utility. Each meter and server were equipped with a GSM module which served the purpose of bi-directional communication between the smart meter and the server. In this project, the energy metering units consisted of an ATmega 32 microcontroller, ADE7751 energy measuring chip, Siemens A62 mobile phone as the GSM module, MAX232, current transformer (CT-1) and potential transformer (PT-1) used for current and voltage measurements, LCD display and a relay. Pulses proportional to the energy consumed by the user are produced by the energy metering chip. Energy consumption calculation is done by the microcontroller which counts the output pulses generated by the energy metering chip on an interrupt basis.

To protect against electricity theft by short circuiting phase and neutral lines, the meter was equipped with two current transformers (CT-1 and CT-2): One in the single phase and the other on the neutral line whose outputs are fed to the Analog-to-Digital Converter (ADC) of the microcontroller. The microcontroller compares the output from these current transformers. If there is a significant difference, the microcontroller instructs the relay to cut-off supply to load and a text-message is sent to the server informing it of the theft occurrence so that actions can be taken by the authority. If the two values vary considerably, the central meter knows that energy theft has occurred. The exact location of theft is found on the basis of zero or low energy consumption based on the individual meter reading data by the observer meter. The observer meter then sends a message to the authority informing it of the energy theft occurrence.

Two lever switches were used at the two sides of the energy metre to guard against meter tampering where one terminal is connected to a 5-V dc supply and the other terminal to the microcontroller. Under normal operating conditions, the switches are closed, and the microcontroller gets a 5-V dc input. Once the meter is opened, the switch is opened, and the microcontroller will notify the server of meter tampering.

2.3. Anti-theft automatic metering interface [9]

Abhijeet Das et al. proposed an anti-theft automatic metering interface system that consists of a microcontroller (Arduino) that will continuously monitor and store the energy meter readings in its memory. GSM module was used for monitoring and controlling the energy meter remotely with the help of an interfacing circuitry which counts the pulses with respect to the amount of power the user consumes. The stored energy value is sent to the microcontroller at the utility base on request usually at 30days count interval for the purpose of billing. To detect meter bypassing, they suggested that a comparator be set in parallel to the meter, such that, two inputs are fed into the comparator, one before the supply enters the meter and the other input taken from the point after it passes the meter. In the case of bypassing, there will be a huge difference between the input values to the comparator and hence a large current passes through this comparator which feeds the microcontroller. A tactile sensor which is sensitive to touch, force, pressure was proposed for detection of meter tampering.

2.4. Development of advanced reduced instruction set computer (ARISC) machine processor-based electricity theft control system using GSM network [2]

In this work, a system which consists of LPC1343, ARM processor, ACS712 30-A range current sensor, potential transformer with four-terminal regulated power supply, GSM module for communication, lever switch and 200W AC load was proposed. The technique of theft detection adopted by this system is very similar to the method used by [1]. The major difference here is the use of the four-terminal output regulated potential transformer instead of using two potential transformers. One of the four terminals is connected directly to the energy measuring unit and the remaining 3 terminals are regulated to 3.3-V DC. One out of the three regulated DC voltages is fed to the interrupt pin of the ARM processor for the purpose of detecting whole meter bypassing and the remaining two terminals are used to charge the battery that powers the GSM module and the ARM processor. Hence, reducing cost and also making the system more efficient. This system was tested for all the four different theft modes using double-pole throw switches to simulate the phase and neutral line shorts. For each of these modes, SMS was sent using GSM. The entire system consumes less power (3.3V for the ARM processor) and current in few milliamps.

2.5. Intelligent power theft detection model for prepaid energy metering in Nigeria [10]

The author proposed a power theft detection model made up of three parts, namely: Intelligent Prepaid Meter (IPEM) which is at the consumer's end, Intelligent Power Theft Detection System (IPTDS) at the transformer end or at the electric pole before distributing to consumer, and the Utility Control Server. Unmetered energy consumption is detected by the IPTDS. The communication channel for this implementation is Radio Frequency and GSM communication. A sent SMS is triggered once, and an unmetered consumption is detected. The IPTDS is based on the principle of installing a tree of meters below the IPTDS such that each meter measures the power consumed by the meter directly below it. An intelligent statistical meter is placed at the node of the residential power grid with additional meters placed below it for measuring the consumption of loads beneath it in the branch. A comparison is done by the system between the readings taken by the main Intelligent Statistical Meter and those obtained from the branch intelligent meters. If the values obtained from the main ISM are far greater than those obtained from the sum of the branches, it indicates the usage of illegal power by the consumers and hence the main ISM sends a SMS to the utility.

2.6. Automatic energy meter with power theft detector using GSM [11]

In this system, R. Pradeep Raja et al. proposed the use of a smart energy meter sensor to be connected between the power lines and an automatic energy meter through microcontroller and GSM module. The energy meter sensor will continuously monitor the amount of power that is drawn from the line before the meter. These values will be stored in the flash memory of the device. It also compares the values stored with that recorded by the smart meter. If there are discrepancies, then energy theft has occurred, and a SMS will be automatically sent to the electricity board. The microcontroller used for this prototype was ATMEGA.

Unlike previous related studies, this present study offers a more accurate and realistic way of detecting energy meter by-passing and energy theft. Previous researchers have presented systems that calculate, estimate and predict user's consumption based on consumption patterns within a specified period

[1, 2, 5, 9, 10, 11]. Such that the energy meter compares the stored and estimated consumption with the current consumption. A spike in the consumption pattern will indicate probable theft which may not always be true as it is not unusual for the user's consumption to increase. Hence, this research paper proposes a system that does real time monitoring and comparison of the current drawn from the point of delivery (i.e. utility pole) and the current drawn by the user's load as recorded by the energy meter in order to detect energy theft. More so, this research study includes a system of implementing energy theft detection that does not incorporate any external circuitry for comparison of currents drawn by the legal load and illegal load as suggested by previous conducted research works. In this system, the microcontroller (Arduino Nano) is responsible for monitoring these values. In essence, it can be seen as a cheaper method of implementing energy theft detection. Furthermore, in addition to detecting energy meter by-passing and energy meter tampering, this study also incorporates energy management. It offers a system where a user can remotely decide to cut-off or turn on energy supply to his load to save energy. He can remotely instantly and view his energy consumption status.

3. RESEARCH MATERIALS AND METHODS

This section discusses in detail and the description of the work done, modelling and design of the proposed system. Figure 1 depicts the functional block diagram of the smart prepaid energy meter for energy theft detection. This shows how the various components are interlinked.

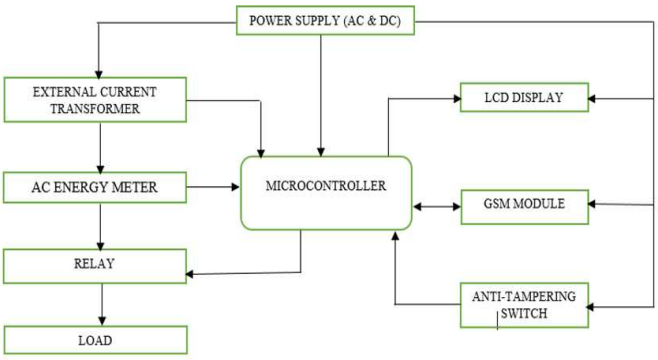

Figure 1. Block diagram of the smart prepaid energy meter for energy theft and meter tampering detection

The design methodology is divided into sub-sections as follows:
1. Power Supply Circuit;
2. Metering Circuit;
3. Energy theft and meter tampering detection circuits;
4. Microcontroller section;
5. Energy Management section; and
6. Communication section.

3.1. Power supply circuit

The microcontroller, LCD and the relay require a 12V DC supply. The microcontroller has an in-built voltage regulator that steps down the voltage level to the required 5V DC. The mains supply is 240V AC which is stepped down to 12V AC using a 240-V/12-V step-down transformer. A bridge rectifier is used to convert the 12V-AC to 12V DC voltage. A high value capacitor of 1000uF is used to remove all the ripples present in order to obtain a pure DC voltage. The GSM SIM 800 module used for communication purpose requires 4.2V-DC supply. An integrated circuit LM317, an adjustable voltage regulator is used to achieve this voltage level.

3.2. Metering circuit

The metering section is made up of the voltage sensing and current sensing circuits. These sensing circuits are used to measure the current drawn by the load from the supply and the voltage supply in order to calculate the power and measure consumption.

3.3. Current sensing circuit

In order to measure the alternating current, a bar primary current transformer with 1,000:1 transformation ratio was used. The output of the current transformer is connected to the ADC pin of the microcontroller. A small value resistor of 220 ohms is connected across the terminals of the current transformer. The microcontroller measures current indirectly by reading the peak-to-peak voltage across the secondary terminal of the current transformer and dividing this value by the burden/resistance connected across the secondary terminal of the current transformer according to Ohm's law (V= I.R). The root mean square value (rms) of the current is obtained by multiplying the current by 0.707. This value is then multiplied by the 1,000 which is the transformation ratio to get the actual primary current.

3.4. Voltage sensing circuit

The voltage across the connected load is measured using a voltage sensor. The voltage sensor is connected across the mains supply with its output connected to the microcontroller. The principle of operation of the voltage sensor employed is based on voltage divider circuits. This is done so as to reduce voltage level across the Analog-to-Digital Converter (ADC) pin of the microcontroller. 3 resistors are connected in series. 100K on the live (R1), another 100K on the neutral (R2) and a 1K joining the two (R3) as shown in Figure 2.

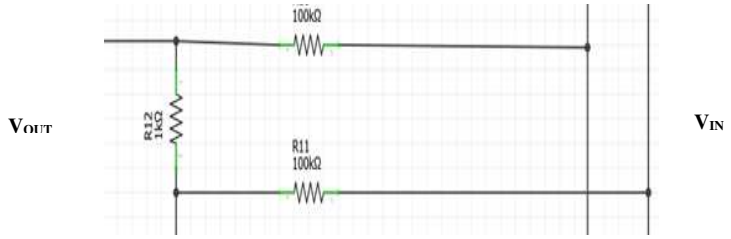

Figure 2. Voltage divider circuit

3.5. Analysis of the voltage sensing circuit

Input Voltage from Primary side of transformer, VIN = 240V
Applying voltage divider rule, we have

$$V_{OUT} = \frac{V_{IN} \times R_3}{R_1 + R_2 + R_3} \quad (1)$$

Using this technique, the maximum amount of voltage that can be sensed by the ADC port of the microcontroller is 1.194V of which the Arduino can handle safely. These values are multiplied by a scaling factor in order to obtain the true voltage value that was read by the voltage sensor. The scaling factor is obtained as follows.

3.6. Derivation of scaling factor

Resolution of Arduino ADC = 10bits;
Resolution in decimal = 0 to 1023 possible combinations;
Arduino reference voltage = 5V;
Value of 1 Least Significant Bit (LSB) is $\frac{5}{1023} = 0.004882$;
Ratio of resistance = $\frac{1K}{100K + 100K + 1K} = 0.00497512$;

$$\text{Scaling factor} = \frac{\text{Value of 1 LSB}}{\text{Ratio of Resistance}} \quad (2)$$

$$\therefore \text{Scaling factor} = \frac{0.004882}{0.00497512} = 0.98090.$$

3.7. Energy theft and meter tampering detection circuits

The energy theft detection or meter bypassing system was achieved by incorporating a second current transformer found externally as shown in Figure 3 which precedes the main current transformer that is used for calculating power. The output of this external current transformer is connected to the analogue pin

of the microcontroller. The current drawn from the live is calculated by the microcontroller the same way it calculates the current for the internal current transformer. The microcontroller compares the values of current that are measured by the external and internal current transformers. Under normal conditions, when there is no bypassing, the values read by the two current transformers should be equal. If the current value read by the external current transformer at any time becomes greater than the value which the second transformer used for calculating energy reads, it means the energy meter has been bypassed. The microcontroller then communicates with the GSM SIM module and a SMS is sent to the administrator.

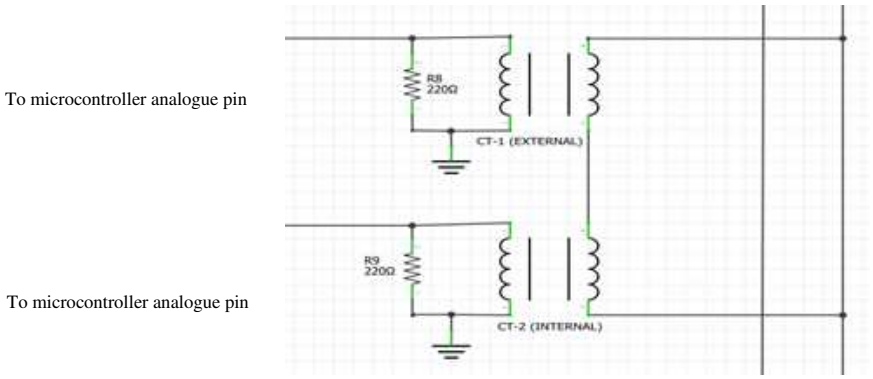

Figure 3. Meter by-passing circuit

Furthermore, the energy meter is protected from fondling with by the user through the use of a momentary switch. The throw part of the switch is connected to one of the digital pins of the Arduino microcontroller (pin D2). Under normal condition, when the energy meter is sealed, the switch is open, the digital pin gets a logic 0. Once the energy meter is opened, the switch closes, the digital pin receives a logic 1 and the microcontroller prompts the GSM SIM module to send a SMS to the administrator informing him that the energy meter has been tampered with.

3.8. Microcontroller section

The microcontroller handles the computation of power, energy and the display on the LCD. The microcontroller is also responsible for reading the values of the analogue pins A0 and A1 which are the values from the internal and external current transformers respectively. It compares these values at all times to check for a huge difference which indicates the occurrence of meter bypassing/energy theft. It instructs the GSM module on when to send alerts and messages to the user or authority. In addition, the microcontroller also handles the decoding of the prepayment voucher pins which are sent by SMS to the GSM module. The microcontroller used in this work is the Arduino Nano which is based on ATmega328.

3.9. Energy management section

A 12V-DC relay was incorporated into this work such that when a "LOAD OFF" command is received by the microcontroller from the GSM module, the relay trips and the load is cut off. Hence, the energy meter does not continue to calculate consumption which saves the user energy. A NPN transistor (BC547) with its base connected to the analogue pin of the Arduino controls the switching of the relay. The transistor switches 'ON' whenever a "LOAD OFF" command is received from the GSM module. It triggers 'OFF' when a "LOAD ON" command is issued. A diode is connected in reverse biased direction across the relay in order to protect the transistor and the microcontroller.

3.10. Communication section

The main device responsible for this communication is the GSM (SIM 800) module. It accepts a SIM card which is a device that can store data such as location, phone number and the user identity of GSM subscribers. It provides connectivity for devices over mobile network. They also provide internet connectivity as well as Short Message Service (SMS). AT (Attention) command sets are required machine instructions used to activate different features on the GSM module. The Rx pin of the gsm module is connected to the Tx pin of the microcontroller, a NPN transistor is used to interface the Tx pin of the GSM module to the Rx pin of the microcontroller since its Tx voltage output is less than the required Arduino's 5V-DC. The algorithm of the energy theft detection/meter bypassing system is illustrated Figure 4.

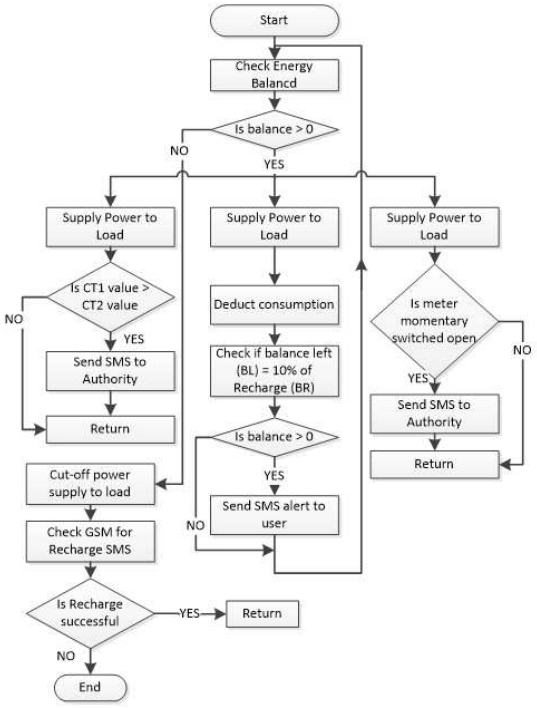

Figure 4. Smart meter for energy detection and tampering flow chart

4. RESULTS AND ANALYSIS

This section discusses how the work was implemented and the tests carried out to ensure it accomplishes its functionality.

4.1. Implementation

Proteus software and Fritzing were used to simulate the components, while coding of the Arduino Nano microcontroller was achieved by the Arduino Integrated Development Environment (IDE) installed on Microsoft Window 8 operating system. The Arduino codes were written in C language.

4.2. Testing

The testing of the system was done in different stages.

4.2.1. Units' testing

The energy metering system consists of different units which are integrated to form the whole system. Tests were carried out on the individual units. Such units' testing includes testing the transformer to be sure it supplies the appropriate step-down voltage and testing the relay unit to ensure its workability.

4.2.2. Power supply section testing

The power supply unit (which consists of the step-down transformer), the bridge rectifier and the smoothening capacitor were tested to ensure that the required voltage level was obtained.

4.2.3. Metering circuit testing

The metering section (which consists of the voltage sensing and current sensing circuits) was tested to ensure that it gives accurate readings of energy consumed. Load of known rated value was connected across the meter and its value was compared with that which was read by the meter displayed on the LCD. A 60-W incandescent bulb was connected, and the meter read it as 58.42W which is practically acceptable.

4.2.4. Energy metering by-passing testing

The meter by-pass was simulated by providing a power terminal connector where another 60-W incandescent bulb was connected just after the external current transformer. Once this load is connected, the microcontroller was able to detect this illegal load by comparing the values of the current transformers. A SMS notification is automatically sent to the utility.

4.2.5. Meter tampering testing

This section of the system was tested by opening the casing of the meter which activates the momentary switch attached to the interior of the plastic packaging. The utility's number was pre-registered on the microcontroller so as to receive the theft and tampering notifications. Once this was done, a SMS was sent to the authority to notify them of the tampering.

4.2.6. Energy management testing

This part of the system was tested by sending "Off" by SMS to the number registered on the GSM SIM module. The relay was triggered which resulted in cutting off the supply to the load by the meter. The Load is turned back on by sending "On" by SMS. The user can also get the status of the energy meter by sending "Status" via SMS.

4.2.7. Prepayment system testing

This section was tested by sending a recharge SMS to the GSM module in this format: *333*(4 digits)# where the 4 digits represent the units of energy in watts/hour that the user intends to recharge, for example, '*333*1000#'. If recharge is successful, the user is notified, and the energy unit is updated else, he is informed that recharge was unsuccessful.

5. CONCLUSION

In this paper, a Smart Prepaid Energy Metering System to detect energy theft by energy meter by-passing and tampering was designed, implemented and tested. The introduction of smart meters with enhanced capabilities and features provides a revolutionary advancement in the innovation of energy metering systems. In addition, it offers a solution to the curbing of the menace of electricity theft which accounts for a huge percentage of non-technical losses in power transmission and distribution. The major objectives of this system were achieved as the energy meter measured accurately the power consumed by the test load, notified the utility by SMS of energy meter by-passing and meter tampering. A remote access to the energy meter was provided to the user using GSM technology.

ACKNOWLEDGEMENTS

The authors would like to express special thanks and gratitude to Covenant University for their support.

REFERENCES

[1] N. Mohammad, et al., "A smart prepaid energy metering system to control electricity theft," *in 2013 International Conference on Power, Energy and Control (ICPEC)*, pp. 562-565, 2013.
[2] K. Dineshkumar, et al., "Development of ARM processor based electricity theft control system using GSM network," *in 2015 International Conference on Circuits, Power and Computing Technologies [ICCPCT 2015]*, pp. 1-6, 2015.
[3] C. Etukudor, et al., "The Daunting Challenges of the Nigerian Electricity Supply Industry," *Journal of Energy Technologies and Policy*, vol. 5, pp. 25-32, 2015.
[4] N. David and M. M. Josephine, "Curtailing Energy Theft by Remote Monitoring Case study: University of Nigeria, Nsukka," 2016.
[5] M. U. Hashmi and J. G. Priolkar, "Anti-theft energy metering for smart electrical distribution system," *in 2015 International Conference on Industrial Instrumentation and Control (ICIC)*, pp. 1424-1428, 2015.
[6] P. Elechi and D. Omorogiuwa, "Economic Effect of Technical and Non Technical Losses in Nigeria," *Power Transmission System*, vol. 10, 2015.
[7] K. O. Okokpujie, et al., "An automated energy meter reading system using GSM technology," 2017.
[8] F. Alrashed and M. Asif, "Trends in residential energy consumption in Saudi Arabia with particular reference to the Eastern Province," *Journal of Sustainable Development of Energy, Water and Environment Systems*, vol. 2, pp. 376-387, 2014.
[9] A. Das and P. P. Talukdar, "Anti-Theft Automatic Metering Interface," *International Journal of Scientific & Technology Research*, vol. 4, pp. 99-101, 2015.
[10] B. Omijeh, et al., "Intelligent Power Theft Detection Model for Prepaid Energy Metering In Nigeria," *International Journal of Electronics Communication and Computer Engineering*, 2012.
[11] P. R. Malhotra and R. Seethalakshmi, "Automatic meter reading and theft control system by using GSM," *International Journal of Engineering and Technology (IJET)*, vol. 5, pp. 806-810, 2013.