JJEE
Jordan Journal of Electrical Engineering
Volume 8, Number 4, December 2022
Pages 322-338
ISSN (Print): 2409-9600, ISSN (Online): 2409-9619

Design and Implementation of a Cloud-Based Load Monitoring Scheme for Electricity Theft Detection on a Conventional Grid

Ayodele I. Abdullateef[1*], Abdullah Sulaiman[2], Abdulkabir O. Issa[3], Sikiru O. Zakariyya[4]

[1, 2, 3, 4] Electrical and Electronics Engineering Department, Faculty of Engineering and Technology, University of Ilorin, Kwara State, Nigeria
E-mail: abd_lateef.aii@unilorin.edu.ng

Received: June 29, 2022 *Revised: September 04, 2022* *Accepted: September 10, 2022*

***Abstract*—** Electricity theft is one of the problems - encountered by the utilities - that leads to losses of revenue. Manual monitoring of the consumers' activities which shows the energy data consumed on the conventional grid has largely contributed to electricity theft on the grid. Significantly, the energy meter deployed to monitor the load cannot store and transmit energy data in real-time. This has made electricity theft on the grid unnoticed. This paper presents the development of a monitoring scheme for an electronic meter on the conventional grid with the capability to monitor, store and transmit consumers' energy data to the cloud. It consists of two units: the indoor and the outdoor unit. Energy data is transferred wirelessly between the units via the Wi-Fi modules. The outdoor unit compares the data and transfers the outcome to the ThinkSpeak cloud server. The transferred energy data can be accessed in real-time from the cloud or downloaded in comma-separated values format for further use. In order to verify the functionality of the proposed scheme, two scenarios of electricity theft - partial bypassing and full bypassing - are carried out. The obtained results show that the scheme can detect the theft and log the data to the cloud successfully.

***Keywords*—** Electricity theft; Monitoring scheme; Conventional grid; Distribution network; Energy meter.

1. INTRODUCTION

Electricity theft has been classified as a major component of non-technical losses (NTL) in power system operations [1-3]. It is the practice of using electricity from the utility without the utility's authorization or consent [4, 5]. Electricity theft is a result of unmetered energy use which could occur due to meter tampering, direct tapping of wires, computation errors, false and delays in meter reading, bribing of meter readers, irregular bill submission, faulty energy meters and ignored unpaid bills [6]. Non-technical losses due to illegal or unauthorized consumption of electricity account for 10 – 40% worldwide [7]. The reports in both the developed and developing countries show that the menace of electricity theft is unabated despite efforts made to eradicate it [8, 9]. For instance, the USA and Canada recorded revenue losses amounting to $6 billion and $100 million, respectively to electricity theft in 2010 [10, 11]. Recently, a total of $96 billion was lost to electricity theft and other non-technical losses [12]. Additionally, in Pennsylvania, a utility report shows that the 16% increase in energy theft in 2016 compared to 2008 is due to illegal consumption of electricity by the local business sectors and residential consumers [13].

Furthermore, in Jordan, a total amount of JD 38.17 million due to electricity theft was recovered between 2016 and late 2019 [14]. An improvement of 13% reduction in the number of electricity thefts in the first quarter of 2018, in Jordan, has been reported [15]. Likewise,

* Corresponding author
Article's DOI: 10.5455/jjee.204-1656498918

over five thousand cases of electricity theft perpetrated by nefarious consumers were uncovered in Jordan in 2018 [16]. The mode of monitoring on the conventional grid which is predominantly manual gives rise to this huge number of consumers without notice.

The African continent is not immune from losses incurred by the utilities due to the stealing of electricity. Electricity distribution companies in Nigeria lost a sum of N97 billion to energy theft in the first quarter of 2021 [17]. Also, in South Africa, an average loss of R20 billion per annum incurred by the utility is due to electricity theft [18]. In Liberia, about 60% of the electricity generated annually in the country equivalent to about $35 million is stolen [19]. In Egypt, electricity theft reports that were filed against citizens in nine months exceeded EGP 2.4 billion [20].

Recent technological advancements have necessitated the development of smart energy meters with the ability to store and transmit data over time in a two-way communication mode [21]. Consequently, this has led to the development of the power smart grid (SG) network, which is the electricity network that can intelligently integrate the behaviour and actions of users connected to it [22]. SG has changed the dynamics of the traditional power system architecture and improved its operations. Besides, SG architectures based on advanced meter infrastructure to monitor and detect electricity theft from consumers has become a critical issue among the stakeholders in recent time [23]. Thus, experts in power industries and academia have proposed different methods to detect energy theft using data acquired from smart grids [24-28].

Some researchers proposed support vector machines to classify the stealing [6, 29, 30]. A statistical method has also been proposed [31]. Others leveraged the advantages of advanced meter infrastructure (AMI) for energy theft identification and detection [32-34]. Regrettably, most of these methods have not been fully implemented and those implemented have not solved the problem, as stealing of electricity is still being reported [9, 35]. Moreover, a larger percentage of these methods assumed/focused on SG structure and the data used are cumulative data of the consumers connected as a cluster and this can hardly identify individual consumers stealing electricity on the distribution network. To identify the perpetrators, each consumer's data needs to be stored and accessed in real time.

The conventional power grid is an interconnection of power equipment such as transformers, switchgears, electromechanical and electronic energy meters. The energy meter is essential among the equipment, being the primary source of data required to monitor and track the activities on the power network. Regrettably, these meters can only monitor consumer energy data but lack the capacity to store and transmit such data because they are not embedded with storage facilities and communication modules. Thus, the activities on the grid are manually carried out by physical inspection when required. This allows for the stealing of electricity without notice on the power distribution network by the utilities and has practically made it impossible to monitor - in real-time - the consumers' activities on the grid which show in the energy data consumed. It is worth noting that despite advancements made in making the power system components smart, a greater number of countries and utilities are nevertheless heavily dependent on the conventional grid for the transportation of power to the end users as a smart grid is a future concept. Hence, the meters have to be made smart in order to reduce electricity theft on the conventional grid since the mass replacement will require a huge amount of money and time.

This study focuses on the design and implementation of a real-time cloud-based monitoring scheme for existing energy meters on a conventional grid. The scheme can store and transmit the energy data consumption of individual consumers which can be used to detect electricity theft.

2. PROPOSED SCHEME ARCHITECTURE FOR LOAD MONITORING

Fig. 1 shows the architecture of the proposed scheme. It consists of an indoor unit (IDU) which is installed to monitor the consumer's load and an outdoor unit (ODU) installed on the pole to monitor the IDU and also transfer the data into the cloud. Each unit has a transceiver module which aids data transfer within the units on one hand and between the ODU and the cloud on the other hand. With this, the ODU is capable of comparing the data as seen by the units. In addition, an internet module is integrated into the ODU to facilitate data transfer to the cloud server for remote monitoring.

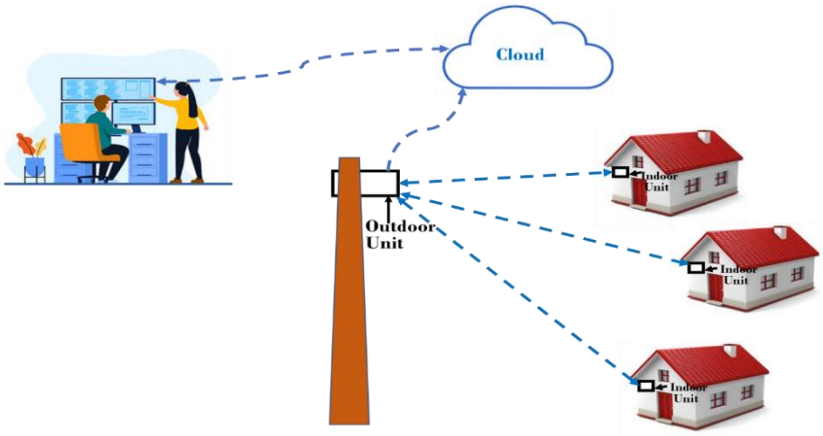

Fig. 1. The proposed scheme for load monitoring.

2.1. Development of the IDU

The IDU as shown in Fig. 2 comprises mainly the electronic energy meter (EEM), the transceiver and the pulse calibrator circuit as illustrated in Fig. 3. EEM has no moving parts and uses digital micro technology. In EEM, the accurate functions are controlled by the application specified integrated circuit (ASIC). The output of ASIC is available as "Pulses" indicated by the light emitting diode (LED) placed on the front panel of the meter. The number of pulses equals the average kilowatt hour (kWh) consumed.

Fig. 3 illustrates the pulse circuit output of the energy meter with pulse widths T_{high} and T_{low}. The pulse width T_{high} varies depending on the energy meter. However, it can be fixed such that it remains constant during operation. In that case, the time between the pulses T_{low} varies according to the pulse rate which indicates the power measured by the meter.

For this meter, 1000 pulses = 1kWh

then 1 pulse = 1Wh = 3600 Ws

Then, the approximate power at a given time t_d is:

$$P = \frac{3600}{t_d} \text{W} \tag{1}$$

where P is the IDU power; t_d is the time between the falling edge of each pulse.

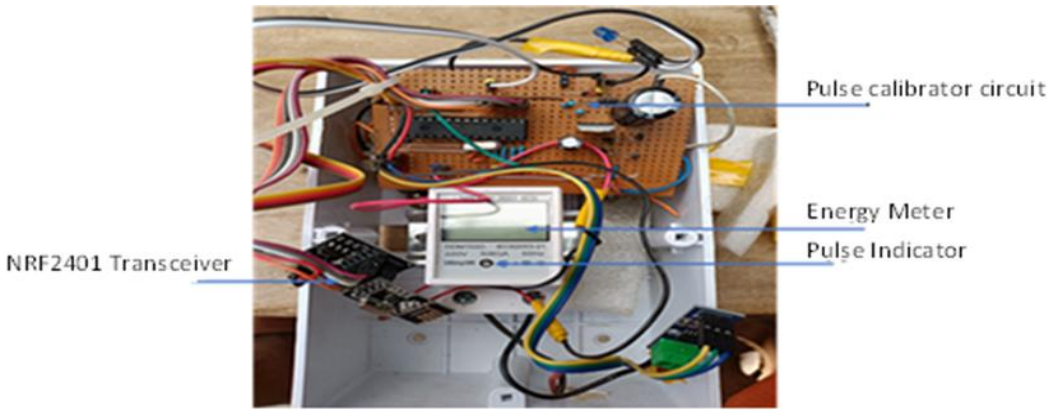

Fig. 2. The indoor unit.

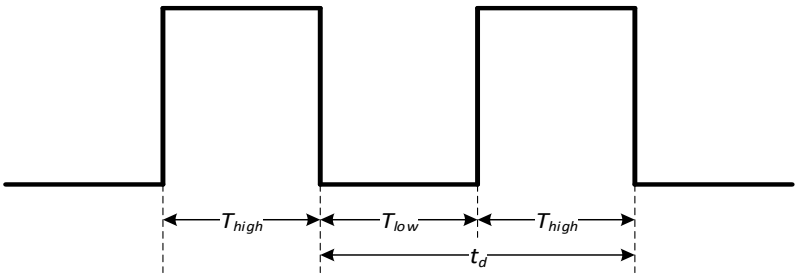

Fig. 3. Output pulse of the energy meter

The power consumed by the load corresponding to the meter values are computed using Eq. (1). Fig. 4 shows the experimental set-up of the indoor unit. The data acquired from the energy meter through the processing unit are fed to the analogue-to-digital converter (ADC) pin of the microcontroller which is calibrated using the pulse rate of the meter. The result of the calibrated signal is displayed on the serial monitor.

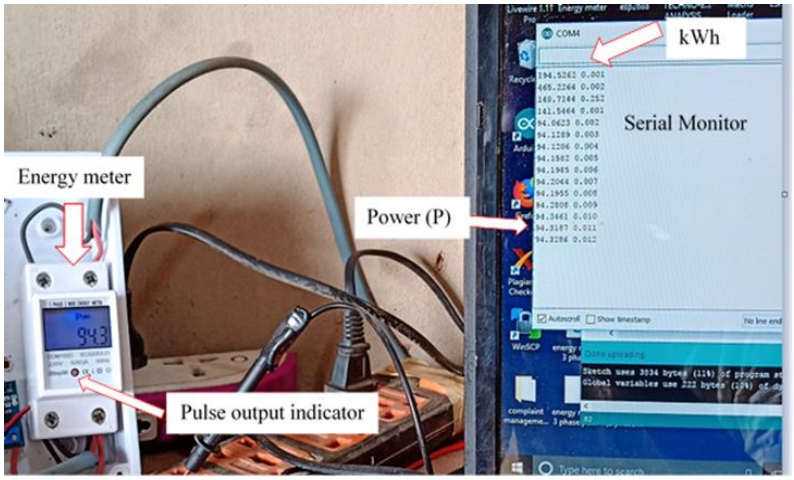

Fig. 4. Experimental setup and testing of the IDU.

2.2. Development of the ODU

Fig. 5 shows the complete circuit diagram of the ODU. Its design involves both hardware and software. The hardware components comprise majorly a voltage sensor circuit, a current sensor module, the transceiver, the data logger module and the microcontroller.

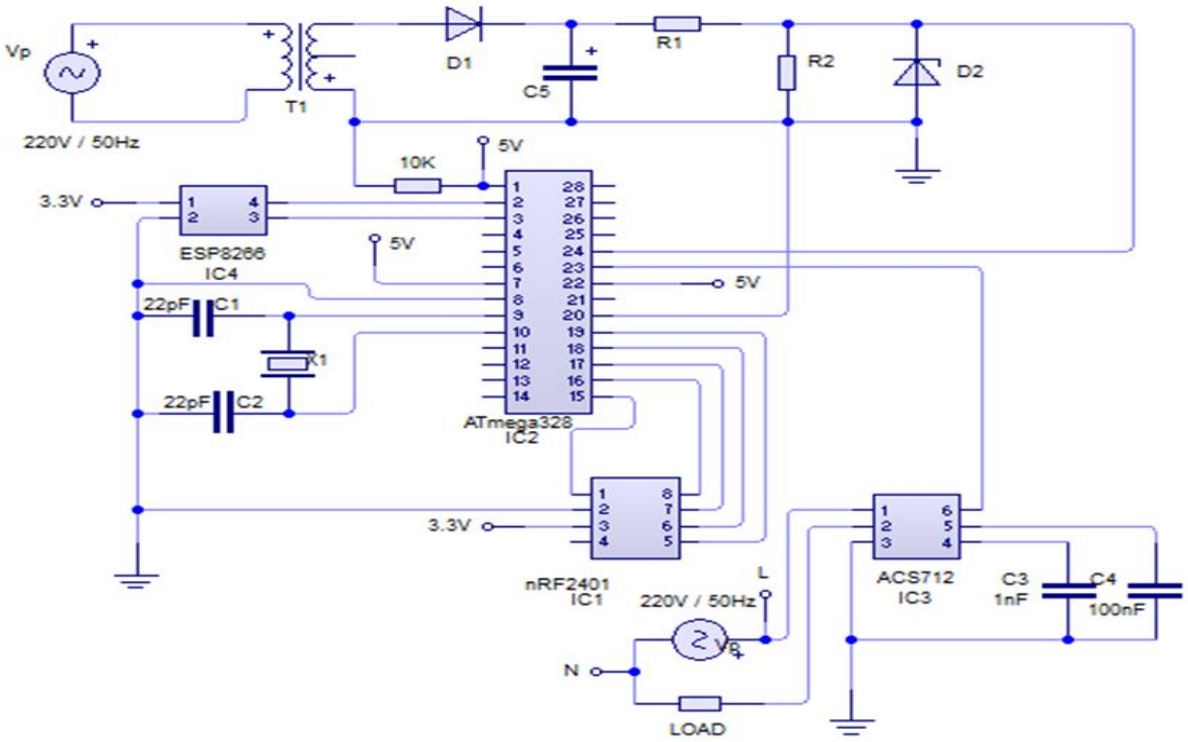

Fig. 5. Circuit diagram of the ODU.

The control circuit contains notably the microcontroller and the oscillator circuit. Voltage and current sensors are connected to pins 24 and 23 (or ADC pins A0 and A1), the transceiver makes use of the single available serial peripheral interface (SPI) while the Esp8266 is connected to the UART pins. The software involves the development of the algorithms which are executed through the microcontroller.

2.2.1. Calibration of the Components

Figs. 6 and 7 depict voltage and current validation experimental set up. These are necessary to ascertain the status of the components before they are soldered on the veroboard. The calibrated and the measured values are practically equal.

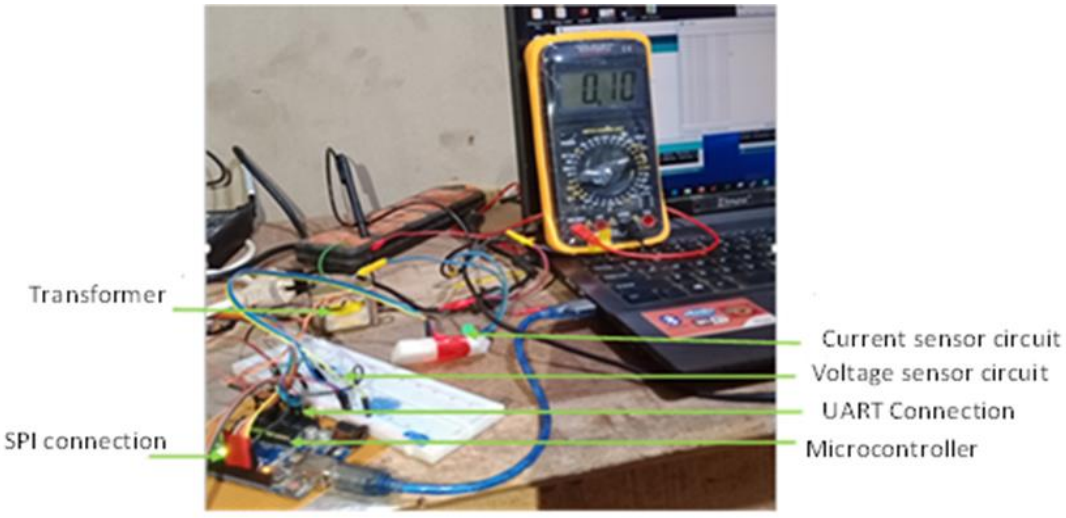

Fig. 6. Experimental set-up for voltage calibration.

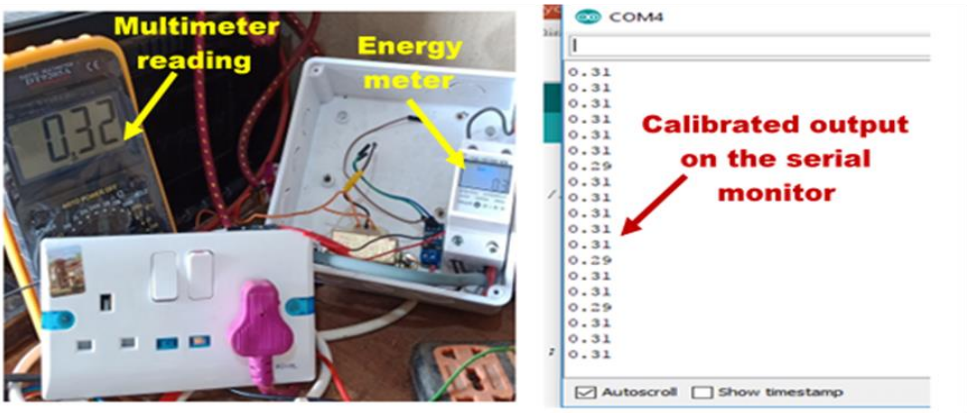

Fig. 7. Experiment setup results for the current sensor on the serial monitor.

Summary of the calibration of voltage and current results are shown in Table 1. The difference between the experimental and energy meter values of current is 0.014. This value is also favourably small when compared with allowable equipment accuracy given in the datasheet. This implies that the experimental voltage value read of 209 V is much closer to the value read by DT9205A.

Table 1. Experimental and DT9205A real value.

Quantity	DT9205A Meter	Experimental	Error
Voltage	208.000 V	209.000 V	1.000 V
Current	0.320 A	0.306 A	0.014

To improve the system accuracy, the DDM15SD energy meter was also used for calibration of voltage, current and power values. The results, shown in Table 2, indicate that the instantaneous voltage of the DDM15SD is 208.7 V which is closer to the experimental or calibrated value of 209 V, and this, in turn, reduces the percentage error recorded in Table 1.

Table 2. Experimental and DDM15SD real value.

Quantity	DDM15SD Meter	Experimental	Error
Voltage	208.7 V	209.00 V	0.3 V
Current	0.300 A	0.306 A	0.006
Power	59.5	59.56	0.06

2.3. Development of Algorithm for the IDU and ODU

The algorithms for the IDU and ODU operations are shown in Figs. 8 and 9, respectively. These algorithms are meant to monitor the consumer's energy data, compare the data from the units to detect electricity theft and send the result to the cloud.

After initialization, a wireless connection between IDU and ODU will be established through NRF2401 transceiver, then a pulse signal is sensed and conditioned to compute the real-time power and the kWh consumed. The first stage of theft checking is activated by comparing the IDU with the ODU, then these values will be sent to the cloud through the data logger

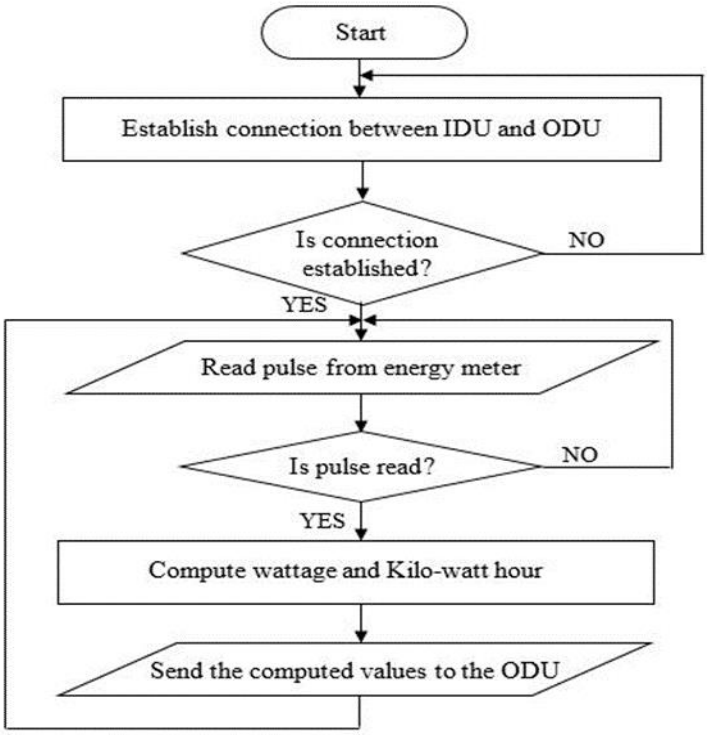

Fig. 8. Algorithm flowchart for the IDU.

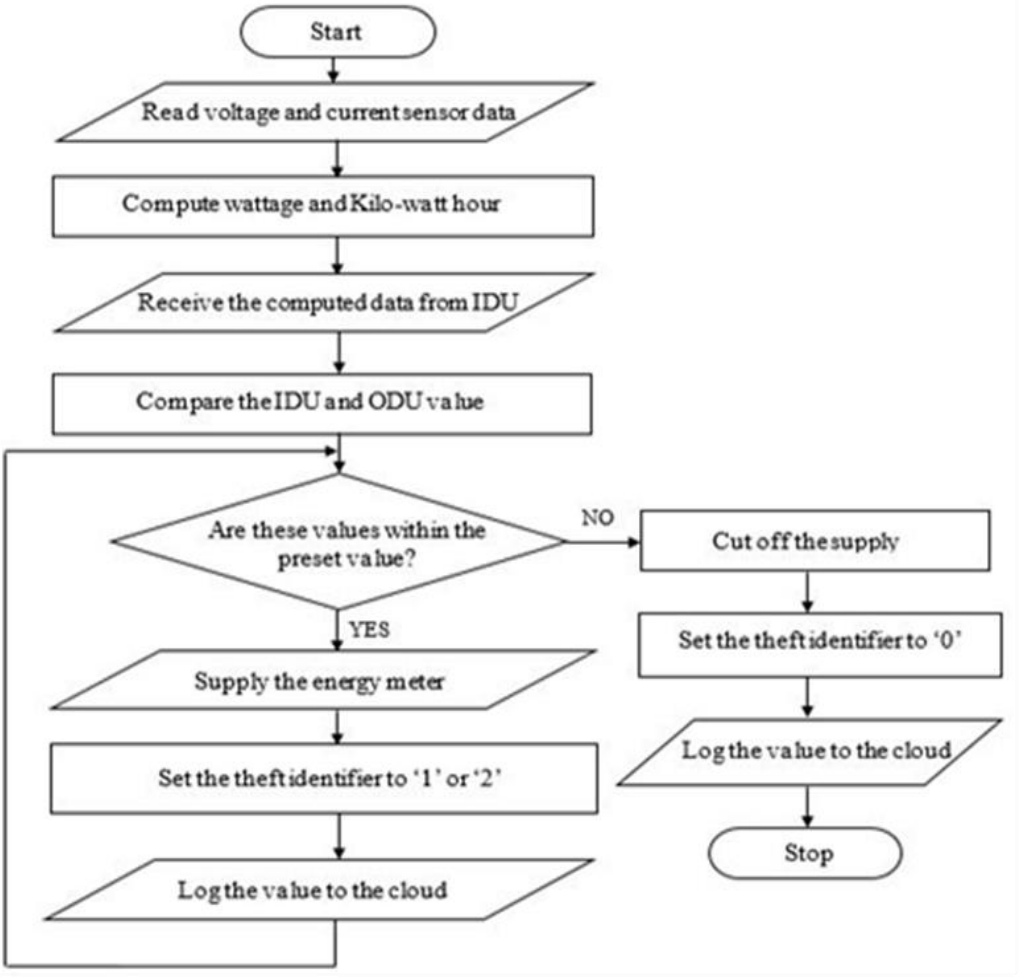

Fig. 9. Algorithm flowchart for the ODU.

3. IMPLEMENTATION OF THE SCHEME FOR LOAD MONITORING AND THEFT IDENTIFICATION

The system is arranged as shown in Fig. 10. The IDU and the ODU are connected through a connecting cable representing the service mains. The load is connected to the IDU via the knife switch which provides the bypassing cable for the theft load by switching from contact A to contact B. The system was tested under three different conditions: normal connection, partial meter bypass and full meter bypass.

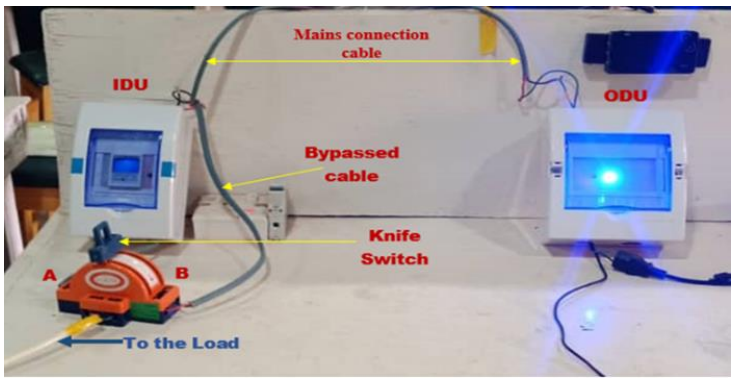

Fig. 10. Real time implementation of the scheme for load monitoring and theft identification.

3.1. Normal Condition

The system is said to be normal when all the loads are connected to the IDU via the energy meter as expected. During this period, the consumers' loads will be directly connected to the IDU by changing the knife of the switch to contact "A" as shown in Fig. 11. Furthermore, for the system to operate, WiFi connection is expected to be established between the IDU and ODU. If this WiFi connection is successfully established, there will be a power supply from the ODU to the IDU, to point 'A' and the load. Thus, Fig. 11 indicates that the load is directly connected to the IDU. The ODU logs the load data to the cloud storage.

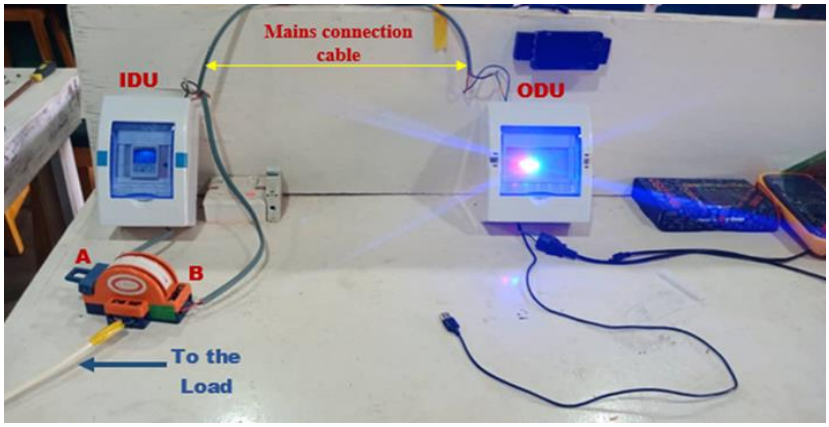

Fig. 11. System testing under normal conditions.

3.2. Partial Meter Bypass

Partial meter bypass occurs when the consumer deliberately connects light loads to point "C" and other loads to point "B" while the knife is on contact "A" of the switch. This

situation - depicted in Fig. 12 - is carried out to reduce the billing cost while deceiving the utility. With this arrangement, two different readings are logged in the cloud by the ODU. The ODU will continue to monitor the load at both points B and C, while the IDU will monitor the load at point C only.

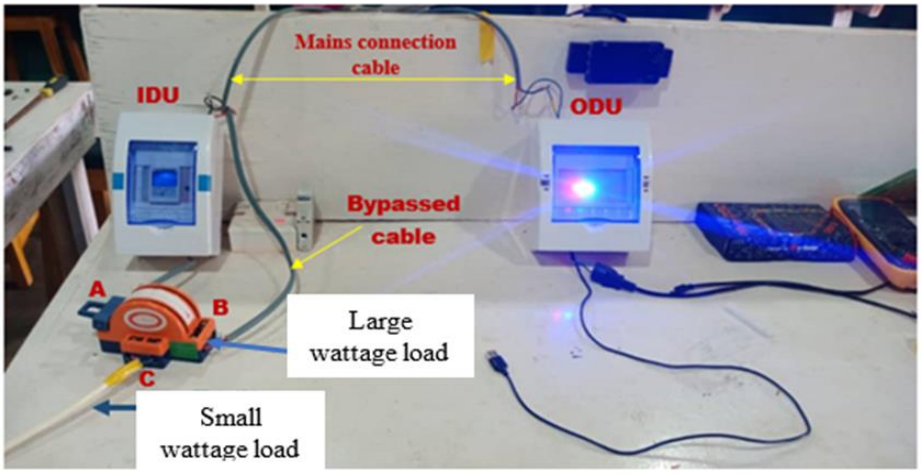

Fig. 12. System testing under partial meter bypass.

3.3. Full Meter Bypass

This involves connecting the loads directly to point B as shown in Fig. 13. Here, the IDU is completely bypassed and hence, only the ODU will continuously monitor the load at point C and log the data to the cloud.

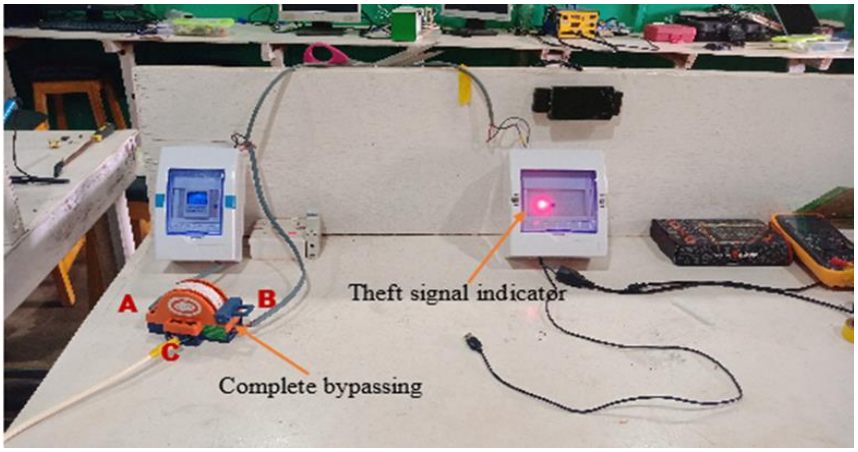

Fig. 13. System testing under full meter bypass.

4. DATA CLOUD STORAGE

Cloud storage is a computer data storage which stores digital data in logical pools. The physical storage spans multiple servers (sometimes in multiple locations), and the environment is typically owned and managed by a hosting company. Cloud storage providers are responsible for the maintenance of the data as well as for making it accessible to authorized users. Individuals and organizations could buy or lease storage capacity from the providers to store information. Cloud storage services may be accessed through a co-located cloud computing service, a web service application programming interface (API) or

by applications that utilize the API, such as cloud desktop storage, cloud storage gateway or web-based content management systems.

ThingSpeak is a cloud storage that is widely used to store data. It is an open-source internet of things (IoT) application and API to store and retrieve data using the hyper-text transfer protocol (HTTP) and message queuing telemetry transport (MQTT) protocol over the Internet or via a local area network (LAN). ThingSpeak enables the creation of sensor logging applications, location tracking applications and a social network of things with status updates. This storage facility was used to store the data acquired from the IDU and the ODU. These data are stored in the server and can be downloaded in CSV excel format for further applications. A typical human interface of the ThngSpeak is shown in Fig. 14.

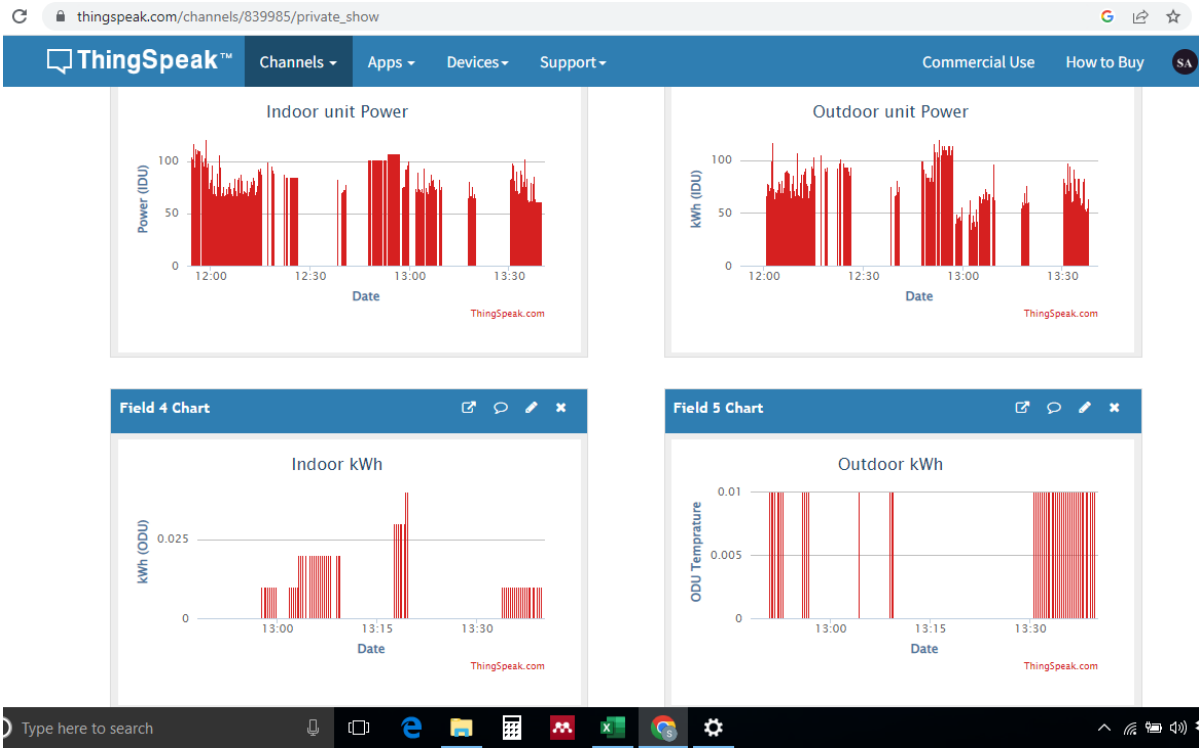

Fig. 14. A typical display of power and energy data from ThingSpeak server.

5. RESULTS AND DISCUSSION

Figs. 15 and 16 show the power and energy load data monitored and logged into the cloud by the ODU at a normal connection. It is seen that in both cases, the IDU and ODU data are practically the same. Although there are slight differences in the values of power consumed as indicated by IDU and ODU. This is due to calibration errors; however, it is insignificant and the values can be assumed to be practically equal. Generally, the power consumed by the IDU is less by 0.023 kW when compared with the ODU. For instance, a difference of 0.014 kW is noted at the 8 min between the IDU and ODU while the energy recorded for both are the same. This proves that the deviation in the power can be neglected. The data logger is sampled every 60 s as stealing within this period can be insignificant and neglected, as the time interval is very small. For adequate monitoring at the utility centre, numbers 0, 1 and 2 were employed as state (theft) identifiers as shown in Fig. 17. The values '1' or '2', indicate no theft case, while 0 represents a theft condition.

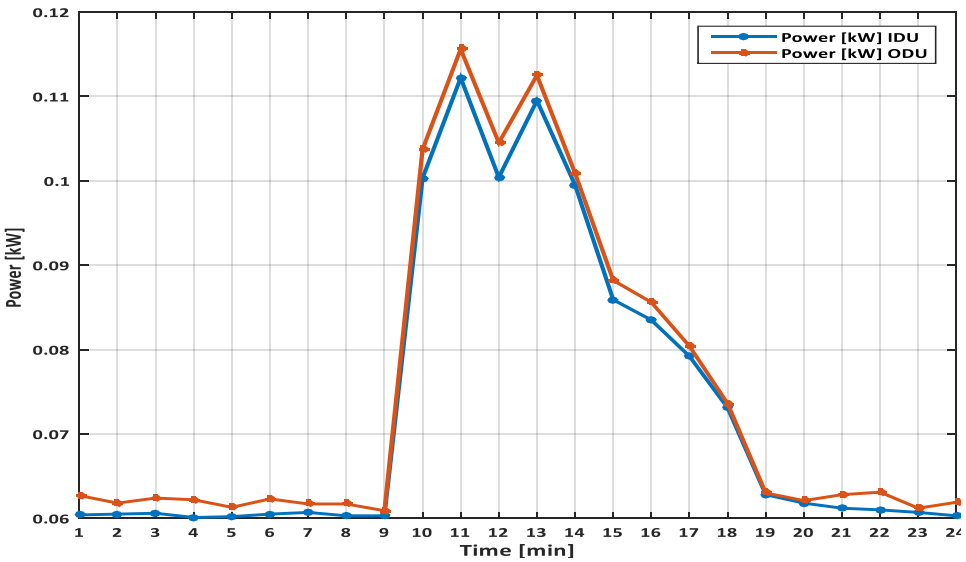

Fig. 15. IDU and ODU power data logged under normal condition.

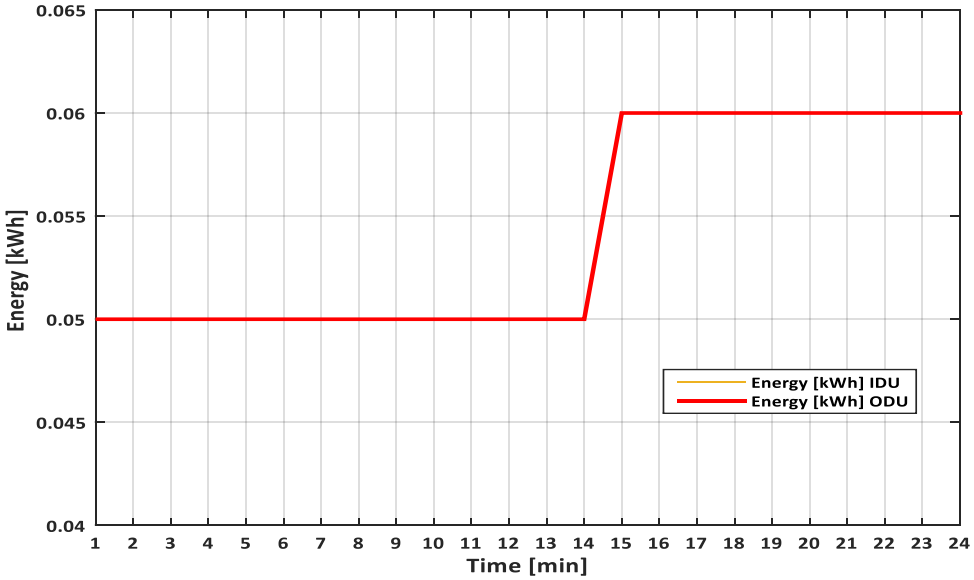

Fig. 16. IDU and ODU energy data logged under normal condition.

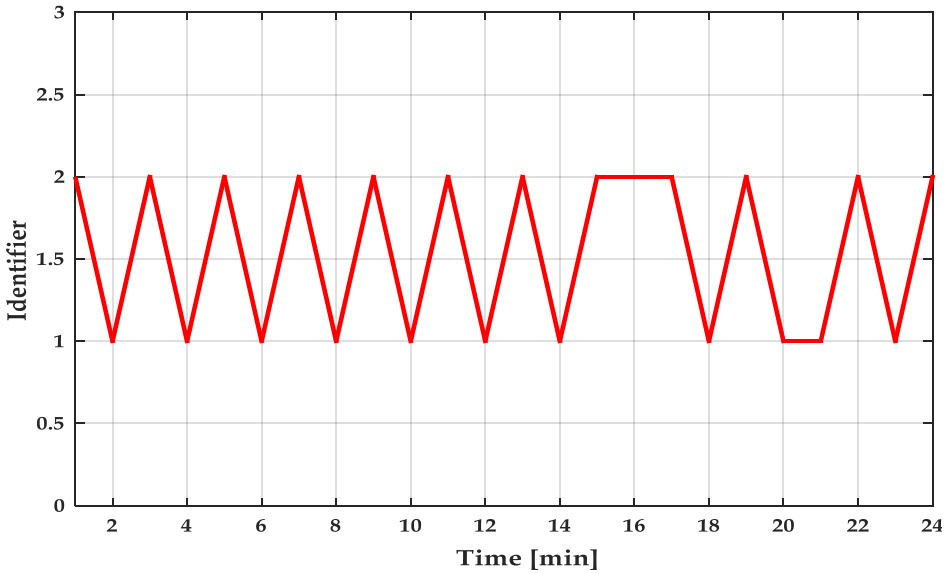

Fig. 17. Electricity theft identification.

Figs. 18 and 19 show the power and energy load data monitored and logged into the cloud by the ODU during partial bypassing of the meter. The first seven readings of the IDU and ODU are similar. This indicates no meter bypass and the identifier maintains the numbers '1' or '2'. However, as soon as partial bypassing occurs in the 8 min, the values read by the IDU and ODU change. The IDU indicates 0.0321 kW while the ODU indicates 0.0799 kW. The IDU maintains a lower value as compared to the ODU. Thus, the state identifier in Fig. 20 records a value of '0' continuously until the bypassing is stopped.

Fig. 20 shows the state identifier which stays at '1' or '2' when there was no stealing between 1 min and 8 min . However, the identifier goes to '0' and indicates a meter bypass.

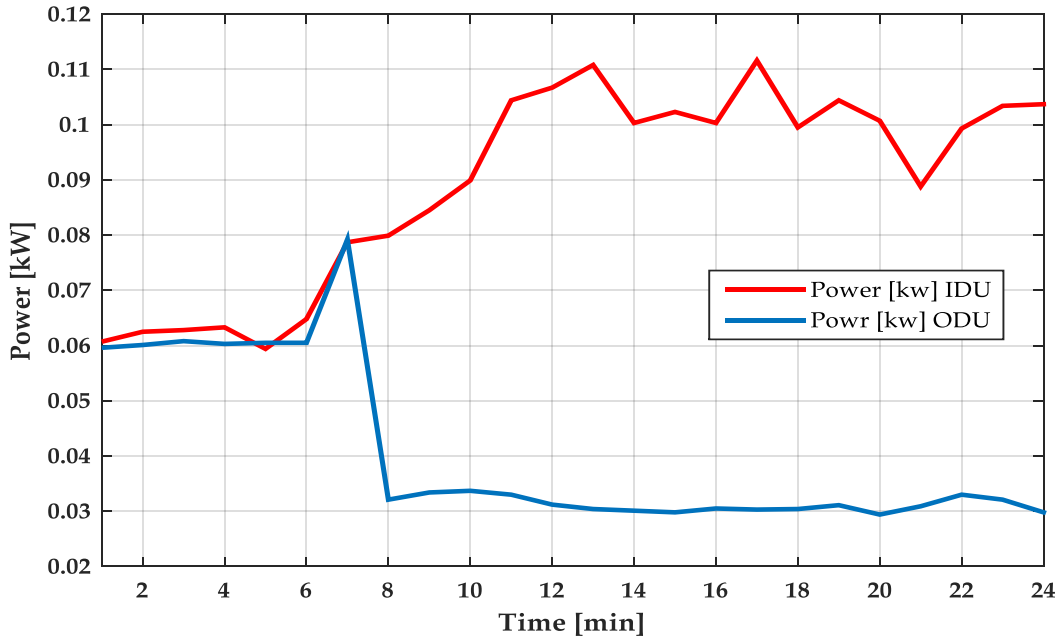

Fig. 18. IDU and ODU power data logged under partial meter bypass.

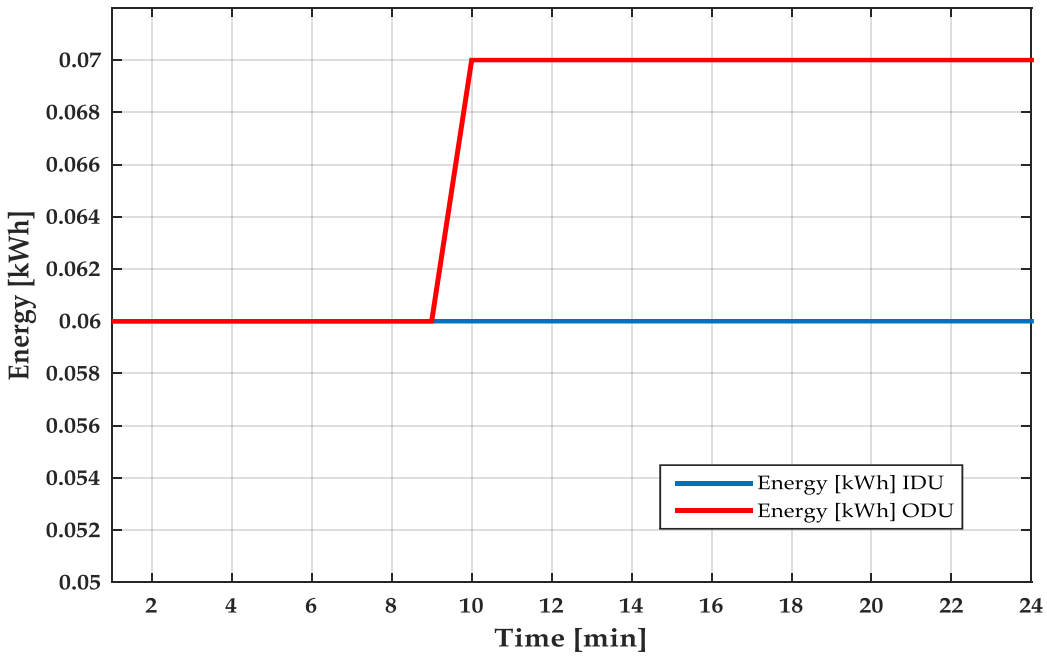

Fig. 19. IDU and ODU energy data logged under partial meter bypass.

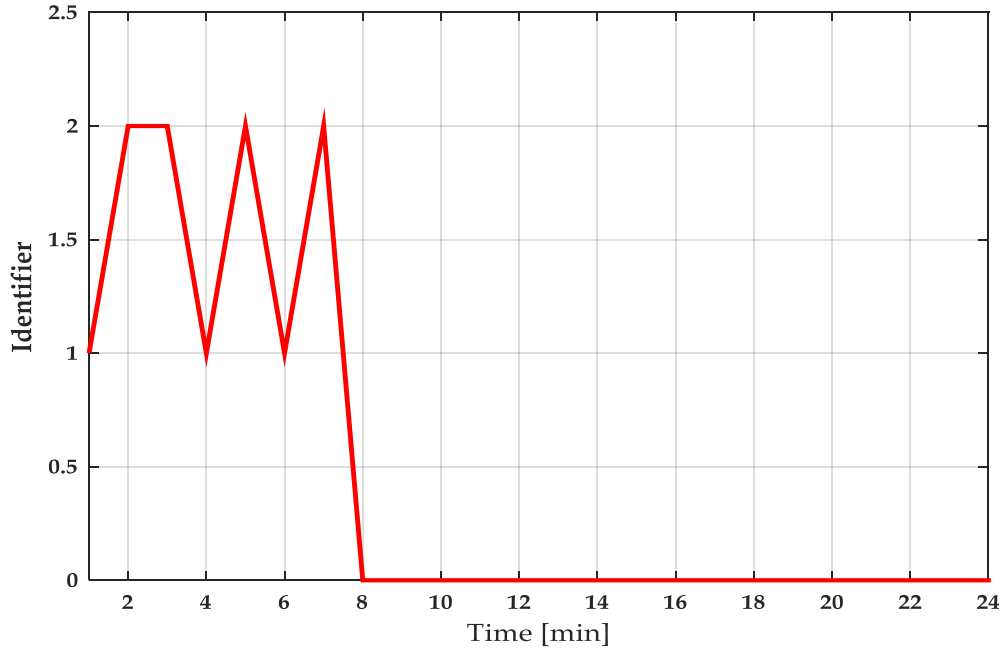

Fig. 20. Electricity theft identification under partial meter bypass.

Furthermore, Figs. 21 and 22 illustrate the plot of data logged into the cloud when the meter is fully or completely bypassed. The power consumed as read by the ODU fluctuates between 0.0542 kW and 0.06 kW while the IDU readings were constant at zero. Also, the energy data read by the IDU and the ODU are constant at 0.09 kWh and 0.12 kWh, respectively. The state identifier reading was zero throughout indicating a complete meter bypass condition as shown in Fig. 23.

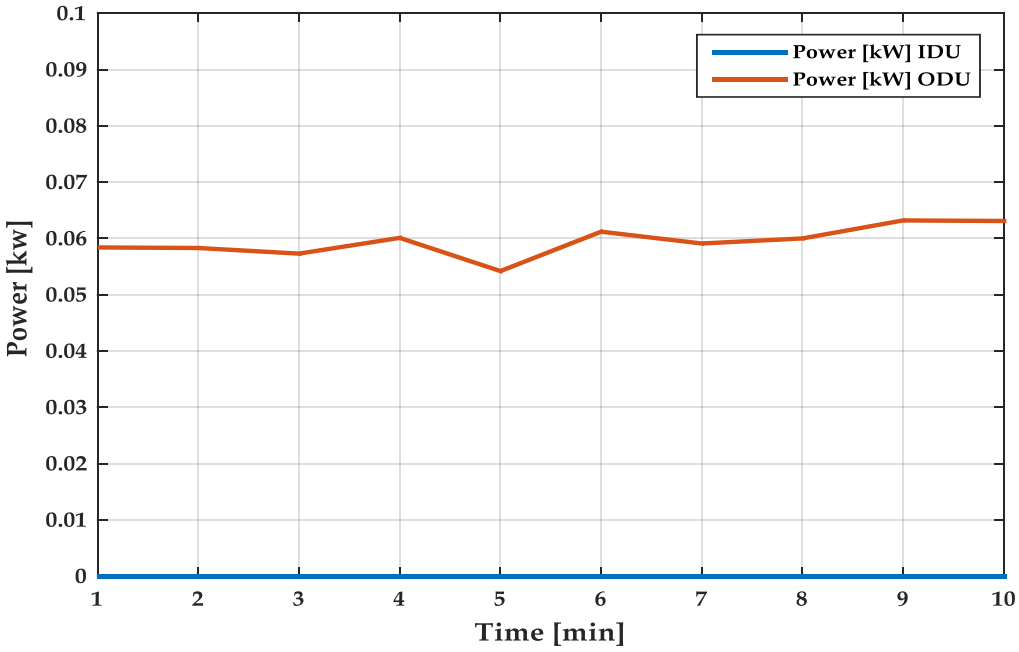

Fig. 21. IDU and ODU power data logged under full meter bypass.

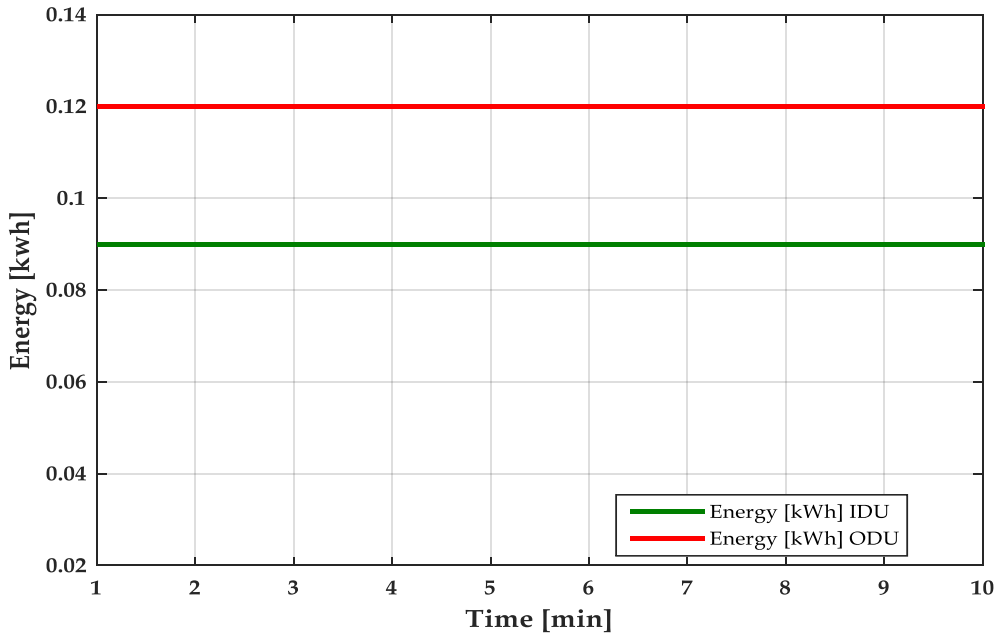

Fig. 22. IDU and ODU energy data logged under full meter bypass.

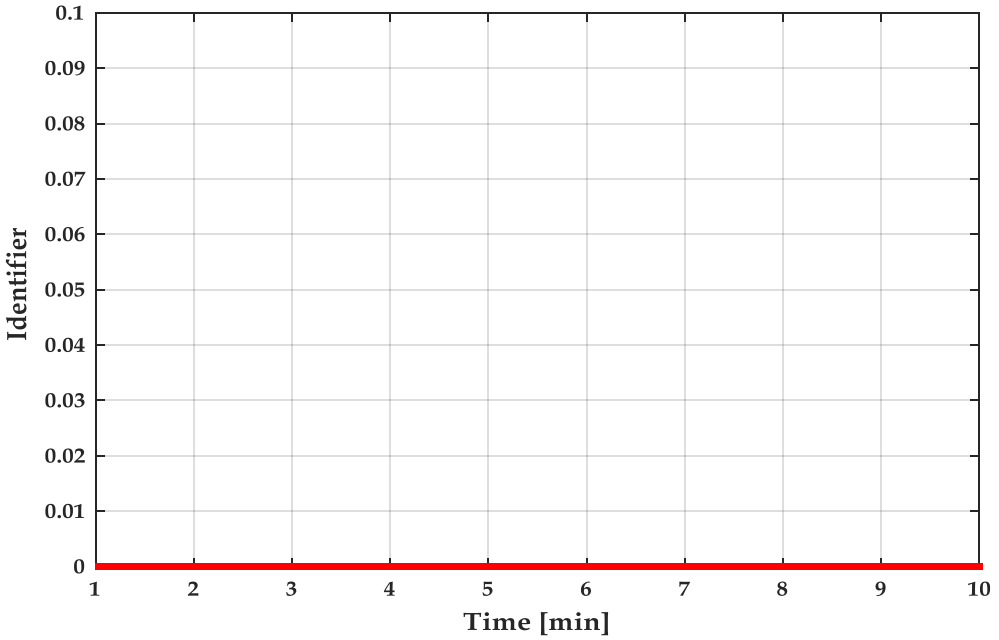

Fig. 23. Electricity theft identification under full meter bypass.

6. CONCLUSIONS

A monitoring scheme for a conventional grid capable of detecting electricity theft was developed and tested in this paper. This improves the manual monitoring of the grid and makes the grid smart. The developed IDU and ODU were able to transfer data between themselves on one hand and between the ODU and the cloud on another hand. These data were stored in the ThingSpeak server and can be accessed in real-time and downloaded in comma-separated values (CSV) format. Two scenarios of electricity theft, partial bypassing and full bypassing were carried out to verify the functionality of the scheme. The scheme detected the theft and logged the data to the cloud successfully.

REFERENCES

[1] J. Nagi, K. Yap, F. Nagi, S. Tiong, S. Koh, S. Ahmed, "NTL detection of electricity theft and abnormalities for large power consumers in TNB Malaysia," in *2010 IEEE Student Conference on Research and Development*, pp. 202-206, 2010.

[2] J. Leite, J. Mantovani, "Detecting and locating non-technical losses in modern distribution networks," *IEEE Transactions on Smart Grid,* vol. 9, no. 2, pp. 1023-1032, 2016.

[3] O. Darteh, C. Adjei, R. Anaadumba, S. Sarker, G. Christian, A. Blay, "Design of internet of things based electricity theft detection using Raspberry PI," *International Journal of Engineering Research and Technology*, vol. 10, no. 2, pp. 506-511, 2021.

[4] A. Abdullateef, M. Salami, M. Musse, M. Onasanya, M. Alebiosu, "New consumer load prototype for electricity theft monitoring," *IOP Conference Series: Materials Science and Engineering,* vol. 53, no. 1, pp. 012061, 2013.

[5] A. Jain, M. Bagree, "A prepaid meter using mobile communication," *International Journal of Engineering, Science Technology,* vol. 3, no. 3, 2011.

[6] R. Toma, M. Hasan, A. Nahid, B. Li, "Electricity theft detection to reduce non-technical loss using support vector machine in smart grid," in *2019 1st International Conference on Advances in Science, Engineering and Robotics Technology*, pp. 1-6, 2019.

[7] Z. Aslam, N. Javaid, A. Ahmad, A. Ahmed, S. Gulfam, "A combined deep learning and ensemble learning methodology to avoid electricity theft in smart grids," *Energies*, vol. 13, no. 21, pp. 5599, 2020.

[8] M. Saeed, M. Mustafa, N. Hamadneh, N. Alshammari, U. Sheikh, T. Jumani, S. Khalid, I. Khan, "Detection of non-technical losses in power utilities—a comprehensive systematic review," *Energies*, vol. 13, no. 18, pp. 4727, 2020.

[9] H. Elizabeth, *Electricity Thefts Soar to Record Levels in England and Wales as Thieves Tamper with Lines or Bypass Meters to Dodge Rising Bills*, MailOnline, 2022. <https://www.dailymail.co.uk/news/article-11083997/Electricity-thefts-soar-record-levels-thieves-tamper-lines-bypass-meters.html>

[10] A. Abdullateef, M. Salami, M. Musse, A. Aibinu, M. Onasanya, "Electricity theft prediction on low voltage distribution system using autoregressive technique," *International Journal of Research in Engineering and Technology,* vol. 1, no. 5, 2012.

[11] B. Koay, S. Cheah, Y. Sng, P. Chong, P. Shum, Y. Tong, X. Wang, Y. Zuo, H. Kuek, "Design and implementation of Bluetooth energy meter," in *Fourth International Conference on Information, Communications and Signal Processing, 2003 and the Fourth Pacific Rim Conference on Multimedia, Proceedings of the 2003 Joint*, vol. 3, pp. 1474-1477, 2003.

[12] A. Theron-Ord, *Electricity Theft and Non-Technical Losses Total $96bn Annually*, Smart Energy International, 2017. <https://www.smart-energy.com/regional-news/africa-middle-east/electricity-theft-96bn-annually/#:~:text=Electricity%20theft%20and%20non%2D technical%20losses%20total%20%2496bn%20annually%20%E2%80%93%20report,-By&text=According%20to%20new%20research%20conducted,%2496%20billion%20per%20year%20globally.>

[13] M. Khiyal, A. Khan, E. Shehzadi, "SMS based wireless home appliance control system (HACS) for automating appliances and security," *Issues in Informing Science Information Technology,* vol. 6, 2009.

[14] Jordan News, *JD38m in Electricity Theft Recovered*, 2021. <https://www.jordannews.jo/Section-109/News/JD38m-in-electricity-theft-recovered-8235>

[15] Roya News, The Shocking Consequences of Electricity Theft in Jordan, 2022. <https://en.royanews.tv/news/14184/The-shocking-consequences-of-electricity-theft-in-Jordan>

[16] Environment and Climate in the Middle East, *5,671 Cases of Electricity Theft Uncovered since January*, 2018. <https://mideastenvironment.apps01.yorku.ca/2018/04/5671-cases-of-electricity-theft-uncovered-since-january-jordan-times/>

[17] J. Kingsley, *Energy theft registry will reduce electricity challenges in Nigeria,* 2022. <https://guardian.ng/energy/energy-theft-registry-will-reduce-electricity-challenges-in-nigeria/#:~:text=In%20the%20first%20three%20months,N86%20billion%20in%20Q4%202020>

[18] N. Nicholas, *Analysis: Electricity theft in South Africa*. <https://www.smart-energy.com/features-analysis/electricity-theft-south-africa/>

[19] B. News, *Liberia Electricity Crisis: About 60% of Power Stolen*. <https://www.bbc.com/news/world-africa-46452326>

[20] Teller Report, *4 Million Reports of Electricity Theft in Egypt Within One Year ... Why?*, 2021. <https://www.tellerreport.com/news/2021-03-07-%0A---4-million-reports-of-electricity-theft-in-egypt-within-one-year-----why-%0A--.SyB0axFfXO.html>

[21] S. Priyadharshini, C. Subramani, J. Roselyn, "An IOT based smart metering development for energy management system," *International Journal of Electrical Computer Engineering,* vol. 9, no. 4, pp. 3041, 2019.

[22] X. Yu, C. Cecati, T. Dillon, M. Simoes, "The new frontier of smart grids," *IEEE Industrial Electronics Magazine,* vol. 5, no. 3, pp. 49-63, 2011.

[23] R. Jiang, R. Lu, Y. Wang, J. Luo, C. Shen, X. Shen, "Energy-theft detection issues for advanced metering infrastructure in smart grid," *Tsinghua Science Technology,* vol. 19, no. 2, pp. 105-120, 2014.

[24] A. Otuoze, M. Mustafa, O. Mohammed, M. Saeed, N. Surajudeen-Bakinde, S. Salisu, "Electricity theft detection by sources of threats for smart city planning," *IET Smart Cities,* vol. 1, no. 2, pp. 52-60, 2019.

[25] A. Abdullateef, M. Salami, I. Tijani, M. Onasanya, "Novel technique for detecting electricity theft on low voltage distribution network," in *Proceeding of National conference of electrical and electronics engineering*, pp. 199-204, 2012.

[26] P. Jokar, N. Arianpoo, V. Leung, "Electricity theft detection in AMI using customers' consumption patterns," *IEEE Transactions on Smart Grid,* vol. 7, no. 1, pp. 216-226, 2015.

[27] S. Amin, G. Schwartz, A. Cardenas, S. Sastry, "Game theoretic models of electricity theft detection in smart utility networks," *IEEE Control Systems,* 2015.

[28] M. Hasan, R. Toma, A. Nahid, M. Islam, J. Kim, "Electricity theft detection in smart grid systems: A CNN-LSTM based approach," *Energies*, vol. 12, no. 17, pp. 3310, 2019.

[29] A. Jindal, A. Dua, K. Kaur, M. Singh, N. Kumar, S. Mishra, "Decision tree and SVM-based data analytics for theft detection in smart grid," *IEEE Transactions on Industrial Informatics,* vol. 12, no. 3, pp. 1005-1016, 2016.

[30] S. Depuru, L. Wang, V. Devabhaktuni, "Support vector machine based data classification for detection of electricity theft," in *2011 IEEE/PES Power Systems Conference and Exposition*, pp. 1-8, 2011.

[31] J. Tao, G. Michailidis, "A statistical framework for detecting electricity theft activities in smart grid distribution networks," *IEEE Journal on Selected Areas in Communications,* vol. 38, no. 1, pp. 205-216, 2019.

[32] M. de Souza, J. Pereira, G. Alves, B. de Oliveira, I. Melo, P. Garcia, "Detection and identification of energy theft in advanced metering infrastructures," *Electric Power Systems Research,* vol. 182, pp. 106258, 2020.

[33] S. Singh, R. Bose, A. Joshi, "Entropy-based electricity theft detection in AMI network," *IET Cyber-Physical Systems: Theory Applications,* vol. 3, no. 2, pp. 99-105, 2018.

[34] Z. Yan, H. Wen, "Electricity theft detection base on extreme gradient boosting in AMI," *IEEE Transactions on Instrumentation Measurement,* vol. 70, pp. 1-9, 2021.

[35] F. Jamil, E. Ahmad, "Policy considerations for limiting electricity theft in the developing countries," *Energy Policy,* vol. 129, pp. 452-458, 2019.