Journal of Engineering and Technological Advances (JETA)
https://jeta.segi.edu.my/index.php/segi
2024 Vol. 10 No. 2

IOT-BASED SMART ENERGY METER MONITORING WITH THEFT CONTROL

[1]Chong, H.S.*, [1]Ramli, N., [2]Kannan, M., [1]Anwar, A.M., [1]Amgad, M.

[1] Centre for Sustainability in Advanced Electrical and Electronic Systems (CSAEES), Faculty of Engineering, Built Environment and Information Technology, SEGi University, 47810 Petaling Jaya, Selangor, Malaysia.

[2] United Institute of Technology, Faculty of Electronics and Communication Engineering, G. Koundampalayam, Periyanaickenpalayam, Coimbatore, 641020, Tamil Nādu, India.

* Corresponding Author: chonghocksiong@segi.edu.my TEL: (603)-61451777

Received: 17 November 2024; Accepted: 28 December 2024; Published: 31 December 2024
doi: 10.35934/segi.v9i2.122

Highlights:

- Cloud-based smart metering is expanding in developing nations
- IoT revolutionizes energy consumption monitoring
- Electricity theft causes financial setbacks and compromises safety
- Validates a real-time IoT-based energy theft monitoring and analysis prototype

Abstract: Electricity theft is an escalating issue, worsened by global warming, which contributes to unbalanced power supply and increased safety concerns. Unauthorized power usage exceeding supply limits often leads to system shutdowns and reduced transmission efficiency. Illegal circuit bypassing has also caused fires, resulting in property damage and threats to public safety. This study presents the design and development of a real-time Internet of Things (IoT)-based smart meter using Arduino technology to monitor energy usage and detect electricity theft. The proposed system involves partial circuit simulation and the development of a full prototype using a direct current (DC) circuit. A Global System for Mobile Communications (GSM) module is integrated to provide remote monitoring and control through Short Message Service (SMS), offering reliable and cost-effective connectivity. When theft is detected, the system triggers a buzzer alarm, displays warnings, and sends power shutdown alerts via GSM. Authorities can then intervene using SMS commands to restore safety. Energy consumption is monitored in real time with updates every 30 seconds. The prototype was tested and successfully validated, showing a maximum error margin of 18% when comparing real and measured power data. The system demonstrated efficient theft detection, real-time monitoring, and remote power control capabilities. This study confirms the feasibility of an Arduino-GSM-based IoT smart meter for real-time electricity monitoring and

theft detection. The proposed solution enhances grid safety and efficiency by providing accurate energy tracking, early warning systems, and remote intervention tools.

Keywords: Electricity Theft Detection; Energy Usage Tracking; Real-time Monitoring; Remote Control; Safety Preventive Measures

1. Introduction

Metering technology is critical in determining how much energy is being used in a residence and in calculating utility bills. Cloud-based smart metering is now extensively marketed, particularly in developing nations. Internet of Things (IoT) refers to item that has been issued an IP address and is capable of collecting and transmitting data across a remote network without the need for human involvement, which in turn revolutionised the energy management, usage monitoring and billing control system. With growing population and town development, the power energy consumption problem has become a major concern. The current power monitoring system is error-prone, labour-intensive, and time-consuming. (Behrendt, 2019; Gatsis & Pappas, 2017; Kumar *et al.*, 2019; Umang & Mitul, 2015; Langhammer & Kays, 2012; Sfar *et al.*, 2018; Yao *et al.*, 2018; Zhou *et al.*, 2017).

With the smart grid immense network of power distribution, the rampant power theft leads to unstable and unpredictable electrical system has a significant impact on the society livelihood. Electricity theft has become a major issue in the electricity industry, particularly in developing nations, whilst the government continues to subsidize the power industry in order to keep energy prices affordable. Due to the financial setback, governments lack the resources necessary to invest in new power plant expansions, resulting inability to meet the rising energy demand, with certain power systems are on the verge of bankruptcy. (Bayram & Ustun, 2017; Jiang *et al*., 2013; Pereira *et al*., 2015).

Tampering meters, bypassing meter, and unpaid bills are all examples of electricity theft. False meter readings and intentional bill manipulating for illegal payments are billing anomalies that have been reported to regulators. Various non-technical and technological approaches for detecting energy theft have been presented in the past. Despite the fact that regular inspections and improved technological measures may have significantly prevent power theft, such a strategy demands large amount of effort and cost. Electricity is crucial to home and industrial growth activities, and must be secured and managed to ensure that consumers get reliable and

efficient power. (Vadda & Seelam, 2013; Deb *et al.*, 2011; Visalatchi & Sandeep, 2017; Maitra, 2008).

Essentially, power theft often leads to the overloading of generating units, which impacted on the utility performance and transmission efficiency. Power theft poses threat to public safety, where electric shocks may cause death, injury and property damages. One of the difficulties in preventing electricity theft is the difficulty in discovering it, especially challenging to gather real-time data that tracks precise spot where power theft occurs. (Hossain *et al.*, 2010; Lorek *et al.*, 2015; Deb *et al.*, 2011; Visalatchi & Sandeep, 2017).

Poor income population is serious issue for the power business in developing nations. Unable to pay bills concerted to illicit power use, which occurs mostly via meter manipulation and bypassing circuit, illegally drawing power from the feeder. Meter manipulation is often done by grounding the neutral wire and direct connection to incoming power source without passing an electric meter. According to a survey, 80% of the overall theft discovered throughout the globe comes from residential structures, while 20% from the commercial and industrial sites (Depuru *et al.*, 2011; Every *et al.*, 2017; Visalatchi & Sandeep, 2017).

This study employs a partial simulation to validate alternate current conversion and power regulation. The simulation also is able to demonstrate the display of date, time, current, voltage, power in kWh, energy cost, and power ON/OFF status. Subsequently, a prototype for real-time energy theft monitoring of utility load, focusing on net consumption, was designed and developed using low-cost current and voltage sensors, a widely available microcontroller with embedded GSM, and designated programming control. The designed system is also able to observe the efficiency of real-time power analysis with intelligent theft detection and information delivery via an IoT platform.

2. Materials and Methods

At initial simulation, a laboratory power generator was used to create a small-scale alternating current (AC) power supply for safety reasons. To keep track of the theft detection, this study included a bypass meter's switch. To minimize noise effect, direct current (DC) load (variable) was used instead of AC, hence bridge rectifier and regulator was applied. Programming was written in such way to stream and track real-time power usage trend, display on mobile, and to identify power theft using data from the current and voltage sensors attached on both supply and load sides. The AC supply energy must be rectified to the necessary DC level depending on the load rating in the study since DC variable loads are being utilized (for safety reason).

The user may operate the driver relays remotely to switch on/off the loads using mobile phone via GSM system. The system was designed to monitor and display data to the users, the load's power consumption and statistics highlight in detail about the maximum used of power and theft detection. Specific usage and features information such as current, voltage, power, kWh, energy cost and timing occur will be shown on the LCD and also on remote mobile. Buzzer was used as alarm to trigger by theft detection. The overall block diagram of the system design is shown in **Figure 1**.

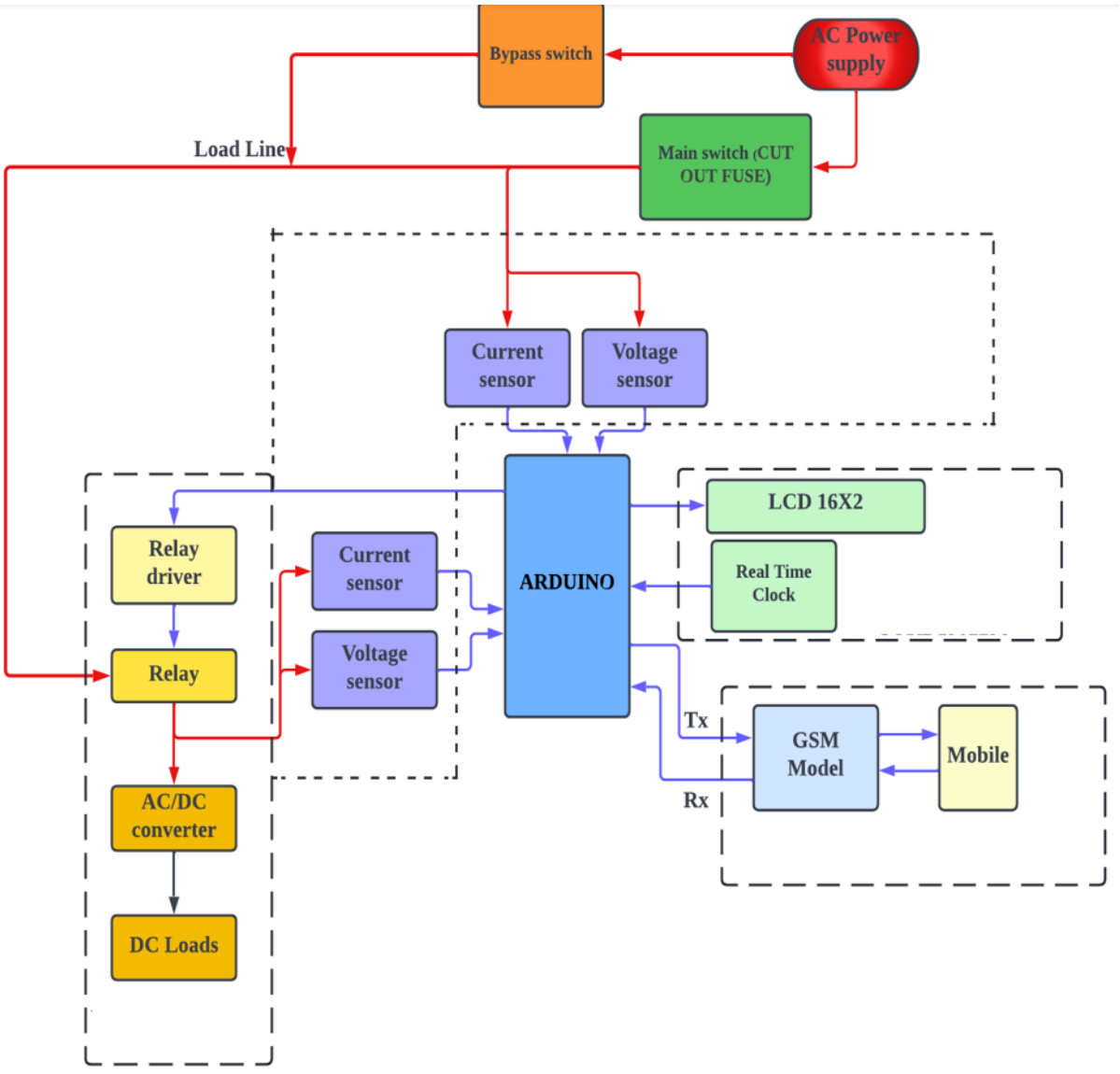

Figure 1. Overall block diagram of the system design

System design flow diagram is shown in **Figure 2**. After initializing and connecting, the sensors will begin detecting power (calculated from current and voltage obtained using assigned formulas) at two locations (P1 and P2). P1 is the meter-supplied power, whereas P2 is the theft power (bypass meter) provided to the load. Both powers were calculated using assigned

formulas with calibrated constant and shall the power differences between these two spots within % allowable range, the power usage data will be shown on Liquid Crystal Display (LCD), and also sent to the consumers and providers via SMS.

In the event of consumer bypass meter (theft), the calculated comparison of P1 & P2 data will show significant differences, therefore the system will trigger energy theft status at instant, on LCD with buzzer on, and delivered SMS to the authority to investigate on spot, to take the appropriate steps to mitigate illegal circuitry. Real-Time Clock (RTC) integrated circuit was attached with the microcontroller to track exact timing/duration of theft, enable monitor the power consumption kWh in real time by torque control of DC motor and detect the peak demand on specific time. Once theft issue is mitigated and that circuit is safe to engage, provider can use mobile phone to send SMS to the microcontroller to turn on/off power supply.

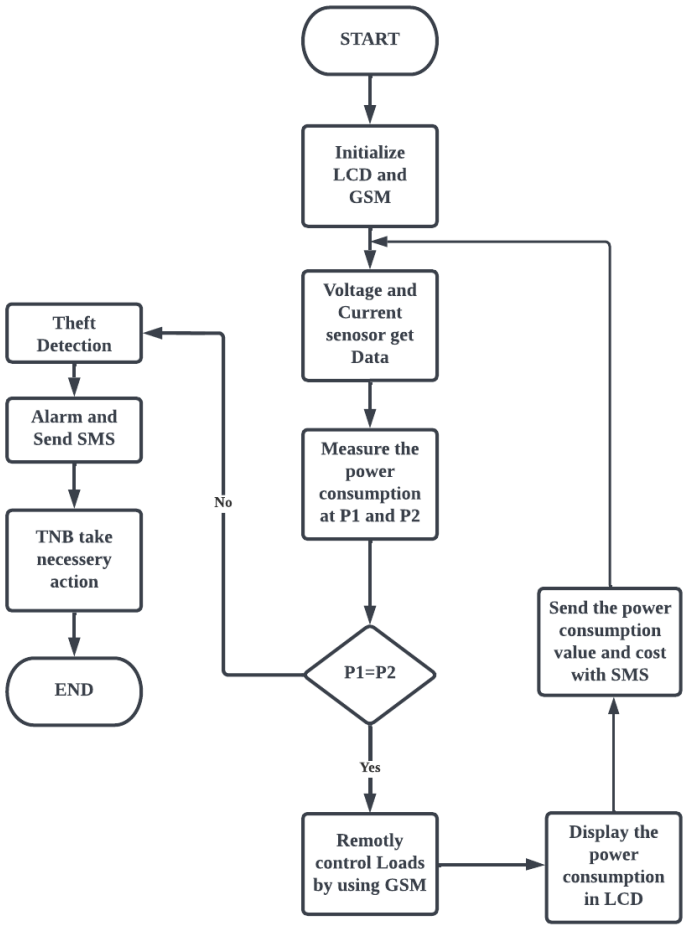

Figure 2. Design flow chart of the study

Figure 3 illustrates the power measurement methodology used in the study. Since small scale voltage and current was engaged, the sensors (voltage sensor – inductive transformer type; current sensor – hall effect type) output level ranges from 0 to 5V was employed. To begin,

accurate calculation and measurement should be used to determine the true values with proper calibration using appropriate constant and formulas.

To detect power theft, two side points of the design must obtain power measurements. If P1 does not equal P2 (with 30% difference allowance due to noise, electrical disturbance), then power theft detection must be considered. Depending on how long the period, and the capacity of current and voltage is operating, the energy consumption in KWh unit shall be calculated for energy billing and record-keeping purposes, and to be displayed on LCD and delivered to remote mobile.

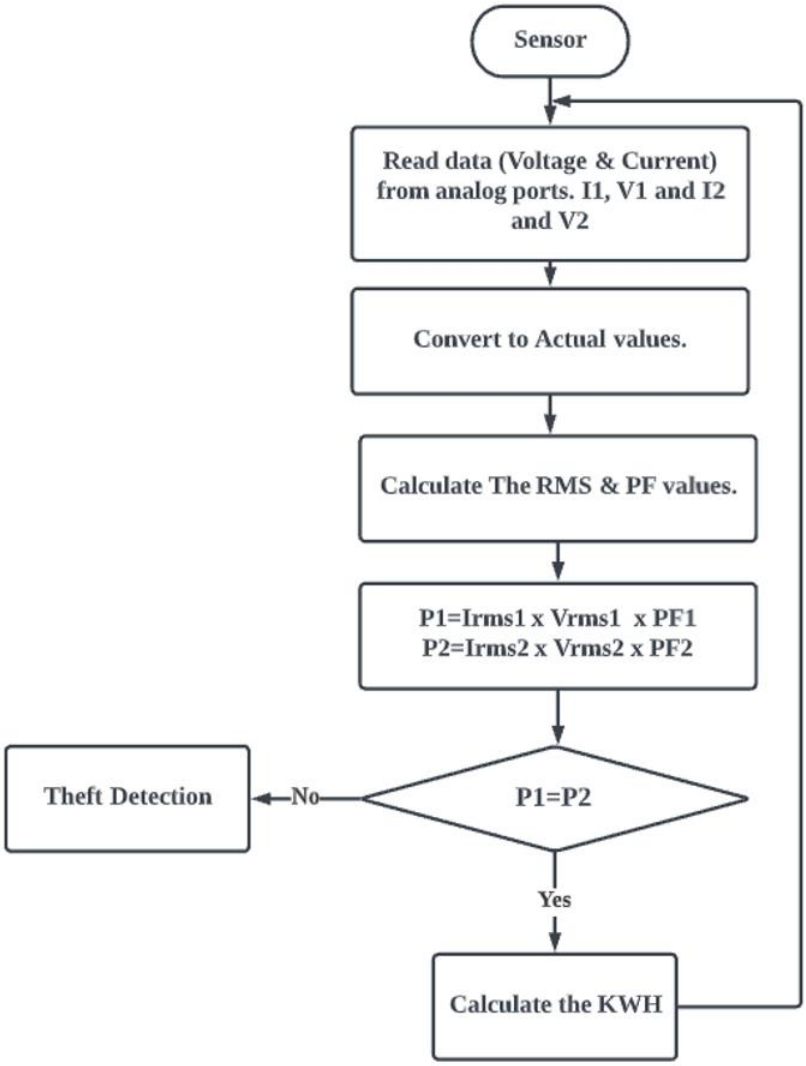

Figure 3. Power measurement and theft detection flows

A GSM module takes a SIM card and functions on a mobile operator's subscription presents an interface of which SMS may send and receive messages, compatible with Arduino Uno and other 5V-capable controller boards. The cost of message send/receive is charged by the mobile operator. Data transmission via cellular network needs no extra hardware or software, saving

time and money to deploy it. Encryption method is used in cellular technology to protect data from being intercepted by outside source. Real-time notifying, alarm and event reporting, power loss reporting, and power cut-off/restoration are possible with the cellular network.

In this study, GSM was used to inform the user about energy theft, and display energy consumption with feature. Also, the user should be able to control the power On/Off (remotely) to the load by SMS. Therefore, GSM should be able to operate in two basic flows, send and receive data from authority to control load and transmit the data of energy consumption and energy theft warning to users. Authority is able to keep track until theft circuit is resolved, then send SMS to turn on the power to the load. Meanwhile, the GSM will send real-time energy usage KWh or bill to the user within certain period of loop.

This study was evaluated in two stages, the first being the partial design simulation to validate using software, and the second being the full hardware implementation and testing. By using the selected software for simulation purpose, voltage supply was measured at 21V AC, frequency at 50 Hz in accord to the study assumption. As explained earlier, power theft will trigger alarm, as well tripping the power off. Authority is to turn ON power back after theft issue is mitigated, using mobile SMS via driver relay therefore relay is essential element in the design. When the 5V relay (RL1) is triggered, it'll turn ON the power to the DC load.

The AC voltage will be stepped down to 14V AC using transformer (X1), then with full bridge rectifier, the DC voltage of 18V DC will be generated where each diode has about 1V cut in voltage and in each cycle the current pass through two diodes. **Figure 4** shows that the regulator (U1) maintains a steady output DC voltage level of 12V. When the relay (RL1) is not conducting (Power OFF scenario), the output voltage drops to 0V, turning off the DC load.

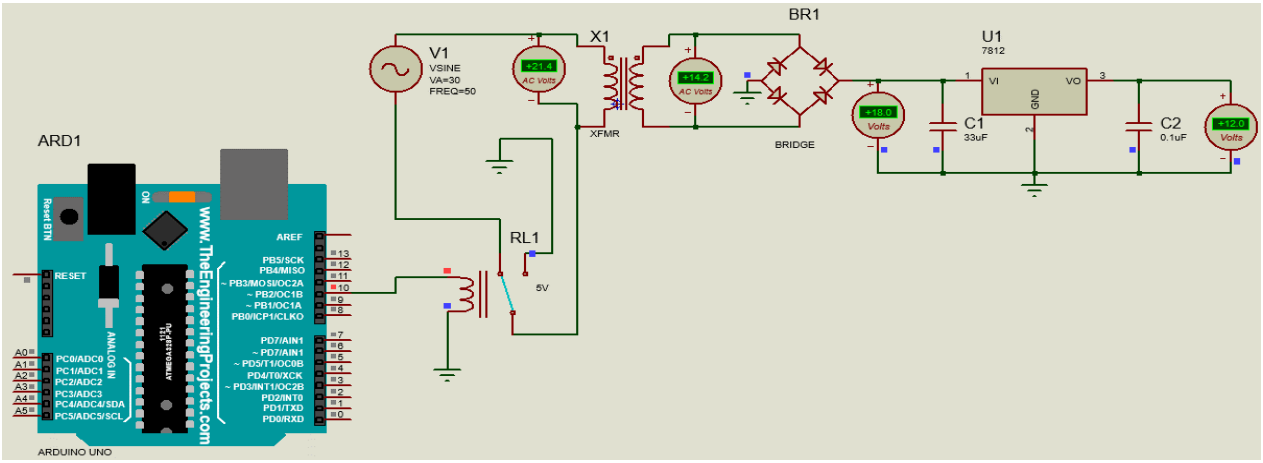

Figure 4. Simulation of drive relay (RL1) ON/OFF power to load

A widely available microcontroller in the market was employed to keep track of current date and time for a variety of purposes such as book logs. Clocks created using an Arduino UNO's integrated with RTC operate as timers, enabling users to schedule actions and have them performed calculation/display on certain loop time. **Figure 5** depicts integrated simulation of an RTC (U1) and LCD display. The LCD is able to display the date and time, current, voltage, power in kWh, energy cost, and acknowledge of power trip OFF/ON.

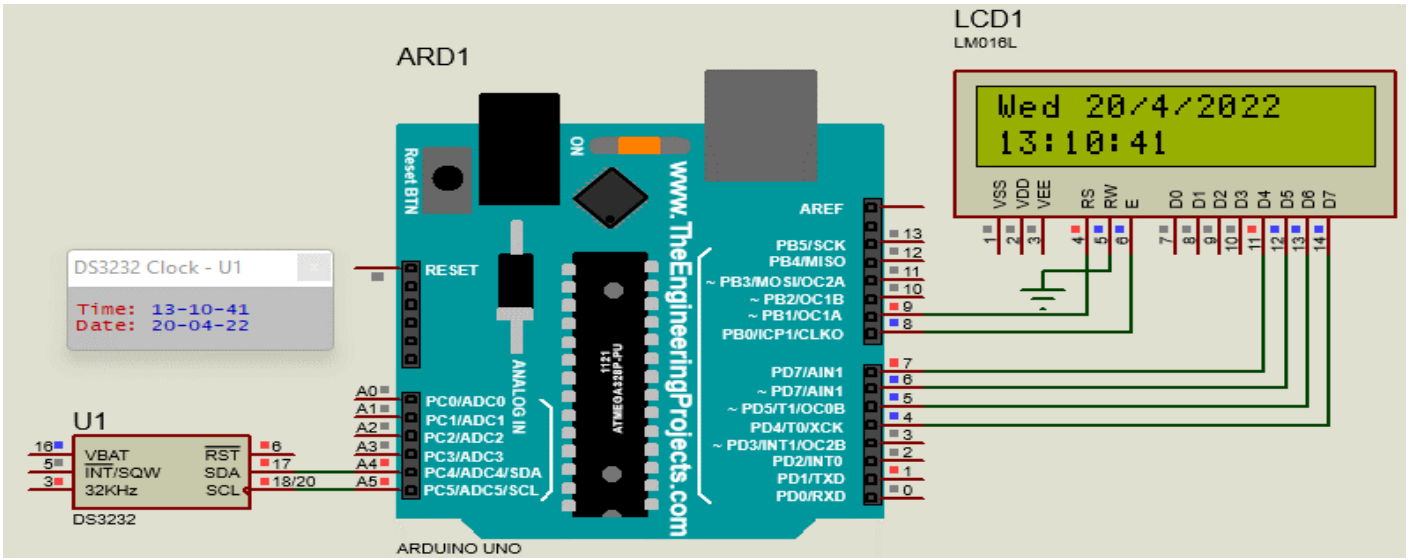

Figure 5. RTC and LCD display

3. Results and Discussion

3.1. Current, Voltage and Power Consumption

Power theft detection was measured by comparing power readings at two different locations, one after metering, and the other was close to the load, while simultaneously observing power consumption using current and voltage sensors, integrated with an IoT platform for remote control and monitoring. **Figure 6** shows prototype with relay at P1 (with meter) and P2 (bypass meter). The voltage sensor ZMPT101B was calibrated approximately similar reading to the second voltage sensor. Measured valued was multiplied with coefficient for better comparison based on the observation from the serial monitor and plotter. LCD shows the output response of the measurements at the P1 (top row) and P2 (bottom row).

As the power factor is almost unity due to small DC load, therefore, the power was calculated with root mean square (rms) voltage and current. When bypass switch is ON, the current that flow through meter in P1 will be zero but current is detected in P2. As such, the power at P1 will be zero, but P2 measured power as it shown in **Figure 7**. Analysis by comparing differences between P1 and P2 at certain allowance is the fundamentals for energy theft detection.

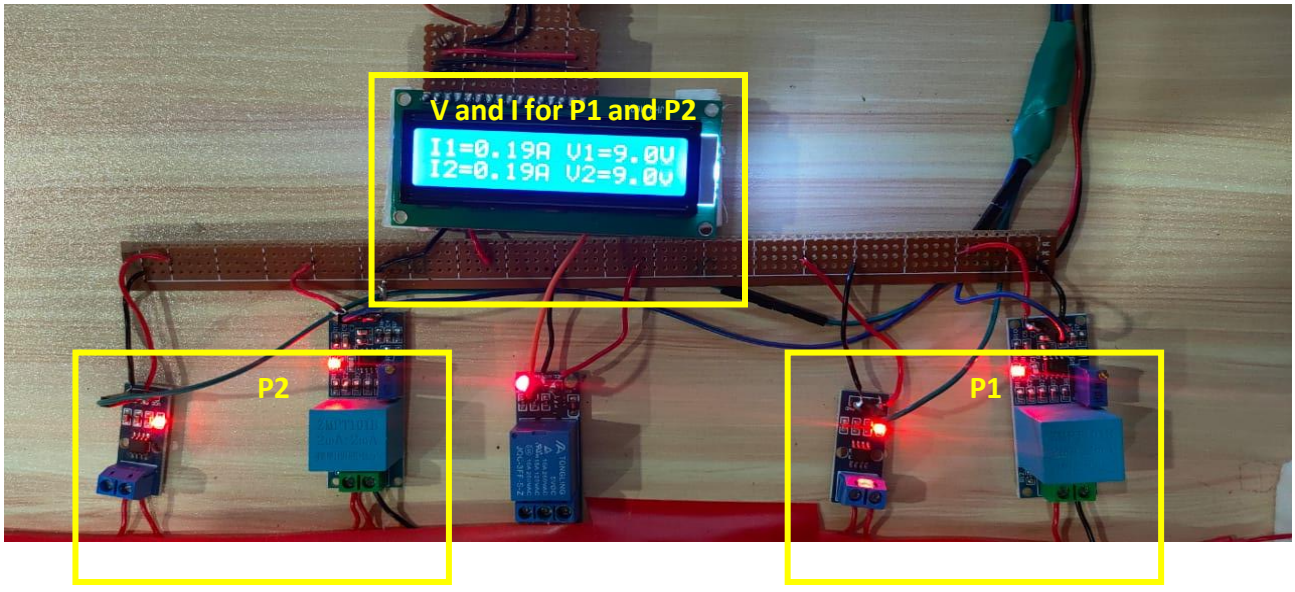

Figure 6. Normal operation or bypass Off – power at 2 points (similar I and V for P1 & P2 on LCD)

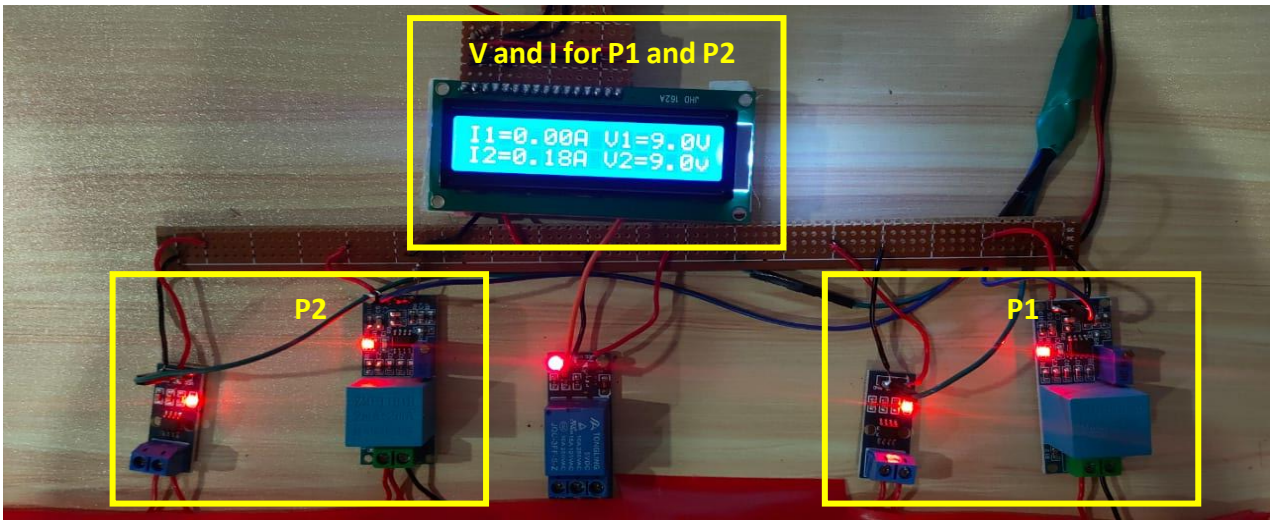

Figure 7. Power theft detected (bypass On) – P1 is 0W (top row), P2 is 1.62W (bottom row)

Using real-time clock, targeted loop duration sampling, proper formula and calculation, **Figure 8** shows LCD displays of real-time current, voltage, power in Watt-hour (Wh) is used instead of kilowatt-hour (kWh) due to low power load. In every 30 s, sampling of power was taken over a period of 14 minutes duration under varying torques applied to the DC load. **Figure 9** displays plot of varying power consumption, where input current with the increase of torque on load and data are selected using one channel of data streamer. From the plot of the received data, consumer can observe the exact timing of when the maximum power consumption occurs, for example 3.21W at 23:17:05 hour.

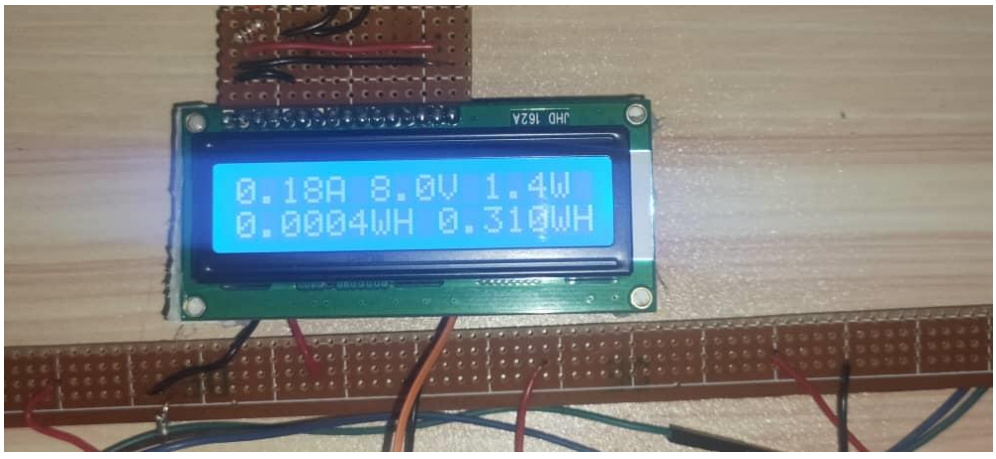

Figure 8. Real-time energy consumption display

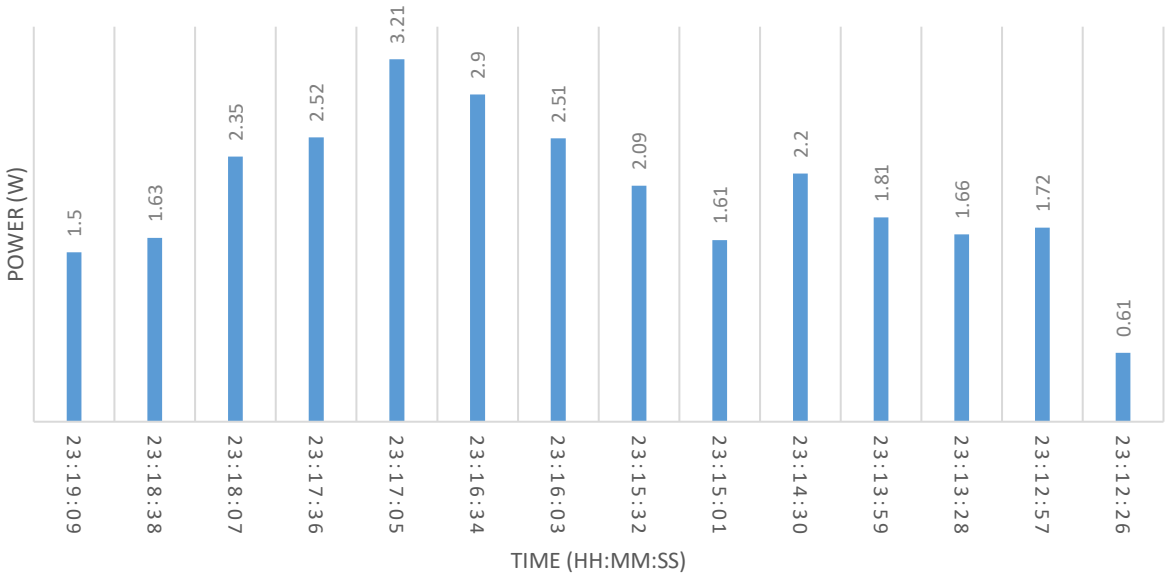

Figure 9. Real-time energy consumption calculation and display

3.2. GSM Model and Wireless Communication

Figure 10 shows screenshot from authority's mobile contact number +6011-61946909. SMS is sent to the consumer home via integrated GSM module with registered Simcard +6017-2962815. The SMS carries message; 'A' – Turn On DC motor, or 'B' – Turn Off DC motor.

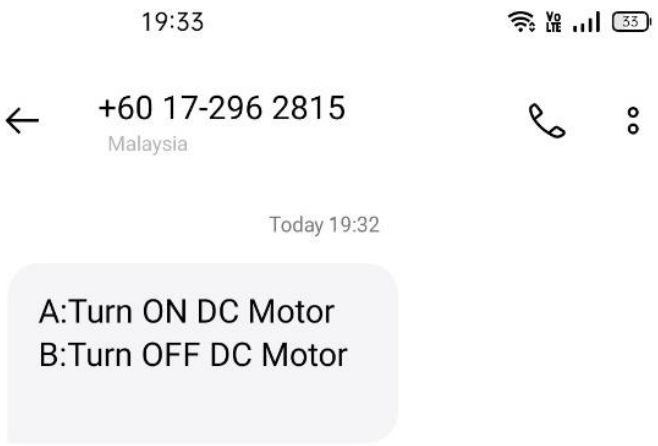

Figure 10. Authority command to GSM Module at consumer home via SMS

Figure 11 shows the LCD displayed 'DC MOTOR OFF' which responses to 'B' command from authority SMS when theft was detected. A function is defined to send the message to user and authority after detecting the theft while LCD display text "Theft Detected" for 5s and automatically shut down the relay which will disconnect the power to the load.

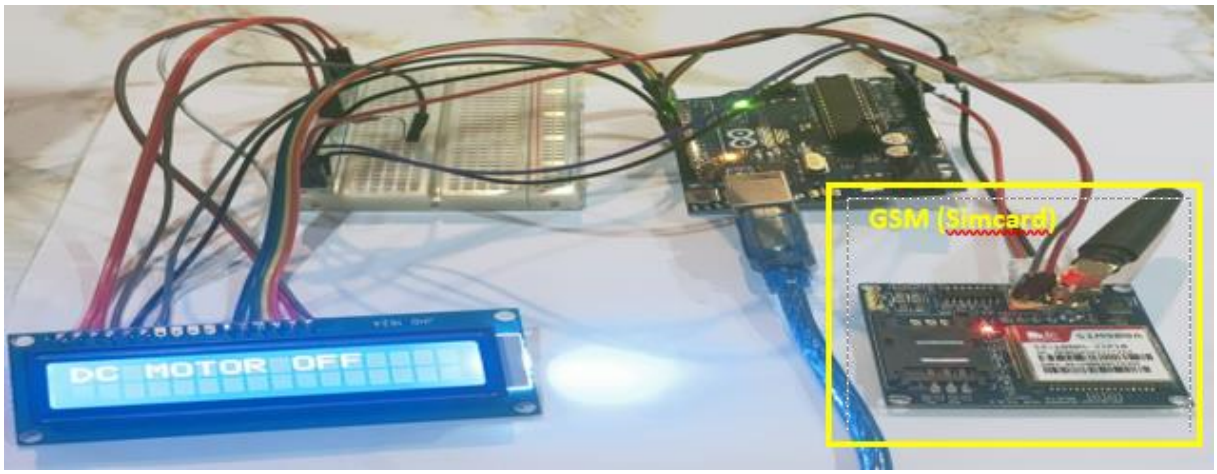

Figure 11. System responses to "B" command from authority via SMS when theft detected

As previously explained, there were two sensors at two points to measure the power consumption. When the system operates normally, these two points should measure identical power. However, as there is error in detecting the current and voltage and all sensors are subjected to electrical noise, hence slight gap of power differences can be detected in the calculation plot. **Figure 12** presents the plot of data collected/calculated as power consume over time at these two points (red – P2, blue – P1).

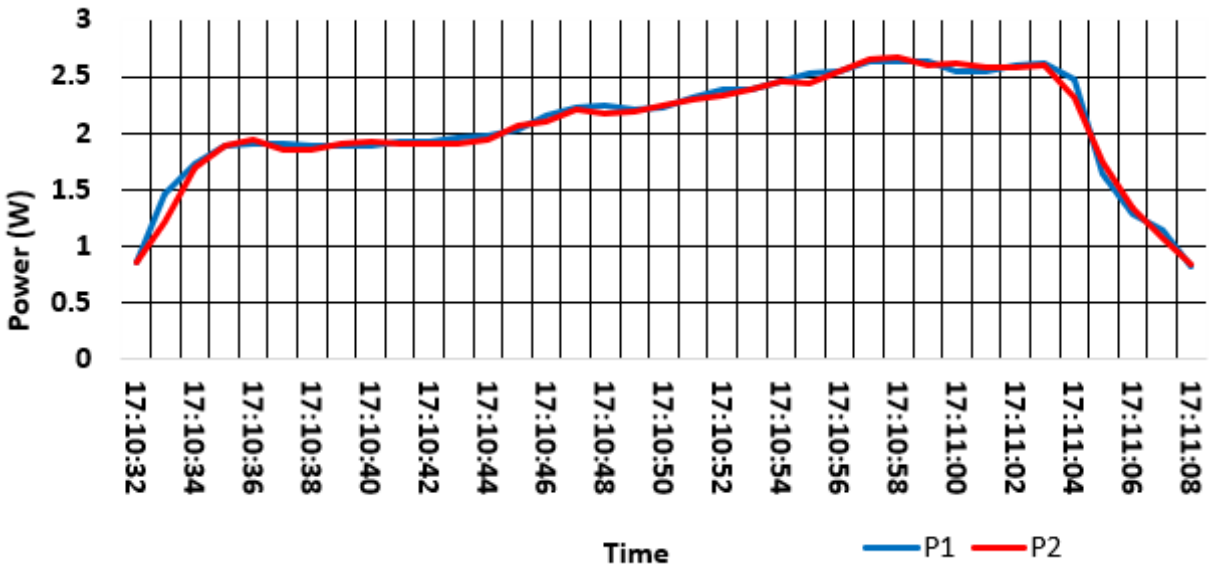

Figure 12. P1 and P2 power comparison at the same timing (real-time).

Figure 13 represents the calculated error occurred between the power comparison, when under normal operation. The maximum error is detected 18%. Hence, for theft detection, the percentage of error is set to 30% to avoid false alarm of turning off power to home.

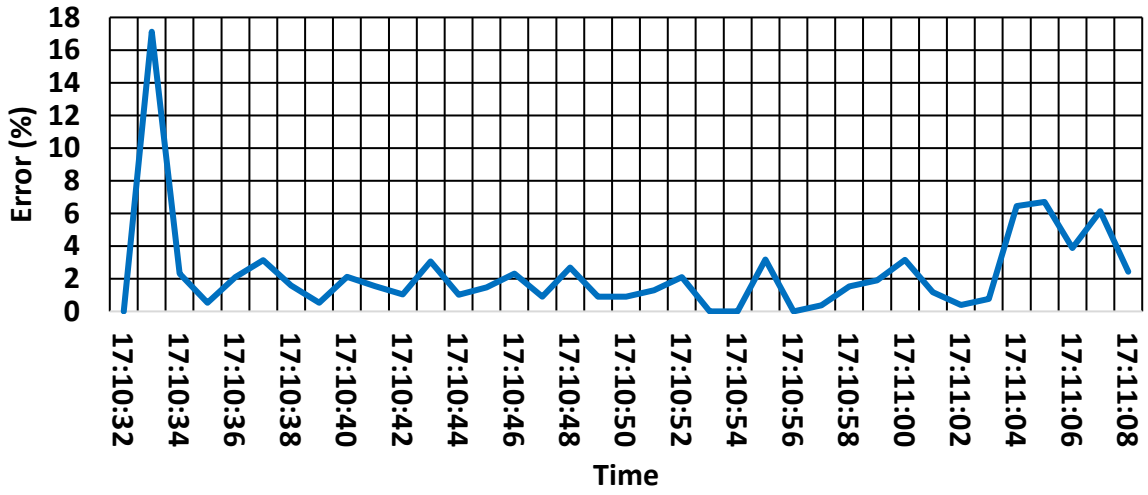

Figure 13. Error in power calculation at 2 points

4. Conclusion

Tampering with meters, bypassing meters to steal power, adjusting billing discrepancies, and unpaid bills are all examples of electricity theft. False meter readings and intentionally manipulating bills for illegal payments are among the many billing anomalies. Unbalanced electricity power supply and demand have caused shocks and fires, damaging countless homes and endangering lives. The results showed that the study was successfully simulated, a prototype was developed and tested to observe recorded real-time energy consumption, and theft monitoring and power on/off control via IoT were achieved. Consumers were able to observe power consumption patterns in real time (daily) and control usage accordingly. Combined with IoT capabilities, power monitoring and electricity supply control could be easily executed via SMS remotely to targeted consumers or locations, with authorities informed accordingly. Power remained off until the theft circuitry was mitigated by authorized personnel as evident in SMS control. The results obtained demonstrate the functional circuit design with real-time remote theft detection (buzzer warning and LCD display), real-time remote observation of energy consumption every 30 s, remote power on/off control via GSM, and validation of real power against measured power data with a maximum error of 18%. Recommendations for future works include minimizing the power measurement error and

enhancing the robustness and security of the remote control and theft detection mechanisms for broader real-world application.

Acknowledgement

The authors would like to thank the Centre for Sustainability in Advanced Electrical and Electronics Systems (CSAEES), Faculty of Engineering, Built Environment, and Information Technology of SEGi University and the Faculty of Electronics and Communication Engineering of United Institute of Technology, India for supporting the research of this study.

Credit Author Statement

Conceptualization and methodology, Chong, H.S., Anwar, A.M. and Amgad, M.; software and validation, Anwar, A.M. and Amgad, M.; formal analysis, Anwar, A.M., Amgad, M. and Chong, H.S.; investigation, Anwar, A.M., Amgad, M. and Chong, H.S.; writing—original draft preparation, Anwar, A.M., Amgad, M. and Chong, H.S.; writing—review and editing, Ramli, N. and Kannan, M.; supervision and project administration, Chong, H.S.

Conflicts of Interest

The authors declare no conflict of interest.

References

Bayram, I. S., & Ustun, T. S. (2017). A survey on behind the meter energy management systems in smart grid. *Renewable and Sustainable Energy Reviews*, 72, 1208-1232.

Behrendt, F. (2019). Cycling the smart and sustainable city: analyzing EC policy documents on internet of things, mobility and transport, and smart cities. *Sustainability*, 11(3), 763.

Deb, S., Bhowmik, P. K., & Paul, A. (2011). Remote detection of illegal electricity usage employing smart energy meter-A current based technique. In *ISGT2011-India*. (pp. 391-395). IEEE.

Depuru, S. S. S. R., Wang, L., Devabhaktuni, V., & Gudi, N. (2011). Smart meters for power grid—Challenges, issues, advantages and status. In *2011 IEEE/PES Power Systems Conference and Exposition* (pp. 1-7). IEEE.

Every, J., Li, L., & Dorrell, D. G. (2017). Leveraging smart meter data for economic optimization of residential photovoltaics under existing tariff structures and incentive schemes. *Applied Energy*, 201, 158-173.

Gatsis, K., & Pappas, G. J. (2017). Wireless control for the IOT: Power, spectrum, and security challenges. In *Proceedings of the Second International Conference on Internet-of-Things Design and Implementation* (pp. 341-342).

Hossain, M. R., Oo, A. M. T., & Ali, A. S. (2010). Evolution of smart grid and some pertinent issues. In *2010 20th Australasian Universities Power Engineering Conference* (pp. 1-6). IEEE.

Jiang, R., Lu, R., Lai, C., Luo, J., & Shen, X. (2013). Robust group key management with revocation and collusion resistance for SCADA in smart grid. In *2013 IEEE global communications conference (GLOBECOM)* (pp. 802-807). IEEE.

Kumar, S., Tiwari, P., & Zymbler, M. (2019). Internet of Things is a revolutionary approach for future technology enhancement: a review. *Journal of Big data*, 6(1), 1-21.

Langhammer, N., & Kays, R. (2012). Performance evaluation of wireless home automation networks in indoor scenarios. *IEEE Transactions on Smart Grid*, 3(4), 2252-2261.

Lorek, M. C., Chraim, F., & Pister, K. S. (2015). Plug-through energy monitor for plug load electrical devices. In *2015 IEEE SENSORS* (pp. 1-4). IEEE.

Maitra, S. (2008). Embedded Energy Meter-A new concept to measure the energy consumed by a consumer and to pay the bill. In *2008 Joint International Conference on Power System Technology and IEEE Power India Conference* (pp. 1-8). IEEE.

Pereira, R., Figueiredo, J., Melicio, R., Mendes, V. M. F., Martins, J., & Quadrado, J. C. (2015). Consumer energy management system with integration of smart meters. *Energy Reports*, 1, 22-29.

Sfar, A. R., Natalizio, E., Challal, Y., & Chtourou, Z. (2018). A roadmap for security challenges in the Internet of Things. *Digital Communications and Networks*, 4(2), 118-137.

Umang, P., & Mitul, M. (2015). A review on smart meter system. *International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering*, 3(12), 70-73.

Vadda, P., & Seelam, S. M. (2013). Smart metering for smart electricity consumption, *Blekinge Institute of Technology*, Karlskrona, Sweden.

Visalatchi, S., and Sandeep, K.K. (2017). Smart energy metering and power theft control using arduino & GSM, *2nd International Conference for Convergence in Technology (I2CT)* (pp. 858-961), IEEE.

Yao, H. W., Wang, X. W., Wu, L. S., Jiang, D., Luo, T., & Liang, D. (2018). Prediction method for smart meter life based on big data. *Procedia engineering*, 211, 1111-1114.

Zhou, J., Cao, Z., Dong, X., & Vasilakos, A. V. (2017). Security and privacy for cloud-based IoT: Challenges. *IEEE Communications Magazine*, *55*(1), 26-33.