Design of Electricity Theft Monitoring System Using Differential Power Method Based on Internet of Thing

Hartono*, Rifdian Indrianto Sudjoko, Fiqqih Faizah, Kustori, Slamet Hariyadi

Politeknik Penerbangan Surabaya, Jemur Andayani I/73 Wonocolo Surabaya, Jawa Timur, Indonesia, 60236
**Corresponding Author Email:hartono.asempapan@gmail.com*

ABSTRACT
Electricity theft by some unscrupulous people is very detrimental to PLN. Theft can be done by households or industries. The theft is not only financially detrimental to PLN but also damages the transformer in the distribution network due to overloading. In this research, a prototype of an electricity theft detection system integrated with the Internet of Thing (IoT) and mobile applications has been made using the differential power method. The differential power method compares real-time power measurements with a reference network average power, so that when the measured power exceeds the reference value, there is an indication of theft on the network. The sensor data processor and theft detection algorithm use an ESP8266 microcontroller. The test results show that the measurement errors of the voltage, current, and power sensors are 0.45%, 1.57%, and 1.15%, respectively. The data transmission delay from the microcontroller to the cloud is less than 1 second. The mobile application is able and successful to display measurement results and provide real-time theft alarm notifications

Keywords: *Electricity theft, Microcontroller, IoT, Mobile Application, Cloud.*

1. INTRODUCTION

Indonesia as a third world country, consumes a large amount of electricity due to high consumer demand. The use of electrical loads has increased in various sectors, be it residential, commercial, or industrial sectors. Electricity is a very reliable partner and plays an important role in our daily lives [1] [2]. In accordance with the law of supply and demand, when electricity supply is low and demand is high, its price will increase [3]. This means that a surge in electricity consumption can lead to price increases, which can make it difficult for some people to cope with the cost, and this often results in electricity theft [4]. Every year, the number of cases of electricity theft at household electricity connections increases significantly [5]. If this crime continues on a larger scale, it could have a negative impact on the country's economic status [6]. Electricity has a central role in national development [2]. Essentially, electricity provides livelihoods for communities, improves the way services are performed, thus making life better and easier for people [7].

Research into detection methods and the development of electrical theft devices in Indonesia has been ongoing for quite some time. Most of this research comes from vocational education and results in simple detection devices that function at a local level in homes. One example of a simple application is comparing the power recorded on the electricity meter at the Mini Circuit Breaker (MCB) with the data obtained from the tool developed by the researcher [8]. Some researchers perform theft detection based on monthly customer consumption data. By adopting the load profile anomaly approach, if there is a sudden use of electricity, electricity theft can be detected [9].

In this research, a prototype of an electricity theft detection system integrated with the Internet of Thing (IoT) and mobile applications has been made using the differential power method. The differential power method compares real-time power measurements with a reference network average power, so that when the measurement power exceeds the reference value, there is an indication of theft on the network.

2. THEORY BASIS

The power measurement process involves measuring the current and voltage on the power grid. Some common methods used to measure current on the AC power grid are Current Transformers (CT). CT is a device that converts high current into low current for measurement purposes. CTs are very commonly used in the measurement of large AC currents, such as in electrical substations and industrial equipment. The results from the CT must be fed to an ammeter or other measurement system. Another method is with a shunt resistor. A shunt resistor is a resistor placed in parallel with the device whose current is to be measured. The voltage drop along the shunt resistor is used to measure the current through Ohm's law. Shunt resistors are typically used in low current applications. Another method is with a Hall Effect Sensor. A Hall Effect Sensor is a semiconductor device that produces an output voltage according to the magnetic field it receives. It is used in AC current measurement applications by placing the sensor around a current-carrying wire. The output of the Hall Effect sensor will correlate with the amount of current flowing through the wire.

2.1. Current Transformer (CT)

A CT is an electromagnetic device used to measure high electric currents with lower secondary currents suitable for measurement and monitoring. The working principle of CT is based on Faraday's electromagnetic law and Lenz's electromagnetic induction law. A change in electric current in the primary coil of the CT will produce a changing magnetic flux in the iron core of the CT. This will induce an electric voltage in the secondary coil according to the change in magnetic flux, in accordance with Faraday's law. The voltage generated in the secondary coil of the CT will have the opposite direction to the change in current in the primary coil. This produces a secondary voltage that corresponds to the primary current, allowing for safe measurements.

Each CT has a transformer ratio that determines how much current the secondary coil of the CT will provide for each current flowing through the primary coil. For example, a CT with a ratio of 100:5 will produce 5 amperes of secondary current for every 100 amperes of primary current. The use of CTs to measure current has several advantages, among others:

- Converting high currents into currents that can be measured with smaller and safer measurement devices.
- Protects equipment and measurement devices from overcurrent.
- Enables accurate measurement of current in electrical circuits.

2.2. PZEM-004 Module

PZEM-004 is an electrical energy measurement module used to measure various electrical parameters on an electrical circuit, such as voltage, current, active power, reactive power, apparent power, frequency, and electrical energy (kWh). The PZEM-004 uses voltage measurement technology that matches the electrical circuit being measured. It can operate at a reference voltage that is typically 220V AC at a frequency of 50Hz. The PZEM-004 module uses a shunt resistor sensor to measure the electric current flowing through a particular cable or circuit. Figure 2.1 is a photo of the PZEM-004 module.

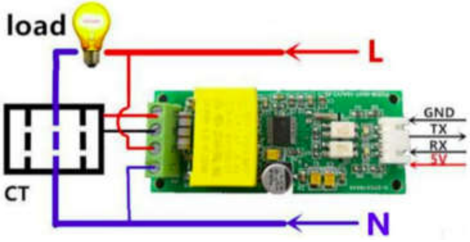


Figure 2.1. Photo of the PZEM-004 power meter module.

Based on voltage and current measurements, PZEM-004 can calculate active power, reactive power, apparent power, and electrical energy used. The data generated by PZEM-004 can be used for monitoring and analyzing electrical energy consumption. Some versions of PZEM-004 have data communication capabilities with asynchronous serial data format with TTL level. This data can be captured, recorded, and analyzed to monitor the use of electrical energy in specific applications.

2.3 IoT Platform

Internet of Things (IoT) is a brilliant idea to develop the utilization of internet connectivity. Every IoT device has one main purpose, which is to bridge the device with the application to transmit information through the internet transfer protocol. To overcome the gap between device sensors and data networks, the IoT Platform was created. This platform is tasked with connecting data networks to control these sensors and generate in-depth understanding through backend applications related to hundreds of data generated by these sensors.

The IoT Platform is a multi-layered technology capable of providing, managing, and automating devices directly connected to the IoT. In other words, it connects hardware to the cloud in a highly flexible way, provides enterprise-grade security mechanisms, and powerful data processing capabilities.

The position of the IoT Platform with respect to hardware devices and software applications is shown in Figure 2.2. The IoT Platform provides a set of ready to use features that greatly accelerate application development for connected devices and maintain scalability and cross device compatibility.

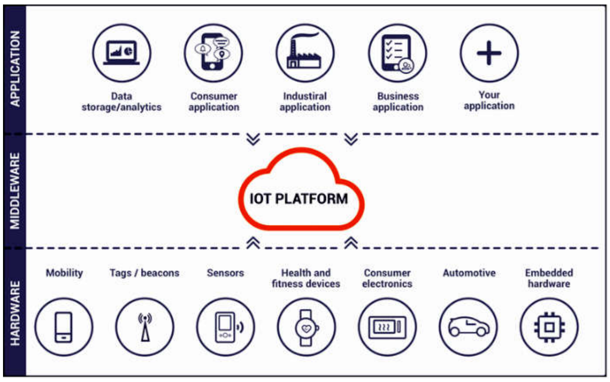


Figure 2.2. IoT Platform positioning of sensor hardware and software applications.

3. SYSTEM DESIGN

The electricity theft monitoring system using the differential current method detects electricity theft based on the difference between the current measured in real time and the reference current value. The reference current is the monthly average current in a distribution network. If the measured current value exceeds the reference current value, the system will provide warning information about theft in the network.

3. 1. System Block Diagram

The functional diagram of the electricity theft monitoring system is shown in Figure 3.1.

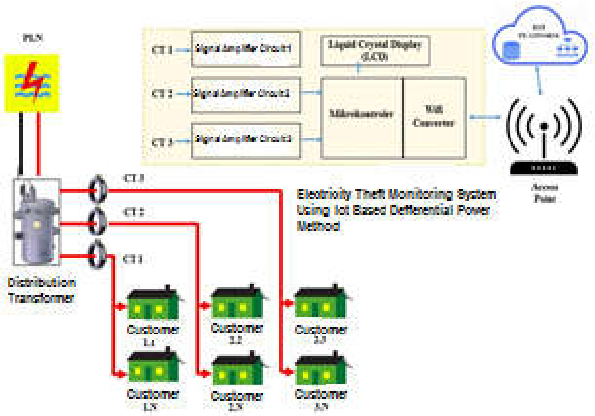

PLN
CT 1
CT 2
CT 3
Signal Amplifier Circuit 1
Signal Amplifier Circuit 2
Signal Amplifier Circuit 3
Liquid Crystal Display (LCD)
Mikrokontroler
Wifi Converter
Access Point
Electricity Theft Monitoring System Using Iot Based Defferential Power Method
Distribution Transformer
Customer 1.1
Customer 2.2
Customer 3.3
Customer 1.N
Customer 2.N
Customer 3.N

Figure 3.1. Functional diagram of the electricity theft monitoring system.

This theft monitoring system has 4 main parts, namely:

1 Sensor and signal conditioning circuit
2 Microcontroller system
3 IoT Platform
4 Mobile Application

3.1.1. Sensor and Signal Conditioning Circuit

This monitoring system measures the power on each network connected to the distribution transformer. The current flowing in each network is measured using a current transformer-based current sensor. In addition to the current, the system also measures the voltage on the network. Based on these two measurements, the power in the network can be known.

The signal conditioning circuit is part of the system that functions to amplify the signal from the sensor and process it into data that can be read by the controller. The signal conditioning circuit in this system uses the PZEM-004 module. The schematic of the PZEM-004 circuit is as shown in Figure 3.2. This module uses a digital power meter IC with serial data output. The interface between the IC power meter and the microcontroller has used optical isolation.

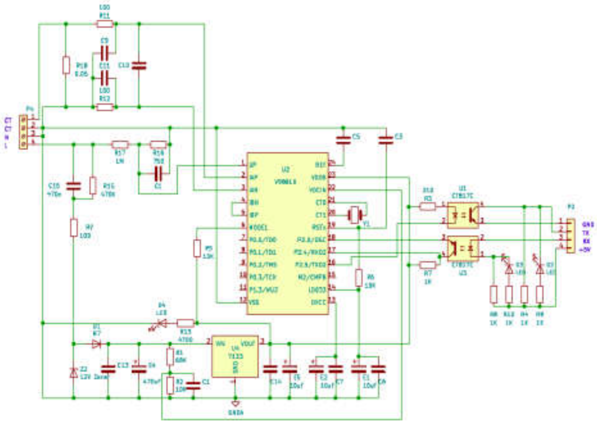


Figure 3.2. Schematic diagram of the PZEM-004 signal conditioning circuit.

3.1.2 Microcontroller System

This monitoring system uses an ESP8266 type microcontroller. ESP8266 is a microcontroller developed by Espressif System with WiFi communication capabilities. The WiFi feature allows the ESP8266 to connect to wireless networks and communicate via the Internet. ESP8266 has a high-speed processor, so it can run various IoT applications well. In addition, there are I/O pins that can be used to connect sensors, actuators, and other devices. ESP8266 has extensive software support, such as Arduino IDE, MicroPython, and

NodeMCU, which makes project development easier. Figure 3.3 is the ESP8266 microcontroller circuit.

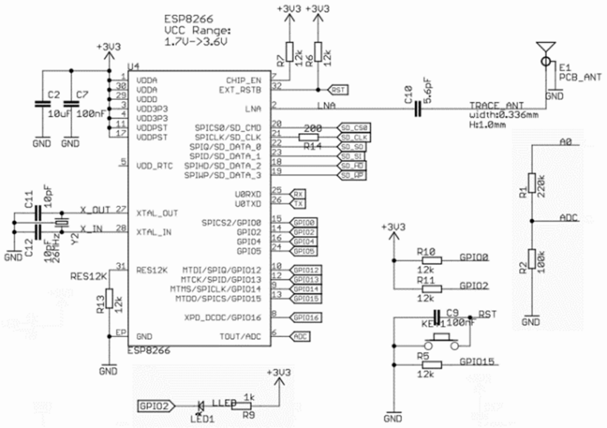


Figure 3.3. Schematic diagram of the ESP8266 microcontroller.

The three current sensors and the signal conditioning system in each of the electricity distribution networks are connected to the microcontroller via TTL level serial communication on pinouts D5 and D6. The display system for the measurement results uses an OLED LCD Shield. This LCD is a type of graphic LCD with a resolution of 64x48 pixels. The connection between the microcontroller and LCD uses I2C communication.

The theft detection algorithm using the power differential method has a flow chart diagram as shown in Figure 3.4. This algorithm compares the total power or power on the network with the average total power on the network. The average total power value in real conditions can be obtained from the total bill on one network divided by the total time. If the measured power value exceeds the average power, the controller will send an alarm signal and locate the network.

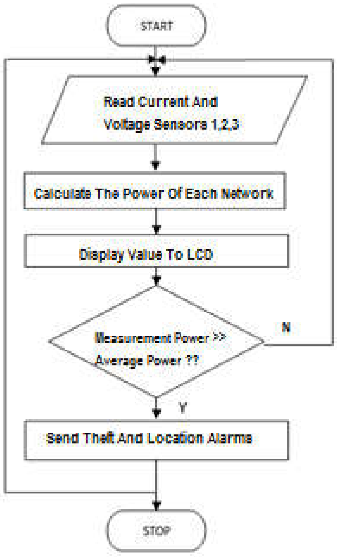
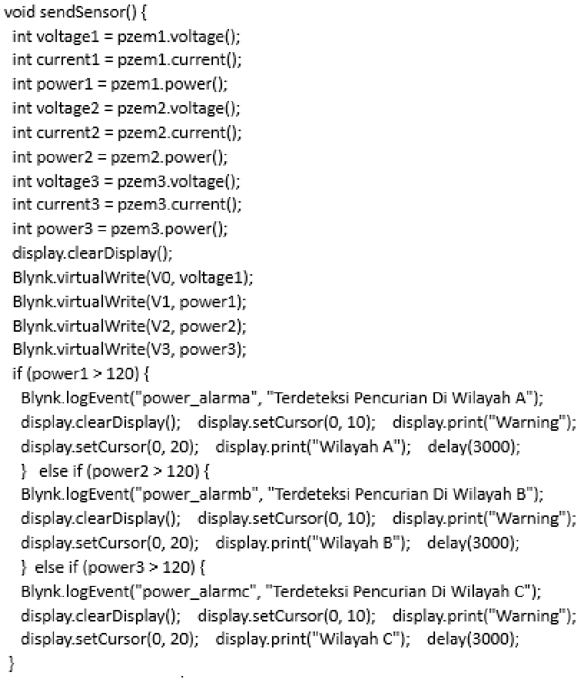

START
Read Current And Voltage Sensors 1,2,3
Calculate The Power Of Each Network
Display Value To LCD
Measurement Power >> Average Power ??
N
Y
Send Theft And Location Alarms
STOP

Figure 3.4. Flow chart of theft detection algorithm with power differential method.

Figure 3.5. Theft detection program script.


```
void sendSensor() {
  int voltage1 = pzem1.voltage();
  int current1 = pzem1.current();
  int power1 = pzem1.power();
  int voltage2 = pzem2.voltage();
  int current2 = pzem2.current();
  int power2 = pzem2.power();
  int voltage3 = pzem3.voltage();
  int current3 = pzem3.current();
  int power3 = pzem3.power();
  display.clearDisplay();
  Blynk.virtualWrite(V0, voltage1);
  Blynk.virtualWrite(V1, power1);
  Blynk.virtualWrite(V2, power2);
  Blynk.virtualWrite(V3, power3);
  if (power1 > 120) {
    Blynk.logEvent("power_alarma", "Terdeteksi Pencurian Di Wilayah A");
    display.clearDisplay();   display.setCursor(0, 10);   display.print("Warning");
    display.setCursor(0, 20);   display.print("Wilayah A");   delay(3000);
    }  else if (power2 > 120) {
    Blynk.logEvent("power_alarmb", "Terdeteksi Pencurian Di Wilayah B");
    display.clearDisplay();   display.setCursor(0, 10);   display.print("Warning");
    display.setCursor(0, 20);   display.print("Wilayah B");   delay(3000);
    }  else if (power3 > 120) {
    Blynk.logEvent("power_alarmc", "Terdeteksi Pencurian Di Wilayah C");
    display.clearDisplay();   display.setCursor(0, 10);   display.print("Warning");
    display.setCursor(0, 20);   display.print("Wilayah C");   delay(3000);
 }
```

The prototype theft system uses three networks with a nominal load of 100 W on each network. An additional load of 100W in each network simulates the theft in the network. Therefore, if the load is less than 120 W then there is no indication of theft, and if the network load is more than 120 W then there is an indication of electricity theft on the network. Figure 3.5. is a snippet of the microcontroller program script that detects the theft. Figure 3.6. is a photo of the prototype that has been made

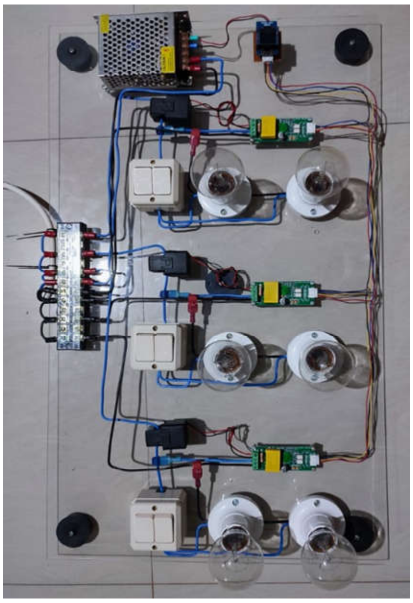


Figure 3.6. Photograph of the prototype of the electricity theft monitoring system.

3.1.3 IoT Platform Based On Blynk Application

The IoT platform in this monitoring system uses the Blynk application. Blynk is one of the Internet of Things (IoT) platforms that has provided many libraries for monitoring and controlling equipment connected to End devices. Some of the advantages of using the Blynk application include:

- Easy to develop IoT-based microcontroller applications.
- Easy to use graphical interface.
- Support for various devices and microcontrollers.
- Broad connectivity, where Blynk supports various connectivity protocols, including Wi-Fi, Ethernet, Bluetooth, and even SMS.
- Has a strong layer of security as it can set access permissions and authentication to control who can access the device.

The integration diagram between the theft monitoring system hardware as End device with mobile application as shown in Figure 3.7.

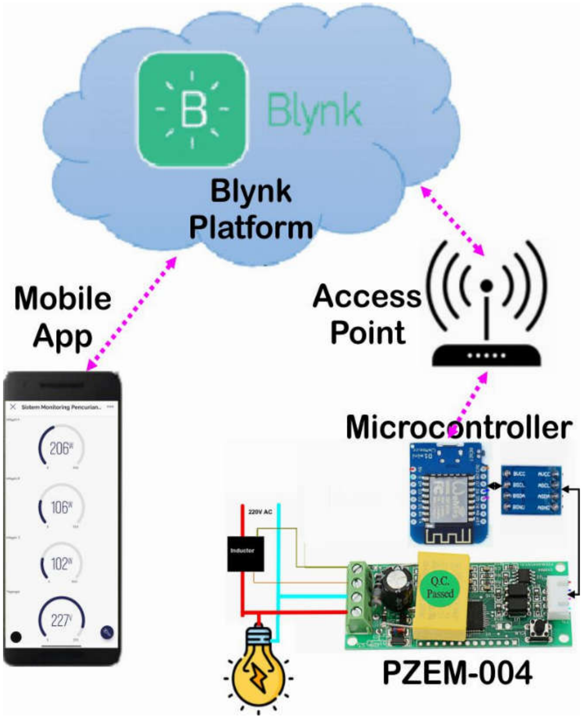
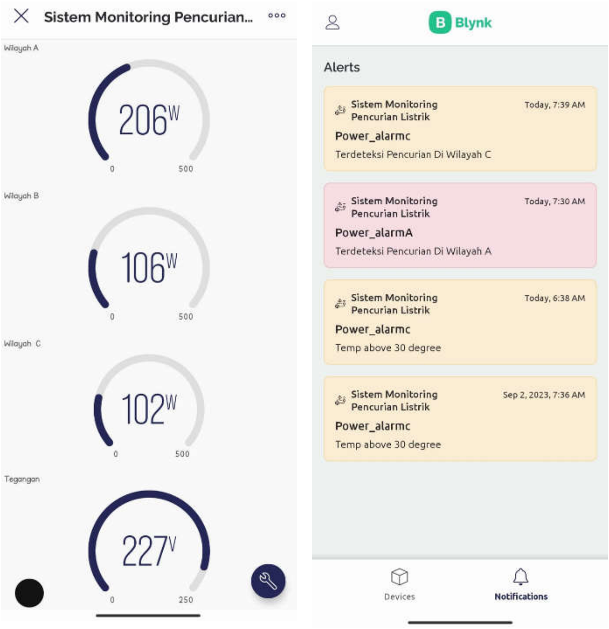


Figure 3.7. IoT network topology from end device to mobile application.

3.1.4 Mobile Application

The application on android or mobile application in this research uses the features of the Blynk platform. There are 2 mobile application displays, namely the real-time display of power measurements, and the alarm system. The real-time display of power measurement time is as shown in Figure 3.8.a, and the alarm display is as shown in Figure 3.8.b



Sistem Monitoring Pencurian Listrik — Today, 7:39 AM
Power_alarmc
Terdeteksi Pencurian Di Wilayah C

Sistem Monitoring Pencurian Listrik — Today, 7:30 AM
Power_alarmA
Terdeteksi Pencurian Di Wilayah A

Sistem Monitoring Pencurian Listrik — Today, 6:38 AM
Power_alarmc
Temp above 30 degree

Sistem Monitoring Pencurian Listrik — Sep 2, 2023, 7:36 AM
Power_alarmc
Temp above 30 degree

a) b)

Figure 3.8. Mobile application view, a) power measurement, b) alarm system.

4. TESTING AND ANALYSIS

Testing the system aims to determine the performance characteristics of the system. The types of tests carried out include power measurement characteristics, IoT-based communication, and theft detection capabilities.

4.1. Power measurement characteristics testing

Testing the electrical power measurement characteristics using the PZEM-004T sensor module aims to assess the characteristics of current and voltage sensors. The measurement results of the sensor module with a 100-watt lamp load are shown in table 4.1. The test data shows that the monitoring system is able to measure accurately where the measurement error is still below 2%. This monitoring device requires very low power of about 5 W.

4.2. IoT-based communication testing

This test aims to determine the success of sending data from the power sensor to the mobile application. The test is done by sending certain data from the microcontroller to the Blynk cloud, then the time difference between the two devices is compared. Figure 4.1a is a snippet of program script to test the transmission delay from the microcontroller to the mobile application. Figure 4.1b is a serial monitor display showing the timestamp and data in the microcontroller.

The results of the microcontroller to mobile application data transmission pause test are shown in Table 4.2. The test results show that the data transmission delay from the microcontroller to the mobile application is less than 1 second. The delivery data packet is quite small, so the pause is more influenced by the quality of the internet network in that location.

4.3. Theft detection testing

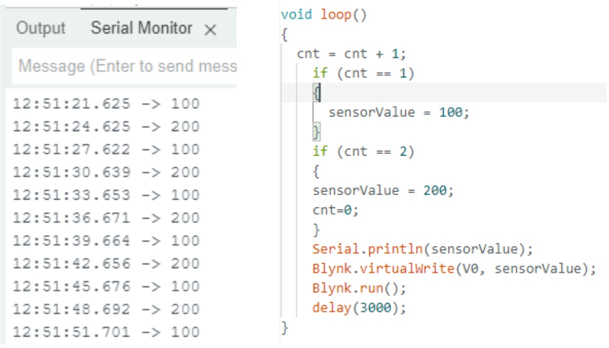
Theft detection testing is intended to determine the ability of the system to detect theft when there is an increase in load power that exceeds the threshold value. Testing is done by providing an additional load of 100 W to the electricity network. If the system detects well, it will send a warning alarm in the mobile application according to the location of the network. Figure 3.8.b is an example of theft alarm information in the mobile application. Table 4.3 shows the theft detection test results for the three networks.

Table 4.2. Test results of data transmission pause from microcontroller to mobile application

No	**Data**	**Time stamp**		**Jeda (Detik)**
		Serial Monitor	Mobile Application	
1	100	12:51:21	12:51:21	0
2	200	12:51:24	12:51:24	0
3	100	12:51:27	12:51:27	0
4	200	12:51:30	12:51:30	0
5	100	12:51:33	12:51:33	0

Table 4.1. Test results of electrical power sensor with 100 W lamp load.

Nu	Load	Voltagr (V)			Current (A)			Power (Watt)		
		Clamp meter	PZEM-004T	% Error	Clamp meter	PZEM-004T	% Error	Clamp meter	PZEM-004T	% Error
1	100 Watt Lamp	222,22	222,02	0,09	0,47	0,47	0,86	105	104	0,95
2		227,23	225,48	0,77	0,45	0,46	1,76	102	103	0,98
3		223,22	221,14	0,93	0,47	0,48	0,94	106	106	0,00
4		225,01	225,15	0,06	0,48	0,47	1,91	108	106	1,85
5		225,14	224,23	0,40	0,46	0,47	2,36	103	105	1,94
Average Error				0,45			1,57			1,15



```
12:51:21.625 -> 100
12:51:24.625 -> 200
12:51:27.622 -> 100
12:51:30.639 -> 200
12:51:33.653 -> 100
12:51:36.671 -> 200
12:51:39.664 -> 100
12:51:42.656 -> 200
12:51:45.676 -> 100
12:51:48.692 -> 200
12:51:51.701 -> 100
```

```
void loop()
{
  cnt = cnt + 1;
    if (cnt == 1)
    {
      sensorValue = 100;
    }
    if (cnt == 2)
    {
    sensorValue = 200;
    cnt=0;
    }
    Serial.println(sensorValue);
    Blynk.virtualWrite(V0, sensorValue);
    Blynk.run();
    delay(3000);
}
```

a) b)

Figure 4.1. a) Program script snippet for data transmission pause testing, b) Serial monitor.

Table 4.3. theft detection test results in all three networks

Nu	**Network**	**Power (Watt)**	**Status**	**Notifikasi**
1	1	102	Normal	Not present
2	2	103	Normal	Not prsent
3	3	100	Normal	Not resent
4	1	201	theft	present
5	2	201	theft	present
6	3	203	theft	present

5. CONCLUSION

The conclusions from the results of planning, prototype implementation to testing the electricity theft monitoring system using the IoT-based differential power method are as follows:

1. Voltage, current, and power measurements using the PZEM-004 module are quite accurate with an average error of 0.45%, 1.57%, and 1.15%, respectively.
2. The microcontroller system is capable and successful in theft detection using the differential power method.
3. The microcontroller system is able to send data to the cloud via the internet network with a delay of under 1 second.
4. Mobile applications can provide power and voltage information on each network.
5. The mobile application is able and successful in providing notification of indications of power theft along with the location of the network.

BIBLIOGRAPHY

[1] T. Gomez dan W. Wellssow, "Power Systems Computation," International Journal on Electrical Power and Energy Systems, vol. 7, pp. 145-151, Juni 2017.

[2] T. B. Smith, "Pencurian Listrik: Sebuah Analisis Komparatif," Elsevier Journal Energy Policy, vol. 32, pp. 2067-2076, Jul. 2015.

[3] R. V. Eastin dan G. L. Arbogast, Analisis Permintaan dan Penawaran: Pengantar, Amerika Serikat: CFA Institute, 2014.

[4] J. Atakari, S. Sutar, V. Birajdar, dan A. B. Kanwade, "Deteksi Pencurian Daya Listrik," Znternational Journal on Recent Innovation Trends in Computing and Communication, vol. 5, hal. 137-141, Juni 2017.

[5] S. Sardar dan S. Ahmad "Mendeteksi dan meminimalisir pencurian listrik: Sebuah tinjauan" International Journal on Electrical Innovation, vol. 4, pp. 121-131, November 2015.

[6] R. Weron, Peramalan harga listrik: Sebuah tinjauan dari state-of-the-art dengan melihat ke masa depan, Polandia: Universitas Teknologi Wroclaw, 2014

[7] E. M. Nejar, "Tinjauan Pajak Energi Terhadap Konsumsi Tenaga Listrik," N7RC Tax Research Journal, vol. 23, pp. 11-31, Oct.2014.

[8] Fiki. A, Pratiwi RN, & Wachid A. "Strategi PT Perusahaan Listrik Negara dalam Pemenuhan Tenaga Listrik dan Peningkatan Pelayanan pada Masyarakat di Pulau Giligenting Kabupaten Sumenep (Studi pada Pembangkit Listrik Tenaga Disel Subrayon Giligenting)". Jurnal Administrasi Publik (JAP) Vol. 1 (6): 1229-1238. 2013.

[9] Jokar. P, Arianpoo. N and Victor. C, “Electricity Theft In AMI Using Consumers’ Consumtion Pattern”, IEEE Transaction on Smart Grid, Vol 7 No.1, January 2016.