International Journal of Modern Developments in Engineering and Science
Volume 4, Issue 3, March 2025
https://www.ijmdes.com | ISSN (Online): 2583-3138

IoT-Based Intelligent Power Surveillance and Theft Detection Framework

Ehikhamenle Matthew[1*], R. O. Okeke[2]
[1,2]*Senior Lecturer, University of Port Harcourt, Port Harcourt, Nigeria*

***Abstract*: Electricity theft is a very common problem in country where population is very high and the use of electricity are ultimately tremendous. The aim of this paper is to design and develop an improved smart power monitoring and theft detection model by developing and designing a smart circuit that senses a higher load compared to what the meter reads and sends an alert to the authorities. This is simulated on Proteus 8 software simulator to validate that Internet of Things (IoT) can be integrated into our electricity billing system. And then we do comparative analysis on the effect of the theft load on the quality of power distributed. The improved smart power monitoring and theft detection model includes several modules such as current sensor, voltage sensor, ATmega32 microcontroller, Liquid Crystal Display (LCD) display, voltage regulator (LM7805), Light bulbs and Raspberry pi module. The ATmega32 microcontroller runs on an embedded C++ program and acts as the power monitoring model while the Raspberry Pi 3 module acts as the power theft detector that runs on Python codes. The voltage and the current sensors are tested and found to be functioning properly. Without any human interface this model provides an effective and easy way to detect electrical theft.**

***Keywords*: theft, IoT, power, electricity, microcontroller, raspberry, load, sensor.**

1. Introduction

Theft of electricity is the criminal practice of stealing electrical power. According to a study the world loses US$89.3 billion annually to electricity theft. The highest losses were in India ($16.2 billion), followed by Brazil ($10.5 billion) and Russia ($5.1 billion). It has been estimated according to the National Electricity Regulation Commission (NERC) that Nigeria loses 30-35% of energy due to electricity theft (StatiSense, 2021).

Electricity theft is a very common problem in country where population is very high and the use of electricity are ultimately tremendous. In Nigeria, every year there is very increasing number of electricity thefts across domestic electricity connection as well as industrial electricity supply, which results in loss of electricity companies energy and because of which we are facing the frequent problems of load shielding in urban as well as rural areas so as to overcome the need of electricity. Also, the ways using which theft can be done are innumerable so we can never keep track of how a theft has occurred, and this issue is needed to be solved as early as possible.

In this project, we propose a smart method electrical power monitoring and theft detection system to minimize electricity theft which is a made by the most common way of doing theft, that is bypassing the meter using a piece of wire. People simply bypass electricity meter which is counting the current unit by placing a wire before and after the meter reading unit. The proposed system will be hidden in such meter and as soon as an attempt is made for the theft, it will send alert to control unit of electricity board.

In this system current transformers are used, here one current transformer is placed in input side of the post line. Other current transformers are placed at the distribution points of the house lines. The output of current transformer values is given as input an ATMEGA32 microcontroller which converts analog inputs to digital. Then ATMEGA32 compares the input current and the same of output current. If compared result has any negative values then this particular post is detected as theft point. This compared value is transmitted to electricity board, this value display in LCD display. The information will then be quickly processed by the microcontroller which is relayed to Raspberry Pi 3 module programmed with Python 3 to send an email to the control station.

According to Thomas Smith, 2004, Electricity theft can be in the form of fraud (meter tampering), stealing (illegal connections), billing irregularities, and unpaid bills. Estimates of the extent of electricity theft in a sample of 102 countries for 1980 and 2000 are undertaken. The evidence shows that theft is increasing in most regions of the world. The financial impacts of theft are reduced income from the sale of electricity and the necessity to charge more to consumers. Electricity theft is closely related to governance indicators, with higher levels of theft in countries without effective accountability, political instability, low government effectiveness and high levels of corruption. Electricity theft can be reduced by applying technical solutions such as tamper-proof meters, managerial methods such as inspection and monitoring, and in some cases restructuring power systems ownership and regulation.

He also identified the problems as an increasing awareness and inefficiency in electric power systems.

G. Sreenivasan, 2013 states in his book titled ‘Power theft’ that power theft causes a substantial loss of revenue to power utilities. Despite their efforts to crack down on power thieves and use of improved detection technology, power utilities have not been fully able to contain the unscrupulous ways used to

*Corresponding author: matthew.ehikhamenle@uniport.edu.ng

steal power. This book, now in its Second Edition, discusses some of the startling methods used to commit power theft, and describes ways to identify, control and combat such power pilferage problems. The book provides a graphic description of the modus operandi of the power thieves and uncovers their ingenuity and imagination in pilfering electricity. To fight this menace of electricity theft, the book presents a vivid account of technical solutions that can go a long way in nipping the problem in the bud. The most striking feature of the book is that it uses suitable photographs to analyze the problems from several angles. In this edition, a new chapter containing major judgements of the Supreme Court as well as High Courts relating to power theft, and a new section on smart grid are included. The book will be of principal interest to professionals engaged in electricity boards, power utilities, power training institutes, and energy auditors and the law enforcement authorities. It will also be of practical interest to the students of Electrical Engineering to understand the metering technology, measuring principles and, above all, the methods used to analyze the causes of power theft.

Olaleye Gbolahan Olaoluwa, 2017 opines that there are two components of losses in power system (technical and non-technical). The technical losses consist of losses from the transmission line, losses from transformer, measurement systems, etc. There are other losses that are outside the control of the utility provider comprising of electricity theft, non-settlement of bills by customers, error in accounting and record keeping. Electricity theft is difficult to estimate. The regulatory instrument (Electricity Theft and Other Related Offences Regulations) was formulated by Nigeria Electricity Regulation Council in 2013 to deter electricity theft, and the destruction of electricity supply infrastructure but this has not have any effect on the rate of electricity theft and electricity vandalism in Nigeria. Electricity theft can be in the form of fraud (meter tampering), stealing (illegal connections), billing irregularities, and unpaid bills. The importance of the eradication of electricity theft cannot be over-estimated especially given our power generation and transmission deficit and the need to attract significant capital investments in order to improve availability, access and service delivery in the industry. The theft of electricity poses significant dangers to all concerned. It can damage equipment and cause power outages, and it costs everyone who is paying for the power they use. This paper discusses the effect, consequences and measures to control electricity theft to improve power quality.

2. Materials and Methods

This paper introduces a wire-based control system designed to address the issue of power theft by implementing a solution constructed using the Atmega32 microcontroller. The system incorporates Atmega32 alongside current and voltage sensors, configured into a network of Master and Slave boards. The proposed design is capable of pinpointing locations where instances of "power theft" or "excessive power usage" occur within a specific household. This capability facilitates the identification of illegal energy consumption.

The microcontroller serves as an interface between the energy meter and the wired communication network, enabling data transfer. In cases where discrepancies arise in the compared values, a signal is transmitted from the consumer's side to the substation. The paper details the methodology for transferring data from the Slave board, positioned on the consumer side, to the Master board, situated at the substation. Although a wired communication network is utilized in this system, employing a wireless communication module for data transmission is highlighted as a simpler, more efficient, and reliable alternative.

A. Hardware Design

The enhanced smart power monitoring and theft detection model comprises modules such as current and voltage sensors, an ATmega32 microcontroller, an LCD display, an LM7805 voltage regulator, light bulbs, and a Raspberry Pi module. A 235V power supply is routed through a relay to the current and voltage measurement units. The ATmega32 microcontroller receives a 5V input from a rectifier circuit and LM7805 voltage regulator. Serial communication is established between the ATmega32 and Raspberry Pi via a USB port.

The system interfaces a GSM module and a 12V relay across the load through the Raspberry Pi GPIO pins. Sensor readings are displayed on IoT platforms like Ubidots, allowing real-time monitoring of load consumption. In cases of repeated theft, the electricity board can disconnect the supply using the relay.

The model uses 100W, 200W, and 500W bulbs for testing. The current and voltage measurement units capture load data, which the ATmega32 decodes into ADC values and transmits to the Raspberry Pi. Predefined ADC thresholds in Python code, such as 400 for a 200W load, are used to detect theft. If values exceed these thresholds, a theft alert is sent via email to the electricity board. Additionally, if the meter is tampered with, the Raspberry Pi triggers an alert and emails the authorities.

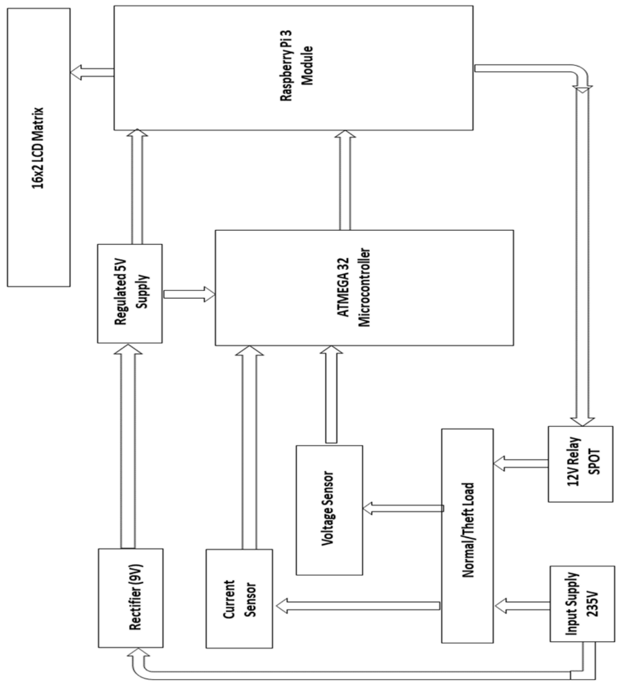


Fig. 1. Block diagram of the model

B. ATmega32 Microcontroller

Power calculation and electricity usage control process used in digital meter prepayment will be made in the form of a program that is embedded in a chip microcontroller. The microcontroller process all the modules that have been integrated. Type of microcontroller used in the design of our digital prepaid meter is ATmega32.

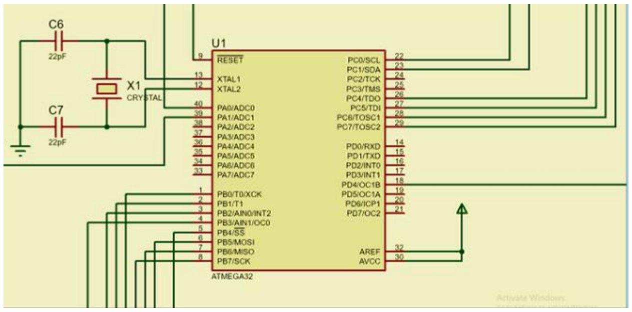


Fig. 2. Atmega32 microcontroller schematics

By executing powerful instructions in a single clock cycle, the ATmega32 achieves throughputs close to 1MIPS per MHz. This empowers system designer to optimize the device for power consumption versus processing speed.

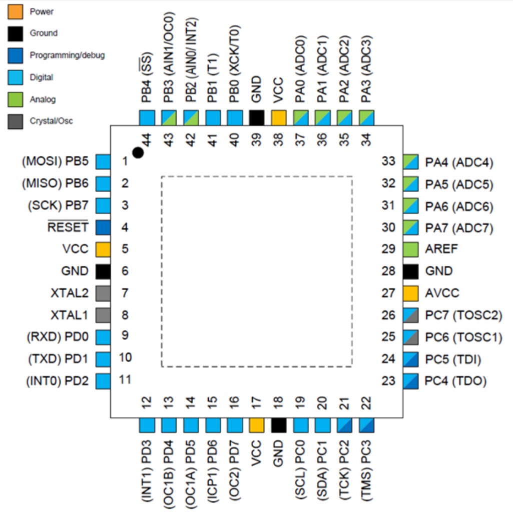


Fig. 3. Pin configuration of ATmega32 microcontroller

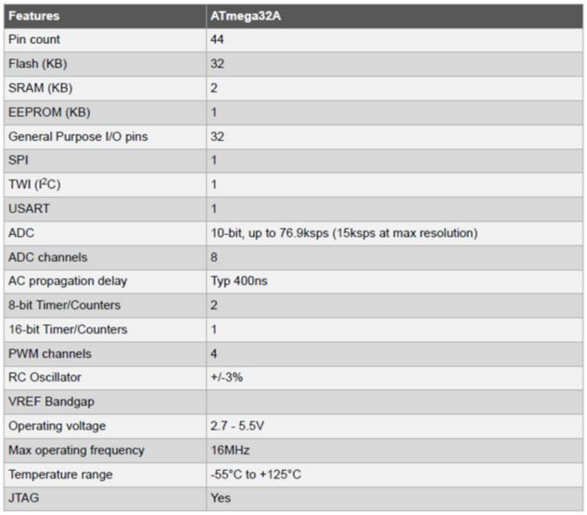
The software used for programming the Microcontroller is the Atmel studion7 (or Microchip studio). The high-level programming language in use is the C language. After the chip is programmed, the C file is debugged into a hex file and further into a source code that can be understood by the microcontroller.

3. Interfacing Raspberry Pi with Atmega32 Microcontroller

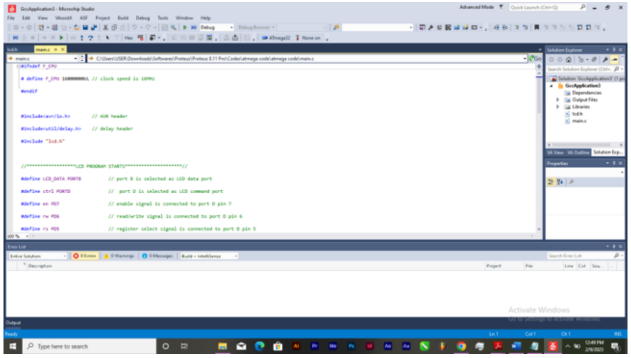
The Raspberry Pi 3 can interface with the Atmega32 microcontroller through several methods, with the most common being: Serial Communication: Utilizing the UART (Universal Asynchronous Receiver/Transmitter) for communication: Connect the TX pin of the Raspberry Pi to the RX pin of the Atmega32, and vice versa. Write Python code using the pyserial library to establish serial communication. Program the Atmega32 to transmit and receive data via UART.

SPI Communication: Using the SPI (Serial Peripheral Interface) for communication: Connect the SCLK, MOSI, MISO, and SS pins of the Raspberry Pi to the corresponding Atmega32 pins. Write Python code using the spidev library to establish SPI communication. Program the Atmega32 for SPI data transmission and reception. The Raspberry Pi 3 operates at 3.3V, while the Atmega32 operates at 5V. Use level shifters or voltage dividers to maintain correct signal voltage levels.

Table 1
Features summary of ATmega32 microcontroller



Features	ATmega32A
Pin count	44
Flash (KB)	32
SRAM (KB)	2
EEPROM (KB)	1
General Purpose I/O pins	32
SPI	1
TWI (I^{2}C)	1
USART	1
ADC	10-bit, up to 76.9ksps (15ksps at max resolution)
ADC channels	8
AC propagation delay	Typ 400ns
8-bit Timer/Counters	2
16-bit Timer/Counters	1
PWM channels	4
RC Oscillator	+/-3%
VREF Bandgap	
Operating voltage	2.7 - 5.5V
Max operating frequency	16MHz
Temperature range	-55°C to +125°C
JTAG	Yes



C:\Users\USER\Downloads\Softwares\Proteus\Proteus 8.11 Pro\Codes\atmega code\atmega code\main.c

```
#ifndef F_CPU
# define F_CPU 16000000UL // clock speed is 16MHz
#endif


#include<avr/io.h>        // AVR header
#include<util/delay.h>    // delay header
#include "lcd.h"


//*****************LCD PROGRAM STARTS*********************//
#define LCD_DATA PORTB          // port B is selected as LCD data port
#define ctrl PORTD              //  port D is selected as LCD command port
#define en PD7                  // enable signal is connected to port D pin 7
#define rw PD6                  // read/write signal is connected to port D pin 6
#define rs PD5                  // register select signal is connected to port D pin 5
```

Fig. 4. Microchip studio IDE used for programming microchips

4. Results and Discussions

Through the proper integration of hardware and software, the model detects irregularities in the current flow through the loads and outputs a theft alert. First of all, the sensitivity of the voltage and current sensors needs to be tested. Sensitivity is the ability of the sensor to detect the smallest change in voltage or current in the model.

Based on Table 2, the results obtained from the simulation, the performance of the voltage sensor is quite effective. The model produces small error of the voltage measurement. Linear presentation of the result is shown in Fig. 6. This result indicates that the model was able to calculate the energy used by customers accurately.

Table 2
Test result of voltage sensors

Data	Volt AC	Voltage Output Sensor	Data ADC	Calculated Volt	Error Voltage AC
1	224	2.55	521	224.16	0.16
2	223	2.54	519	223.30	0.30
3	222	2.52	516	222.01	0.01
4	221	2.51	514	221.15	0.15
5	220	2.50	512	220.29	0.29
6	219	2.49	509	218.99	0.01
7	218	2.47	507	218.13	0.13
8	217	2.47	505	217.27	0.27
9	216	2.45	502	215.98	0.02
10	215	2.44	500	215.12	0.12
Average		**2.49**	**510.50**	**219.64**	**0.15**

Table 3
Test result for current sensor

Data	Ampere Meter	Volt Meter	Data ADC	Voltage Out	Current Out	Error Volt	Error Current
	Ampere	Volt	Digital	Volt	Ampere		
1	0	2.5	512	2.5	0.02	0.0%	2.0%
2	1	2.6	532	2.6	1	0.0%	0.0%
3	1.51	2.65	543	2.65	1.54	0.0%	3.0%
4	2	2.7	553	2.7	2.03	0.0%	3.0%
5	2.5	2.75	563	2.75	2.52	0.0%	2.0%
6	3.03	2.8	574	2.81	3.05	1.0%	2.0%
7	3.57	2.86	585	2.86	3.59	0.0%	2.0%
8	4	2.9	591	2.9	4.03	0.0%	3.0%
9	4.55	2.95	605	2.96	4.57	1.0%	2.0%
10	5	3	614	3	5.01	0.0%	1.0%
Average Error						**0.2%**	**2.0%**

Table 4
Test result of the voltage regulator

Data	Volt AC	Rectified Volt	Data ADC	Regulated Volt	Voltage Diff. from Av. Value (Error)
1	239	17.9	556	5.06	0.02
2	236	17.8	549	5.06	0.02
3	233	17.6	542	5.05	0.01
4	230	17.4	535	5.04	0.00
5	227	16.9	528	5.04	0.00
6	224	16.8	521	5.04	0.00
7	221	16.7	514	5.03	-0.01
8	218	16.5	507	5.03	-0.01
9	215	16.2	500	5.02	-0.02
10	212	15.9	493	5.02	-0.02
Average		**16.97**	**524.50**	**5.04**	**-0.001**

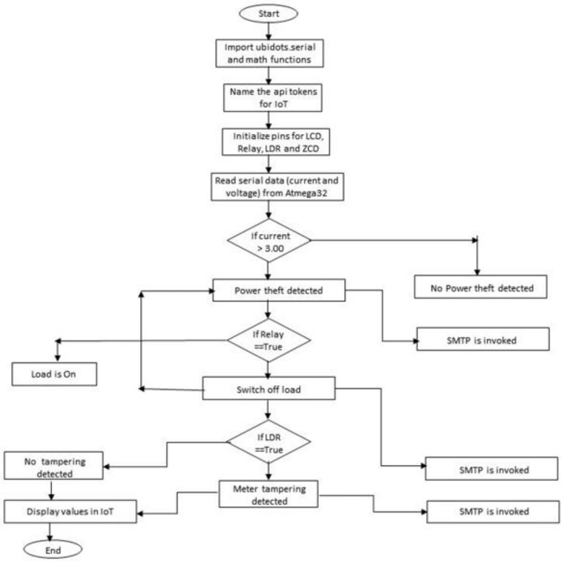


Fig. 5. Flowchart for power theft detection using Raspberry Pi

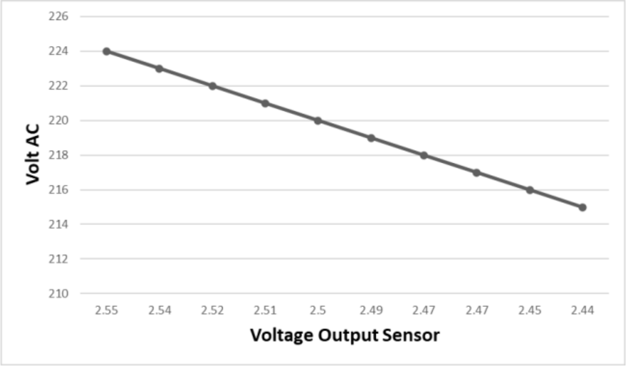


Fig. 6. Graphical representation of the voltage sensor

Table 3 shows the test result of current sensor. The simulation show that the model can work well in reading the current changes that occur from the load varied. The results of the current sensor measurement can also be seen on the Fig. 7. Our experiments show that the proposed prepaid energy meter produces small error of current and voltage sensor.

The above graph shows that the voltage regulator works very well and pins the voltage sent to the microcontroller and the $+V_{CC}$ supply at an average value of 5.04V to an accuracy of

±0.02V. This means that the error rate is minimal and that the voltage does not fluctuate beyond a value greater/less than ±0.02V. This certifies that the voltage regulator has works well.

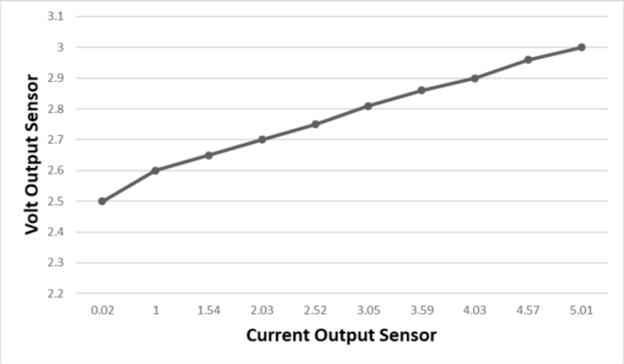


Fig. 7. Graphical representation of the current sensor

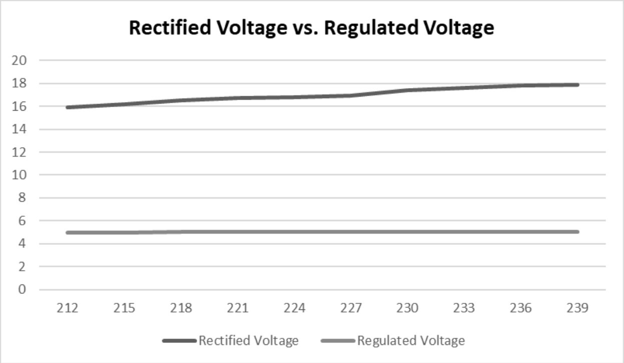


Fig. 8. Graphical representation of the rectified and regulated voltage

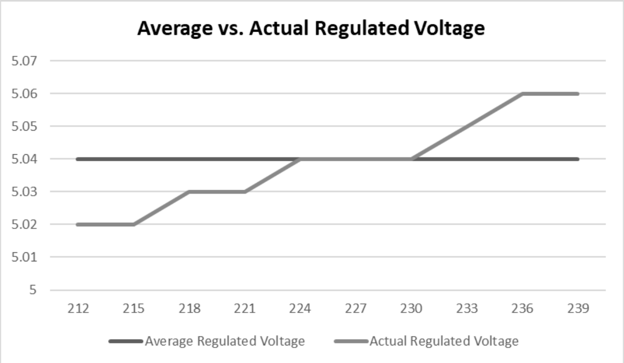


Fig. 9. Graphical representation of the rectified and regulated voltage

Figure 4 shows the working condition of the voltage regulator. The farther the deviation from the average value of the regulated voltage, the poorer the regulation. For the fact that the actual regulated voltage does not deviate much from the average value shows that there is little voltage fluctuation in the regulator and therefore it is safe for use. Microcontrollers are highly sensitive devices making it tricky to selecting the best voltage regulators. But with the right voltage regulator, they will perform well. The lack of a voltage regulator could compromise performance and reliability, potentially causing such issues as LED flicker, controller resets and even burnt electronics.

5. Conclusion

A simulated Wireless Electricity Theft Detection and Monitoring System presented in this paper demonstrates seamless integration of hardware and software components, with embedded computer codes enabling real-world functionality. Operating autonomously, this system efficiently detects power theft without human intervention, leveraging IoT technology to harness the advantages of wireless network communication. Power theft, often involving meter bypassing, is addressed in this design by detecting increased load, offering a cost-effective solution. This approach mitigates significant power and revenue losses caused by unauthorized consumption. The concealed system, embedded within electric meters, triggers automatic alerts when current deviations exceed predefined thresholds. Notifications, including messages, emails, location details, and area images, are instantly sent to relevant authorities, ensuring timely action. While IoT technology holds immense potential, its effectiveness in Nigeria depends on improved internet service reliability and network strength provided by Internet Service Providers (ISPs). This underscores the need for infrastructural enhancements to support IoT-based solutions effectively.

References

[1] T. B. Smith, “Electricity theft: A comparative analysis,” in Energy Policy**,** vol. 32, no. 18, pp. 2067-2076, December 2004.

[2] “Controlling electricity theft and improving revenue", World Bank report on reforming the power sector, 2010.

[3] G. Sreenivasan, Power Theft, Fourth Edition, 2013.

[4] J.L. Parra and E.A.S. Calderon, “Use of shunts detecting equipment for the identification of illegal power outlets,” International Journal of Innovative research in Science, Engineering and Technology, pp. 1–4, 2013.

[5] Ashna. K and Sudhish N George, GSM based automatic energy meter reading system, IEEE Wireless Communications, 2013.

[6] S.K.A. Zaidi, H. Mansoor, S.R. Ashraf, and A. Hassan, “Design and implementation of low-cost electronic prepaid energy meter,” IOSR Journal of Electronics and Communication Engineering, Vol. 2, pp. 548–552, 2014.

[7] M. Jamil, F. Munir, A. A. Khan, and A. Mirza 2014, “Telemetering & billing system for spatially distributed electrical power clients,” Electrical power system research pp. 35–40, 2014.

[8] Pradeep Mittall, “Wireless Electricity billing system,” International Research Journal of Engineering and Technology, vol. 2, pp. 21-34, 2015.

[9] Automatic Energy Meter Reading System with Instant Billing,” International Journal of Scientific Engineering and Technology Research, vol. 4, no. 51, pp. 11091-1109, December 2015.

[10] N. Donald, The Internet of Things: Do-It-Yourself at Home Projects for Arduino, Raspberry Pi and Beagle Bone Black, London: McGraw-Hill TAB Electronics, 2015.

[11] G.L. Prashanthi, K. V. Prasad, “Wireless power meter monitoring with power theft detection and intimation system using GSM,” International journal of engineering science and computing, vol. 9, pp. 330-348, 2016.

[12] Olaleye Gbolahan Olaoluwa, Electricity Theft and Power Quality in Nigeria, vol. 6, no. 6, June 2017.

[13] R. M. Mutupe, S. O. Osuri, M. J. Lencwe and S. P. Daniel Chowdhury, "Electricity theft detection system with RF communication between distribution and customer usage," *IEEE PES Power Africa*, Accra, 2017, pp. 566-572.

[14] "General Python FAQ — Python 3.9.2 documentation". *docs.python.org*. Retrieved 28 March 2021.