iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** IV **Month of publication:** April 2023

DOI: https://doi.org/10.22214/ijraset.2023.50476

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue IV Apr 2023- Available at www.ijraset.com

Implementation of a Powerline Vandalism Monitoring System via the Internet of Things

Abdulhamid Musa
Electrical and Electronic Engineering Department, Petroleum Training Institute, Nigeria

Abstract: ***This study is about implementing a power line vandalism monitoring system over the Internet of Things. The device is a tamper-resistant electronic security device for high-voltage transmission lines, specifically designed for remote monitoring and protection of the lines against vandals. This system detects when the transmission line is vandalized and when the vandals invade the environment where the transmission line tower, transformer, or any infrastructure is installed. The development involves different sections ranging from the power supply to the alarm unit. The power supply was designed by selecting the components based on the required specification for the transformer, diodes, capacitor, and voltage regulator. Based on its unique characteristics, the microcontroller unit was developed using the ATMEGA 328P IC. The communication and the sensor unit were designed considering their different specifications. An ultrasonic sensor and SIM900 for the Global System For Mobile Communications module were chosen. The study was implemented so that the motion sensor detects when vandals litter the restricted area of the power line or substation and communicates with the microcontroller, which triggers the alarm and the Global System for Mobile Communications module to send Short Message/Messaging Service.***

Keywords: Monitoring System, Internet Of Things, Global System For Mobile Communications, Short Message/Messaging Service, Microcontroller.

I. INTRODUCTION

Powerline vandalism is a serious threat to the security and reliability of power grids. Criminals often target power lines, transformers, and other components of the grid, causing power outages and significant economic losses. Traditional methods of powerline monitoring and security have proven to be inadequate, and there is a growing need for more advanced and efficient systems. In recent years, the Internet of Things (IoT) has emerged as a promising solution for powerline vandalism monitoring.

The power grid is the backbone of modern society, providing electricity to homes, businesses, hospitals, and schools. However, this critical infrastructure is vulnerable to various threats, including natural disasters, equipment failures, and cyber-attacks. One of the lesser-known threats to the power grid is vandalism, the intentional destruction, or damage of power equipment, such as transformers, switches, and power lines. Vandalism can be motivated by a variety of reasons, from theft of copper wire to acts of terrorism. Regardless of the motive, the impact of powerline vandalism can be severe, causing power outages, property damage, and even loss of life. Moreover, repairing and replacing vandalized equipment can be time-consuming and costly, disrupting the lives of thousands of people who rely on electricity. It is important for communities to take action to prevent powerline vandalism, such as increasing security measures and reporting suspicious activity. Education and awareness campaigns can also help to discourage individuals from engaging in this destructive behavior. By working together to prevent powerline vandalism, we can ensure the safety and well-being of our communities and minimize the negative impact on our daily lives.

1) *Consequences of Powerline Vandalism:* The consequences of powerline vandalism are significant, as they can cause widespread power outages that can affect entire neighborhoods, cities, or even regions. These outages can disrupt communication systems, transportation networks, and businesses, leading to economic losses and social disruption. Additionally, powerline vandalism can result in the release of hazardous materials, such as oil and chemicals, endangering both human health and the environment. Furthermore, powerline vandalism can compromise the reliability and security of the power grid, making it more vulnerable to other types of attacks, such as cyber-attacks. Therefore, it is critical to detect and prevent powerline vandalism to ensure the smooth and safe operation of the power grid.
2) *The Need for a Powerline Vandalism Monitoring System:* To mitigate the risk of powerline vandalism, it is essential to have a reliable and efficient monitoring system in place. The system should provide real-time monitoring and alerting capabilities to detect any potential threats to the electrical infrastructure. This is where the Internet of Things (IoT) comes in, providing the necessary technology to create an effective powerline vandalism monitoring system.

©IJRASET: All Rights are Reserved

For powerline vandalism prevention, IoT technology can be used to create a monitoring system that can detect and respond to any potential threats. This system can integrate sensors, and other devices to monitor the electrical infrastructure and detect any unusual activity. The IoT technology can also provide remote access to the monitoring system, allowing operators to respond quickly to any incidents.

II. LITERATURE REVIEW

Reference [1] shows Internet of Things (IoT) research is of great interest and a very active research community. IoT is the connection of machines that share data and report necessary information. Many apps, sensors, remote devices, avatars, and robots have made everyday life easier. Most things are at our fingertips, like communication and transportation. Besides, the importance of eliminating power theft cannot be overstated, especially given our power generation and transmission deficit and the need to attract significant capital investment to improve the industry's availability, access, and service delivery. Electricity theft poses significant risks for everyone involved. It can damage devices and cause power outages, costing everyone who pays for their electricity. However, the paper in [2] discusses the impact, consequences, and measures to control electricity theft to improve power quality.

According to [3], IoT-based power monitoring systems and controls involve designing wireless networks to monitor electronic device power consumption. A sensor detects current, a circuit calculates voltage, and power is calculated using both. Control qualities are stored in a cloud database, and commands can be received through an Android app. The Raspberry Pi board transmits commands to change the device status. This system allows energy readings and gadget control from anywhere in the world.

The electrical power system is becoming more complex, with systems like generation, transmission, distribution, and load becoming more intricate. To maintain and protect this system, faults on power lines must be located and repaired. Sensors can continuously measure voltage and amperage on transmission lines, detecting brownouts or overloads and tripping the wire if necessary. The Internet of Things can also identify thefts and report their location automatically. Programming Arduino UNO and Arduino MEGA can detect transmission line faults by detecting changes in current and voltage and sending information to the LCD. The system can be protected through quick monitoring using the impedance technique defect detection system [4]. The paper in [5] discusses a new monitoring system for high-voltage power lines that aims to monitor atmospheric conditions and sag status continuously. It uses sensors to collect data and transmit it to a central controller, which then sends it to a control for display. The system uses the Internet of Things (IoT) and Global Positioning System (GPS) technologies to provide locations and improve the quality of service. The experiment results were reliable and correct, showing that using an IoT monitoring system for transmission lines improves maintenance planning and saves lives. This paper aims to develop a power line vandalism monitoring system that utilizes an electronic system to detect and report any vandalism on the power line. The primary goal is ensuring the safety and security of power system equipment, enabling the distribution company to transmit high-quality and reliable mass flow practically and efficiently.

III. DEVELOPMENT OF THE MONITORING SYSTEM USING IoT.

The development of a powerline vandalism monitoring system via the Internet of Things (IoT) relies on several factors. The first step is to identify the specific requirements of the monitoring system, such as the range, accuracy, and frequency of data collection. Next, the hardware and software components of the system need to be selected and configured.

Thus, this study aims to evaluate the effectiveness and feasibility of this system in real-world scenarios, with the ultimate goal of improving the reliability and resilience of the power grid. Figure 1 depicts a block diagram of an IoT-based power line vandalism monitoring system, which is the focus of this research.

1) *Power Supply Unit* - This unit provides the internal electronic circuitry with the necessary DC power. The power supply from the energy supplier is converted to direct current; This DC voltage is used to power the circuit. The conversion of the AC voltage from the AC voltage network into DC voltage is the task of the DC voltage supply circuit stage. A regulated voltage is important for the smooth functioning of many electronic devices. In addition, microcontrollers must be supplied with a uniformly regulated input voltage to function effectively.
2) *Global System For Mobile Communication (GSM) Module* - The proposed system enables the microcontroller board to utilize a mobile GSM for sending and receiving messages and connecting to the internet through the GPRS network. This configuration makes it easier to send warnings to the control room in the event of any unauthorized activity close to the transformer surface. The GSM Shield transmits data from the serial port to the GSM network via a modem, which operates through a series of AT commands. With this system in place, the microcontroller board can seamlessly communicate with the control room, ensuring prompt action in case of potential threats. The GPRS network guarantees reliable and secure internet connectivity, enabling the system to operate efficiently. The GSM Shield's ability to transmit data via a modem ensures the system can function optimally, even in poor network coverage.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

3) *Motion Sensor Unit* - The motion sensor is a device that can detect human presence with a maximum length of about 10 m. The ultrasonic sensor is available in many configurations for a variety of applications. Motion detection primarily identifies intruders, warns your control panel, and then alerts the security center. When there is movement, the sensors can be set to act as security systems, recording events via a surveillance camera.
4) *Ultrasonic Sensor* - This electronic device can measure infrared (IR) light-emitting objects in its view range. Ultrasonic motion detectors are frequently made using ultrasonic sensors. As a result, this sensor is placed near the transformer to keep an eye on any apparent movement there. When an infrared source, such as the temperature of a human body, passes in front of the transformer, the sensor can detect superfluous movement around it
5) *Alarm Unit* - The buzzer part tells the operator that the microcontroller has received the data sent to it. However, when the sensor detects it, it makes an audible noise.

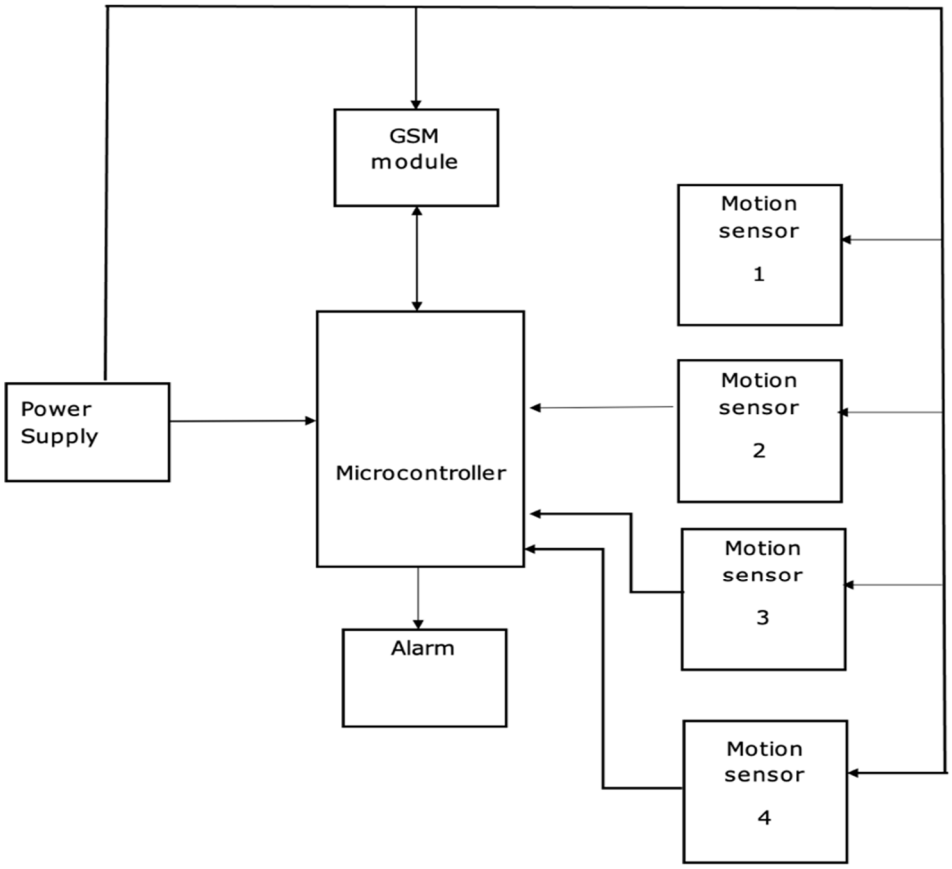


Figure 1: Block diagram of power line vandalism monitoring system using IoT

6) *Microcontroller Unit* - The microcontroller unit is the heart of the design for this study. It is the control unit where all activities of the system are coordinated. It interacts with both the exit and the entrance. The input comes from the user in the form of a command sent through the passive infrared motion sensor to the microcontroller for processing; The output signal comes from the microcontroller to the alarm unit (buzzer), which can attract the attention of people around. A coded message from the GSM phone unit is sent to the microcontroller, where the message is decoded. The performance and overall behavior of the system depend on the program stored in the program memory.

The ATMEGA328p microcontroller serves as the control component in the block diagram. Microchip Technology manufactures the ATMEGA328p, a microcontroller in the ATMEGA series. It is a nano-watt technology 8-bit CMOS microcontroller. The controller features 16 kB of flash memory, which is enough for most applications. The system can connect multiple peripherals thanks to 24 programmable input and output pins rated for 20mA of current (direct LED drive capabilities). The controller, which has an automated watchdog timer reset on failure, can be utilized to design applications for permanent installation.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue IV Apr 2023- Available at www.ijraset.com

IV. METHODOLOGY

This section covers the design and the selection of components used for this study. Thus, designing and developing a power line monitoring system to combat vandalism is a cutting-edge technology that can significantly reduce the financial losses incurred by this illegal activity. Power line vandalism costs millions of dollars annually, making this design a cost-effective solution that provides round-the-clock security. The system is affordable to design, install, and maintain and can be easily installed on transformers, transmission lines or any infrastructures, where it remains undetectable to vandals. In the future, suppliers should consider designing transformers to accommodate this monitoring system. By implementing this innovative technology, we can protect our power lines and save valuable resources.

1) *Design Specification* - The power line vandalism monitoring system has an input voltage of 220-240 V, an operating voltage of 12 V, an operating current of 1.0 A, and a frequency of 50 Hz.
2) *Transformer Design And Windage Calculation* - The choice of the transformer was based on the following, input voltage 220 – 240 V, output voltage 12V, and the power rating for the transformer 0.3 kVA. This is a small transformer with a small power rating. The core and copper losses are neglected.
3) *Core Calculation* - The core area (A-core) can be determined using the following

A-core = length (l) × breadth (b)
A-core = 0.025 × 0.015
= $3.75 \times 10^{-4}\ m^2$

4) *Calculation Of Turns Per Volt* - The number of turns (NT) equation = $1/(4.4 \times f \times B_{MX} \times A\text{-core})$.
B_{max} = magnetic flux density between 1.0 T to 1.2 T since the transformer is small. So we take B_{max} =1.2 Wb/m^2

NT = $1/(4.44 \text{ x}1.2 \text{ x } 50 \text{ x } 3.75 \times 10^{-4})$
= 10.01 turns
Total Number of Turns (TNT) = turns per Volt × Vp
NP = 10 × 220
NP = 2200 turns

Primary current (PC) = Transformer Power Rating (TPR)/Primary Voltage
= 12/220 = 55 mA
Secondary winding calculation
N_s = NT × VP
N_s = 10 × 12
N_s = 120 turns
Secondary Current (SC) = TPR/Secondary Voltage
=12/12 = 1.0 A

5) *Selection Of Bridge Rectifier* - The rectification circuit used in the design is a full wave bridge rectifier that comprises four diodes. The four-diode full wave bridge rectification is used for its added advantage over a two-diode center-tapped full wave rectifier and diode half wave rectification.

The choice of diode used was based on the following.

a) Forward Current: The diode forward current is the maximum current it can conduct before it fails. The diode is chosen so that the current flowing through it is less than the forward current.
b) Sufficient Peak Inverse Voltage: The greatest reverse voltage that a diode can endure without damaging the junction is known as the peak reverse voltage (PIV). When employing the diode as a rectifier, PIV is crucial because when the reverse voltage across the diode is more than this amount, the reverse current spikes rapidly and fractures the junction owing to excessive heat. While using rectifiers, ensuring that the reverse voltage across the diode does not go above its PIV during the AC voltage's negative half cycle is essential.

$V_{peak} = \sqrt{2} \times V_{rms}$
Where V_{rms} is the transformer output voltage using the maximum output voltage.
$V_{peak} = \sqrt{2} \times V_{rms}$ = 16.97 V

©IJRASET: All Rights are Reserved

For a bridge rectifier, the peak voltage equals the PIV. Thus, the 1N4007 diode was chosen for the rectifier since it satisfies the above-stated requirements considering the component's datasheet.
The voltage drop across the diode is given by $2 \times 0.7 = 1.4$ V, Where 0.7 is the forward conducting voltage of a silicon diode.
Voltage drop = 16.97 - 1.4 = 15.57 V
$I_{dc} = (2\times16.97)/(3.142\times1000) = 0.01080 = 10.80$ mA

6) *Selection Of Capacitor And Its Ratings* - This filter capacitor removes AC ripples in the rectified DC output. Electrolytic capacitors come with a capacitance and a voltage rating. However, the choice of the filter capacitor depends on voltage, the ripple factors, and the capacitor breakdown voltage. As such, the capacitor's voltage must withstand twice the output voltage from the diode.

Applying Kirchhoff voltage law at the output of the rectifier to the terminal of the filter capacitor
V_{peak} = bridge rectifier output
V_d = drop across bridge rectifier diode
Capacitor terminal voltage (V_c) = $V_{peak} - V_d$
For full-wave rectification on each half section, 0.7 V is dropped across each of the two-conducting diodes, which gives 1.4 V (= 2 × 0.7)
Therefore, the capacitor voltage is given as follows:
$V_c = 16.97 - 1.4$
$V_c = 15.57$ Volts
In practice, the rule is to use a capacitor with a breakdown voltage (BV_c) double the terminal voltage. Therefore,
BVc = $2\times V_c = 31.14$ V

Thus, a standard value of 35 V was used.
The capacitor smoothens the DC voltage from the bridge rectifier. Its choice depends on the capacitor breakdown voltage and the ripple percentage required, whence a 10% ripple standard for the capacitor selection was used.
$C = I_{tr}/2f\Delta V$ (for full wave)
ΔV is the difference between the maximum and minimum peak voltages, f is the input frequency = 50 Hz, I_{tr} is the transformer current = 0.3 A.

Maximum peak voltage = $\sqrt{2} \times 12 = 16.97$ V
Minimum peak voltage =maximum peak voltage - 10% of maximum peak voltage
$= 0.1\times 16.97 = 1.697$ V
C = $IL/2f\Delta V$ (for full wave)
C = $0.3/(2\times50\times1.697)$
= 0.00177F
Hence, 2500 uF is chosen as a standard capacitor value.

7) *Selection Of Voltage Regulator* - The regulator used is the IC voltage regulator LM7812. A positive fixed 12 Volts regulator gave the circuit the requisite positive voltage level. The rating of the LM7812 voltage regulator from the data sheet is as follows. The input voltage range is between 12 and 35 Volts, a maximum current rating of 1 Ampere, an output voltage range of 12 Volts, and an operating temperature between - 40 to 125 degrees centigrade. The current consumptions in milliamperes by the microcontroller (Imic), GSM module (Igsm), motion sensor (Ims), and Buzzer (Ibz) were given as 200, 500, 150, and 63, respectively.
8) *Selection of a Microcontroller* - The requirements for selecting the microcontroller include the following.
a) The microcontroller must have enough general-purpose input and output to interface all the system units.
b) A Universal Asynchronous Receiver-Transmitter(UART) module to interface the Universal Serial Bus (USB) to the Transistor-Transistor Logic (TLL) module.
c) Analog To Digital Converter (ADC) module to interface the voltage monitor module.
d) The microcontroller should be easy to use in terms of hardware interface and software (programming).

However, the ATMEGA328p is an 8-Bit CMOS microcontroller with nano-watt Technology, and it was selected due to the following.

- It has 28 pins, which is enough for general-purpose input and output
- It has a high flash memory rewrite cycle
- The microcontroller has 16 kilobytes of flash memory which is enough for many applications.
- The microcontroller is available and cost-effective
- The microcontroller has an ADC module required to interface the voltage monitor unit

9) *Flow Chart:* The software components of the monitoring system consist of data analysis algorithms, machine learning models, and a user interface. The data analysis algorithms analyze the data collected from the devices, while machine learning models help identify any potential threats. The user interface provides operators with easy-to-use tools to monitor the electrical infrastructure and respond to incidents. Figure 2 illustrates a flow chart of a cutting-edge Internet of Things (IoT) powered system designed to monitor power line vandalism. This innovative technology utilizes advanced sensors and data analytics to detect and prevent malicious activity on power lines. With this system, power companies can ensure their infrastructure's safety and reliability while minimizing downtime and repair costs. This cutting-edge solution is a testament to the power of IoT and its ability to revolutionize how we monitor and manage critical infrastructure.

10) *Detection Unit*: This unit access information without specific synchronization with the sender. The purpose of this detection unit is to check the presence of an intruder within the map-out range; the ultrasonic sensor is used. Hence, the unit's operating Voltage is between 5 to 12 Volts, the current consumption of 65 milliamperes, and the output Voltage ranges between 0 and 3.3 Volts.

11) *Buzzer Selection:* This help to inform the nearby people and workers when there is an intruder within the map-out range. An electromagnetic buzzer is used for the following reasons. The electromagnetic buzzer is simple, compatible, and small; sound pressure is high and less expensive. The buzzer selected for the implementation of this study has a frequency range is 3300 Hz, an operating voltage of 3 to 24 Volts, and a sound pressure level of 10 cm with 65 milliampere supply current.

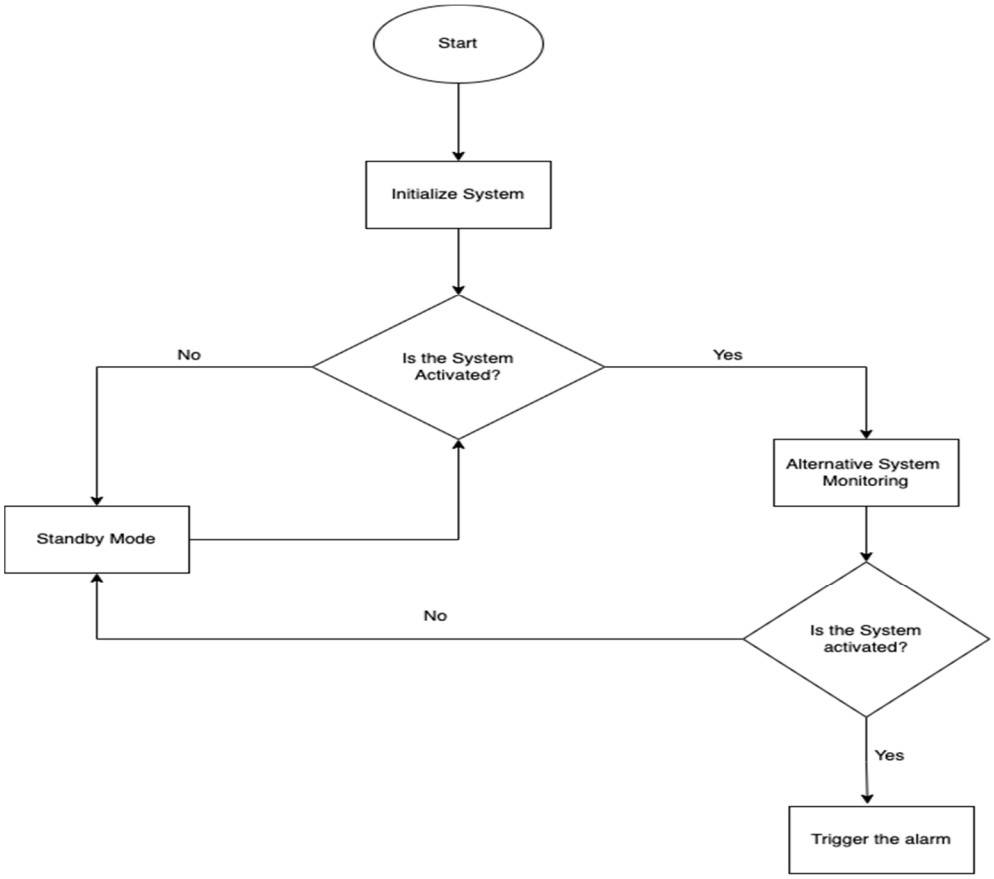


Figure 2: Flow Chart of A Cutting-Edge Internet Of Things (IoT)

12) *Communication Interface Unit:* This unit enables the controller to transmit signals via Short Message Service (SMS) to the operators. The requirements of a communication interface unit include the following. It should be able to transmit data within a reasonable range, and easy operation, and SIM900 GSM and GPRS shield MOD900 is a wireless modem because its application supports writing and sends messages to all phone numbers depending on the number keyed-in in the program.

Thus, the communication interface unit specification is given as follows.

a) Quad-Band of 850/900/1800/1900 Mega Hertz.
b) GPRS multi-slot class 10/8.
c) Class-4 (2 W 850/ 900 MHz).
d) Single Antenna Interference Cancellation (SAIC) support.
e) Dimensions: 24 by 24 by 3 mm^3.
f) Control via AT commands for Global System for Mobile Communications.

V. IMPLEMENTATION OF THE STUDY

In this study, a system that is used for implementing a powerline vandalism monitoring system via the Internet of Things is implemented. When the circuit is activated, the power supply unit provides the power requirement for the entire system.

An AC source powers the circuit, but the electronic components require DC power. Therefore, the AC power is rectified and filtered to provide a 12 V and 5 V DC supply to the electronic components and microcontroller.

It takes roughly 70 milliseconds for the ultrasonic sensor to go from zero to one when motion is sensed within its hardware and software setups to zero instantly. The transmitted signal changes state to one, and the system starts loading setup files as the microcontroller receives a signal state.

When no motion is detected, the ultrasonic sensor is inactive, and its output pin has no output. Only the microcontroller receives a signal that drops from one to zero, indicating that the microcontroller has been powered on. The microcontroller continuously checks the state of the ultrasonic sensor. If it senses a high, it immediately sends messages to the SIM900 after completing the setup files' loading from its memory, which takes about 70 milliseconds. If it senses a low, the loop continues. However, if it senses a high, the device repeats sending a message.

When the ultrasonic sensor outputs a high signal, the microcontroller commences software serial communication with the SIM900 module through "AT commands." Depending on the sensor, these commands are transferred from the microcontroller's Tx pin to the Rx pin of the SIM900 module, which transmits a pre-written text message to pre-assigned phone numbers with the words "Vandal Alert" on line one.

This study is developed on hardware and software configurations. To achieve the desired result, various parts of the hardware are connected, such as the power section, the alarm section, and the detection section, and then connected with the software section, which includes the software program that runs the whole process.

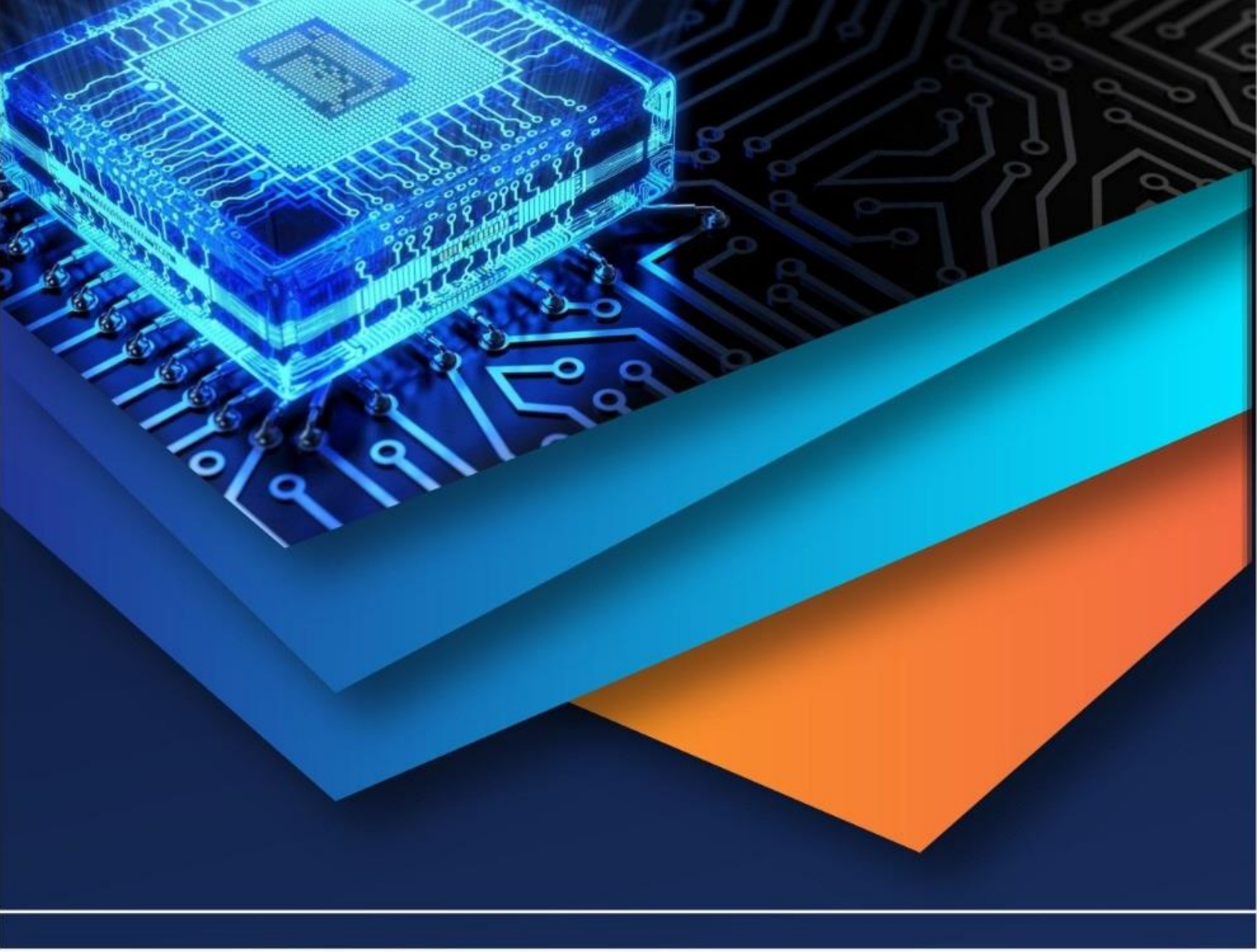
VI. CONCLUSION AND RECOMMENDATIONS

As IoT technologies continue to advance, the future of power grid security looks promising. It is crucial to continue research and development in this area to ensure the safety and reliability of power grids. In conclusion, implementing an IoT-based powerline vandalism monitoring system significantly advances the security and resilience of power grids. By leveraging the power of sensors, data analytics, and real-time alert systems, we can detect and prevent powerline vandalism more effectively than ever before. With the continuing advancements in IoT technologies, we can expect to see even more innovative solutions for power grid security in the future.

REFERENCES

[1] Parashar, A.K. and R.R. Parashar, IOT in Education. JETIR (ISSN - 2349-5162), December 2018. 5(12).
[2] Olaoluwa, O.G., Electricity Theft and Power Quality in Nigeria. International Journal of Engineering Research & Technology (IJERT), June 2017. 6(6).
[3] Raju, D.P.V.R., et al., IOT Based Power Monitoring System and Control. JETIR (ISSN-2349-5162), November 2017. 4(11).
[4] Powalkar, S., et al., Transmission Line Monitoring System Using IoT. International Research Journal of Modernization in Engineering Technology and Science, June 2022. 04(06).
[5] Suliman, A.S., et al., Monitoring System for Overhead Power Transmission Lines in Smart Grid System Using Internet of Things. UofKEJ, February 2022. 12(1): p. 1 - 5.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)