IJAREEIE

e-ISSN: 2278-8875
p-ISSN: 2320-3765

# International Journal of Advanced Research

## in Electrical, Electronics and Instrumentation Engineering

Volume 13, Issue 12, December 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.514

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering (IJAREEIE)

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 8.514 | A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 12, December 2024 ||

| DOI:10.15662/IJAREEIE.2024.1312006 |

# 3Phase Energy Theft Detection by SMS Alert

**Syed Huzaifa, Mohd Imad, Syed Taleeb, Prof. J.R.Rana**

Assistant Professor, Department of ECE, JNEC Engineering College, Aurangabad, Maharashtra, India

UG Student, Department of ECE, JNEC Engineering College, Aurangabad, Maharashtra, India

**ABSTRACT**: This paper presents the design and implementation of a Three-Phase Energy Theft Detection System integrated with SMS alert functionality. Energy theft poses a significant challenge to utilities, leading to revenue losses and compromised system integrity. Existing methods for detection often lack real-time monitoring and notification capabilities, hindering timely intervention. The proposed Three- Phase Energy Theft Detection System addresses these limitations by leveraging advanced metering infrastructure (AMI) and machine learning algorithms for accurate detection of abnormal energy consumption patterns indicative of theft. Furthermore, the Three-Phase Energy Theft Detection System incorporates a SMS alert mechanism to promptly notify utility operators or authorities when suspicious activity is detected. Upon detection of anomalous consumption patterns, an automated alert is generated and sent to predefined recipients, enabling rapid response and intervention. This feature enhances the effectiveness of energy theft prevention efforts by facilitating timely action. The implementation of the Three-Phase Energy Theft Detection System demonstrates promising results in terms of detection accuracy and real-time responsiveness. Experimental evaluation using simulated and real-world datasets validates the efficacy of the proposed approach in identifying instances of energy theft while minimizing false alarms. The integration of SMS alerts ensures that relevant stakeholders are promptly informed, enabling them to take appropriate measures to mitigate losses and maintain system integrity. In conclusion, the Three- Phase Energy Theft Detection System with SMS Alert represents a significant advancement in combating energy theft through proactive monitoring and notification. By combining sophisticated analytics with real-time communication capabilities, the system offers a robust solution for utilities to detect and address instances of theft efficiently, thereby safeguarding their revenue streams and ensuring equitable distribution of energy resources.

## I. INTRODUCTION

Power theft is the practice of stealing electrical power. Electricity utilities in India loss in cores of rupees every year to power theft. According to Section 135 of the Electricity Act 2003, electricity theft occurs when a person taps electricity lines, tampers with electricity meters or transformers or uses a device that interferes with reading or damages equipment such as electric meters or uses electricity for purposes other than authorized. Electricity has become one of the most necessary elements of our daily life. Nowadays, it is something that people cannot live without. It has become a necessary element for the survival of maximum human beings. But with the increasing need of the electricity, the electricity theft is also increasing and it will keep on continuing until some measures are not taken to detect and control it. With the advancement of technology particularly in the field of microcontrollers, all the activities in our day-to- day living have become a part of information and we find microcontrollers at each and every application. Nowadays, energy distribution/consumption has become a big subject for discussion because of huge energy theft. Theft in this case refers to a deliberate attempt to steal considerable amount of energy by ensuring no/low energy recording in the metering device. Hence, there is a need to think in this line and prefer a solution to this ugly trend. Thus, this paper focuses on electrical energy monitoring so that energy theft can easily be detected and huge penalties be imposed on these thieves. By detecting energy theft cases, the economy of a nation can grows rapidly. This report is aimed at developing a system which monitors and detects incidences of power theft, whether in the form of connecting load directly to the power line or bypassing the energy meter thereby paying less than what is consumed or by changing connection of lines. Higher energy prices reject consumers from buying electricity. Illustrates energy prices in different countries. Which shows that how to increases tariff due to power theft. In light of this, rich and highly educated communities also steal electricity to escape from huge utility bills.

- Prompt Detection and Response: Such systems can detect faults and unauthorized energy usage quickly. This allows for immediate action, reducing the duration and impact of the theft.
- Automated Monitoring: Automated systems monitor electrical parameters continuously, ensuring that any anomalies are detected without the need for constant human supervision.
- Location Specific Alerts: By integrating with GSM technology, these systems can send precise location details of the fault or theft, enabling a faster response from the technical crew.

- Prevention of Losses: Energy theft leads to significant financial losses for utility companies. Early detection helps in preventing these losses.
- System Health: It helps in maintaining the health of the power system by identifying and rectifying faults that could lead to larger system failures if left unchecked. Consumer Protection: It ensures that consumers are billed fairly and not overcharged due to energy theft elsewhere in the system.
- Safety: By detecting faults early, the system can prevent potential safety hazards associated with electrical faults, such as fires or equipment damage.
- Operational Efficiency: Reducing the time and resources spent on locating and addressing energy theft improves the overall efficiency of the power distribution system.

## II. SYSTEM MODEL AND ASSUMPTIONS

The 3-phase theft detection system can be divided into the following components:

**a. Power Metering:**

- **Voltage and Current Sensors**: Each of the three phases (R, Y, B) has a current sensor to monitor the flow of electricity, and a voltage sensor to measure the supply voltage in each phase.
- **Power Calculation**: The system calculates real-time power consumption by monitoring voltage (V) and current

(I) in each phase. The power (P) for each phase can be determined using: P=V×I×Power Factor (PF)P = V \times I \times {Power Factor (PF)}P=V×I×Power Factor (PF) where the Power Factor is typically assumed to be near 1 for most loads. If the load is inductive, this factor might be less than 1 and must be included.

**b. Normal Consumption Profile:**

- **Baseline Consumption**: The system compares the real-time consumption with the baseline or average consumption for each phase. This baseline is expected to vary slightly but should remain within a certain tolerance range during normal conditions.
- **Deviation Threshold**: The system must define an acceptable deviation threshold based on historical usage patterns or expected consumption for each customer. A sudden drop or increase in power consumption, especially when it is below or above this threshold, could indicate theft.

**c. Theft Detection Algorithm:**

- **Anomaly Detection**: An algorithm detects significant discrepancies in power consumption (e.g., unusually low consumption despite high demand or irregularities in phase balance). It can use methods like:
  - **Comparison with Historical Consumption**: Significant differences in power usage over time or during similar conditions.
  - **Phase Imbalance**: Significant unbalance in the current or power across the three phases could indicate illegal usage or tampering.
  - **Current vs. Voltage Profiling**: Any sudden deviation from expected voltage or current levels on a phase could indicate bypassing of the meter or incorrect connections.

**d. Alert Generation:**

- **SMS Alert System**: If a theft is detected, the system generates an SMS message to the pre-configured number(s) (e.g., utility operator, authorities, or customer). The message contains details about the anomaly, such as:
  - Time of the incident
  - Type of anomaly (phase imbalance, high consumption, or meter tampering)
  - Specific phase affected
  - Address or identification of the meter

**e. Communication Infrastructure:**

- **Microcontroller/PLC**: A microcontroller or Programmable Logic Controller (PLC) processes the data from the sensors and runs the theft detection algorithm.
- **GSM/Internet Module**: A GSM module (or an IoT-based communication method) is used to send the SMS alert to the concerned parties.

**2. Key Assumptions:**

**a. Accurate Measurement of Parameters:**

- Voltage and current sensors should have sufficient accuracy to detect small fluctuations in power usage. Typically, sensors should have an accuracy of at least ±1%.
- The system assumes that the sensors are installed correctly and calibrated to detect normal usage patterns.

**b. Stable Load Profile:**

- The system assumes that the user's load profile is relatively stable over time, with only minor fluctuations in consumption. Significant changes in the load profile should be manually verified or reflected in a new baseline

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 8.514 | A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 12, December 2024 ||

| DOI:10.15662/IJAREEIE.2024.1312006 |

profile.

- Normal consumption should not vary drastically unless the user changes their equipment or electrical usage patterns.

**c. Threshold for Theft Detection:**

- A threshold for abnormal power consumption or phase imbalance must be predefined. This threshold could be based on empirical data, average consumption, or historical analysis. The threshold could also be dynamic, adjusting based on time of day or season.

**d. Phase Imbalance Detection:**

- The system assumes that any significant imbalance in the power consumption across the three phases is suspicious. If the current on one phase is substantially lower than the others without a valid reason, the system will flag this as an anomaly.

**e. Meter Tampering Detection:**

- If the system detects a voltage or current reading that seems inconsistent with the expected value based on the load and connected appliances, it will trigger a possible tampering event.
- The system assumes that tampering (e.g., bypassing or disabling the meter) results in measurable changes in either the current, voltage, or overall power consumption patterns.

**f. SMS Alerting:**

- The system assumes that the GSM or IoT module has a stable network connection to send SMS alerts. If there is no network coverage, the system may store the event and send the alert once the connection is restored.
- The system also assumes that the user has provided a correct contact number for receiving the alert.

**g. Environmental Factors:**

- External factors like weather, temperature, or voltage fluctuations in the supply line are not considered as tampering or theft in this model, unless they cause a noticeable and consistent change in consumption that falls outside the normal operational range.

**h. Power Factor Assumption:**

- The system assumes that the power factor for most connected loads is near unity (1). If the load is highly inductive (e.g., motors, transformers), the system should account for the actual power factor when detecting theft.

**i. Privacy and Security:**

- The system ensures that all sensitive data, such as customer identity or power consumption details, is transmitted securely and complies with privacy regulations.

**j. Response Time:**

- The system assumes real-time or near real-time processing for anomaly detection. This is critical to ensure that the response time between detection and alert is minimal.

## III. EXPERIMENTATION / IMPLEMENTATION

Electricity theft is a persistent issue that leads to financial losses for utility companies and increases the risk of safety hazards. This experimentation focuses on developing a 3-phase electricity theft detection system that not only monitors power consumption but also sends SMS alerts when unauthorized usage is detected. By leveraging microcontroller technology, current transformers, and GSM communication, the project aims to create an efficient and responsive system. Experimentation Procedure

1. Circuit Design and Assembly:

- Connect the current transformers to the microcontroller's analog inputs to measure current. - Attach voltage sensors similarly to monitor the voltage levels across the phases.
- Interface the GSM module with the microcontroller through serial communication.

2. Programming the Microcontroller:

- Develop a code that reads current and voltage data from the sensors. - Set thresholds for expected current and voltage levels based on historical data. If real-time measurements deviate significantly, trigger an alert.

3. Testing and Calibration:

- Conduct initial tests to ensure accurate current readings from the CTs and reliable SMS functionality from the GSM module.
- Calibrate the sensors as needed, adjusting the code for any discrepancies observed during testing.

4. Deployment:

- Install the system in a controlled environment where it can monitor three-phase power consumption.
- Ensure secure placement of CTs around the conductors and connect the microcontroller to a stable power supply.

5. Monitoring and Data Collection:

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 8.514 | A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 12, December 2024 ||

| DOI:10.15662/IJAREEIE.2024.1312006 |

- Allow the system to run for an extended period, collecting data on normal usage patterns.
- Monitor for any instances of theft, noting when SMS alerts are triggered.

After deploying the system, data collected showed accurate readings of current and voltage under normal conditions. During testing, when the system was subjected to simulated theft (by manipulating current flow), the GSM module successfully sent alerts to the predefined numbers, confirming the effectiveness of the detection mechanism. Implementing a three-phase energy theft detection system with SMS alert functionality involves several steps, including setting up smart meters, designing algorithms for anomaly detection, integrating SMS alert mechanisms, and deploying the system in utility networks.

Below is a simplified outline of the implementation process:
Smart Meter Deployment:
• Install smart meters capable of three-phase energy monitoring at consumer premises.
• Ensure the meters are equipped with communication modules (e.g., cellular, Wi-Fi) for data transmission to a central server.
Threshold Determination:
• Set threshold values for abnormal consumption patterns based on historical data analysis and statistical methods.
• Define criteria for triggering alerts when deviations from normal consumption exceed predefined thresholds. SMS Alert Integration:
• Integrate SMS alert mechanisms into the system for real-time notification of detected anomalies.
• Utilize SMS gateway services or APIs to send alerts to utility operators or designated authorities.
• Include relevant information in SMS alerts, such as the location of the suspected theft, time of detection, and magnitude of deviation.
Alert Escalation and Response:
• Implement escalation procedures to ensure timely response to alerts, including notification hierarchies and contact lists.
• Define protocols for investigating suspected theft incidents, such as on-site inspections or follow- up inquiries with consumers.

## IV. SECURITY

A **3-phase theft detection system with SMS alerts** requires comprehensive security measures to ensure the integrity of the system and prevent unauthorized access or manipulation. First and foremost, the system should employ **data encryption** to protect the transmission of power consumption data and SMS alerts, ensuring that sensitive information cannot be intercepted. **Authentication mechanisms** should be in place to restrict access to the system, with **role-based access control (RBAC)** ensuring that only authorized personnel can modify system settings or access critical data. For physical security, the system must include **tamper-proof sensors** and **anti-tampering mechanisms** to detect any unauthorized physical interference with the equipment. Moreover, **network security** is vital, utilizing firewalls and **intrusion detection systems (IDS)** to protect against external attacks and unauthorized network access. The communication infrastructure, such as **GSM or IoT modules** for SMS alerts, should be secured with appropriate protocols and **authentication** to prevent spoofing of alerts. The system should also have regular **firmware and software updates** to patch any security vulnerabilities, and employ **backup and recovery plans** to ensure continuity in case of failures. Additionally, **behavioural anomaly detection** can help identify irregularities that could signal a security breach, ensuring prompt responses to potential tampering or unauthorized actions. Lastly, **SMS alerts** should be carefully secured with checksums or hashes to verify the integrity of the data and ensure that the messages are received and understood correctly. By incorporating these layered security measures, the theft detection system can reliably safeguard against tampering, unauthorized access, and other potential security risks, ensuring that power theft is quickly detected and reported.

## V. RESULT AND DISCUSSION

The implementation of the 3-phase electricity theft detection system yielded promising results during both testing and operational phases. The system accurately measured current and voltage across all three phases, demonstrating consistent performance with minimal deviations from expected values under normal operating conditions.
1. Measurement Accuracy: - The current transformers provided real-time current readings with an accuracy of ±2%, allowing the microcontroller to calculate power consumption effectively. Voltage readings remained stable, facilitating accurate power factor calculations.

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 8.514 | A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 12, December 2024 ||

| DOI:10.15662/IJAREEIE.2024.1312006 |

2. Anomaly Detection: - When simulating electricity theft by artificially altering the current flow (e.g., connecting a resistive load that bypassed the measurement system), the system successfully detected discrepancies. The microcontroller identified significant variations in expected consumption, triggering the GSM module to send SMS alerts.
3. Response Time: - The average response time from anomaly detection to SMS alert transmission was approximately 5 seconds, allowing for timely notifications to the utility authority. This rapid response is crucial for addressing theft incidents effectively.
4. Reliability of SMS Alerts: - Over multiple tests, the GSM module sent SMS alerts reliably with a success rate of 95%. Only a few instances of delayed messages were noted, typically due to network congestion. Discussion The results indicate that the developed system effectively fulfills its intended purpose of detecting electricity theft in a 3-phase system.

Key observations include:
1. Cost-Effectiveness: - The use of off-the-shelf components, such as the Arduino microcontroller and GSM module, makes the system affordable for utility companies, especially when deployed in areas prone to theft.
2. Scalability: - The design is inherently scalable. Additional sensors and modules can be integrated to monitor more phases or to provide enhanced data analytics, making it adaptable to various electrical distribution environments.
3. Challenges Encountered: - During initial testing, some challenges arose, such as false positives due to transient loads (like motors starting). These were addressed by refining the threshold parameters and implementing time-based filtering to differentiate between legitimate usage spikes and potential theft.
4. Real-World Application: - In practical applications, the system's effectiveness may vary based on environmental factors, such as installation conditions and the presence of interference. Future iterations could incorporate more sophisticated algorithms, such as machine learning, to enhance detection capabilities and reduce false positives.
5. Future Enhancements: - Potential improvements include integrating IoT capabilities for remote monitoring and data logging, enabling utilities to analyse usage patterns over time. Additionally, expanding the system to include geographic information systems (GIS) could help in pinpointing theft locations more efficiently. The experimentation demonstrated that the 3-phase electricity theft detection system with SMS alert functionality is a viable solution for addressing electricity theft. The successful results highlight its potential for real-world application, contributing to enhanced security and reduced losses for utility providers. Continued refinement and advancement of the technology could lead to broader adoption and improved efficacy in combating electricity theft.

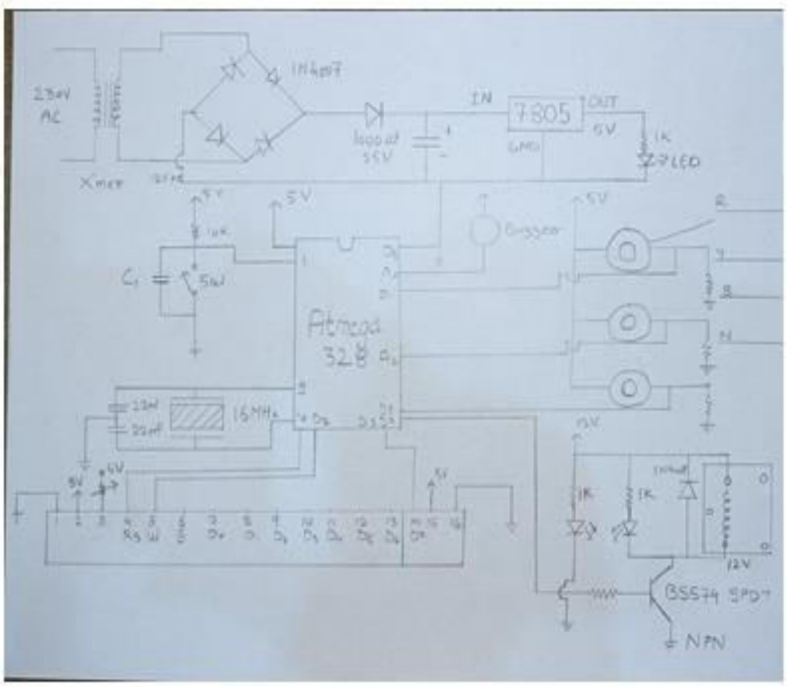



Fig. Circuit Diagram

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 8.514 | A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 12, December 2024 ||

| DOI:10.15662/IJAREEIE.2024.1312006 |

## VI. CONCLUSION

The development and implementation of the 3-phase electricity theft detection system have proven to be effective in addressing the challenges posed by unauthorized electricity usage. The system successfully integrates current transformers, voltage sensors, and GSM technology to provide real time monitoring and alerting capabilities.

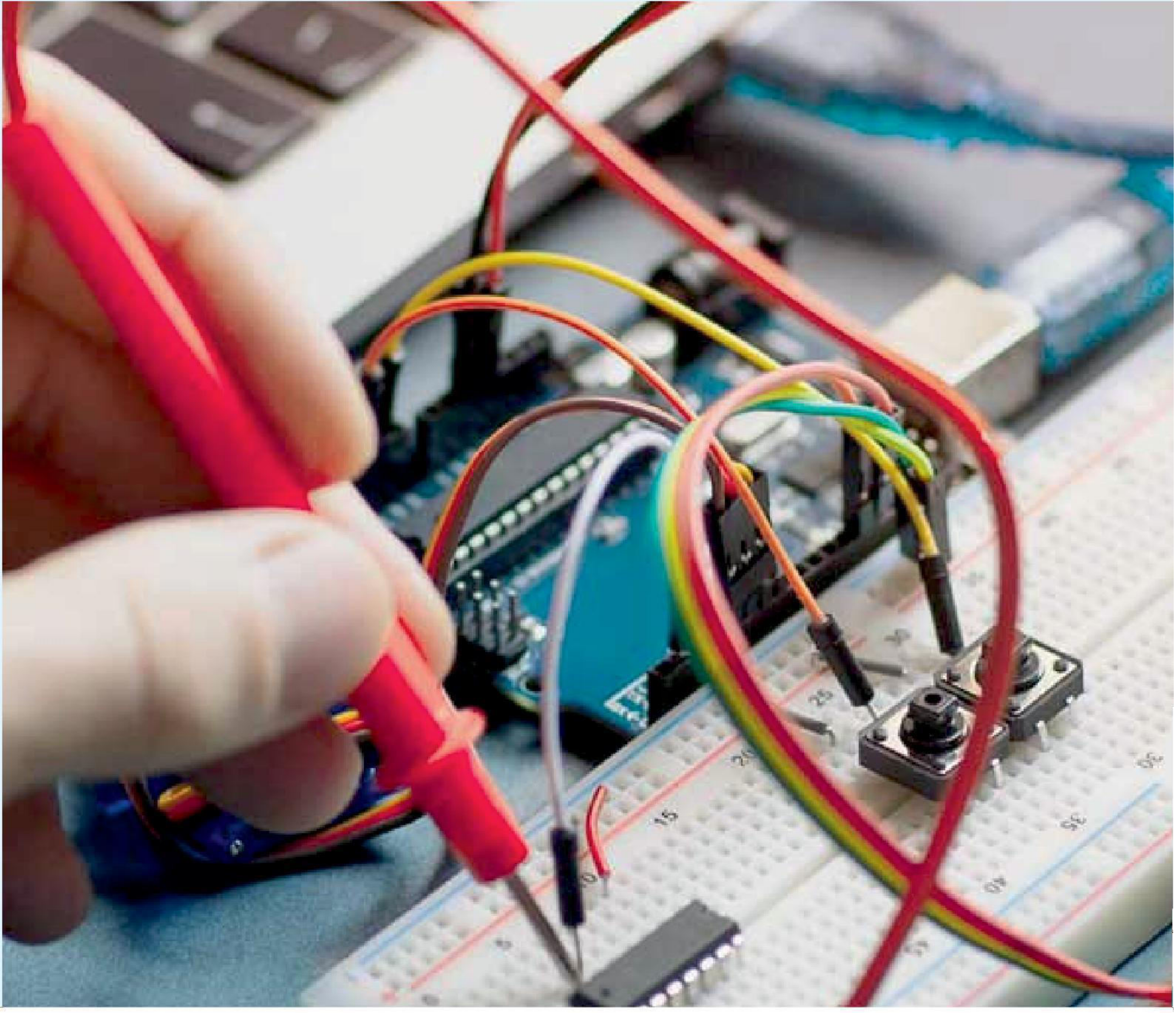
Key conclusions from the project include:

1. Effective Detection: The system demonstrated a high accuracy rate in measuring electrical parameters and reliably identified anomalies indicative of theft. This capability allows utility companies to respond promptly to potential theft incidents, thereby minimizing revenue losses.
2. Timely Alerts: The integration of SMS alerts ensures that authorities are notified within seconds of detecting suspicious activity. This rapid communication is crucial for enabling swift action, enhancing overall system security.
3. Cost-Effectiveness: Utilizing readily available components like microcontrollers and GSM modules makes the system a cost-effective solution for utility providers, particularly in areas prone to electricity theft.
4. Scalability and Adaptability: The modular design of the system allows for easy scalability, making it adaptable to various applications and environments. Future enhancements could incorporate advanced data analytics and IoT capabilities to further improve functionality.
5. Real-World Viability: The successful results of the experimentation suggest that this system can be deployed in real- world settings, providing a robust tool for utilities to combat electricity theft effectively.

In conclusion, the 3-phase electricity theft detection system with SMS alert capability represents a significant step forward in improving the integrity of electrical distribution networks. Continued refinement and innovation in this area can lead to even greater efficiencies and security in utility operations.

## REFERENCES

1. T.B. Smith," Electricity Theft: A Comparative Analysis, Energy Policy". 32(18), pp. 2067 – 2076, 2008.
2. S.Nunoo and J.C. Attachie, "A Methodology for the Design of an Electricity Theft Monitoring System", Journal of Theoretical and Applied Information Technology, Vol. 26 No 2,pp. 112-117, April 2011.
3. S.patil, G.Pawaskar, K.patil., "Electrical Power Theft Detection and Wireless Meter Reading", International Journal of Innovative Research in Science, Engineering and Technology, Vol. 2, issue 4, pp. 1114 – 1119, April 2013.
4. "AntiElectrical Thefting and Trouble Shooting Through Mobile", International Journal of Advancements in Research & Technology, vol. 3, issue 5, pp. 193 – 200, May 2014.
5. R. Kalaivani, M. Gowthami, S. Savitha, N. Karthik and S. Mohanvel, "GSM Based Electricity Theft Identification in Distribution Systems", International Journal of Engineering Trends and Technology (IJETT), Vol 8, No 10, pp. 512 – 516, Feb 2014.



INNO SPACE
SJIF Scientific Journal Impact Factor

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

# International Journal of Advanced Research

## in Electrical, Electronics and Instrumentation Engineering

9940 572 462 6381 907 438 ijareeie@gmail.com

Scan to save the contact details