E-ISSN 2581 – 7957
P-ISSN 2277 – 3916

DOI: 10.32377/cvrjst2512

IoT Enabled Power Theft Detection System

N. Swapna[1] and V. Sreelatha Reddy[2]
[1]Asst. Professor, Guru Nanak Institutions Technical Campus/ECE Department, Hyderabad, India
Email: swapnan.ecegnitc@gniindia.org
[2]Sr. Asst. Professor, CVR College of Engineering/EIE Department, Hyderabad, India
Email: srilathareddy.cvr@gmail.com

***Abstract*: The unauthorized appropriation of electrical power poses a significant challenge within global power system networks, and it is strictly prohibited by legal regulations. The imperative to discern the location of power theft is crucial for enabling legal recourse against perpetrators. The system consists of an ESP32 module, a Long-Range Communication Module, an OLED display, and current transformers. Given the limitations of conventional meters in handling high currents, current transformers are employed for their detection. One current transformer measures the load's current, while the other measures the supply current, both connected to the power supply terminals to ascertain the electrical power output by the source. An IoT-based power theft detection system has been successfully deployed, complemented by Long-Range Communication for enhanced backup protection, as detailed in this research paper.**

***Index Terms*: power theft, Internet of Things (IoT), Sensors, protocol.**

I. Introduction

The issue of power theft is of contemporary significance, inflicting substantial financial losses upon electricity providers, with particular prominence in countries like India where such incidents are alarmingly frequent. Implementing proactive strategies to curb power theft holds the potential for substantial power *conservation. The* application of an electrical power theft detection system plays a pivotal role in the identification of unauthorized tapping on distribution lines, extending its utility to local neighborhoods and broader distribution networks within the electrical power supply system. The existing system grapples with shortcomings in accurately pinpointing the precise location of unauthorized taps. In contrast, the proposed system is meticulously designed to locate the specific electrical line subject promptly and accurately to tampering in *real time*. The paramount importance of a stable and dependable power grid in modern society cannot be overemphasized. The blackout that transpired in India in July 2012 serves as a poignant example, affecting over 60 million individuals and plunging 20 out of 28 Indian states into darkness. This incident served as a stark reminder of the inadequacies of the traditional power grid, which astonishingly still adheres to designs dating back more than a *century. In* response to the advancements in data systems and communication technology, numerous countries are actively engaged in the modernization of their aging power grids, ushering in the era of smart grids. These smart grids offer bidirectional energy transmission, unwavering reliability, and real-time functionalities, empowering them to facilitate demand response, self-healing capabilities, and heightened security. Smart grids encompass a spectrum of operational and energy measures, including the deployment of smart meters, *and* intelligent appliances, harnessing renewable energy resources, and enhancing energy efficiency. This research paper embarks on an exploration of these critical dimensions and their implications.

A. Objective

The fundamental objective of this research project is to detect cases of power theft, dissuade unauthorized power consumption, and ultimately ensure the secure and lawful utilization of electrical power.

Automated Operation: The power theft system aims to automate the authorized power utilization, eliminating the need for manual protection of power systems. By utilizing sensors, actuators, and IoT connectivity, the system can collect data, analyze it, and alert the surroundings and complaints of the electricity board based on predefined algorithms. The objective of a power theft system is to save the power there, enhancing the nation’s wealth.

Remote Monitoring and Control: Another objective of a power theft system based on IOT technology is to enable remote monitoring of power security. By integrating with cloud platforms, the electricity board receives notifications and alerts.

Energy Efficiency: As soon as power energy theft occurs the load gets disconnected, and the system sends the signals to the authorized power station hence utilizing the power energy efficiently.

power theft systems also focus on optimizing energy usage.

B. Motivation

Power burglary alludes to the unlawful or unapproved utilization of power without appropriate installment to the service organization. This can happen through different means, like messing with meters, utilizing sidesteps, or controlling the wiring to keep away from meter readings. Power burglary can have critical unfortunate results for service organizations, purchasers, and society all in all. Here are a few inspirations for executing tasks to battle power burglary.

Monetary Misfortune Counteraction: Influence burglary prompts significant income misfortunes for service organizations, as they can't charge clients precisely for the power consumed. These misfortunes can affect the organization's monetary security and capacity to put resources into framework upgrades.

Received on 18-08-2023, Revised on 02-11-2023, Accepted on 28-11-2023.

Decency and Value: Power robbery puts uncalled-for trouble on fair purchasers who cover their bills instantly. Tending to drive robbery guarantees that all shoppers contribute their reasonable portion toward the expense of power age and appropriation.

Administration Quality: Power burglary can strain the power matrix and lead to blackouts or diminished help quality for authentic clients. By tending to control burglary, service organizations can further develop administration dependability and generally speaking network execution.

Energy Protection: Unapproved utilization of power adds to the wastage of important assets. Tending to drive robbery is in accordance with energy preservation endeavors, advancing reasonable energy rehearse.

Lawful and Administrative Consistence: Power burglary is unlawful and frequently abuses utility guidelines. Carrying out measures to forestall power burglary guarantees consistent with regulations and guidelines overseeing the energy area.

Mechanical Development: Power burglary avoidance projects frequently include the turn of events and sending of cutting-edge innovations, for example, shrewd meters, information investigation, and remote observing frameworks. These activities drive mechanical advancement in the energy business.

Financial Turn of events: Addressing power robbery can add to a steady and solid energy supply, which is critical for monetary development and improvement. Organizations and businesses require a reliable and reasonable energy supply to work proficiently.

Decreasing Carbon Impression: Forestalling power burglary can prompt more exact energy utilization information, which thusly helps service organizations better arrange and upgrade energy age. This can add to a more productive utilization of assets and a decrease in ozone-depleting substance discharges.

Purchaser Training: Power burglary avoidance projects frequently incorporate instructive missions to bring issues to light about the unfortunate results of forcible robbery. Teaching buyers about the significance of paying for the power they use can assist with cultivating a feeling of obligation.

By and large, the inspiration driving power burglary counteraction projects is to make a fair, productive, and maintainable energy dissemination framework that benefits both service organizations and shoppers while advancing capable energy utilization rehearses.

II. Literature Review

[1] The proposed system employs two methods for detecting power theft: the measurement and comparison of current. Current is measured at the distributor box and transmitted to a server database via GSM/GPRS for each household. Simultaneously, electric meters within individual homes gauge and transmit current data to the server, accompanied by user information and a photograph of the residence via a mobile app. Upon detecting a marginal variance between the distributor box and electric meter current readings, the server identifies power theft. Subsequently, user particulars, including the address and an area photograph, are relayed to an authorized mobile app, while latitude and longitude data are utilized to pinpoint the location of the theft on Google Maps. This process is also applied to uncover instances of hooking on individual electric poles.

[2] Muhammad Badar Shahid and colleagues discussed the significant issue of non-technical power losses, primarily resulting from electricity theft in countries like Pakistan. These thefts lead to substantial financial losses and jeopardize the nation's economic stability. The prevalent forms of theft include consumer-side tampering, like meter bypassing, and line-side theft through the "Hooking" system. In order to address these thefts and mitigate their economic repercussions, we introduce an innovative solution. Our theft detection algorithm has the capability to recognize unauthorized power consumption at both the consumer's end (meter tampering) and within the distribution lines (hooking) by means of consumer load profiling. When instances of theft are identified, our prevention algorithm takes prompt action by disconnecting all legitimate consumers and delivering a high-voltage pulse to the distribution line, rendering illicit connections nonfunctional.

[3] This paper discusses the controller-based system that gathers voltage and current data from the LT side of distribution transformers and household energy meters. The energy meter data is wirelessly transmitted to the main control unit on the LT side of the distribution transformer. By analyzing voltage drops and current changes in the distribution line caused by power theft, the system detects and locates the theft. It then signals the circuit breaker to interrupt power and rechecks for theft. In case theft persists even after four attempts, the system initiates a complete system reset and dispatches an alert message to the electricity provider or the nearest substation, providing precise information about the location of the theft. Testing of this system using MATLAB has yielded satisfactory results.

[4] This paper presents an inventive approach to measuring and billing energy consumption, offering an alternative to conventional methods. In light of the growing adoption of renewable energy sources and decentralized power generation, the advancement of smart grid technologies has become ever more crucial. The proposed smart energy meter system seamlessly integrates an embedded controller and a GSM module to transmit data, including energy consumption in kilowatt-hours (kwh), billing information, and security alerts, over GSM mobile networks. This system also maintains continuous monitoring of energy meter readings and sends notifications such as low balance and zero balance alerts to designated phone numbers via a GSM modem.

[5] Discussed the various kinds of Electricity theft have been a persistent problem and emerged as a significant issue, particularly in developing countries like India. This illicit activity has adverse effects on the economy and hampers the

overall growth of the nation, as the progress of the power sector is intricately linked with the country's economic development. In India, power theft takes various forms, with tapping into power lines being a common method. To address this challenge, a system based on Arduino Uno has been developed for the automatic detection and measurement of power theft. Whenever unauthorized power consumption is detected by this system, it promptly alerts the relevant authorities.

[6] Proposed that Energy theft is a significant problem in developing countries like India, Pakistan, and Sri Lanka. Illicit electricity use can severely disrupt a country's economy. Detecting and addressing such theft at the individual level in real-time applications is challenging. Various methods of energy theft, such as meter tampering, meter bypassing, and direct line hooking exist. This paper presents a solution for detecting energy theft using Arduino and a GSM module. An LCD displays power usage data, including the discrepancy between legitimate consumption and theft, which is then transmitted via GSM to the electricity board and the consumer, along with transformer details. The system is equipped with power backup, ensuring uninterrupted message transmission even during power failures, streamlining the reporting process to the electricity board.

[7] The paper addresses the critical issue of electricity theft, which is on the rise, especially in developing nations such as India, leading to various challenges. In response, this paper proposes a method for identifying theft, notifying users, and discontinuing the power supply upon detecting unauthorized activities. The system utilizes GSM technology to send SMS notifications to users and is integrated with a specialized energy meter equipped with a relay, effectively tackling non-technical losses, billing discrepancies, and voltage fluctuations.

[8] To address power theft, a system has been proposed that relies on current measurement and comparative analysis. The process of current distribution initiates from the electric pole, extending to an intermediary distributor box, and ultimately reaching individual residences. The distributor box periodically measures current and forwards this data to the respective server database for each household via the GSM/GPRS network. Simultaneously, each household is equipped with an electric meter for current measurement, and this data is regularly transmitted to the server database through the use of GSM/GPRS technology. Additionally, during the installation of the electric meter, user information is entered into the database using a user-friendly mobile application. This information encompasses the user's address, latitude, and longitude, which are obtained from the mobile GPS, and includes a photographic record of the user's residence or the surrounding area.

[9] Discussed that the importance of electrical energy in both industrial and household contexts cannot be overstated. However, the escalating demand for electricity has given rise to a pressing concern – the rampant issue of power theft. In nations like India, power theft contributes to a substantial 30%-40% of the total generated power, resulting in significant financial losses for electricity boards. This paper introduces an innovative approach to tackle power theft by detecting unauthorized activities, promptly notifying consumers, and disconnecting the supply as needed. The system is designed to automatically send SMS alerts to users via a GSM module. Moreover, the system incorporates a distinctive energy meter equipped with a relay to effectively address non-technical losses, billing discrepancies, and voltage fluctuations.

[10] This paper addresses power theft issues in low-voltage distribution using smart meters and IoT. The system utilizes real-time power theft detection through linear regression, complemented by Android applications to monitor consumer data and promptly notify relevant authorities. The system detects theft from meter bypass, tampering, and line hooking. Additionally, it enables distribution authorities to control the power supply for individual consumers using a prototype circuit with ATmega328P and NodeMCU.

[11] Proposed a method in Southeast Asian countries experiencing rapid economic growth, largely driven by power generation. However, transformer theft is a prevalent issue hindering progress. To address this, a GSM-based system has been developed to protect distribution transformers from theft and monitor their health parameters using sensors like magnetic, IR, and weight sensors. The system alerts authorities via SMS about theft attempts and provides real-time information on transformer health, including temperature and oil level.

III. Implementation

An IoT-enabled power theft detection system that utilizes IoT technology requires various hardware components to detect the power theft. The key components of this system include the ESP32, meter reading, current, voltage sensors, OLED, Zigbee, Relay Driver, and buzzer. By integrating these hardware components, the power theft detection system effectively oversees, identifies, and manages power theft incidents. The integration of IoT technology empowers efficient authorized power usage, leading to the country's economic growth.

Figure 1 illustrates a block diagram for an IoT-based power theft detection system. The system includes the following components.

Sensors: Different sensors are sent into the framework to gather pertinent information. These sensors can incorporate meter perusing, current, and voltage sensors. They give continuous data about the power essential for compelling power robbery and control frameworks.

IoT: The Internet of Things (IoT) represents yet another breakthrough technology in the field of Information Technology. It facilitates the interconnection of a wide array of devices, including sensors, actuators, PLCs, and various smart embedded electronic devices and controls, as well as diverse software applications. This connectivity and network infrastructure enable seamless communication among these diverse devices, facilitating the exchange of information.

ESP32: The ESP32 is a series of robust, energy-efficient, cost-effective microcontrollers equipped with integrated Wi-Fi and dual-mode Bluetooth capabilities. It is a single 2.4 GHz WIFI-and-Bluetooth combination chip developed using TSMC's super low-power 40 nm technology. Designed to deliver optimal power and RF performance, it exhibits resilience, versatility, and reliability across a wide range of applications and power scenarios.

A. Block diagram

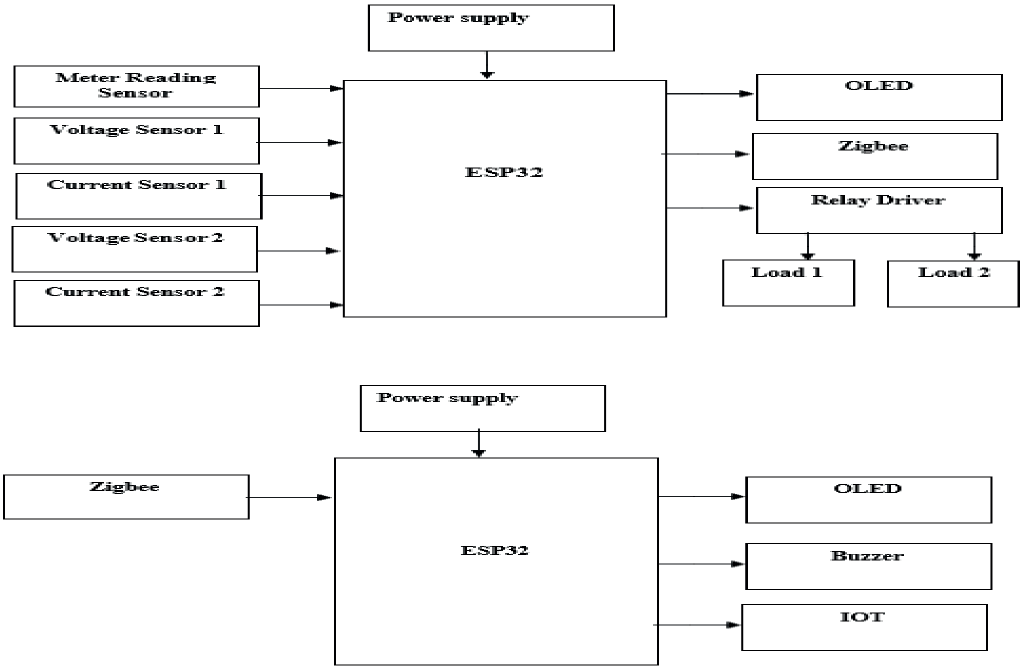

Figure 1. Block Diagram for Power Theft Detection System

OLED: OLED, which stands for Organic Light Emitting Diodes, is a flat-panel light-emitting technology achieved by placing a series of organic thin films between two conductors. When an electrical current is applied, it emits vibrant light. OLEDs are self-illuminating displays that do not require a backlight, making them thinner and more efficient compared to LCD displays, which rely on a white backlight. Notably, OLED displays offer not only slimness and efficiency but also the highest image quality, with the potential for transparency, flexibility, foldability, and even rollability and stretchability in the future. OLEDs represent the future of display technology.

Actuators (Relay Driver): The ULN2003 is a solid IC comprised of seven NPN Darlington semiconductor matches with high voltage and flow capacity. It is commonly employed in various applications such as relay drivers, motor drivers, display drivers, LED light drivers, logic buffers, line drivers, solenoid drivers, and other high-voltage current applications. The ULN2003 is extensively utilized in relay control and stepper motor control applications.

Zigbee: Zigbee is a specification for the establishment of high-level communication protocols utilized to establish functioning personal area networks from small, low-power digital radios. Based on the IEEE 802.15 standard, Zigbee devices, while low-powered, can often transmit data over extended distances by relaying information through intermediate devices to reach more distant ones, creating a mesh network. This network operates without centralized control or a high-power transmitter/receiver capable of reaching all of the networked devices.

The decentralized nature of these wireless ad-hoc networks makes them well-suited for situations where reliance on a central node is not feasible. Zigbee protocols are designed for embedded applications that demand low data rates and minimal power consumption. As a result, the resulting network operates with minimal power requirements, with individual devices expected to have a battery life of at least two years to meet Zigbee certification standards.

A bell or beeper is a signaling device, typically electronic, commonly found in vehicles, household appliances like microwaves, or game shows. It typically consists of multiple switches or sensors connected to a control unit that determines if a button has been pushed or a preset time has elapsed. It often illuminates a light on the corresponding button or control panel and emits a warning signal in the form of a continuous or intermittent buzzing or beeping sound. Initially, this device was based on an electromechanical system, similar to an electric bell without the metal gong that produces the ringing noise. These units were frequently mounted on walls or ceilings and used the structure as a resonating surface.

Another approach, especially with some air conditioner-related devices, involved implementing a circuit to capture the air conditioner's current noise, amplifying it to the extent it could drive a speaker, and then connecting this circuit to an inexpensive 8-ohm speaker. Nowadays, it's more common to use a ceramic-based piezoelectric sounder like a son alert, which generates a high-pitched tone. Typically, these sounders were linked to "driver" circuits that could modify the sound's pitch or toggle it on and off.

The power supply section is responsible for providing +5V to the components for their operation. The LM7805 IC is employed to deliver a stable +5V power source. To ensure the power theft system functions effectively, it necessitates a consistent power supply to operate sensors, IoT devices, technical equipment, and actuators. This can be achieved through a combination of mains power, batteries, solar chargers, or other sustainable energy sources.

B. Schematic Diagram

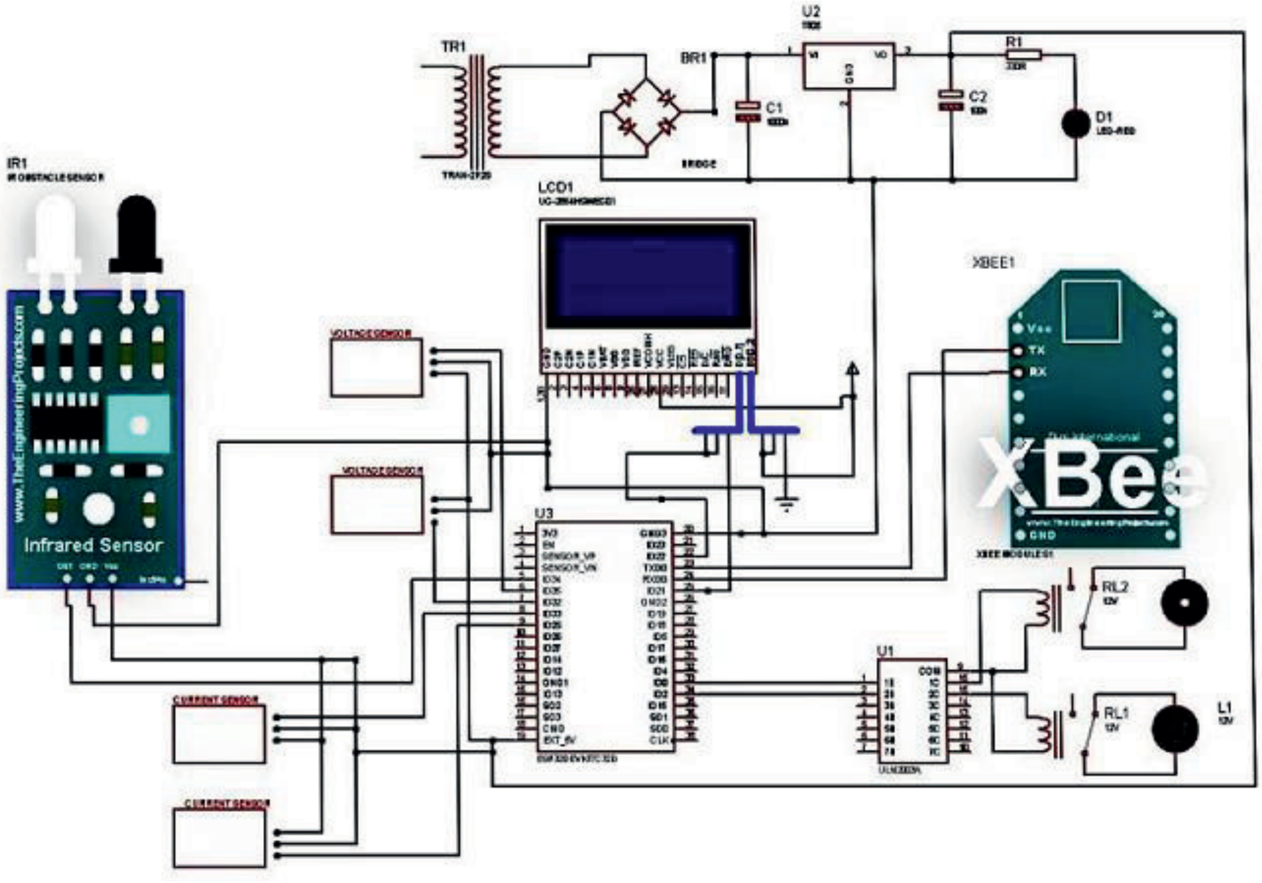

Figure 2. Schematic diagram of the System

The schematic diagram of the system is depicted in Figure 2. An IoT-based power theft detection system typically comprises multiple components and sensors working collaboratively to safeguard power from unauthorized usage. Below is an overview of a standard schematic diagram for this system:

1. IR sensor: The framework starts with an IR sensor. Working on IR sensors is extremely straightforward, and the working standard is completely founded on a change in the obstruction of the IR recipient. Here in this sense, we associate IR recipient in switch predisposition, so it gives exceptionally high obstruction on the off chance that it isn't presented to IR light. The obstruction for this situation is in the scope of the Super ohms, however when the IR light is considered back and falls IR recipient. The opposition of Rx comes in a range between Kilo ohms to many ohms. We convert this adjustment of protection from a change in voltage. Then, at that point, this voltage is applied to a comparator IC which contrasts it and an edge level. On the off chance the voltage of the sensor is more than the limit, the yield is high it is low which can be utilized straightforwardly for microcontrollers.

2. Voltage Sensor: A Voltage Sensor is a device that converts the voltage measured between two points in an electrical circuit into a physical signal proportional to that voltage. The voltage sensor circuit is a combination of various electronic components, allowing the precise measurement of voltage values. Potentiometers and ADC (Analog-to-Digital Converter) are key components commonly used in voltage sensors.

3. A current sensor is a device that detects and transforms current into a readily measurable output voltage, directly proportional to the current passing through the measured path. This output can be utilized to display the measured current on an ammeter, stored for further analysis in a data acquisition system, or employed for control purposes.

4. Microcontroller: Upon detecting power theft, the controller supplies a 5V operating voltage to the relay, disconnects the load from the power source, and halts any further power theft attempts. Consequently, this system automatically alerts and isolates the supply from the load, effectively preventing theft.5. Driver: at whatever point the transfer driver gets the high voltage from the regulator, the ringer makes a blaring sound, and the bulb (load) gets detached from the supply.

6. OLED: The situation with activity is shown obviously on OLED i.e., when power robbery happens, we can notice the text "power burglary occurred" on OLED. Simultaneously, the signal makes a blaring sound.

7. Zigbee: Finally, the Zigbee convention is liable for correspondence among every one of the parts of the power-robbing framework.

C. Flowchart

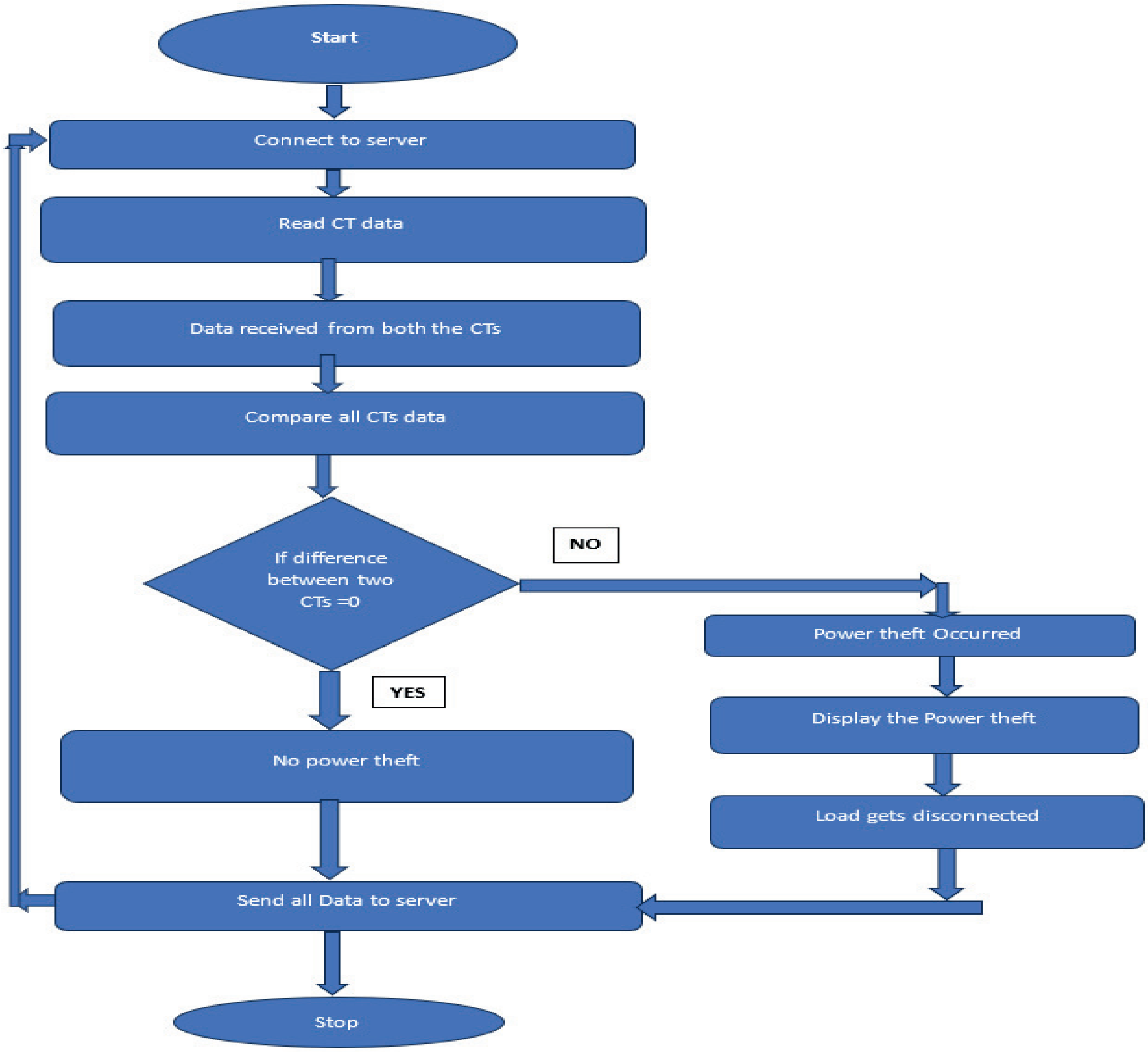

Figure 3: System Flowchart

IV. Results

The implementation of an efficient power theft system using IoT technology can yield several positive outcomes. Here are some potential results:
1. Real-time monitoring: The power theft system monitors the power theft and used in various fields like Utility companies, Residential and commercial buildings, Law Enforcement Agencies, and Electrification.
2. Wireless connectivity: As the technology used here is IOT so much wiring equipment is avoided.
3. Timely Alerts and Notifications: Using the Zigbee protocol integrated with IoT technology and different actuators, whenever the power theft occurs it not only protects the unauthorized power usage but also alerts the people surrounding and the electricity board in time.
4. Efficient Resource Allocation: As the power theft system uses different components and due to the automation process the manual intervention was reduced. This saves time and effort for users, allowing them to focus on other important t5. Enhanced Security Measures: The IoT-based power theft system provides more security for the electricity by alerting authorized persons. The system also protects the unauthorized usage of power in an illegal manner. Overall, the power theft system using IoT technology can result in power protection, Acknowledgment the authorized persons, cost savings, improved national property and yield, and time efficiency. These outcomes demonstrate the potential of IoT-enabled power theft systems. The complete hardware setup is shown in Figure 4
This system also used in
1. Utility companies- used to monitor and detect instances of power theft within theirdistribution networks.
2. Residential and commercial buildings- used to monitor electricity consumption anddetect any unauthorized tapping.
3. Law Enforcement Agencies- utilized to support their investigations and crack down on illegal activities related to power theft.
4. Electrification- used to curb power theft effectively ensures the availability to all consumers and promotes fair electricity distribution in underserved regions.

A. Abbreviations

TABLE I.
Abbreviations

Abbreviation	Definition
CT	Current Transformer
OLED	Organic Light Emitting Diode.

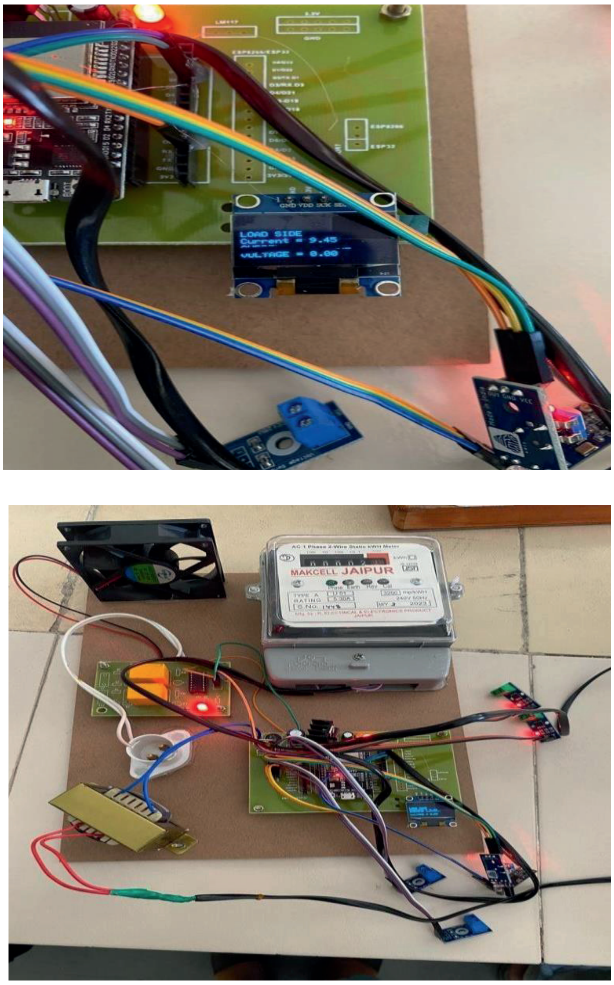

Figure 4. Hardware Setup of the system

V. Conclusions

In summary, the deployment of an IoT-based power theft system presents notable advantages within the realm of smart city advancements. This research project places a primary emphasis on bolstering connectivity and networking elements within the IoT framework. Over the course of this study, we have achieved successful power theft detection, fault identification, and precise fault location tracking, enabling the implementation of necessary corrective measures. The proposed system adeptly tackles various prominent challenges inherent in the current Indian grid infrastructure, encompassing energy conservation, power theft prevention, and cable fault management. It is worth highlighting that the system's efficient power utilization leads to substantial cost reductions, establishing its economic viability for the electricity board.

The project demonstrated that utilizing Internet of Things (IoT) technologies for power theft detection can significantly enhance accuracy compared to traditional methods. By integrating smart meters, sensors, and data analysis techniques, the system achieved a high level of precision in identifying and distinguishing between legitimate power consumption and unauthorized usage.

Future Directions: The project identified potential avenues for further research and development, such as exploring advanced machine learning techniques to enhance detection accuracy, integrating renewable energy sources into the IoT framework, and investigating novel approaches to user-friendly interfaces for end-users.

REFERENCES

[1] N. K. Mucheli *et al.*, “Smart Power Theft Detection System,” *2019 Devices for Integrated CircuitDevIC)*, March 2019.

[2] Muhammad Badar Shahid, Muhammad Osama Shahid, T. Hasan, and S. Saleem, “Design and Development of An Efficient Power Theft Detection and Prevention System through Consumer Load Profiling,” *2019 International Conference on Electrical, Communication, and Computer Engineering (ICECCE)*, Jul.2019.

[3] Mohd Uvais, “Controller Based Power Theft Location Detection System,” *International Conference on Electrical and Electronics Engineering*, Feb.2020,

[4] C. Santhosh, S. V. Aswin Kumar, J. Gopi Krishna, M. Vaishnavi, P. Sairam, and P. Kasulu, “IoT based smart energy meter using GSM,” *Materials Today: Proceedings*, vol. 46, Mar. 2021, doi: Accessed: Oct. 30, 2023.

[5] V. R. Pawar, J. J. Jadhav, J. Saha, and S. S. Jadhav, “Arduino Uno Based Automatic Power Theft Detection,” *Journal For Basic Sciences*, vol. 23, no. 5, May 2023.

[6] T. Shahzad Gill *et al.*, “IoT Based Smart Power Quality Monitoring and Electricity Theft Detection System,” *IEEE Xplore*, Dec. 01, 2021.

[7] Bandarupalli Deepthi, V. Naga, and P. V. Naidu, “Detection of Electricity Theft in the Distribution System using Arduino and GSM,” 2019 International Conferenceon Computation of Power, Energy, Information and Communication (ICCPEIC), Mar. 2019.

[8] V. Jaiswal, Hritik Kumar Singh, and K. Singh, “Arduino GSM based Power Theft Detection and Energy Metering System,” 2020 5th International Conference on Communication and Electronics Systems (ICCES), Jun. 2020.

[9] M. J. Jeffin, G. M. Madhu, A. Rao, G. Singh, and C. Vyjayanthi, “Internet of Things Enabled Power Theft Detection and Smart Meter Monitoring System,” 2020 International Conference on Communication and Signal Processing (ICCSP), pp. 0262–0267, Jul. 2020.

[10] X. Feng et al., “A Novel Electricity Theft Detection

[11] Scheme Based on Text Convolutional Neural Networks,” Energies, vol. 13, no. 21, p. 5758, Nov. 2020.

[12] R. E. Ogu and G. A. Chukwudebe, “Development of a cost-effective electricity theft detection and prevention system based on IoT technology,” Nov. 2017.