

IOT BASED SYSTEM FOR REAL-TIME ELECTRICITY THEFT DETECTION

Submitted in partial fulfillment of the
requirements for the award of
Bachelor of Technology degree in
Information Technology

By

AMRITHAA ASHOK

(40120011)



**DEPARTMENT OF INFORMATION TECHNOLOGY
SCHOOL OF COMPUTING**

**SATHYABAMA
INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)**

**Category-1 University by UGC
Accredited with Grade “A++” by NAAC 12B Status
by UGC |Approved by AICTE
JEPPIAAR NAGAR, RAJIV GANDHI SALAI,
CHENNAI - 600 119
APRIL - 2024**



SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)

Accredited "A++" Grade by NAAC | 12B Status by UGC | Approved by AICTE

www.sathyabama.ac.in

DEPARTMENT OF INFORMATION TECHNOLOGY

BONAFIDE CERTIFICATE

This is to certify that this Project Report is the bonafide work of **AMRITHAA ASHOK (Reg. No. 40120011)** who carried out the project as a "IoT Based System for Real-time Electricity Theft Detection" under our supervision from January 2024 to April 2024.


12/4/24

Internal Guide

Dr. R. Subhashini, M.E., Ph.D.


12/4/24

Head of the Department

Dr. R. Subhashini, M.E., Ph.D.

Submitted for Viva voce Examination held on 17 April 2024


Internal Examiner


External Examiner



SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY

(DEEMED TO BE UNIVERSITY)

Accredited "A++" Grade by NAAC | 12B Status by UGC | Approved by AICTE

www.sathyabama.ac.in

DECLARATION

I **Amrithaa Ashok** hereby declare that the Project Report entitled **IoT Based System for Real-time Electricity Theft Detection** done by me under the guidance of **Dr. R. Subhashini, M.E., Ph.D.** is submitted in partial fulfillment of the requirements for the award of Bachelor of Technology degree in Information Technology.

DATE:

17/4/2024

PLACE:

CHENNAI

SIGNATURE OF THE CANDIDATE

ACKNOWLEDGEMENT

I am pleased to acknowledge my sincere thanks to **Board of Management of SATHYABAMA** for their kind encouragement in doing this project and for completing it successfully. I am grateful to them.

I convey my thanks to **Dr. T.Sasikala M.E., Ph.D., Dean**, School of Computing **Dr.R.Subhashini M.E.,Ph.D.**, Head of the Department of Information Technology for providing me necessary support and details at the right time during the progressive reviews.

I would like to express my sincere and deep sense of gratitude to my Project Guide **Dr. R. Subhashini, M.E., Ph.D** for her valuable guidance, suggestions and constant encouragement paved way for the successful completion of my project work.

I wish to express my thanks to all Teaching and Non-teaching staff members of the **Department of Information Technology** who were helpful in many ways for the completion of the project.

ABSTRACT

Electricity theft remains a significant challenge in many regions, leading to financial losses for utility providers and unreliable power supply for consumers. This paper presents an innovative approach to electricity theft detection using a sensor network connected to an ESP32 microcontroller. The system employs voltage and current sensors at both the power pole and the main supply meter, allowing for real-time monitoring and analysis. The proposed methodology involves comparing the power consumption readings from the pole and the meter. If the readings match, no theft is indicated; however, discrepancies suggest potential illicit activities. The ESP32 facilitates data acquisition, processing, and communication between the sensors, enabling a robust and scalable solution for theft detection. Experimental results demonstrate the effectiveness of the system in identifying instances of electricity theft. Furthermore, the project provides insights into the magnitude of theft based on the variations in sensor readings. This research contributes to the ongoing efforts to enhance the reliability and security of power distribution systems, offering a practical solution for utilities to combat electricity theft.

TABLE OF CONTENT

CHAPTER	TITLE	PAGE NO
1	INTRODUCTION	1
1.1	SCOPE OF THE PROJECT	3
2	LITERATURE SURVEY	5
2.1	LIMITATIONS AND EXISTING METHODS	10
	SYSTEM ANALYSIS	14
3.1	EXISTING SYSTEM	14
3.2	PROPOSED SYSTEM	16
3.3	REQUIREMENTS SPECIFICATIONS	19
3.3.1	HARDWARE REQUIRMENTS	20
3.3.2	SOFTWARE REQUIRMENTS	23
4	SYSTEM DESIGN	24
4.1	SYSTEM ARCHITECTURE	24
4.2	CIRCUIT DIAGRAM	25
5	MODULE DESCRIPTION	27
5.1	PROJECT MODULES	27
5.2	CONCLUSION	29
5.3	FUTURE WORKS	30
	APPENDIX	32

LIST OF FIGURES

FIG.NO	TITLE	PAGE NO
3.1	WORKFLOW OF SOLUTION	18
4.1	CIRCUIT DIAGRAM OF PROTOTYPE	24
5.1	SOFTWARE PROCESSFLOW	28
6	OUTPUT	34

CHAPTER 1

I. INTRODUCTION

The contemporary landscape of power distribution systems grapples with an escalating challenge - the surreptitious drain on electrical resources through unauthorized channels, commonly known as electricity theft. This perennial problem not only burdens utility providers with substantial financial losses but also compromises the stability and efficiency of the power grid. In response to this imperative, our research introduces a sophisticated methodology for electricity theft detection, leveraging advanced sensor networks intricately connected to the ESP32 microcontroller.

Electricity theft remains an intricate issue, often eluding conventional detection methods. Our approach transcends these limitations by deploying voltage and current sensors strategically at both the power pole and the primary supply meter. The fundamental premise of our system involves a meticulous analysis of power consumption readings from these sensors. The synchrony in readings implies harmonious power usage, signaling an absence of theft. Conversely, disparities between pole and meter readings serve as robust indicators of potential illicit activities, necessitating swift countermeasures.

The ESP32 microcontroller serves as the nerve center of this system, orchestrating seamless communication between sensors, real-time data acquisition, and intricate processing. Its integration not only amplifies the responsiveness of the theft detection mechanism but also ensures scalability and adaptability across diverse deployment scenarios.

The crux of our innovation lies in its technical prowess. The ESP32 facilitates high-speed data transfer, ensuring minimal latency in sensor response. Complex algorithms govern the real-time analysis of voltage and current differentials,

enabling precise identification of abnormal power consumption patterns indicative of theft. Furthermore, the system is designed with cybersecurity measures to thwart potential tampering and ensure the integrity of collected data.

As we delve into subsequent sections, we will expound on the intricacies of our methodology, present empirical results, and discuss the broader implications of our approach. By combining technological innovation with a robust analytical framework, our project stands as a testament to the potential of advanced sensor networks in fortifying power distribution systems against the clandestine threat of electricity theft.

IoT (Internet of Things) is a transformative paradigm that involves connecting everyday objects to the internet, allowing them to collect and exchange data. In this context, IoT is the underlying framework that enables the smart functionalities of our project.

In the modern age, where energy conservation is a global imperative, the integration of IoT into our daily lives has become more than just a convenience; it's a necessity. The "Smart Switch with Power Theft Detection" project is a pioneering exploration of how IoT can be harnessed to enhance the efficiency, safety, and sustainability of our electrical systems.

Power Theft Detection involves the monitoring and identification of unauthorized or illegal consumption of electricity. This is a critical issue in many regions, as it contributes to financial losses for utility providers and can compromise the stability of electrical grids.

This project encompasses an interdisciplinary approach, merging aspects of electrical engineering, computer science, and data analytics to not only enable the remote and intelligent control of electrical devices but also to detect and mitigate the critical issue of power theft, a significant challenge in many regions. The

project leverages IoT to empower users with real-time monitoring and control, ensuring energy conservation and securing their electrical infrastructure.

As we journey deeper into the intricacies of this project, we will uncover the technical intricacies, design considerations, and real-world applications of this innovative solution. We will explore the underlying technologies that make it all possible, shedding light on how IoT sensors, connectivity, and data analytics merge seamlessly to create a Smart Switch capable of not only enhancing convenience but also contributing to a sustainable energy future

1.1 Project Scope

- Development of a user-friendly interface utilizing the ESP32 microcontroller to ensure optimal user experience, providing real-time monitoring capabilities and incorporating alerting mechanisms for immediate response to potential theft incidents.
- Rigorous testing, including simulations for theoretical validation and field testing for real-world performance evaluation.
- Comprehensive documentation, including detailed project reports and user manuals, ensuring transparency and serving as a valuable reference for future development.
- Presentation and demonstration phases showcasing the operational prowess of the system to stakeholders, with a focus on the user interface facilitated by the ESP32.
- Preparation of a manuscript tailored for scholarly journals, highlighting the technical intricacies and advancements achieved.
- Continuous improvement phase involving systematic collection of user feedback and iterative updates to refine system efficiency, particularly focusing on enhancing the user interface and overall user experience.
- Integration of a dedicated mobile application for remote monitoring capabilities, real-time alerts, and intuitive controls.

- Exploration of machine learning algorithms for improved theft detection accuracy over time.
- Expansion of the sensor network to cover broader areas, amplifying scalability and catering to larger distribution networks.
- Implementation of advanced security measures such as biometric authentication or blockchain technology to fortify the system against potential vulnerabilities.

CHAPTER 2

LITERATURE REVIEW

Zulu, C.L., Dzobo, O. Real-time power theft monitoring and detection system with double connected data capture system. Electr Eng 105, 3065–3083 (2023). <https://doi.org/10.1007/s00202-023-01825-3>

Leak detection systems, as discussed by various researchers, play a key role in identifying and curbing thefts. Artificial intelligence has also proven to be a valuable tool for planning maintenance and managing resources efficiently. In this context, Zulu and Zoo propose a real-time electricity theft monitoring and detection system as a comprehensive solution. For communication, the system uses smart meters equipped with Arduino ATmega328P microcontrollers and GSM modules. Cloud storage is used to store smart meter data, enabling analysis and alerting in the event of an energy imbalance. Using MATLAB Online and Thing Speak IoT channels for cloud storage also fits with current trends in data analysis and visualization. The results of simulations performed using Proteus Design Suite v.8.10 SP3 confirm the effectiveness of the proposed system and illustrate its potential for practical applications. Integrating SMS alerts to notify authorities in the event of electricity theft demonstrates a proactive approach to quickly resolve issues. The proposed system fits the current trend in the use of advanced technologies for real-time monitoring and detection, thereby demonstrating its potential to make a significant contribution to the ongoing efforts to combat electricity theft in distribution systems. This literature review provides the context for the development of such innovative solutions and highlights the importance of technological advances and multidimensional strategies to address the complex challenge of energy theft

Rajasekaran, A., Sai, P. A., Teja, P. B., & Swetha Priya, P. G. S. (2020, March). IOT BASED POWER THEFT DETECTION. International Journal of Scientific Development and Research, 5(3), 249.

This literature addresses a key problem common in India and around the world: the unauthorized use of electricity, which results in significant losses and possible power outages. The article highlights the importance of a stable and modern electricity grid and notes the significant impact of India's power outage in July 2012 on millions of people. It supports the transition to smart grid technology, including operational and energy measures to increase reliability, real-time monitoring and security. The focus was on electricity theft, which is seen as a major challenge for energy companies and has potential consequences for electricity tariffs. It highlighted the ineffectiveness of the existing system, which mainly consists of reading energy meters without the introduction of preventive measures. In response, the proposed system leverages IoT applications for real-time sensing, sending transmission line status, capturing event photos, and location tracking to overcome the limitations of the current system. The verification phase demonstrated the effectiveness of the proposed system compared to the existing system and highlighted the importance of acting immediately upon discovery. The final step highlights the importance of not only detecting electricity theft, but also responding to it quickly. In summary, the paper presents a high-tech solution to reduce energy theft problems, particularly in the Indian context, with practical implementation and testing of the proposed system being the next necessary steps for validation [2].

Meenal, R & Kuruvilla, Kevin & Denny, Adrin & Jose, Rejin & Roy, Renoy. (2019). Power Monitoring and Theft Detection System using IoT. Journal of Physics: Conference Series. 1362. 012027. 10.1088/1742-6596/1362/1/012027.

An IoT and GSM Integrated Approach for Sustainable Power Management

The proposed system integrates IoT and GSM technology to combat power theft effectively. Interfacing Raspberry Pi and Arduino via serial communication, sensors connected to the Raspberry Pi detect load current and voltage, thereby preventing electricity theft. The current power system addresses issues like power theft, energy wastage, and transmission line faults. With electricity theft increasing yearly, the project aims to design a system that monitors power consumption, detects and eliminates theft, and communicates this information to the Electricity Board (EB) through IoT. The use of Raspberry Pi facilitates theft detection, and the GSM module sends theft information to the EB. The project's implementation is expected to significantly reduce electricity theft, alleviating the challenges faced by the entire country. The literature review underscores the prevalence of power theft in India, its economic impact, and the proposed project's potential to address this issue. Previous studies on power theft detection and related solutions are briefly discussed, emphasizing the need for an effective system like the one proposed in this project. The review sets the stage for the project's significance in mitigating power theft and its potential positive impact on the power sector in India [3].

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), Chennai, India, 2020, pp. 0262-0267, doi: 10.1109/ICCSP48568.2020.9182144.

The literature discusses the pervasive issue of power theft at the low voltage distribution end, causing significant revenue losses for distribution companies. With the integration of smart grid technologies, this paper proposes a solution using smart meters equipped with Information Communication Technology (ICT) for detecting and alerting against power theft. The application of Internet of Things (IoT) is introduced for real-time monitoring of smart meters, employing the Linear Regression method to continuously analyze data and detect power theft occurrences. Additionally, Android applications are developed for consumers to monitor their consumption and billing information, with built-in alert systems for authorities in case of theft. The system not only identifies meter bypass, tampering, and direct line hooking but also enables distribution authorities to control smart meters, granting or denying power supply to individual consumers. The validation of the proposed system is demonstrated through a prototype circuit using ATmega328P micro-controller and NodeMCU as a WiFi module [4].

Darteh, Oscar & Liu, Xiaodong & Liu, Qi & Anaadumba, Raphael & Adjei, Charity & Sarker, Sajib. (2020). Internet of Things Based Electricity Theft Detection Using Raspberry Pi.

The paper addresses the crucial link between a country's economic growth and its electricity production and consumption. Recognizing that electricity theft poses a significant threat to economic development, the paper emphasizes the distinction between technical losses (TL) and non-technical losses (NTL). While technical losses are inherent in the network and controlled to a considerable extent, non-technical losses result from metering inaccuracies, electricity theft, and unmetered energy. The focus on NTL, particularly electricity theft, is highlighted as a major challenge for utility authorities worldwide.

The literature underscores the complexity of detecting electricity theft, often categorized as a non-technical loss. The drawbacks in existing systems lead to significant losses for utility authorities. The paper proposes leveraging Internet of Things (IoT) technology, specifically using Raspberry Pi, to enhance the detection of electricity theft. The anticipated increase in the number of connected devices to the internet aligns with the need for utility sectors to adopt such technology for loss reduction.

By introducing an architecture designed to detect illegitimate activities between the utility server and energy meters at customers' premises, the research aims to provide a real-time monitoring solution over the internet. The literature review sets the stage for the innovative approach proposed in the paper, highlighting the potential impact on reducing electricity theft and its subsequent economic benefits [5].

M. U. Hashmi and J. . G. Priolkar, “Anti-theft energy metering for smart electrical distribution system,” in 2015 International Conference on Industrial Instrumentation and Control, ICIC 2015, Maharashtra, 2015

Internet of Things is a term used for a system where devices are given IP addresses, and everybody makes the device recognisable on the internet via that IP address. The web, which started with the internet of computers, is developing. Researchers have predicted a volatile increase in the number of sensors, devices or things connected to the internet. The product network is known as the Internet of Things (IoT) [1]. IoT has the propensity to alter peoples lifestyles. People prefer to monitor things through automatic systems in todays world rather than through any manual system. The Raspberry Pi and the relay, together with the circuitry driving the system, are the main elements of the IoT-based electricity theft detection system introduced in this paper. The indicators of the size and development of an economy are dependent on its production and consumption of electricity, so electricity theft contributes to slow economic growth. Although few countries gain profit from electric power exportation, most production is for consumption. Although few countries gain profit from electric power

exportation, most output in developing countries is for consumption. Most developing countries have suffered undesirable economic consequences to meet the demands of electricity for real estate and industrialisation due to electricity theft. According to the World Bank's development indicator collection, the percentage of distribution and losses due to transmission in Ghana was at 23% in 2014, gathered from officially recognised sources [2]. Reducing transmission and distribution losses is the greatest challenge to power utility authorities.

We can categorise the losses in to technical (TL) as well as non-technical (NTL) [3]. Technical losses are in-built in the system which is reduceable to an appreciable level; the remaining is due to power dissipated in equipment and conductions used to for the distribution and transmission lines[4]. NTL happens due to inaccuracy of metering, stealing or theft of electricity, as well as energy consumed but unrecorded by the energy meter [5]. Electricity theft

is the energy consumed by a customer that is unaccounted for or not measured by the energy meter. Theft of electricity happens due to meter tampering, meter bypassing, and service lines tapping to the customers premises. Due to the deficiencies in the metering system and the lack of transparency and accountability in billing customers of electricity in public utilities, customers take advantage to steal electricity to avoid paying the realistic tariff. Electricity theft causes a very high negative impact on the financial status of power distribution and utility companies, which puts pressure on the future investment of the power sector. The ripple effect is that the losses incurred due to the theft are passed as the cost to the paying consumers in either poor quality service and higher tariff [6]. Reports suggest 25 per cent of Ghanas current annual average losses are due to electricity theft [7]. However, the emergence of smart grid technologies has informed researchers to utilise the smart grid platform to detect and monitor electricity theft. Our research proposes a generalised IOT based design using raspberry pi to detect electricity theft by comparing the recorded values of current at the utility service intake to the recorded value of current at the energy meter intake. The result of the compared values is stored on the firebase server, which is accessible in real-time. The paper is structured as follows: Methods employed by fraudsters in electricity theft are described in section 3; Literature works on electricity theft detection is described in section 2; In chapter 4,

2.1 Limitations on Existing Methods

The existing literature on power theft monitoring and detection systems highlights several limitations inherent in current approaches. In the case of the Real-Time Electricity Theft Monitoring and Detection System proposed by Zulu and Zoo, a potential limitation is the reliance on GSM modules for communication. This choice may introduce challenges related to coverage and reliability, particularly in areas with limited connectivity. Moreover, the study does not explicitly address the issue of false positives or false negatives in theft detection, leaving room for further investigation into the system's accuracy and reliability. Similarly, the Power Theft with IoT System identifies the ineffectiveness of the current system, which predominantly involves reading energy meters without introducing preventive measures. While the proposed IoT-based solution addresses detection, the integration challenges, including considerations of cost, compatibility, and cybersecurity, are not extensively discussed. In the case of the IoT and GSM Integrated Approach for Sustainable Power Management, the literature lacks an in-depth exploration of potential vulnerabilities in the proposed system, particularly concerning the security of the communication and control mechanisms. These limitations underscore the need for a comprehensive understanding of the challenges associated with existing power theft detection systems, providing valuable insights for the development of more robust and effective solutions in the future.

As a whole in current power theft detection systems the important limitations are listed below.

a. Real-Time Electricity Theft Monitoring and Detection System:

Limitation: Reliance on GSM modules for communication.

Consideration: Lack of discussion on false positives/negatives in theft detection.

b. Power Theft with IoT System:

Limitation: Ineffectiveness of the current system, primarily based on reading energy meters without preventive measures.

Consideration: Limited exploration of IoT integration challenges, including cost, compatibility, and cybersecurity.

c. IoT and GSM Integrated Approach for Sustainable Power Management:

Limitation: Lack of in-depth exploration of potential vulnerabilities, particularly in communication and control security.

Consideration: The need for a more comprehensive understanding of integration challenges and system security.

The cumulative impact of limitations in IoT-based power theft detection systems entails potential obstacles to widespread adoption and operational efficiency. High implementation costs may restrict access for financially constrained regions, while infrastructure compatibility issues and reliance on communication networks may disrupt timely responses to power theft incidents. Increased energy consumption could negate conservation benefits, and data security concerns may erode public trust. Implementation complexity, scalability challenges, and regulatory hurdles may impede deployment, limiting overall effectiveness. Consumer cooperation is vital, and resistance or privacy concerns could undermine the system's impact. Moreover, the risk of technological obsolescence raises sustainability concerns in an ever-evolving technological landscape.

CHAPTER 3

SYSTEM ANALYSIS

3.1 EXISTING SYSTEM

The existing landscape of power theft monitoring and detection systems grapples with a myriad of limitations, each posing significant hurdles to effective and comprehensive mitigation strategies. These limitations encompass a spectrum of challenges, ranging from inherent ineffectiveness to dependencies on GSM modules for communication, all the way to the dearth of thorough explorations into potential vulnerabilities. Take, for instance, the prevailing Real-Time Electricity Theft Monitoring and Detection System; while it represents a step forward in addressing electricity theft, its reliance on GSM modules for communication introduces a layer of complexity fraught with challenges related to coverage and reliability. Moreover, this system falls short in explicitly tackling the issue of false positives or false negatives in theft detection, leaving a critical gap in its effectiveness and reliability. Similarly, the Power Theft with IoT System, while demonstrating promise in its approach, primarily revolves around the passive reading of energy meters without proactive measures to deter theft. Furthermore, the proposed IoT-based solution, while innovative in its concept, lacks a thorough discussion on the integration challenges that may arise, including but not limited to considerations of cost-effectiveness, compatibility with existing infrastructure, and cybersecurity implications. Another example is the IoT and GSM Integrated Approach for Sustainable Power Management, which, despite its holistic approach, fails to delve deeply into potential vulnerabilities within the system, particularly concerning the security of communication and control mechanisms, leaving it susceptible to exploitation.

- **Existing Limitations in Power Theft Monitoring Systems:**
 - Inherent Ineffectiveness: Current systems struggle to provide comprehensive mitigation strategies due to various limitations.
 - Dependency on GSM Modules: Many systems rely on GSM modules for communication, introducing challenges related to coverage and reliability.
 - Lack of Thorough Vulnerability Exploration: There's a notable absence of thorough explorations into potential vulnerabilities within existing systems.
- **Examples of Existing Systems and Their Shortcomings:**
 - Real-Time Electricity Theft Monitoring and Detection System:
 - Relies on GSM modules, leading to complexity and potential coverage issues.
 - Doesn't effectively address false positives or false negatives, impacting reliability.
 - Power Theft with IoT System:
 - Primarily focuses on passive reading of energy meters, lacking proactive theft deterrence measures.
 - Proposed IoT-based Solution:
 - Lacks comprehensive discussion on integration challenges, including cost-effectiveness and cybersecurity implications.
 - IoT and GSM Integrated Approach for Sustainable Power Management:
 - Despite a holistic approach, fails to thoroughly address potential vulnerabilities, particularly concerning communication and control security.

3.2 PROPOSED SYSTEM

Our proposed Smart Electricity Theft Detection System represents a paradigm shift in the realm of electricity theft detection and mitigation strategies. Leveraging advanced sensor networks intricately connected to the ESP32 microcontroller, our system is poised to revolutionize real-time monitoring and detection of potential theft instances with unprecedented precision and agility. By meticulously addressing the limitations of existing systems, our solution is engineered to provide not only a robust defense against electricity theft but also a user-friendly interface that prioritizes ease of use and accessibility. Through rigorous testing, comprehensive documentation, and a commitment to continuous improvement, our system endeavors to set new standards in the realm of electricity theft detection. The user-friendly interface, meticulously crafted utilizing the capabilities of the ESP32, not only empowers users with real-time monitoring capabilities but also integrates sophisticated alerting mechanisms for immediate response to potential theft incidents, ensuring swift action when needed most. Furthermore, our project underscores the paramount importance of a continuous improvement phase, where user feedback is systematically collected and iterative updates are implemented to refine system efficiency and effectiveness, with a particular emphasis on enhancing the user interface and overall user experience. In essence, our proposed system represents a holistic approach to addressing the multifaceted challenges posed by electricity theft, integrating advanced sensor networks with a robust analytical framework to fortify power distribution systems against this pervasive threat, and pave the way for a more resilient and sustainable energy future.

- **Proposed Solutions and Innovations:**
 - **Leveraging Advanced Sensor Networks:** Our proposed solution aims to overcome existing limitations by utilizing advanced sensor networks.

- **ESP32 Microcontroller Integration:** The system integrates the ESP32 microcontroller to enhance communication, data processing, and scalability.
- **Robust Analytical Framework:** Incorporating a robust analytical framework to address false positives/negatives and enhance reliability.
- **Continuous Improvement:** Emphasizing a continuous improvement phase to gather user feedback and implement iterative updates for enhanced effectiveness.
- **Overall Vision:**
 - The proposed system seeks to revolutionize power theft detection and mitigation strategies by addressing existing limitations and integrating innovative technologies.
 - Through comprehensive testing, documentation, and user-centric design, we aim to set new standards in power theft monitoring systems, ensuring reliability, effectiveness, and scalability.
 - Ultimately, our goal is to fortify power distribution systems against the pervasive threat of electricity theft, contributing to a more resilient and sustainable energy infrastructure.

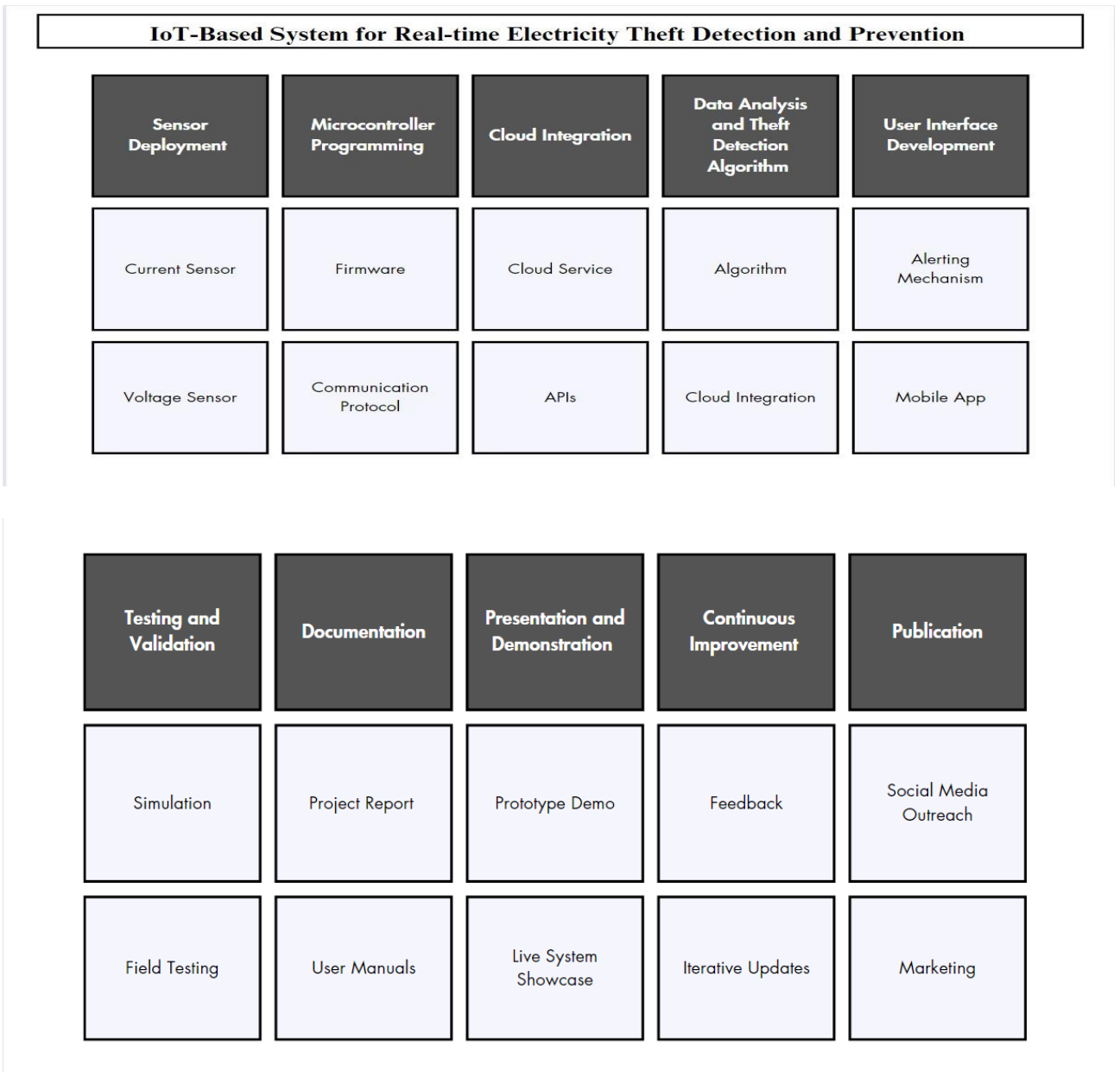


Fig. 3.1 Workflow of the solution

3.3 REQUIREMENT SPECIFICATION

- The Smart Electricity Theft Detection System introduces a sophisticated methodology for electricity theft detection, leveraging advanced sensor networks connected to the ESP32 microcontroller.
- The final prototype of the system integrates cutting-edge hardware components, including the ESP32 microcontroller, ZMPT101B AC single-phase voltage sensor, and ACS712 5A current sensor, offering a robust and sophisticated solution.
- The system involves rigorous testing, including simulations for theoretical validation and field testing for real-world performance evaluation.
- Comprehensive documentation, including detailed project reports and user manuals, ensures transparency and serves as a valuable reference for future development.
- The project culminates in a continuous improvement phase, where user feedback is systematically collected and iterative updates are implemented to refine system efficiency, particularly focusing on enhancing the user interface and overall user experience.
- The ESP32 microcontroller serves as the nerve center of the system, orchestrating seamless communication between sensors, real-time data acquisition, and intricate processing.
- The system's technical prowess includes high-speed data transfer, real-time analysis of voltage and current differentials, and cybersecurity measures to ensure the integrity of collected data.
- The system's architecture involves the strategic deployment of voltage and current sensors at critical points, microcontroller programming, cloud integration, algorithmic core enriched by machine learning, user interface development, rigorous testing, and comprehensive documentation.
- The system's hardware components include the ZMPT101B AC single-phase voltage sensor, ACS712 5A current sensor, and ESP32 microcontroller, while the software requirements encompass firmware development, communication protocols, backend/cloud-based software, and user interface development.

- The system not only provides a sophisticated solution to unauthorized power consumption but also ensures a commendable balance of simplicity and accuracy, leveraging the capabilities of the ESP32 microcontroller and efficient communication protocols to achieve real-time monitoring and swift detection of potential theft instances.

3.3.1 HARDWARE REQUIREMENTS

1. ESP32 Microcontroller:

- Acts as the central processing unit for data acquisition, communication, and analysis.
- Required for interfacing with sensors, managing data transmission, and executing detection algorithms.

2. Voltage Sensors:

- Deployed at power poles and primary supply meters to measure voltage levels.
- Essential for monitoring variations in voltage that may indicate electricity theft.

3. Current Sensors:

- Positioned at critical points in the distribution network to measure electrical currents.
- Necessary for detecting abnormal current flows associated with unauthorized power consumption.

4. Temperature Sensors:

- Installed at key locations to monitor environmental conditions and detect anomalies.

- Helps in identifying potential overheating or tampering of electrical infrastructure.

5. Communication Module:

- Enables wireless communication between the ESP32 microcontroller and external devices.
- May utilize Wi-Fi, Bluetooth, or other wireless protocols for data transmission.

6. Power Supply Unit:

- Provides stable power to the ESP32 microcontroller and connected sensors.
- Ensures continuous operation of the system without interruptions due to power fluctuations.

7. Enclosure/Casing:

- Protects the hardware components from environmental factors such as moisture, dust, and physical damage.
- Ensures durability and longevity of the system in outdoor or harsh conditions.

8. Mounting Hardware:

- Includes brackets, screws, and other mounting accessories for securely installing sensors and other components at designated locations.
- Facilitates proper positioning and alignment of hardware for accurate data collection.

9. Data Storage Device:

- Stores collected data for later analysis and reference.

- Can be in the form of internal memory within the ESP32 or external storage such as an SD card.

10. Backup Power Source:

- Optional but recommended for ensuring system functionality during power outages.
- Could be a battery backup or alternative power source to maintain operation continuity.

11. Networking Equipment:

- Includes routers, switches, and access points for establishing and maintaining network connectivity.
- Enables remote monitoring and control of the system through internet or intranet access.

12. Testing and Debugging Tools:

- Multimeter, oscilloscope, and other diagnostic instruments for verifying sensor accuracy and troubleshooting hardware issues.
- Essential for ensuring the reliability and performance of the system during installation and maintenance.

3.3.2 SOFTWARE REQUIREMENTS

The software requirements for the Smart Electricity Theft Detection System are meticulously outlined to ensure a robust and efficient implementation. The embedded software for ESP32 microcontrollers plays a central role, requiring the development of firmware to handle data acquisition, real-time analysis algorithms for theft detection, and support for secure wireless communication. Communication protocols between the ESP32 and other components within the sensor network are crucial, with a focus on standardized interaction and potential use of MQTT for IoT communication. The backend/cloud-based software involves

creating APIs for secure communication, implementing advanced algorithms, and ensuring stringent security measures. User interface development emphasizes a user-friendly experience with features for real-time data display and intuitive system status interpretation. Data logging capabilities, security features, remote control functionalities, alerting mechanisms, simulation tools, and comprehensive documentation and reporting tools contribute to the holistic software requirements. Seamless integration and compatibility among these software components are essential, with regular testing and debugging integral to ensuring reliability and accuracy throughout the development process.

CHAPTER 4

SYSTEM DESIGN

4.1 SYSTEM ARCHITECTURE

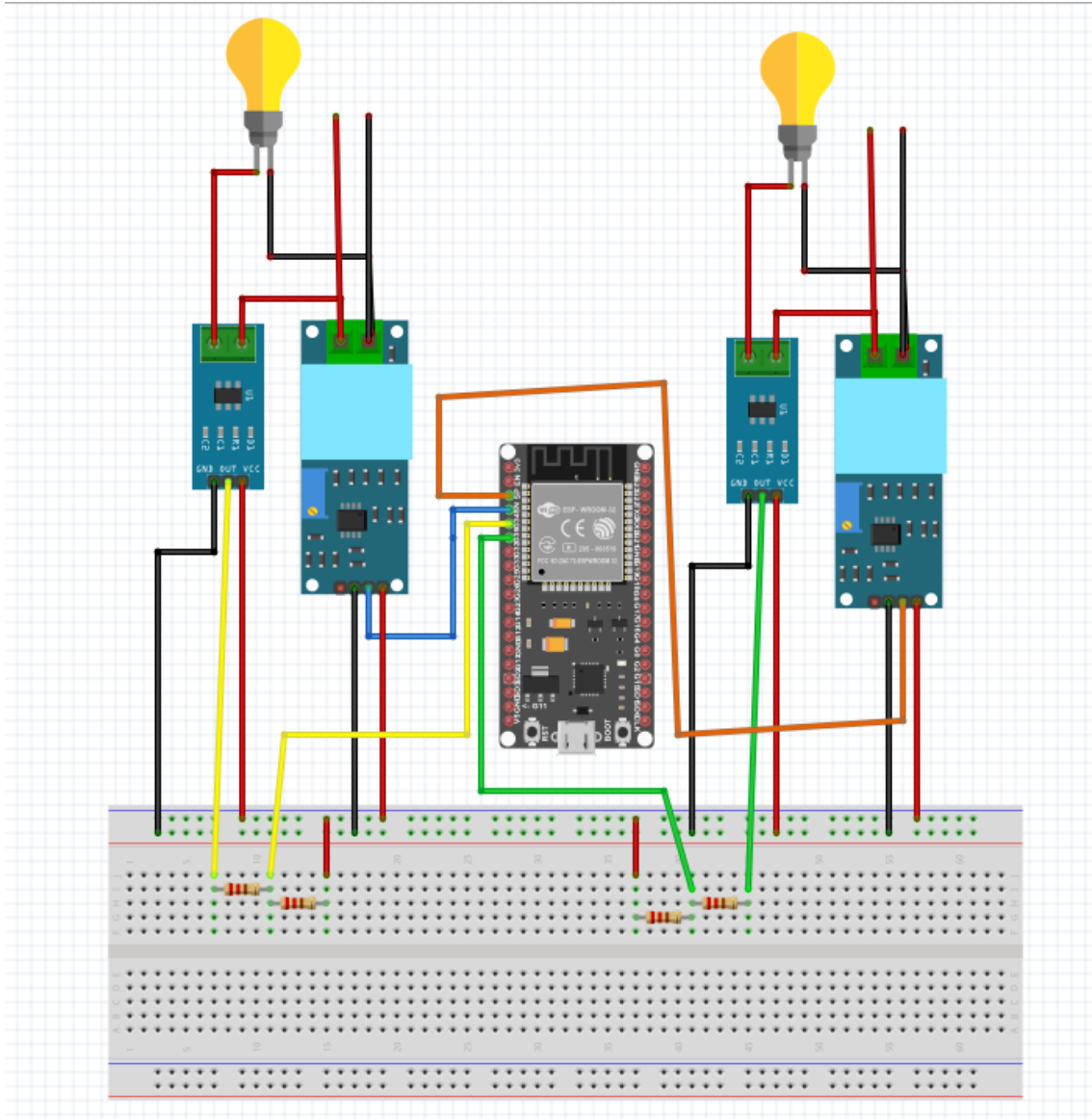


Fig. 4.1 Circuit diagram for the prototype

4.2 CIRCUIT DIAGRAM

The circuit for the Smart Electricity Theft Detection System involves a strategic integration of components to ensure accurate and efficient operation. At its core, the ESP32 microcontroller serves as the central processing unit, orchestrating the entire system. The voltage and current sensors, such as the ZMPT101B AC single-phase voltage sensor and the ACS712 5A current sensor, are deployed at critical points, namely power poles and meters. These sensors feed data to the ESP32 for real-time monitoring.

The ESP32 is programmed to handle data acquisition, theft detection algorithms, and wireless communication with the backend system. Communication protocols, possibly utilizing MQTT for IoT efficiency, facilitate seamless interaction between the ESP32 and the backend or cloud-based software. The backend, responsible for data storage, API development, and analysis algorithms, ensures a comprehensive approach to theft detection.

The user interface, whether through a web or mobile application, provides a real-time display, dynamic data visualization, and an intuitive design for easy interpretation. Additionally, the system incorporates data logging capabilities for historical data recording, security measures such as access control and encryption, and remote control functionalities.

The circuit diagram illustrates the interconnected components, showcasing a systematic design that enables a streamlined flow of information and effective electricity theft detection. This holistic approach to circuit design ensures the accuracy and reliability of the Smart Electricity Theft Detection System

The electricity theft detection system relies on a meticulously curated selection of sensors strategically positioned to ensure precise and reliable monitoring of the power distribution network. At the forefront of this sensor network is the voltage sensor, designed as a non-contact device capable of accurately measuring voltages within the expansive range of 0-1000V AC, boasting an impressive accuracy level of $\pm 1\%$. Its counterpart, the hall-effect current sensor, seamlessly complements the voltage sensor by covering a similarly broad range of 0-100A AC with a matching accuracy level, ensuring comprehensive coverage of current fluctuations indicative of potential theft activities.

Both the voltage and current sensors are equipped to provide either analog or digital output, a critical feature essential for seamless interfacing with the central processing unit, the ESP32 microcontroller. This powerhouse of a microcontroller, with its dual-core processor capable of reaching clock frequencies of up to 240 MHz, not only serves as the brain of the system but also facilitates wireless communication functionalities through Wi-Fi and Bluetooth protocols. Furthermore, the ESP32's integration of a 12-bit analog-to-digital converter ensures precise and accurate conversion of analog sensor readings into digital data, enabling sophisticated analysis and detection algorithms to be applied with confidence.

Optionally, the system may incorporate additional sensors to provide supplementary contextual data for a more comprehensive understanding of the environment. Temperature and humidity sensors offer insights into environmental conditions that may impact electrical infrastructure, while accelerometers can detect sudden movements or vibrations that could indicate tampering or unauthorized access. Additionally, GPS modules may be employed to track the geographical location of sensor nodes, enhancing situational awareness and facilitating targeted response strategies.

CHAPTER 5

MODULE DESCRIPTION

5.1 PROJECT MODULES

- The methodology involves the strategic deployment of voltage and current sensors at critical points, such as power poles and meters, to enable precise and reliable monitoring of power consumption.
- The subsequent phase delves into the intricacies of programming microcontrollers, specifically leveraging the ESP32, to develop firmware tailored for precise data collection and the implementation of intricate communication protocols.
- Following the sensor data collection, the project seamlessly integrates cloud services, involving the careful selection of a provider and the establishment of robust APIs for secure and seamless data transfer.
- The algorithm for real-time data analysis and theft detection is meticulously crafted and seamlessly incorporated into the cloud platform, with the ESP32 playing a central role in facilitating efficient communication between sensors and the cloud.
- The ESP32's capabilities, such as low power consumption and versatile communication interfaces, contribute to the project's overall efficiency.
- The system's architecture involves the strategic deployment of voltage and current sensors at critical points, microcontroller programming, cloud integration, algorithmic core enriched by machine learning, user interface development, rigorous testing, and comprehensive documentation.

- The culmination of these steps results in a robust project, with special emphasis on the ESP32's pivotal role in the system's architecture.
- The project culminates in a continuous improvement phase, where user feedback is systematically collected and iterative updates are implemented to refine system efficiency, particularly focusing on enhancing the user interface and overall user experience.

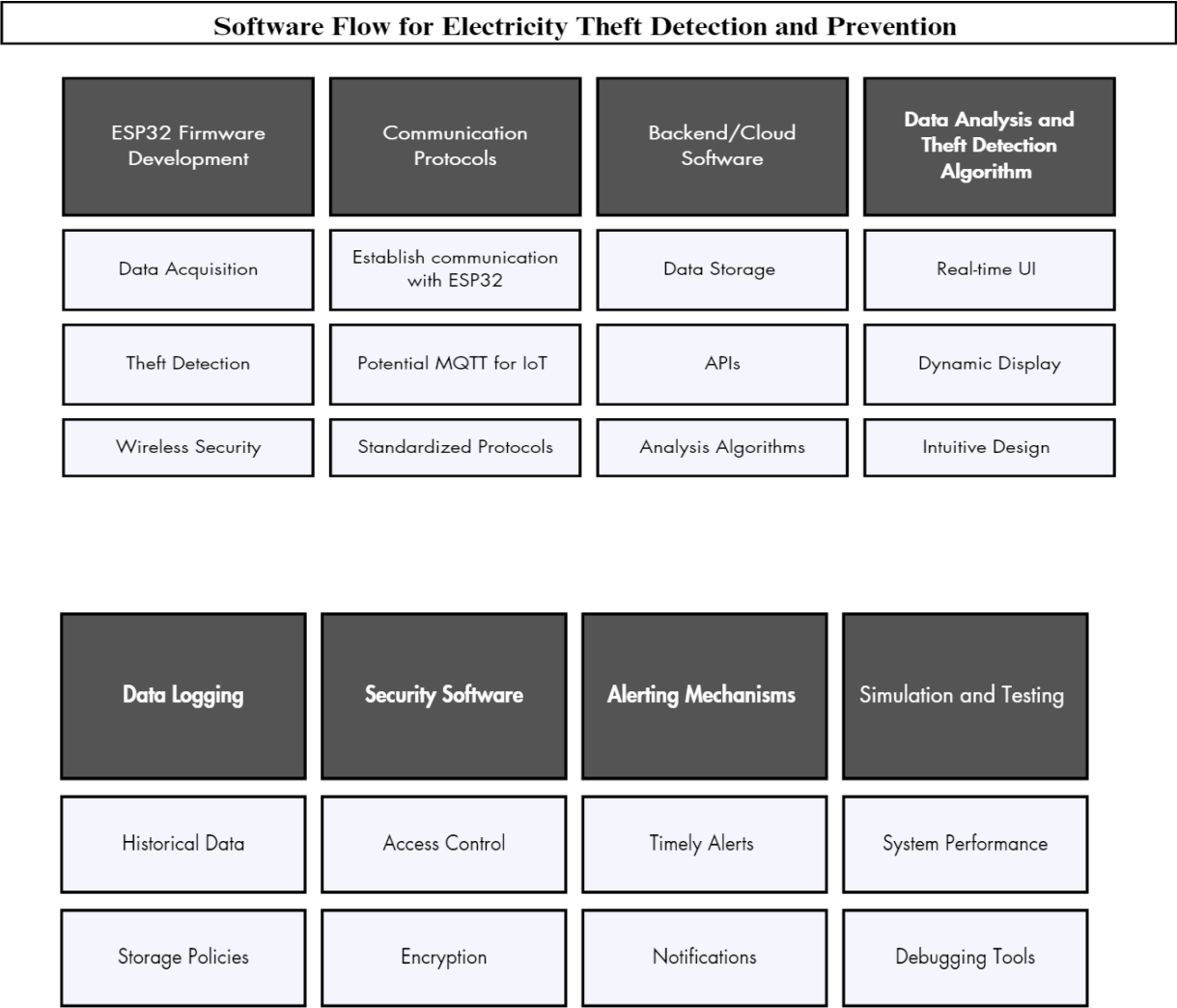


Fig. 5.1 Software process flow

5.2 CONCLUSION

In summary, the Smart Electricity Theft Detection System not only provides a sophisticated solution to the persistent challenge of unauthorized power consumption but does so with a commendable balance of simplicity and accuracy. Leveraging the capabilities of the ESP32 microcontroller, coupled with efficient communication protocols and a robust backend infrastructure, the system achieves real-time monitoring and swift detection of potential theft instances. The user-friendly interface adds an extra layer of accessibility, allowing users to effortlessly interpret and respond to the system's status. The incorporation of simulation tools and comprehensive testing ensures the reliability and effectiveness of the system. This project represents a noteworthy stride in the ongoing efforts to fortify the security and efficiency of power distribution systems, showcasing the potential impact of a straightforward yet precise approach to electricity theft detection.

5.3 FUTURE WORKS

- **Development of a Dedicated Mobile Application:**

- Empower users with remote monitoring capabilities.
- Provide real-time alerts and intuitive controls for enhanced user experience.

- **Integration of Machine Learning Algorithms:**

- Adapt and improve theft detection accuracy over time.
- Enable the system to dynamically respond to evolving patterns and behaviors.

- **Expansion of Sensor Network:**

- Cover broader areas for increased scalability.
- Cater to larger distribution networks and diverse deployment scenarios.

- **Exploration of Advanced Security Measures:**

- Implement biometric authentication or blockchain technology.
- Fortify the system against potential vulnerabilities and unauthorized access.

- **Incorporation of Detailed Energy Consumption Analysis:**

- Provide insights into consumption patterns and anomalies.
- Enhance understanding of electricity usage trends and potential theft indicators.

- Integration with Smart Grids:
 - Enable seamless interaction with existing infrastructure.
 - Enhance system efficiency and interoperability with grid management systems.

- Community Outreach Programs and Collaborations:
 - Engage with stakeholders and utility providers.
 - Foster partnerships to increase awareness and promote adoption of the detection system.

Through these future endeavors, the Smart Electricity Theft Detection System is poised to evolve into a sophisticated and holistic solution. It will not only address current challenges but also anticipate and mitigate emerging issues in the realm of electricity theft detection and prevention, ultimately contributing to a more secure and resilient power distribution network.

APPENDIX

SOURCE CODE :

```
#define BLYNK_PRINT Serial

#define BLYNK_TEMPLATE_ID "TMPL3xFPwMJz0"

#define BLYNK_TEMPLATE_NAME "1st House"


#include "EmonLib.h"

#include <WiFi.h>

#include <WiFiClient.h>

#include <BlynkSimpleEsp32.h>


EnergyMonitor emon;

EnergyMonitor emonmeter;

#define vCalibration 106.8

#define currCalibration 0.52

#define vCalibrationmeter 106.8

#define currCalibrationmeter 0.52

BlynkTimer timer;


char auth[] = "wddde50GdLs4RUPA8PLiWe-8EhN9ZghJ";
```

```

char ssid[] = "Amrithaa";

char pass[] = "Amrithaa000";


float kWh = 0;

float kWhmeter = 0;

float polewatt = 0;

float meterwatt = 0;

unsigned long lastmillis = millis();

unsigned long lastmillismeter = millis();


void pole(){

    emon.calcVI(20, 2000);

    Serial.print("Vrms: ");

    Serial.print(emon.Vrms, 2);

    Serial.print("V");

    Blynk.virtualWrite(V0, emon.Vrms);

    Serial.print("\tIrms: ");

    Serial.print(emon.Irms, 4);

    Serial.print("A");

    Blynk.virtualWrite(V1, emon.Irms);

    Serial.print("\tPower: ");

    polewatt = emon.apparentPower;

```

```

Serial.print(emon.apparentPower, 4);

Serial.print("W");

Blynk.virtualWrite(V2, emon.apparentPower);

Serial.print("\tkWh: ");

kWh = kWh + emon.apparentPower*(millis()-lastmillismeter)/3600000000.0;

Serial.print(kWh, 4);

Serial.println("kWh");

lastmillismeter = millis();

Blynk.virtualWrite(V6, kWh);

}

```

```

void meter(){

  emonmeter.calcVI(20, 2000);

  Serial.print("Vrms: ");

  Serial.print(emonmeter.Vrms, 2);

  Serial.print("V");

  Blynk.virtualWrite(V3, emonmeter.Vrms);

  Serial.print("\tlrms: ");

  Serial.print(emonmeter.Irms, 4);

  Serial.print("A");

  Blynk.virtualWrite(V4, emonmeter.Irms);

  Serial.print("\tPower: ");

  meterwatt = emonmeter.apparentPower;

```

```

Serial.print(emonmeter.apparentPower, 4);

Serial.print("W");

Blynk.virtualWrite(V5, emonmeter.apparentPower);

Serial.print("\tkWh: ");

kWhmeter      =      kWhmeter      +      emonmeter.apparentPower*(millis()-
lastmillis)/3600000000.0;

Serial.print(kWhmeter, 4);

Serial.println("kWh");

lastmillis = millis();

Blynk.virtualWrite(V7, kWhmeter);
}

void alert(){

  if (((polewatt - meterwatt) > 200) || ((meterwatt - polewatt)>200)){

  }

}

void myTimerEvent() {

  pole();

  meter();

  alert();

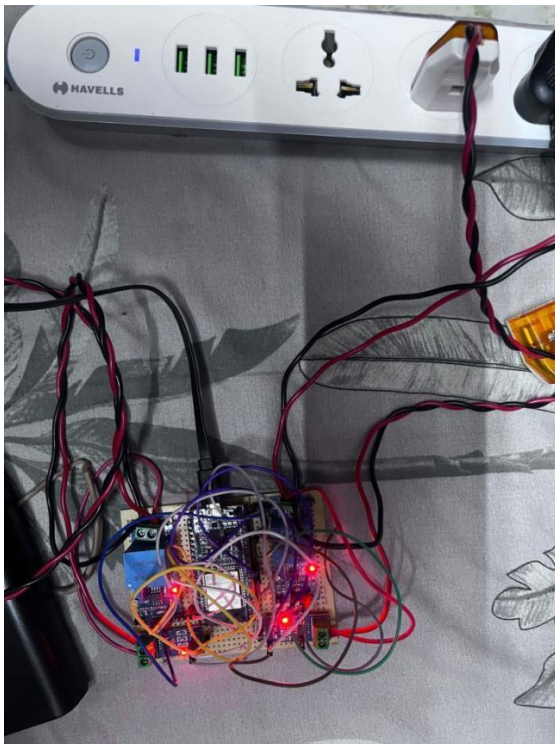
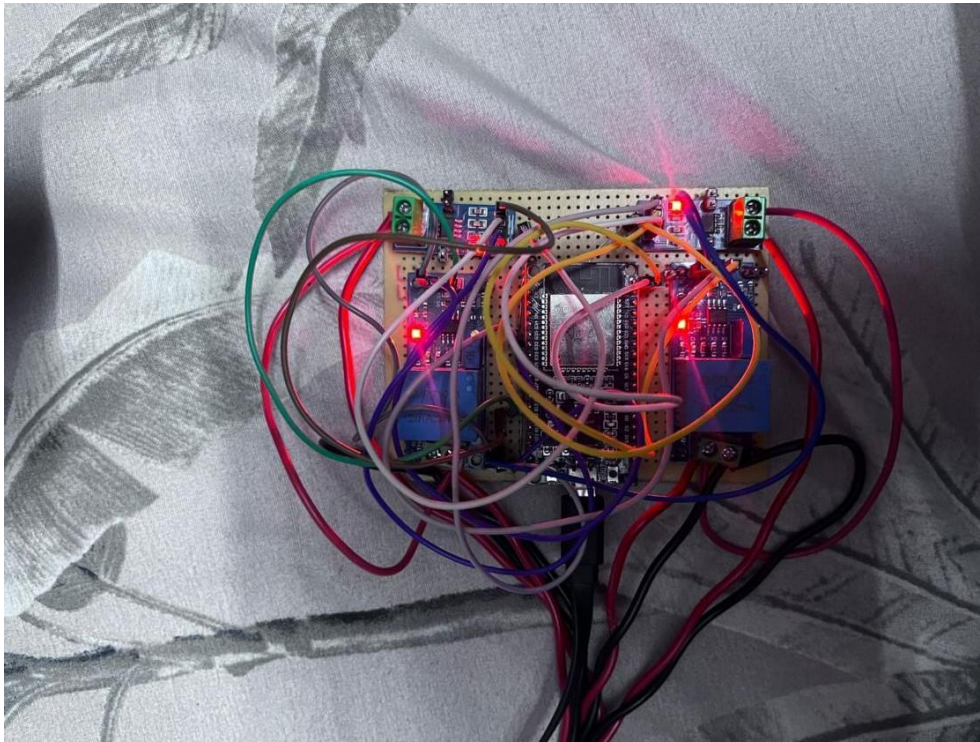
}

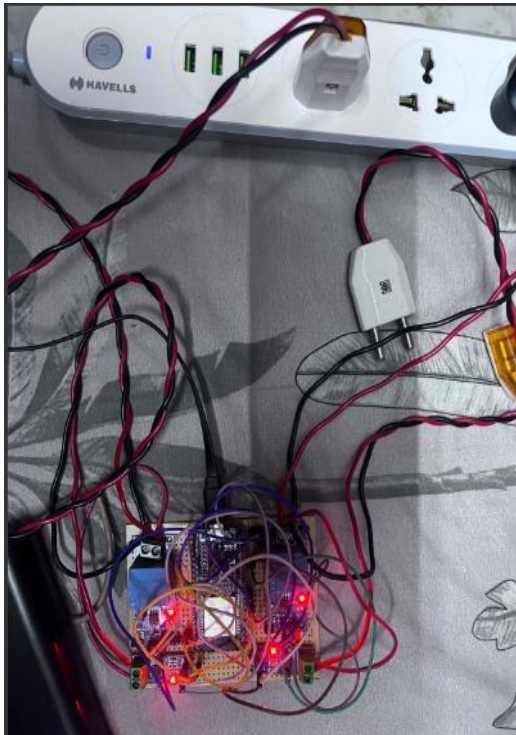
```

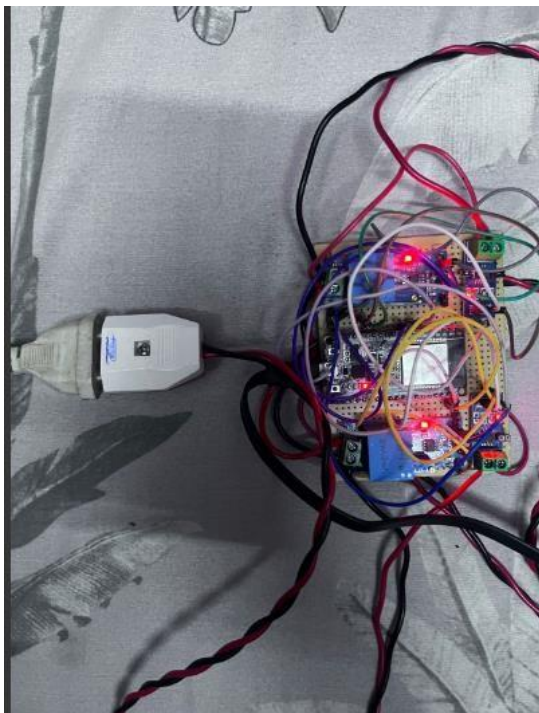
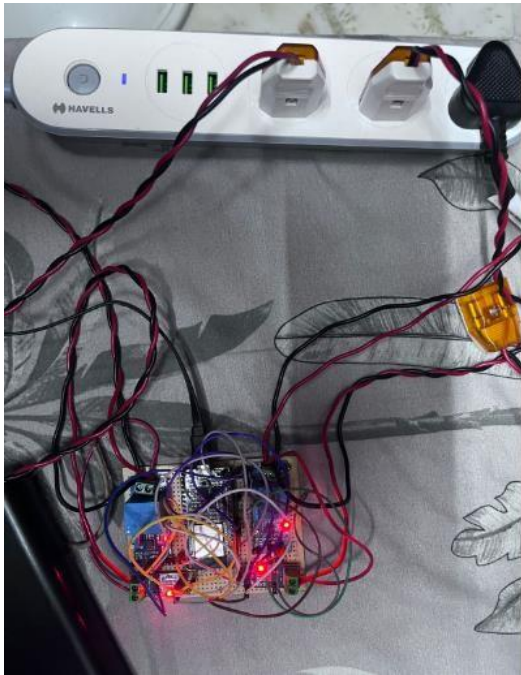
```
void setup() {  
  
  Serial.begin(9600);  
  
  emon.voltage(35, vCalibration, 1.7);  
  
  emon.current(34, currCalibration);  
  
  emonmeter.voltage(33, vCalibrationmeter, 1.7);  
  
  emonmeter.current(32, currCalibrationmeter);  
  
  Blynk.begin(auth, ssid, pass);  
  
  timer.setInterval(2000L, myTimerEvent);  
  
}
```

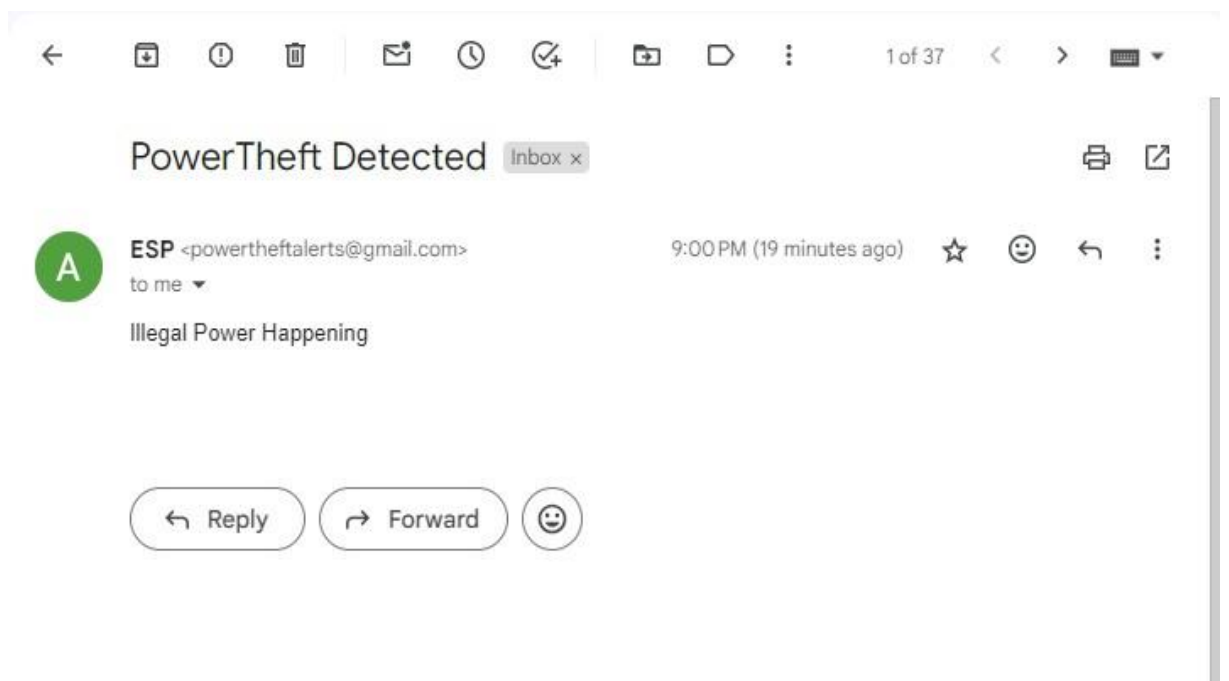
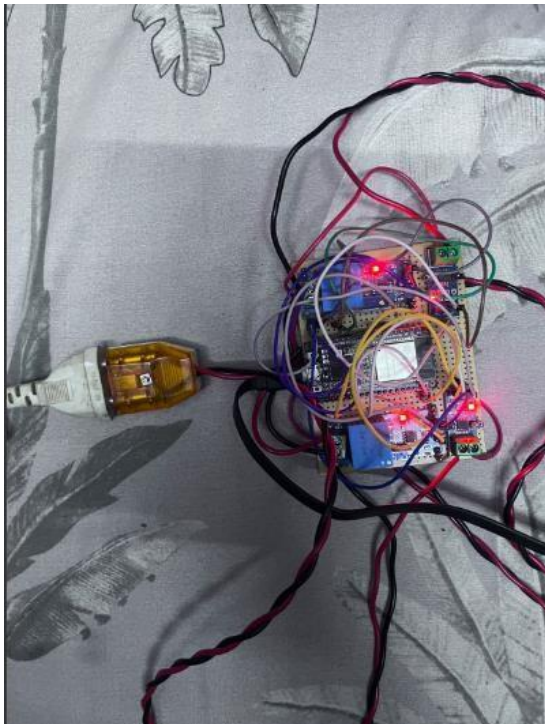
```
void loop() {  
  
  Blynk.run();  
  
  timer.run();  
  
}
```

OUTPUT :









REFERENCES

- [1] Zulu, C.L., Dzobo, O. Real-time power theft monitoring and detection system with double connected data capture system. *Electr Eng* 105, 3065–3083 (2023). <https://doi.org/10.1007/s00202-023-01825-3>
- [2] Rajasekaran, A., Sai, P. A., Teja, P. B., & Swetha Priya, P. G. S. (2020, March). IOT BASED POWER THEFT DETECTION. *International Journal of Scientific Development and Research*, 5(3), 249.
- [3] Meenal, R & Kuruvilla, Kevin & Denny, Adrin & Jose, Rejin & Roy, Renoy. (2019). Power Monitoring and Theft Detection System using IoT. *Journal of Physics: Conference Series*. 1362. 012027. 10.1088/1742-6596/1362/1/012027.
- [4] 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), Chennai, India, 2020, pp. 0262-0267, doi: 10.1109/ICCSP48568.2020.9182144.
- [5] Darteh, Oscar & Liu, Xiaodong & Liu, Qi & Anaadumba, Raphael & Adjei, Charity & Sarker, Sajib. (2020). Internet of Things Based Electricity Theft Detection Using Raspberry Pi.
- [6] M. U. Hashmi and J. . G. Priolkar, "Anti-theft energy metering for smart electrical distribution system," in 2015 International Conference on Industrial Instrumentation and Control, ICIC 2015, Maharashtra, 2015.
- [7] S. N. Vinay and M. R. Shubham , "WSN-POWER THEFT CONTROL," *International Research Journal of Engineering and Technology (IRJET)*, vol. 04, no. 01, p. 1984, 2018.
- [8] S. Thiruvalluvan, B. Swardheep and S. Arunachalam, "Power Theft Identification system using Power Line Carrier Communication (PLCC) technique in Distribution system based on Binary Search Algorithm," *International Conference on Computation of Power, Energy, Information and Communication (ICCPEIC-2013)*, p. 978, 2013. J. Clerk Maxwell, *A Treatise on Electricity and Magnetism*, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68-73.
- [9] S. Tshikomba, "How wireless electricity theft detection can assist in reducing electricity theft," 26th AMEU Technical Convention, Tshwane, 201.
- [10] S. Sardar and S. Ahmad, "Detecting And Minimizing Electricity Theft : A Review," Peshawar, 2016.

