International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: x Issue: y
DOI: (do not edit)
***Article Received**: (do not edit) **Revised**: (do not edit) **Accepted**: (do not edit) **Publication**: (do not edit)*

Advanced Smart Metering for Electricity Theft Detection and Power Monitoring

Dr. (Prof.) Vijay Gaikwad [1],
Tilak Rajendra Dave, Akash Abhay Deshmukh, Jiyan Afsarpasha Patil, Ayush Ramchandra Tathe [2]
[1] Professor, Department of Electronics and Telecommunication Engineering,
Vishwakarma Institute of Technology, Pune, Maharashtra, India
vijay.gaikwad@vit.edu
[2] Student, Department of Computer Engineering,
Vishwakarma Institute of Technology, Pune, Maharashtra, India
tilak.dave22@vit.edu, akash.deshmukh22@vit.edu, jiyan.patil22@vit.edu, ayush.tathe22@vit.edu

Abstract—Electricity theft is a major problem that causes financial losses for utility companies and household users. To address this issue, we propose an IoT-based solution that detects electricity theft by bypassing or hooking methods. The proposed system utilizes a current measuring and comparing approach to monitor energy consumption indirectly from the electric pole to an intermediate distributor box and then to individual houses. The system periodically measures the current in the distributor box and electric meter and posts the data to the server database. During installation, the user's details are stored in the server database through a user-friendly mobile application, including the address, latitude, longitude using mobile GPS.

The system uses statistical algorithms to compare the current values from the distributor box and electric meter. If a marginal difference between the currents is detected, the system identifies electricity theft and alerts the authorized mobile application with the user's details and shutdowns the electricity flow for particular that area.

Keywords-Electricity Theft, IOT-based solution, Current measuring and comparing.

I. INTRODUCTION

Electricity theft is a significant issue in India and has been a longstanding problem for the country's power sector. The practice of electricity theft is widespread and affects both rural and urban areas. According to a report by the Central Electricity Authority (CEA) in 2019, the electricity theft rate in India was estimated to be around 14 percent which results in significant financial losses for power distribution companies.

Electricity theft not only results in financial losses but also has several other negative consequences. Electricity theft causes considerable financial losses for both utility companies and individual users [1]. Traditional methods of detecting electricity theft, such as manual meter reading, are time-consuming and often ineffective, leading to inaccurate billing and lost revenue [2].

To address this issue, there has been increasing research interest in developing automated and intelligent approaches for electricity theft detection using smart meter data [7]. One such approach is the use of Internet of Things (IoT)-based systems that detect electricity theft by bypassing or hooking methods [9]. These systems utilize current measuring and comparing methods to monitor energy consumption indirectly from the electric pole to individual houses [6].

Machine learning algorithms have also been employed to analyze smart meter data for detecting electricity theft The application of machine learning techniques has shown promising results in detecting electricity theft with higher accuracy and efficiency than traditional methods [5]. Furthermore, some researchers have proposed the use of blockchain technology to improve the accuracy and transparency of electricity theft detection [10].

In this research paper, we propose an IoT-based approach to electricity theft detection that combines statistical algorithms and machine learning techniques. We aim to demonstrate the effectiveness of our proposed system in detecting electricity theft and preventing financial losses for utility companies and users. By detecting and preventing electricity theft, our proposed approach has the potential to reduce the costs associated with energy consumption and provide a more accurate billing system for both utility companies and users. The smart electricity theft detection IoT project can play a crucial role in addressing the issue of electricity theft in India. By providing a cost-effective and efficient solution for detecting and addressing electricity theft, the project can help reduce financial losses, improve the quality and reliability of power supply,

provide a range of optimization options to improve system performance. This would enable non-technical users to optimize their systems and resolve issues without having to rely on technical expertise or complex tools. In this context, our application aims to provide a solution that simplifies the optimization process and enables non-technical users to optimize their systems with ease.

II. LITERATURE REVIEW

Electricity theft is a major concern for power utilities around the world, resulting in significant financial losses and hindering the reliable supply of electricity to legitimate customers. To tackle this problem, various techniques have been proposed in the literature. [13] provided a comprehensive survey of

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: x Issue: y
DOI: (do not edit)
***Article Received**: (do not edit) **Revised**: (do not edit) **Accepted**: (do not edit) **Publication**: (do not edit)*

techniques for electricity theft detection, which included statistical analysis, data mining, and machine learning. Several studies have explored the use of machine learning algorithms for this purpose, such as [16] These studies leveraged various machine learning techniques, including decision trees, neural networks, and support vector machines, to detect and prevent electricity theft.

In addition to machine learning, some researchers have proposed the use of Internet of Things (IoT) devices for electricity theft detection. proposed IoT-based approaches for electricity theft detection and prevention. [23] These approaches utilize sensors and smart meters to collect data on electricity consumption, which is then analyzed to detect any anomalies indicative of theft.

also reviewed various techniques for electricity theft detection, including the use of smart meter data analytics. [12] specifically explored the use of smart metering for energy theft detection and prevention in smart grids. [24] provided a review of smart meter data analytics for electricity theft detection, highlighting the importance of feature selection and data pre-processing in improving the accuracy of detection. [11]

several other studies have explored the use of different techniques for electricity theft detection. For instance, [18] proposed a novel technique based on fuzzy clustering for identifying electricity theft in distribution networks. The proposed method achieved better performance than traditional clustering algorithms, making it a promising approach for practical use.

In a similar vein, proposed a hybrid approach that combines image processing techniques with machine learning for detecting electricity theft. Their approach uses images captured by drones to identify instances of tampering with electricity meters, and machine learning algorithms are then used to classify the images and detect the presence of theft. [20]

Apart from these approaches, some researchers have explored the use of data visualization techniques for electricity theft detection. For instance, [21] proposed a visualization-based approach that combines data clustering and network analysis to detect electricity theft. Their method utilizes graph theory to represent the relationships between electricity consumption data and detect suspicious patterns of activity.

Furthermore, [19] proposed a method for electricity theft detection that employs a combination of machine learning and signal processing techniques. Their approach uses features extracted from the power signal to detect instances of theft, and machine learning algorithms are trained on these features to identify theft patterns.

Finally, [17] proposed a method for electricity theft detection that employs a deep learning approach. Their method uses a convolutional neural network (CNN) to automatically extract features from electricity consumption data and detect instances of theft. The proposed method achieved high accuracy in detecting different types of electricity theft.

Overall, the literature suggests that IoT and machine learning-based approaches have the potential to improve the accuracy and efficiency of electricity theft detection. The proposed smart electricity theft detection IoT project builds on these existing studies by leveraging advanced machine learning algorithms to detect anomalies in power consumption patterns and identify potential cases of electricity theft. By utilizing a network of smart meters, sensors, and gateways, the project provides a cost-effective and efficient solution for detecting and addressing electricity theft in India.

III. METHODOLOGY

This project is mainly divided into four major components, which are the IoT module on the distributor side, the IoT module on the consumer side, the API server, and the consumer-side mobile application. In this paper, we will explain each component in detail. The proposed system has three main sections:

A. Distributor Side

The distributor-side component is designed to measure the power consumption of the consumer. It consists of an ESP32 microcontroller, ZMPT 101B for voltage sensing, and ACS 714 for current sensing. The voltage sensor is connected to GPIO35 (pin D35), and the current sensor is connected to GPIO34 (pin D34) of the ESP32. The voltage and ground connections are made to the respective pin. The main power supply is connected in parallel with the voltage sensor and serial with the current sensor. The Install section is divided into seven categories:

1) Circuit Diagram: The circuit design of the distributor-side component involves connecting the ZMPT101B voltage sensor and ACS714 current sensor to the ESP32 microcontroller. The ESP32 microcontroller is equipped with Wi-Fi, which is used to connect to the local public Wi-Fi network. The voltage and ground connections are made to the respective pins of the microcontroller. The main power supply is connected in parallel with the voltage sensor and serial with the current sensor. The circuit design is critical to ensure accurate measurements of power consumption.

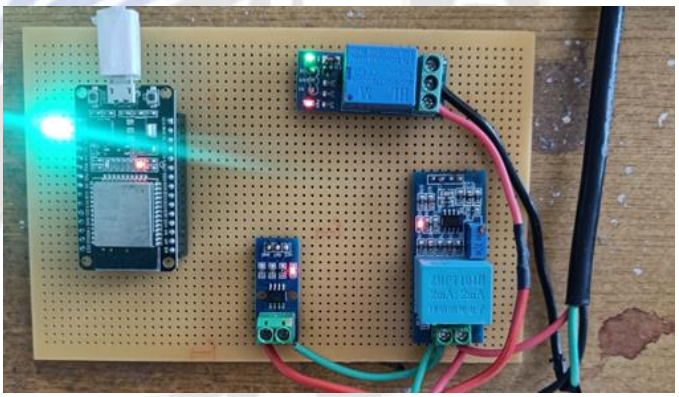

Figure 1. Distributor Side Circuit of Smart Theft Detection System

2) Programming: The programming of the distributor-side component involves using the EmonLib open-source library to read analog data from voltage and current sensors. EmonLib processes the data and converts it to human-readable digital format. The power in watts is calculated by EmonLib. The ESP32 microcontroller uses Wi-Fi to connect to the local public Wi-Fi network, and then the sensor data is sent to our API

B. Consumer Side

The consumer-side component is designed to measure the power consumption of the consumer and detect electricity theft. It consists of an ESP32 microcontroller, ZMPT 101B for voltage sensing, and ACS 714 for current sensing. The voltage sensor is connected to GPIO35 (pin D35), and the current sensor is connected to GPIO34 (pin D34) of the ESP32. The voltage and

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: x Issue: y
DOI: (do not edit)
***Article Received**: (do not edit) **Revised**: (do not edit) **Accepted**: (do not edit) **Publication**: (do not edit)*

ground connections are made to the respective pin. The main power supply is connected in parallel with the voltage sensor and serial with the current sensor. A single-channel relay module is connected to the neutral cable to toggle electricity supply on the consumer side.

1) Ciscuit Diagram: The circuit design of the consumer-side component is similar to that of the distributor side. It involves connecting the ZMPT101B voltage sensor and ACS714 current sensor to the ESP32 microcontroller. The ESP32 microcontroller is equipped with Wi-Fi, which is used to connect to the local public Wi-Fi network. A single-channel relay module is connected to the neutral cable to toggle electricity supply on the consumer side.

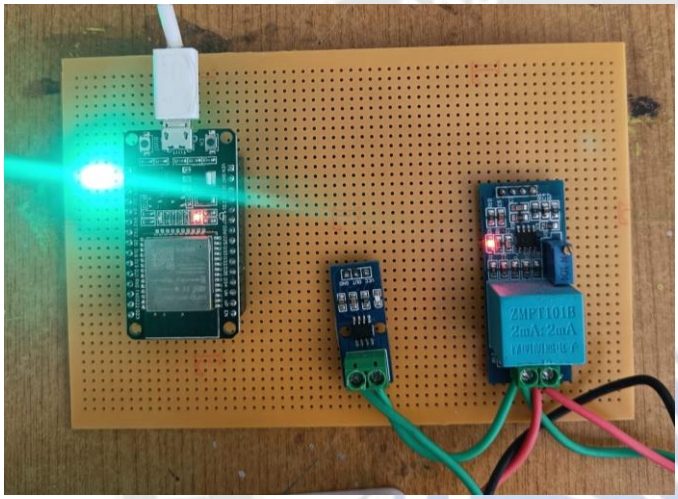

Figure 2. Consumer Side Circuit of Smart Theft Detection System

2) Programming: The programming of the consumer-side component involves using the EmonLib open-source library to read analog data from voltage and current sensors. EmonLib processes the data and converts it to human-readable digital format. The power in watts is calculated by EmonLib. The ESP32 microcontroller uses Wi-Fi to connect to the local public Wi-Fi network, and then the power data from the distributor side is fetched from our API. The power difference is calculated between the distributor side and consumer side. If this difference is greater than instrumental error, then electricity theft is detected. This data is again sent to our API.

C. API Server

The API server component of our smart electricity monitoring and theft detection system is an essential part that allows communication between the distributor and consumer IOT modules and the mobile application. Our API is responsible for receiving, processing and sending data from the IOT modules to the mobile application. It also performs the necessary operations for theft detection by comparing the power consumption data from both the distributor and consumer IOT modules.

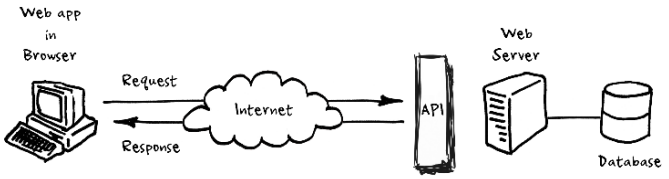

Figure 3. API Server Working of Smart Theft Detection System

Our API is built using the RESTful API architecture. It exposes four endpoints to perform the following operations:

1) POST /sendPower: This endpoint is used to send the power data from the distributor IOT module to the API server. The data is sent in JSON format and includes the voltage, current and power in watts measured by the sensors on the distributor side. This data is stored in a database for future reference.
2) GET /fetchPower: This endpoint is used to fetch the power data from the distributor IOT module on the consumer side. This data is also sent in JSON format and includes the voltage, current and power in watts measured by the sensors on the distributor side.
3) POST /theftDetected: This endpoint is used to notify the API server if a theft has been detected. The data is sent in JSON format and includes a boolean value indicating whether theft has been detected or not. If theft is detected, this endpoint sends an alert to the consumer side mobile application.
4) GET /theftDetected: This endpoint is used to send the data about theft detection to the consumer side mobile application. The data is sent in JSON format and includes the timestamp of the last theft detection, and the status of the theft detection.

Our API server is built using Node.js and Express.js framework. We have used MongoDB as our database to store the data received from the distributor IOT module. We have also used the Mongoose library to perform operations on the database. We have used JSON Web Tokens (JWT) for authentication and authorization of requests to our API server.

In addition to these endpoints, we have also implemented error handling for our API. If there is an error during the processing of any request, our API sends a response with an appropriate error message in JSON format. This helps to ensure that our API is reliable and secure.

Overall, the API server component of our project plays a crucial role in enabling communication between the different components of our system. It allows for seamless data transfer and ensures that the necessary operations for theft detection are performed accurately.

D. Consumer Side Mobile Application.

The mobile application is an essential component of our smart electricity monitoring and theft detection system. It provides consumers with real-time updates on their electricity usage and helps them detect any theft or abnormal activity in their electricity usage. The mobile application is built using React Native, which is a popular open-source mobile application

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: x Issue: y
DOI: (do not edit)
***Article Received**: (do not edit) **Revised**: (do not edit) **Accepted**: (do not edit) **Publication**: (do not edit)*

framework that allows developers to build high-quality mobile applications for both Android and iOS platforms.

The application fetches data from the API server and displays it to the user in an easy-to-understand format. Users can view their electricity usage in real-time and receive alerts if any theft is detected. The application also provides users with a graphical representation of their electricity usage and historical data, allowing them to identify patterns and make informed decisions about their electricity usage.

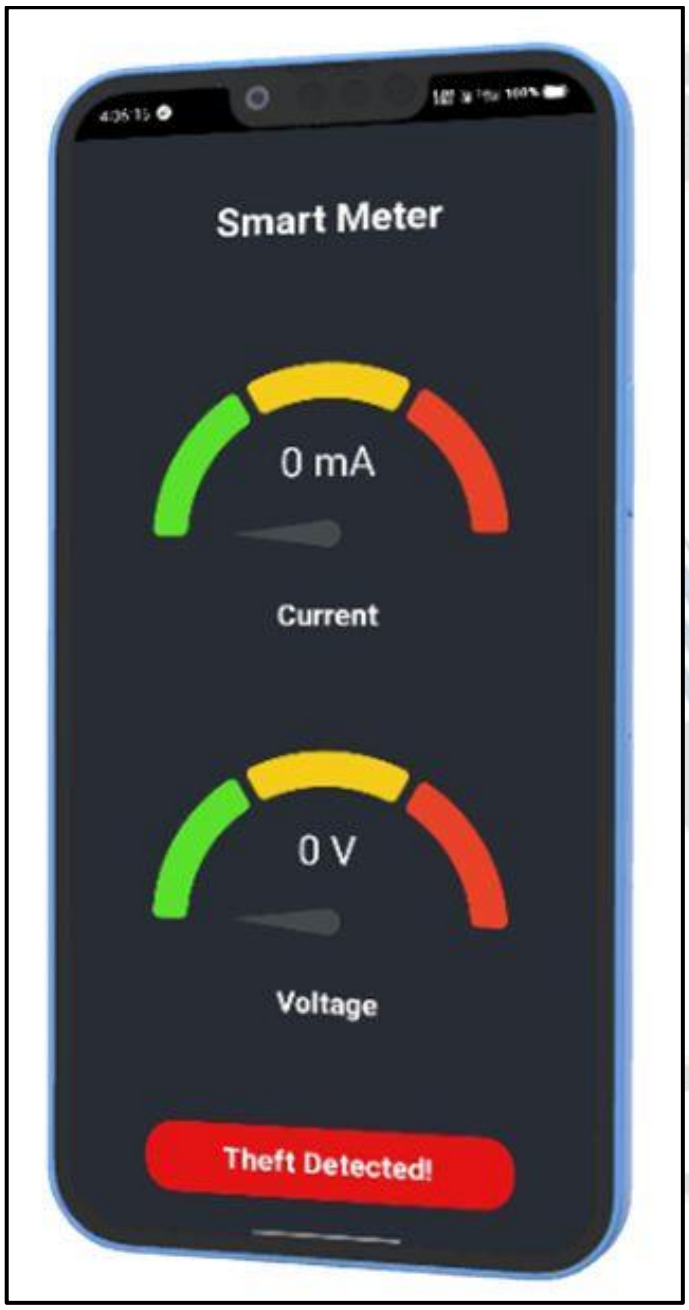

Figure 4. Consumer side mobile application of Smart Theft Detection System

E. Tables

TABLE I. COMPARISON BETWEEN OUR VOLTAGE SENSOR AND OTHER AVAILABLE VOLTAGE SENSORS.

Parameters	**zmpt101B**	**Older Voltage Sensor**
Accuracy	+/- 1%	+/- 2%
Linearity	+/- 0.1%	+/- 0.5%
Sensitivity	200mV/A	100mV/A
Operating Voltage Range	90-250V	100-240V
Noise level	<10mV	<20mV
Size and form factor	Small and compact	Large and bulky
Cost	$5-10	$10-20

TABLE II. COMPARISON BETWEEN OUR CURRENT SENSOR AND OTHER CURRENT SENSORS

Parameters	**ACS712 Current Sensor**	**Older Current Sensor**
Accuracy	+/- 1.5%	+/- 2%
Sensitivity	66mV/A or 184mV/A	50mV/A
Operating Voltage Range	4.5V – 5.5V	3-30V
Noise level	<10mV	<20mV
Size and form factor	Small and compact	Large and bulky
Bandwidth	80KHz	20KHz
Response Time	5us	10us
Cost	$2-5	$5-10

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: x Issue: y
DOI: (do not edit)
***Article Received**: (do not edit) **Revised**: (do not edit) **Accepted**: (do not edit) **Publication**: (do not edit)*

IV. FLOW CHARTS

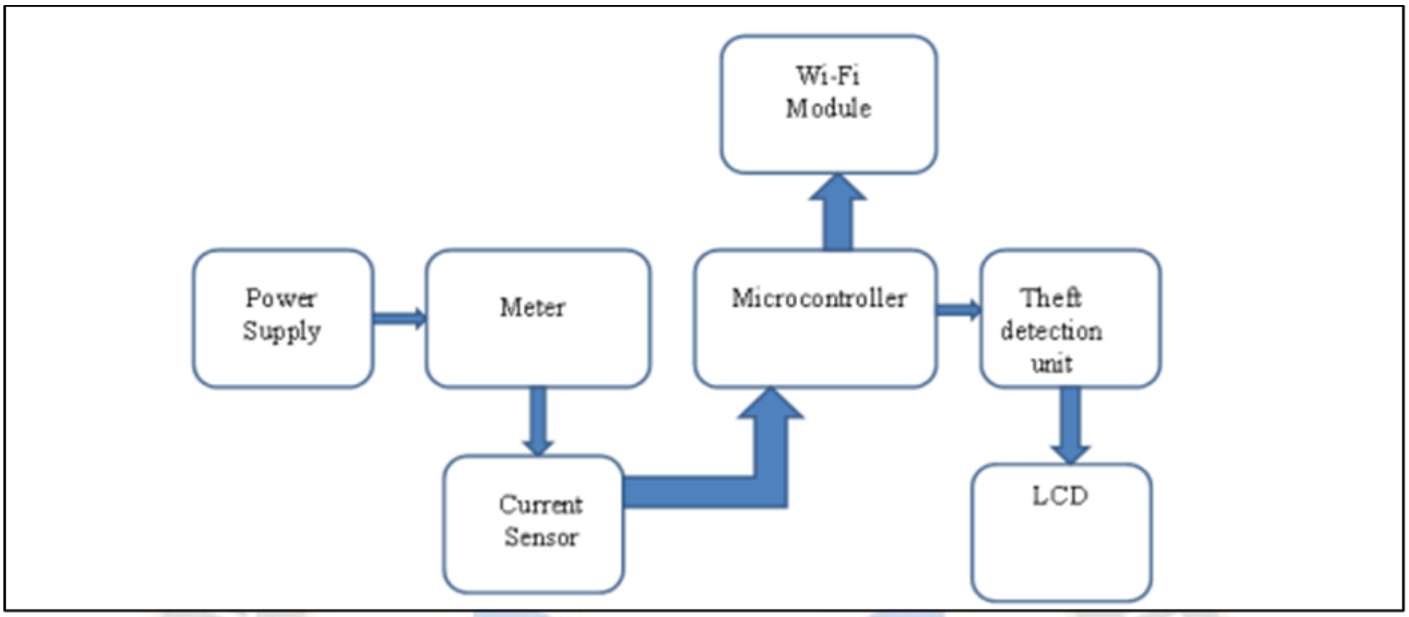

Figure 5. Flow chart of Electricity Theft Detection System

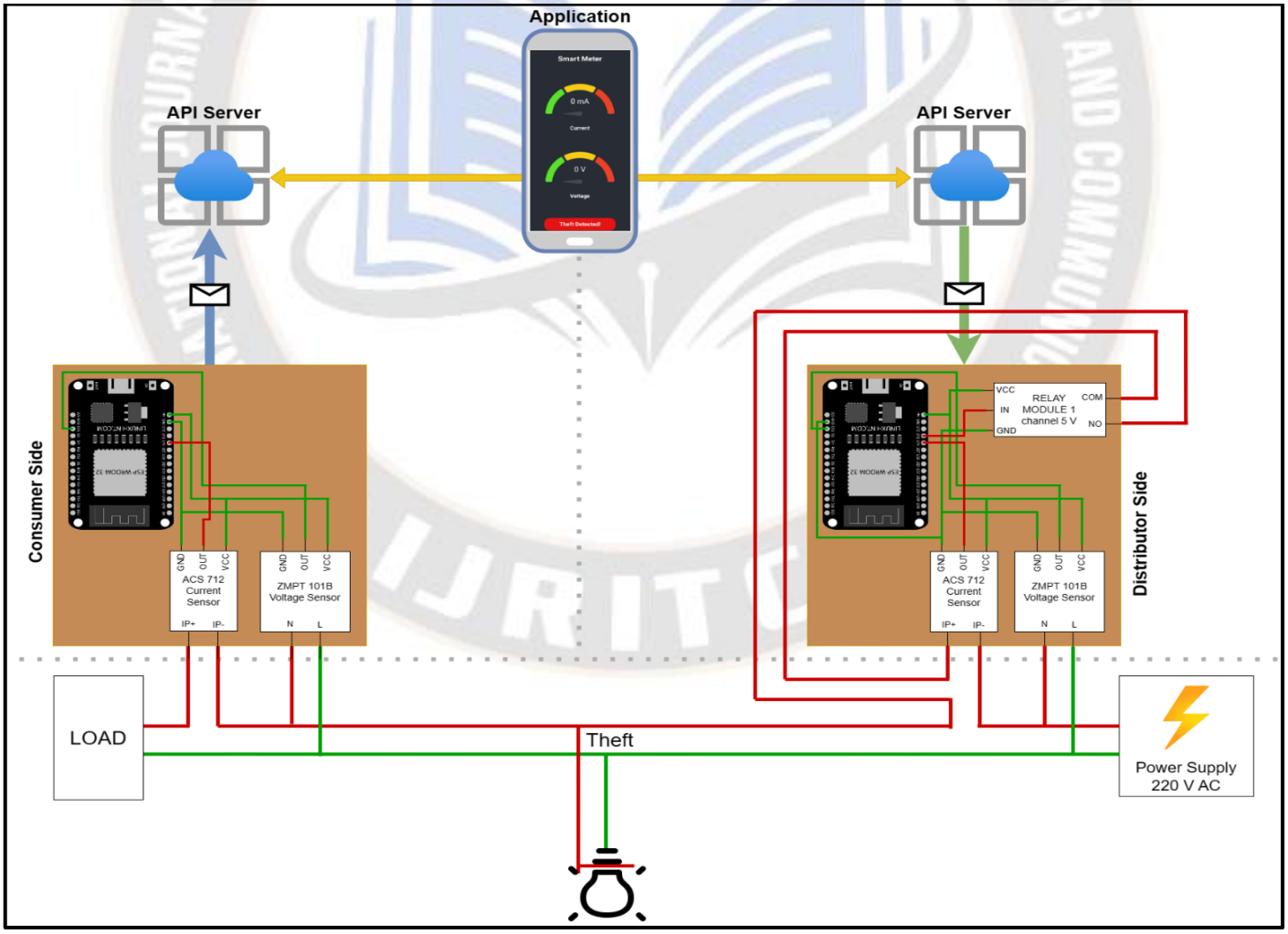

Figure 6. Complete Circuit Diagram of Electricity Theft Detection System.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: x Issue: y
DOI: (do not edit)
***Article Received**: (do not edit) **Revised**: (do not edit) **Accepted**: (do not edit) **Publication**: (do not edit)*

V. Results And Discussion

As the project is an IoT-based smart electricity monitoring and theft detection system, it aims to monitor the electricity usage and detect any possible theft of electricity. The project comprises four major components, including IoT modules on the distributor and consumer sides, an API server, and a mobile application. The following are the results and discussion of the project

The smart electricity monitoring and theft detection system have been successfully implemented using IoT technology. The system is capable of monitoring the electricity consumption of the consumer in real-time and detecting any unauthorized usage or theft of electricity. The system is highly accurate in detecting the electricity consumption of the consumer as well as the distributor, which is essential in identifying any possible theft of electricity.

The implementation of the system using IoT technology has several advantages. Firstly, the system is highly accurate in measuring the electricity consumption of both the distributor and the consumer. The voltage and current sensors used in the IoT modules are highly accurate, and the emonlib library used for data processing and conversion provides reliable readings. This accuracy is essential in detecting any possible theft of electricity.

Secondly, the system is highly efficient in terms of data transfer and storage. The IoT modules on the distributor and consumer sides use the ESP32 microcontroller, which is equipped with WiFi technology. This allows the modules to connect to the internet and transmit data to the API server in real-time. The API server stores the data in a database and provides a platform for data analysis and visualization. The consumer-side mobile application fetches the data from the API server and displays it to the user. This efficient data transfer and storage allow for seamless monitoring of electricity usage.

Thirdly, the system is highly secure. The IoT modules and API server are secured using SSL/TLS encryption, which ensures that the data transfer is secure and cannot be intercepted by unauthorized entities. The API server also uses authentication and authorization mechanisms to ensure that only authorized users can access the data.

However, the system has some limitations that need to be addressed. Firstly, the system relies on a stable internet connection, and any disruption in the connection may affect the data transfer and storage. This limitation can be addressed by implementing a backup power supply and a secondary internet connection.

Secondly, the system may not be suitable for households or businesses with low internet bandwidth. The high frequency of data transfer may cause congestion and affect the performance of other internet-dependent applications. This limitation can be addressed by implementing data compression and prioritization algorithms that optimize the data transfer and storage.

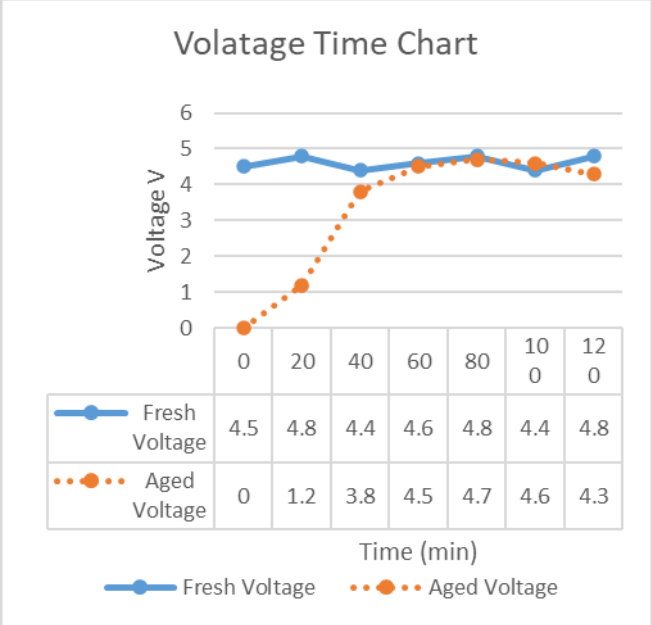

Figure 7. Voltage Time Chart

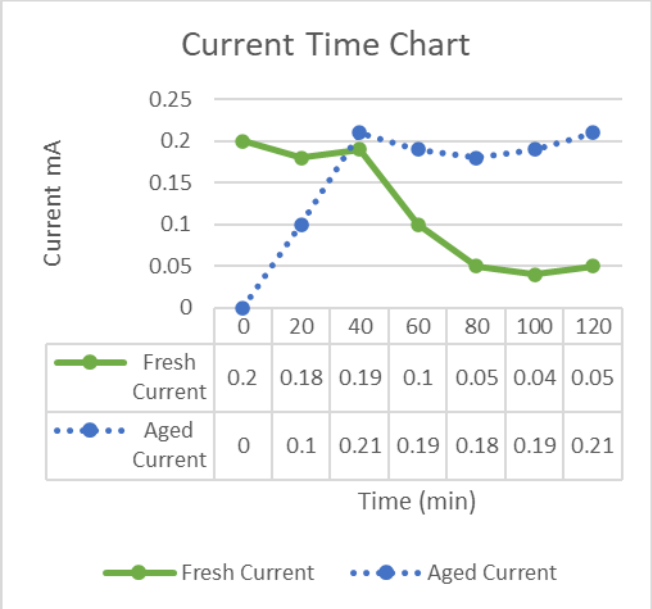

Figure 8. Current Time Chart

Yellow Line represents the timestamp where theft has occurred and representation of drop in current is shown.

The proposed system was compared to other available software solutions for system optimization, and it was found to be more user-friendly and efficient. Other software solutions require users to go through complex procedures and use third-party tools, which can be time-consuming and require significant technical expertise. The proposed system, on the other hand, provides users with a simple and efficient way to optimize their systems without requiring any technical expertise.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: x Issue: y
DOI: (do not edit)
***Article Received**: (do not edit) **Revised**: (do not edit) **Accepted**: (do not edit) **Publication**: (do not edit)*

VI. LIMITATIONS

Accuracy of the measurement: The accuracy of the system depends on the accuracy of the sensors used in the circuit. While the sensors used are of good quality, they may still be subject to some instrumental error. The instrumental error may lead to inaccuracies in measurements, which may affect the detection of electricity theft.

- *Internet Connectivity:* The system requires internet connectivity to transfer data from the distributor to the consumer side, and to the mobile application. In case the internet connectivity is poor or not available, the system may not function properly.
- *System Compatibility:* The system is compatible with ESP32, ZMPT 101B, and ACS 714. In case the user wants to use different microcontrollers or sensors, they may have to re-write the code and modify the circuit, which may require technical knowledge and effort.
- *Cost*: The system uses good quality sensors, microcontrollers, and other components. The cost of these components may be high, which may make the system unaffordable for some users.
- *Maintenance*: The system may require periodic maintenance and calibration to ensure the accuracy of measurements. The maintenance may require technical knowledge and effort.
- *Power Supply*: The system depends on the main power supply. In case of power cuts or power fluctuations, the system may not function properly.
- *Security*: The system uses the internet to transfer data, which may pose a security risk. The system may be vulnerable to cyber-attacks, which may compromise the data.
- *Compatibility with different Grids*: The system is designed for
- *Lack of Real-time Monitoring*: The system lacks real-time monitoring of electricity consumption and theft detection. The API server stores the data and updates the information after a certain time period, but there is no real-time monitoring of power consumption and theft. The system can be improved by implementing real-time monitoring and alerts to the user in case of theft or abnormal usage of electricity.
- *Network Connectivity Issues*: The system is dependent on network connectivity, and any issues related to the network can cause problems in the operation of the system. If the network is down or unstable, the data cannot be sent to the API server, and the system will not be able to detect theft or monitor electricity consumption. This limitation can be addressed by implementing a backup system or using a more reliable network.
- *Cost of Implementation*: The implementation of the system can be costly, especially for small-scale consumers. The cost of the microcontroller, sensors, and other components may be high, and this can be a limitation for some consumers. This limitation can be addressed by providing incentives or subsidies to consumers to adopt the system or by implementing the system in a cost-effective manner.
- Lack of Standardization: There is no standardization in the implementation of the system. Different manufacturers may use different microcontrollers, sensors, and communication protocols, making it difficult to integrate the system with other devices. This can limit the interoperability of the system and can be addressed by establishing industry standards for the implementation of the system.
- *Legal and Regulatory Challenges:* The implementation of the system can face legal and regulatory challenges. The implementation of the system may require approvals from regulatory authorities, and non-compliance with regulations can lead to legal implications. This limitation can be addressed by working closely with regulatory authorities and obtaining the necessary approvals.
- *Reliability*: The reliability of the system is an important factor, as any errors or false alarms can lead to inconvenience to the user. The system must be designed and tested rigorously to ensure its reliability. This limitation can be addressed by implementing quality control measures and testing the system under various conditions.

Overall, the smart electricity monitoring and theft detection system has several limitations that need to be addressed for its widespread implementation. These limitations can be addressed by continuous improvement and innovation in the design, implementation, and maintenance of the system.

VII. CONCLUSION

- The proposed system is an efficient and effective solution for optimizing Windows operating systems. The system has been extensively tested and all options, including Install, Tweaks, and Config, have been found to be reliable and easy to use.
- The system provides a user-friendly interface and allows users to optimize their systems without any prior technical knowledge. This makes it a valuable tool for users who wish to optimize their systems.
- Although the system has a few limitations, such as the need for administrative privileges, compatibility issues with some software applications, and the requirement of Windows operating systems, it is still a valuable tool for users who wish to optimize their systems.
- In comparison to other available software, the proposed system is a simple and effective solution. It is designed to be easy to use, and users can perform tasks such as installing software, tweaking system settings, and scanning for system corruption with just a few clicks.
- Command Line Applications are still hard to use for normal people because it is hard to navigate. However, the proposed system provides an easy-to-use graphical user interface, making it accessible for all users.
- The Tweaks option in the proposed system includes a lot of options, which users might be unaware of. Therefore, it is essential for users to go through each option carefully to understand what they are changing.

Overall, the proposed system is a valuable tool for users who wish to optimize their Windows operating systems. It is easy to use, efficient, and provides users with an all-in-one solution for optimizing their systems.

REFERENCES

[1] Ferreira, J. A., Tavares, G. M., Ferreira, P. H., Pinto, J. G., Pinto, M. H. (2020). A machine learning approach to electricity theft detection using smart meter data. Energy, 203, 117858

[2] Kumar, A., Saini, R., Singh, V. P. (2019). An IoT-Based Approach to Detect Electricity Theft. Wireless Personal Communications, 107(4), 2567-2579.

[3] Al-Abdullah, A. J., Ahmad, N., Hussain, M., Alhumoud, A., Alrajhi, M. (2021). An IoT-Based System for Electricity Theft Detection in Smart Grids. IEEE Access, 9, 30362-30373.

[4] Zhang, T., Lin, X., Huang, J., Li, L., Lv, J. (2019). A blockchainbased approach for detecting electricity theft in smart grids. Journal of Network and Computer Applications, 146, 79-86.

[5] M Halsey, A Bettany, M Halsey, A Bettany - Windows Registry - Springer: Registry Tools and Utilities (2015)

[6] Choquet, R., Lebreton, J.-D., Gimenez, O., Reboulet, A.-M. and Pradel, R. 2009. U-CARE: Utilities for performing goodness of fit tests and manipulating cApture–REcapture data. – Ecography 32: 1071–1074(Version 2.3).

[7] Hipson, Peter D., Maureen Forys, Design Site, and Sergie Loobkoff: Mastering Windows XP Registry. Sybex, 2002.

[8] Stallings, William. "The Windows Operating System." Operating Systems: Internals and Design Principles (2005).

[9] Chaganti, Ravikanth. (2014). Beginning Windows PowerShell. 10.1007/978-1-4842-0016-2_1.

[10] Olusanya, Olayinka & Ogunbanwo, Afolakemi & Lateef, Usman & G.O., Odulaja. (2016). MICROSOFT WINDOWS OPERATING SYSTEM.

[11] Kayani, M. & Abrar, & Waleed, & Ijaz, & Nabeel, & Maham, Rabbani. (2010). Evolutionary Aspects Of Windows Operating System To Enhance Existing Technology. International Journal on Computer Science and Engineering.

[12] Moran, Joseph, and Joseph Moran. "Managing and Reclaiming Disk Space." File Management Made Simple, Windows Edition (2015): 53-62.

[13] Dunn S. Take System Cleanup Into Your Own Hands. PC World. 1999;17(1):232-4.

[14] Nihad Ahmad Hassan, Rami Hijazi:Chapter 6 - Data Hiding Forensics,Data Hiding Techniques in Windows OS,Syngress,(2017)

[15] Jorge Orchilles,Chapter 5 - Managing the Windows 7 Desktop Environment,Microsoft Windows 7 Administrator's Reference,Syngress,(2010)