International Research Journal of Education and Technology
Peer Reviewed Journal
ISSN 2581-7795

ANTI POWER THEFT BY USING IOT BASED WEBSERVER

Abinayasaraswathy.T[1], Aarthi P[2], Anusha C[3], Rajasri S[4]
Assistant Professor[1], Student[2,3,4],
Department of Electrical and Electronics Engineering,
Sri Manakula Vinayagar Engineering College, Puducherry

Abstract—**This project introduces an Anti Power Theft system by using an IoT-based web server to combat electrical power theft, a critical issue causing economic losses and hindering progress. By integrating IoT technology and Anti Power Theft principles, the system efficiently detects and monitors power theft in distribution networks. It collects data from transformers and consumers, analyses it for irregularities indicating theft, and triggers alerts to the grid substation for swift resolution. Emphasis is placed on precise data collection, robust comparison algorithms, and maintaining privacy and security throughout implementation, ensuring the system's reliability and effectiveness in combating power theft.**

Keywords **–** Power theft, IoT technology, ESP8266, Power board, real-time data, Communication protocol, Webserver.

I. INTRODUCTION

Electricity theft remains a significant challenge for power distribution systems worldwide, leading to financial losses and operational inefficiencies. The Anti-Power Theft Control System represents an advanced monitoring and prevention solution aimed at tackling this issue head-on. Its primary objective is the swift detection and prevention of illicit activities, including tapping from transmission lines and tampering above meter boxes.

The approach involves integrating state-of-the-art technologies into existing power grid infrastructure to enhance its capabilities. A key component is the installation of intelligent meters equipped with tamper detection features, capable of identifying and reporting unauthorized access or tampering above meter boxes. These meters utilize advanced machine learning algorithms and data analytics to promptly detect anomalies indicative of theft.

Combatting theft at both consumer and transmission line levels is a pivotal focus. Specialized sensors deployed on Remote Terminal Units (RTUs) at strategic points along transmission cables serve as an early warning system for potential theft activities, detecting abnormal load fluctuations and irregularities. Moreover, integrated communication networks and fault detection algorithms enable swift responses, such as alerting authorities or initiating automated isolation procedures.

Security remains paramount in the Power Theft Control System, with robust authentication and encryption measures safeguarding against cyber threats and ensuring secure communication between system components. The solution adheres to national and international regulations governing electricity distribution and monitoring, providing a comprehensive and compliant approach.

An economically viable approach is adopted, leveraging scalable solutions and existing infrastructure to minimize losses for utility companies and ensure a favorable return on investment. The solution adopts a proactive stance against power theft by offering remote control and automation features, facilitating immediate corrective actions upon the detection of suspicious activity.

Overall, this initiative presents a comprehensive and innovative strategy to combat power theft, contributing to long-term sustainability and efficiency in electricity distribution networks.

II. PROPOSED SYSTEM

The primary aim is to create an advanced C# application seamlessly integrated with a robust web server. This integrated system targets the optimization of data management, user interaction, and content delivery, aiming for a streamlined and enhanced experience. By leveraging the extensive capabilities of C# programming, our goal is to design a responsive and user-friendly application interface that ensures smooth and intuitive experiences for users. The integration with a powerful web server expands the project's capabilities significantly,

enabling efficient data storage, retrieval, and real-time updates to keep the application dynamic and up-to-date.

Key objectives within this project include the development of a secure authentication system to protect user data and privacy. Additionally, we aim to optimize data transfer protocols to ensure fast and reliable communication between the application and the web server. Another crucial aspect is the implementation of dynamic content delivery through the web server, allowing for personalized and relevant information to be presented to users in real-time.

International Conference on Electrical Electronics & Communication Technology (ICEECT'24) ISBN: 978-93-340-6066-9, PERI INSTITUTE OF TECHNOLOGY, Chennai. © 2024, IRJEdT Volume: 06 Issue: 05 | May -2024

At the core of our project lies the seamless integration of the C# application with the web server, creating a dynamic and responsive system that maximizes the strengths of C# programming. The application will act as a user-friendly interface, offering a wide range of functionalities carefully designed to enhance data management, improve user interaction, and overall usability. Simultaneously, the integration with the web server introduces a web-based dimension, facilitating efficient data handling, retrieval, and real-time updates to keep the system agile and responsive to user needs.

Our project's fundamental concept extends beyond mere functionality; it aims to strike a perfect balance between user-centric design and robust server-side functionalities. This approach ensures that the solution we develop is versatile, scalable, and capable of meeting diverse user requirements while prioritizing security and scalability. Ultimately, our goal is to deliver a seamless and interactive experience within a web-based environment, catering to the evolving needs of modern users.

COMPOUNDS USED

1. Sensors
2. NodeMCU
3. ESP32 WIFI Module
4. Energy Meter
5. LCD display
6. 12V Channel Relay board

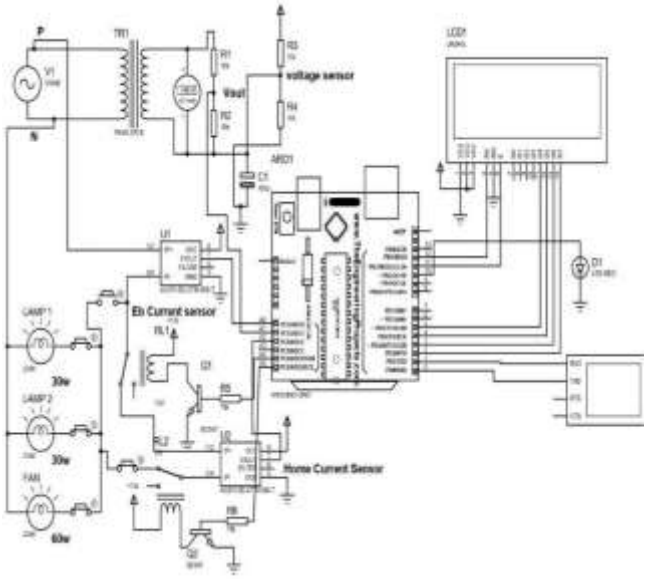

Fig.1 Circuit Diagram

III. BLOCK DIAGRAM

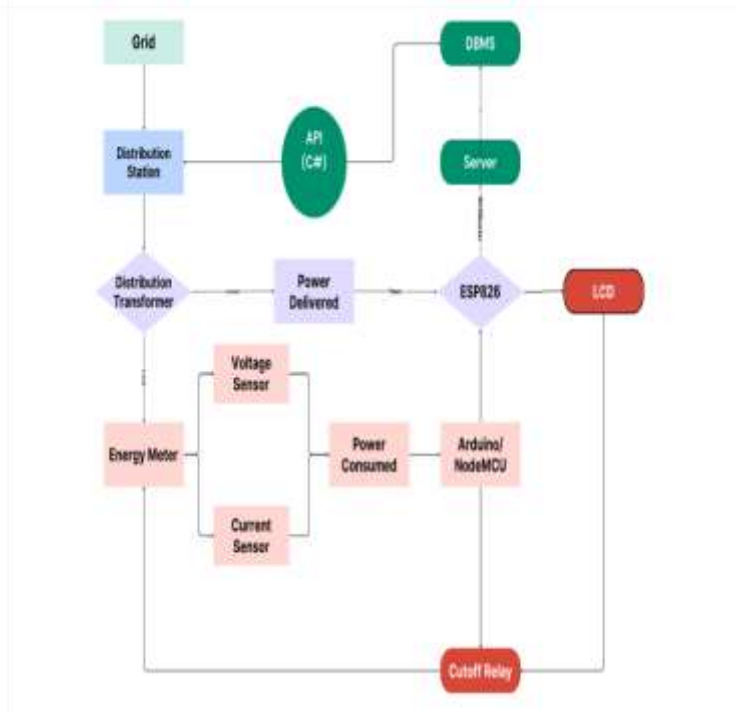

Fig.4.1 Block Diagram

The anti-power theft system utilizing an IoT-based web server is meticulously crafted to monitor electricity usage closely and thwart unauthorized consumption effectively. The process commences with strategically positioned sensors within the electrical network, meticulously measuring current flow and voltage levels. These sensor readings are then relayed to a microcontroller or edge device, which locally processes the data before transmitting it securely to an IoT gateway for cloud server communication.

From the user's perspective, a web server hosts a user interface that is accessible through web browsers or dedicated mobile applications. This interface offers real-time insights into current and voltage levels across various network points. Additionally, it provides historical data analysis and visual representations such as charts. Furthermore, the system is designed to send alerts in case of unusual consumption patterns, empowering authorized users like utility company personnel to take swift remote actions, such as cutting off power to specific areas suspected of theft.

Security forms the cornerstone of this system, with robust measures like user authentication, data encryption, and stringent access controls in place. These measures ensure the protection of sensitive information and control functions, thereby bolstering overall system integrity. Such a comprehensive security approach not only enhances operational efficiency but also enables early detection and prevention of power theft incidents, making the

International Conference on Electrical Electronics & Communication Technology (ICEECT'24) ISBN: 978-93-340-6066-9, PERI INSTITUTE OF TECHNOLOGY, Chennai. © 2024, IRJEdT Volume: 06 Issue: 05 | May -2024

system exceptionally effective and reliable in combating unauthorized electricity consumption.

.The various ways to increase the system performance are:

1. To reduce the voltage sag in peak demand.
2. To maintain the voltage stability.
3. To increase the lifespan of the electric system.
4. To provide a uninterrupted power to the consumers.

The system's components include:

Power Supply: Supplies power to a load by converting input current to the required frequency, current, and voltage.

Transmission Line: A network of conductors that transmit electrical signals between points.

Current Transformer: Scales alternating current and generates proportional secondary current from primary current.

Microcontroller: Embedded system component that controls specific functions by processing data from Input/Output peripherals.

Wi-Fi Module: Facilitates wireless communication within the IoT framework.

Theft Detection Unit: Detects manipulation of energy meters, cuts power supply, and notifies management. Utilizes magnetic sensors for tamper detection.

IV. FLOW CHART

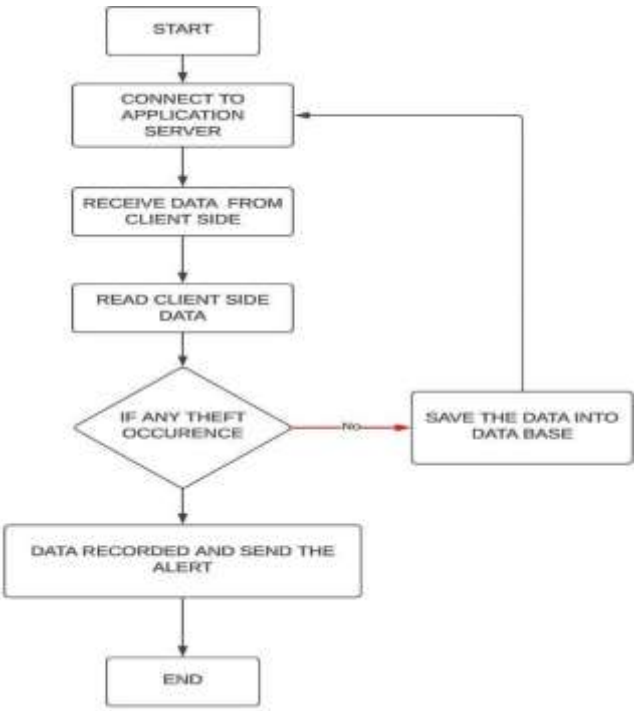

Fig.3 Flow Chart

The flow diagram illustrates the operational steps of an anti-power theft system integrated with an application server. It commences with establishing a connection to the application server, acting as the central processing unit responsible for managing client-side data. Upon reception of data, encompassing details on electricity usage and consumption patterns from clients, the system proceeds to analyse this data.

Upon detecting any suspicious activity indicative of power theft, the system records the relevant data pertaining to the incident. Simultaneously, it triggers an immediate alert to notify relevant authorities or personnel about the potential theft occurrence. Conversely, if no indications of theft are identified based on the analysed data, the system archives this information in a database for subsequent reference and in-depth analysis.

This operational flow ensures the system's active monitoring and response to potential power theft instances in real-time. Swift recording and reporting of such incidents aid in curbing further unauthorized consumption, thus safeguarding the integrity of the electrical distribution network. Furthermore, storing all data in a database facilitates historical tracking, trend analysis, and reporting, enabling informed decision-making and continual enhancement of the implemented anti-power theft measures.

V. HARDWARE IMPLEMENTATION

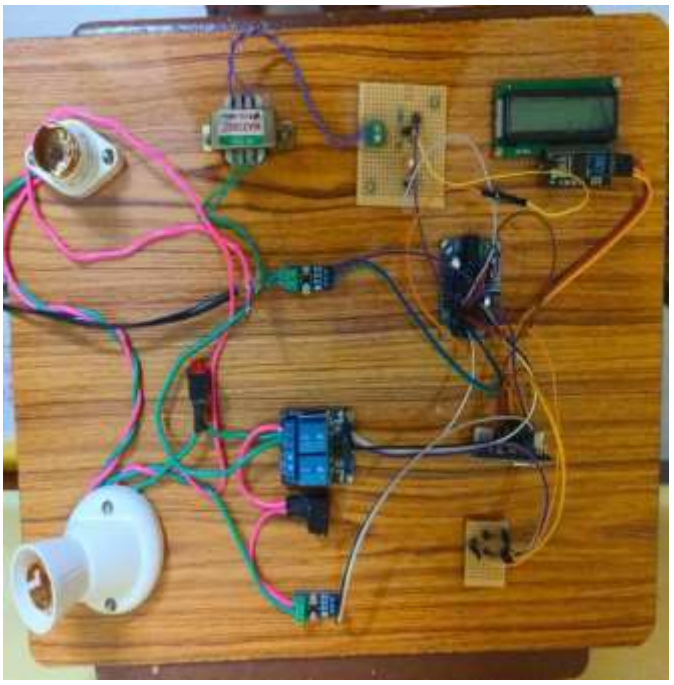

Fig.4 Hardware Connection for Power Detection

International Conference on Electrical Electronics & Communication Technology (ICEECT'24) ISBN: 978-93-340-6066-9, PERI INSTITUTE OF TECHNOLOGY, Chennai. © 2024, IRJEdT Volume: 06 Issue: 05 | May -2024

The working principle of an anti-power theft system leveraging an IoT-based web server revolves around the integration of various components and processes aimed at detecting, preventing, and addressing instances of electricity theft. At its core are microcontroller-based IoT devices strategically deployed at consumer premises, such as smart meters and sensors. These devices continuously collect real-time data on power consumption, voltage levels, current flow, and other electrical parameters.

The collected data is then transmitted securely to the IoT-based web server via communication protocols like MQTT, HTTP, or WebSocket. The web server serves as a central hub for receiving, processing, and analysing the incoming data. Sophisticated algorithms and data processing techniques are employed to interpret the data, detect abnormalities, and identify potential indicators of theft. These algorithms may include statistical analysis, machine learning models, and pattern recognition techniques tailored to detect irregular consumption patterns or meter tampering attempts that could signify electricity theft.

The web server hosts a user-friendly web application interface accessible to authorized personnel, such as utility company administrators or system operators. This interface provides real-time data visualizations, theft detection alerts, historical trends, and actionable insights related to power consumption and theft detection. It allows users to monitor the system's status, investigate incidents, and take corrective actions as needed.

When the theft detection algorithms identify suspicious activities or anomalies indicative of power theft, the system generates alerts and notifications. These alerts are sent to designated stakeholders via email, SMS, or push notifications, informing them about detected theft incidents and providing relevant details for further investigation and action. Response mechanisms may be activated, such as remotely disconnecting power supply to suspected premises, activating alarms, notifying customers about anomalies, or initiating legal actions against offenders.

Additionally, the system maintains a centralized database or data warehouse to store historical data, alert logs, and system events. This data is utilized for further analysis, trend identification, forensic investigations, and generating reports or dashboards for stakeholders, regulatory compliance, and decision-making purposes. In essence, the integrated approach of IoT devices, web server functionalities, data processing algorithms, user interfaces, and response mechanisms enables efficient detection, prevention, and mitigation of electricity theft, contributing to improved energy management and revenue protection for utility providers.

VI. RESULT

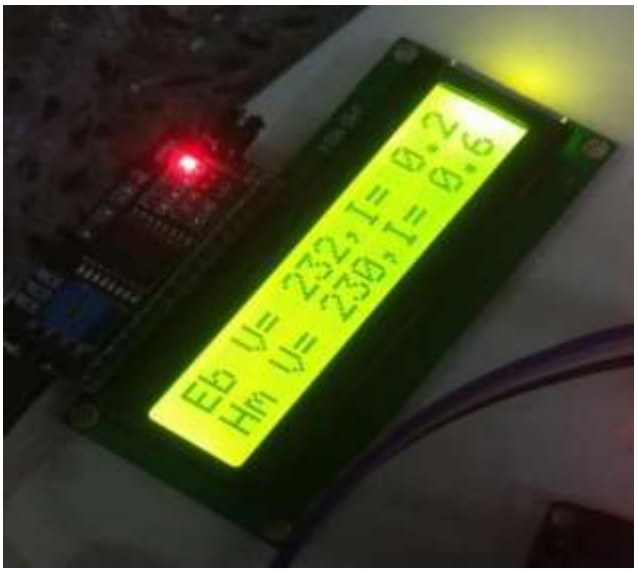

Fig.5 Result1

Fig.6 Result2

International Conference on Electrical Electronics & Communication Technology (ICEECT'24) ISBN: 978-93-340-6066-9, PERI INSTITUTE OF TECHNOLOGY, Chennai. © 2024, IRJEdT Volume: 06 Issue: 05 | May -2024

Table 1 Result

Distribution Region			Consumer Region			Power Theft	
V1 (V)	I1 (A)	P1 (W)	V2 (V)	I2 (A)	P2 (W)	P1-P2 (W)	Theft Occurred
230	0.1	23	230	0.1	23	0	No
230	0.2	46	230	0.4	92	46	Yes
230	0.3	69	230	0.3	69	0	No
230	0.3	69	230	0.5	115	46	Yes
230	0.5	115	230	0.5	115	0	No
230	0.6	138	230	0.6	138	0	No

GRAPH RESULT

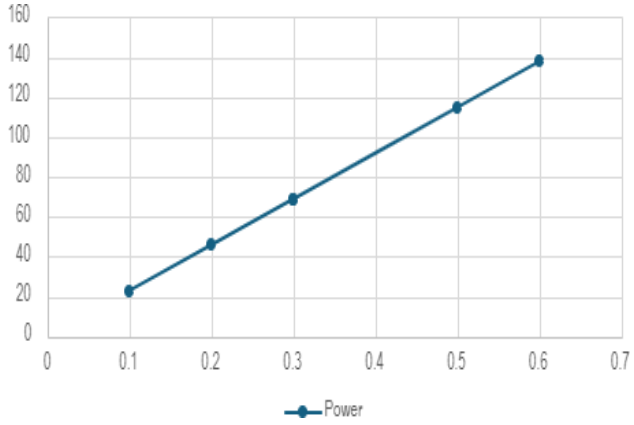

Fig.7 Distribution Power Chart

VII. DATABASE IMPLEMENTATION

In an anti-electricity theft system that utilizes an IoT-powered web server, databases serve as foundational components for storing, organizing, and analysing extensive datasets related to electricity usage, theft detection, user details, and system configurations. These databases are pivotal in ensuring the system's efficiency, reliability, and effectiveness in combating electricity theft.

Initially, a database is crucial for storing and managing electricity consumption data collected from IoT devices such as smart meters and sensors. This database contains both real-time and historical data regarding energy usage patterns, load fluctuations, voltage levels, and current flows. Organizing this information with a relational database management system (RDBMS) like MySQL, PostgreSQL, or Microsoft SQL Server enables efficient querying, retrieval, and analysis of electricity consumption data for theft detection and analysis purposes.

Another vital database is necessary for storing user profiles, authentication details, and device information. This database maintains records of registered users, their roles and permissions, connected devices, and associated metadata. It facilitates user authentication, access management, and device administration functions within the anti-electricity theft system. Depending on scalability and adaptability needs, NoSQL databases like MongoDB or Cassandra may be preferred due to their schema-less design and horizontal scalability.

Additionally, a dedicated database can be used to store records of theft detection events, alert logs, and notification details. This database captures data concerning suspicious activities, instances of theft, alarms triggered by devices, and notifications sent to administrators or authorities. It enables the system to monitor and analyse theft-related data, generate reports, and support forensic investigations into theft occurrences.

Moreover, a database plays a critical role in storing system configuration settings, activity logs, and audit trails. This database logs changes made to system configurations, records system events, tracks user interactions, and maintains a historical log of system activities. It aids in system monitoring, troubleshooting, optimizing performance, and ensuring compliance with regulatory standards.

Furthermore, the system may integrate with external data sources such as weather APIs, energy consumption trends, or customer billing information. These external data sources might require separate databases or data pipelines for integration, transformation, and storage. Tools such as Apache WiFi or customized processes can be utilized to synchronize data from external sources into the anti-electricity theft system's databases.

Overall, databases are integral components of an anti-electricity theft system employing an IoT-based web server, playing a critical role in data storage, organization, analysis, user authentication, system monitoring, and integration with external data sources. The choice of databases depends on factors such as data volume, complexity, scalability, performance needs, and compatibility with the overall system architecture and technologies utilized. Efficient design and implementation of databases ensure streamlined data management, insightful analytics, and dependable operation of the anti-electricity theft system.

International Conference on Electrical Electronics & Communication Technology (ICEECT'24) ISBN: 978-93-340-6066-9, PERI INSTITUTE OF TECHNOLOGY, Chennai. © 2024, IRJEdT Volume: 06 Issue: 05 | May -2024

Fig.8 Web Result

VIII. FUTURE SCOPE

1. The device can be further extended by making it use multiple load detector modules.

2. It can be an algorithm to count the initial value of current and if any sudden increment in load is shown it can be treated as theft also.

3. The whole system can also be interfaced with the wifi module so that the user can also be informed from time to time.

4. The present system, IOT energy meter consumption is controlled by Wi-Fi and it helps consumers to avoid wastage use of electricity.

5. It requires only one time installation cost after installation this can be used with ease for lifetime which acts as a great advantage.

6. The current IoT energy meter system, managed via Wi-Fi, aids consumers in reducing electricity wastage.

7. Connecting all household appliances to IoT enables efficient power consumption management.

8. A system capable of sending SMS alerts to the designated meter reader when theft is detected at the consumer's end can be developed.

IX. CONCLUSION

The successful development and implementation of an IoT-based web server to combat power theft have marked a significant achievement. This comprehensive system addresses various aspects of electricity theft, encompassing issues such as unaccountability among service personnel and billing irregularities that contribute to revenue losses for utility companies. By eliminating direct interactions between end-users and workers, this system relies on remote monitoring of meter readings and promptly sends SMS alerts for abnormal readings, assisting utilities in reducing instances of household electricity theft.

A notable feature of the system is its incorporation of an automatic circuit breaker that can be integrated to remotely cut off power supply to properties engaged in theft. This functionality primarily targets single-phase electrical distribution systems and automates customer billing by tracking consumer load in a timely manner. This design optimizes meter readings, eliminating time-consuming processes and preventing bill manipulations, which not only impact the company's bottom line but also result in higher bills for consumers.

Furthermore, the system streamlines disconnection and reconnection processes based on recharge levels, minimizing additional costs and ensuring transparency in operations. This setup enables efficient energy distribution while empowering the utility to pinpoint theft locations accurately. Additionally, RF modules are leveraged for cellular communication, enabling consumers to receive theft alerts via SMS from the utility. This wireless communication method is independent of physical lines, ensuring seamless data transmission regarding power consumption.

The benefits of employing an IoT-based web server for anti-power theft initiatives are manifold, encompassing affordability, high accuracy, reliability, flexibility, and user-friendliness. The system leverages radio frequency signals for data transmission, making it an optimal choice for wireless communication between Arduino boards and the web server. This hardware implementation not only enhances the consumer experience but also improves utility management, fostering efficient energy distribution and effectively reducing instances of power theft.

X. REFERENCE

[1] Celimpilo Lindani Zulu, Oliver Dzobo “Real-time power theft monitoring and detection system with double connected data capture”[2023]

[2] Yang Xin, Zhang Jiahong, Shen Xin et al., "Design of Anti-theft Electricity Online Monitoring System Based on PCB Rogowski Coil", Sensors and Microsystems, vol. 2021, no. 40, pp. 41-47, May 2021.

[3] Liu Yan, Yuan Ruiming, Zheng Sida et al., "Research on anti-stealing technology of electric energy metering using DBN deep learning algorithm", *Computing Technology and Automation*, vol. 40, pp. 15-19, April 2021

[4] Suraj Rajendra Bhole , Vishvajeet Tukaram Dabhole , Rihan Kashim Mulani , Kuldeep Sanjay Salunke, "Iot Based Smart Energy Meter Monitoring With Identification Of Electricity Theft", IJCRT, 2022.

[5] Jennica Astronomo, Mariel Dane Dayrit, Christopher Edjic, Engr. Richard T. Regidor, "Development of Electricity Theft Detector with GSM Module and Alarm System", IEEE, 2020.

[6] Du Xuxin, Lin Ruitao, Huang Chaokai et al., "Design of an online intelligent analysis system for electricity consumption inspection and anti-stealing electricity", Application of Single Chip Microcomputer and Embedded System, vol. 20, pp. 41-45, June 2020.

[7] Machine Learning applications in grid Security[2020] Authors: Wang.X, Chen.Y, Zhang.Q

[8] Darshan N, Dr. K A Radhakrishnan Rao, "IoT Based Energy Meter Reading, Theft Detection and connection and Disconnection using PLC and Power optimization", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 5, Issue 8, 2015.

[9] Shraddha Make, Pallavi Vethekar, Kavita More, Prof. V. K. Bhusari, "A smart wireless electronic energy meter reading using embedded technology", Internation journal of engineering research and application, volume 4, issue 1(version 3), January

[10] R Meenal, Kevin M Kuruvilla, Adrin Denny, Rejin V Jose, "Power Monitoring and Theft Detection System using IoT", Journal of Physics Conference, 2019. [5] Anubhuti Anand, Yashee C

[11] Nabil M, Ismail M, Mahmoud M, Shahin M, Qaraqe K, Serpedin E (2019) Deep learning-based detection of electricity theft cyber-attacks in smart grid AMI networks. In: Alazab M, Tang M (eds) Deep learning applications for cyber security. Advanced sciences and technologies for security applications. Springer

[12] Sagar Patil, Gopal Pawaskar, Kirtikumar Patil, "Electrical Power Theft Detection and Wireless meter reading", IJIRSET, vol-2, issue 4, April 2013, ISSN: 2319-8753

[13] Gao Y, Foggo B, Yu N (2019) A physically inspired data-driven model for electricity theft detection with smart meter data. IEEE Trans Industrial Inform 15(9):5076–5088

[14] Darshan N, Dr. K A Radhakrishnan Rao, "IoT Based Energy Meter Reading, Theft Detection and connection and Disconnection using PLC and Power optimization", International Journal of

Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 5, Issue 8, 2015.

[15] S.patil, G.Pawaskar, K.patil., "Electrical Power Theft Detection and Wireless Meter Reading", International Journal of Innovative Research in Science, Engineering and Technology, Vol. 2, issue 4, pp. 1114 – 1119, April 2013

[16] E. Moni Silviya, K. Meena vinodhini, Salai Thillai, Thilagram. J., "GSM based automatic energy meter system with instant billing", ICSECSRE'14, ISSN:2278-8875

[17] L.K.Lekha, G.Jegan and M.D.Ranganath, "Iot Based Household Appliances Control and Tampering Detection of Electricity Energy Meter", ARPN Journal of Engineering and Applied Sciences, vol. 11(11), pp. 7376-7379, 2016.

[18] Dr.B.R.Tapas Bapu, Divyadharashini.J.A, Senthamil Selvi.D, Ulageswari.S 1.IOT based reduction of electricity theft[2023]