

# IoT Based Electricity Theft Detection and Monitoring

Aaditya Nandrekar<sup>1\*</sup>, Amar Pawar<sup>2</sup>, Prachoday Sutar<sup>3</sup>, Aakanksha Kadam<sup>4</sup>, Amit Jadhav<sup>5</sup>

<sup>1,2,3,4</sup>UG Student, Department of Electrical Engineering, Annasaheb Dange College of Engineering and Technology, Ashta, India

<sup>5</sup>Assistant Professor, Department of Electrical Engineering, Annasaheb Dange College of Engineering and Technology, Ashta, India

**Abstract:** Smart homes, smart meters, and the Internet of Things are now widely used to replace traditional analogue meters. This data can be transferred wirelessly, reducing the amount of human labour required. However, there is a possibility of theft. Due to the unavailability of specific approaches in the existing solution, these thefts are not accurately identified. The proposed project's goal is to create a system that can track the amount of electricity used per load and trace as well as eliminate electricity theft in the existing line and meter. This initiative also entails to alert the officials from the Electricity Board about the theft that occurred as a result of IoT. A network of connected devices, such as sensors, aids in the transmission of real-time data over the Internet. The Atmega328p microcontroller is used to detect power theft and relay the information to the Wi-Fi module, which further passes stealing to the electricity board.

**Keywords:** Electricity, Theft detection, Current sensors, Internet of Things, Wi-Fi module, Microcontroller, ThingSpeak.

## 1. Introduction

The Internet of Things-based energy theft detection technique is the first of its kind. It has the ability to detect power theft as well as tampering with electric meters. The system uses Hall sensors to detect meter tampering or direct load connections before the meter in the supply. When it detects a theft, it uses a microcontroller to create a log for the nature and timing of the theft, which it then saves on an IOT platform for backup and simultaneously publishes on the internet page. When the number of theft attempts exceeds, it sends a Signal to web site. It requires only one time installation cost after installation this can be used for life time. It will completely eliminate the power theft and will increase revenue for the Government and saves electricity.

This project more users friendly by introducing a system. Customers' costs rise as a result of electricity theft, which can also have serious safety implications. It causes misuse of costs among suppliers, which can distort challenge and obstruct the market's efficient functioning. An electricity supplier's costs of order to detect fraudulent actions by its consumers may be higher than the industry's overall costs. When a supplier senses electricity theft by its customers, it may be liable for generation, network, and trying to balance associated costs with the entry of forecasts of the quantity of electricity theft by that customer into the settlement system.

But at the other side, this operation does not result in an increase in overall costs for the industry. Physical field checks of adulterate seals have traditionally been used to detect electricity theft. Personal and through the use of balance meters. These techniques, while effective in reducing unmeasured and unbilled electricity consumption, are insufficient. Tamper-evident guards can be easily broken, and while balance meters can detect that some consumers are fraudulent, they are unable to pinpoint the perpetrators.

Despite smart meters' security flaws, the higher-resolution data they collect is seen as a promising technique that will supplement traditional detection tools. They have a great deal of potential to strengthen metering, billing, and collection processes, as well as fraud detection and unmetered connections detection. Theft can take many forms, ranging from affecting the security controls of meters to connecting loads directly to electricity supply lines. Payment default has been a major issue as a result of insufficient monitoring and enforcement. This problem was exacerbated by a lack of new tech and insufficient supplier incentives.

The main issue in the current situation is the availability of power generation for residential as well as commercial users also there is increase in cases of line tappings. To minimize the particular problem this proposed project "IoT based electricity theft detection and monitoring."

The main objective is reducing the illegal power usage in domestic/commercial are following.

- To develop the portable electricity pilferage detection system.
- To detect the pilferage using Hall sensor.
- To monitor the theft using IOT and separate web site of the project.
- To control the pilferage using microcontroller.

## 2. Methodology

The proposed system uses concept of Internet of things to communicate theft detection information to Electricity Board officials. To predict current and voltage, this system communicates with the Controller and the detectors that are connected to the Micro-controller. As a result, our project works to avoid and eliminate thefts, saving the economy from

\*Corresponding author: aadityanandrekar@gmail.com

further energy waste. The parameters including power, current, and voltage are checked in this current proposal, and the power is determined by calculating and notified to the consumer and EB via the Internet as a result.

If the load increases, the power to a load is reduced off, and a message about power requirements is sent to an electric board, which is displayed on the LCD. Furthermore, any additional load will cause the power source to the load to be cut off, informing the electric board as well as the individual people who own the house via Wi-Fi, and a buzzer will be installed to notify the stealing to have occurred, notifying the bill based on the usage of electrical supply. A Thing Speak Application is being used to store an average load consumed, find the excess load due to theft, and detect the theft. The Atmega328p-based microcontroller in this project will regularly review a load based on parameters including voltage, current, and power. The system now monitors the load power once more.

### 3. Modelling and Analysis

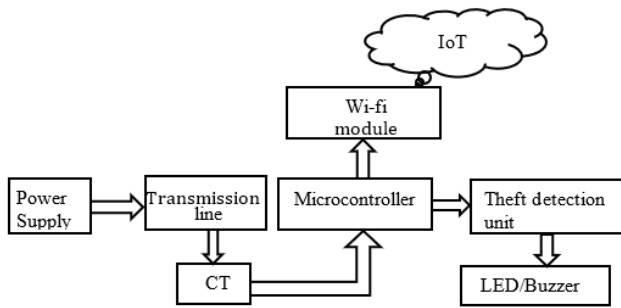


Fig. 1. Block Diagram of IoT based theft detection and monitoring

**Power Supply:** It is a device (Electrical) that provides electrical power to a load. A power supply's primary system that converts electric current from an input to the proper frequency, current and voltage.

**Transmission Line:** A transmission line is a network of conductors used to transport signal (Electrical) from one location to another.

**Current Transformer:** It is a transformer that minimizes or multiplies the Alternating current. It creates a proportional current from primary current to secondary current.

**Microcontroller:** A microcontroller is a device that is embedded inside a system and controls a single function. It accomplishes it by using the its central processor to interpret data received from its Input/Output peripherals.

**Wi-Fi Module:** Wi-Fi module (also defined as serial to Wi-Fi module) is a component of the Internet of Things transmission layer.

**Theft Detection Unit:** This module's primary function to detect manipulation with an energy meter, turn off the supply, and sent the power theft message to the managerial side. When a customer continues to try tamper with meter, it detects using magnetic sensors.

**LED:** It produces light energy from electrical energy, as opposed to traditional light source that convert electrical energy into heat and then into light, resulting in efficient light generation with minimal electricity waste.

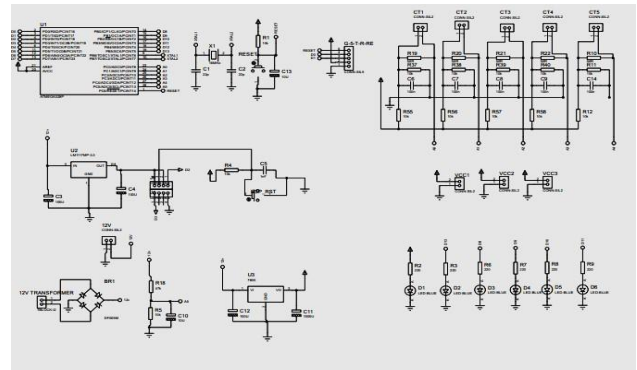


Fig. 2. Schematic circuit diagram

#### A. Things Speak

Thing Speak [9] is just an open - source platform (IoT) Internet of Things application & API that uses the HTTP protocol to store data and recover (retrieve) data from things over the Internet using a web Browser Area Network, according to its creators. Sensor location tracking applications, logging applications, and a networking site of things with status updates are all possible with Thing Speak." io Bridge first launched Thing-Speak in 2010 like a service to assist IoT applications.

Thing-Speak now include support for MathWorks' MATLAB numerical computing software, enabling Thing-Speak users to process and visualise processing facility using MATLAB without having to purchase a MATLAB licence.

Math-works, Inc. and Thing-Speak have a close working relationship. In fact, the Thing-Speak information is fully integrated into the MathWorks MATLAB documentation site, with able to register Math-Works user accounts serving as login details on the Thing-Speak site. Thing-Speak. Com's terms of service & privacy policy are a contract between the user and Math-works, Inc.

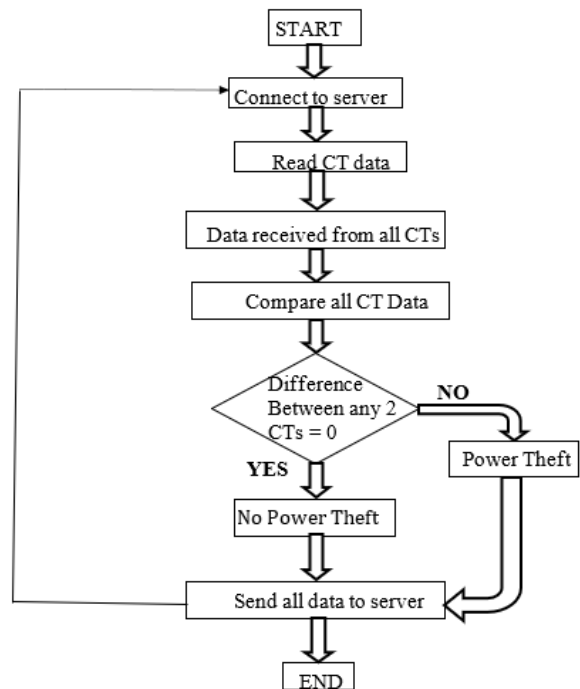


Fig. 3. Flowchart (Client side)

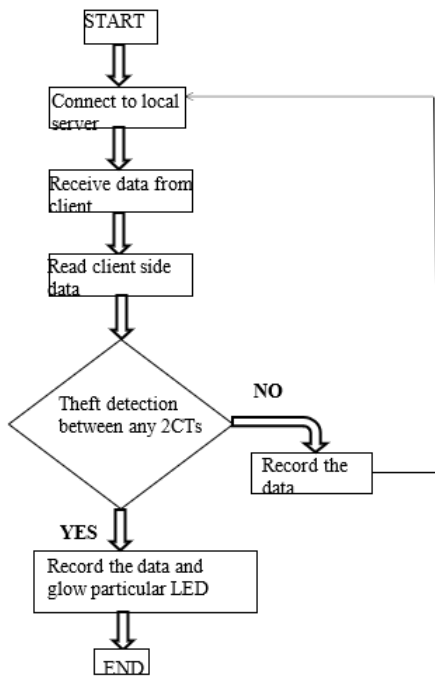


Fig. 4. Flowchart (Server side)

### 4. Results and Discussion

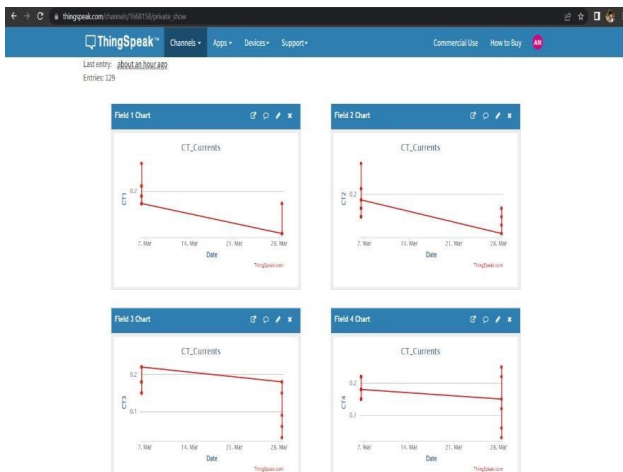


Fig. 5. Screenshot of the output (Current)

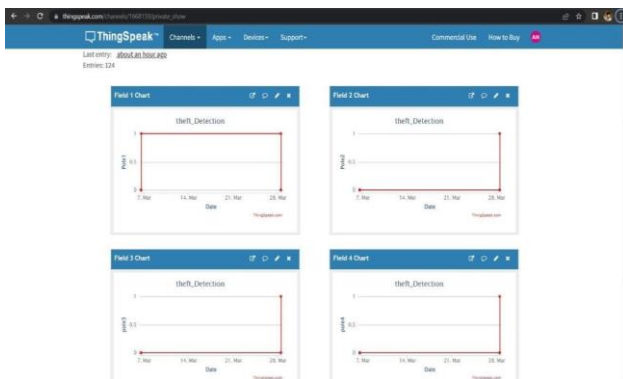


Fig. 6. Screenshot of theft detection

Fig. 5, shows that the current flowing from each pole which is sensed by current sensor and fig. 6 shows that theft detection between two poles. We provided logic here that logic 1 shows theft is detected and logic 0 shows there is no theft between any poles. The document starts here. Copy and paste the content in the paragraphs.

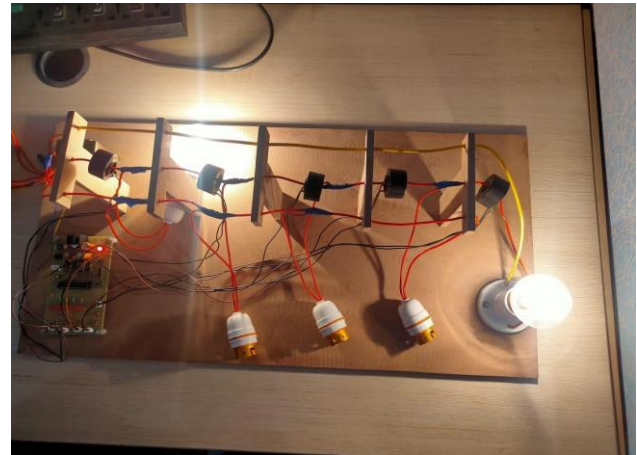


Fig. 7. Hardware result of theft detection

### 5. Conclusion

The system would make it simple to detect electrical energy theft without the need for human intervention. This system is able to detect faults on the pole side of a distribution system. We are going to look forward to implementing smart metres in this system. Grasped the fundamentals of the Internet of Things. The above idea can also be implemented in domestic areas to prevent illegal electricity usage.

### References

- [1] Louis J. Romeo, "Electronic Pilferage Detection Systems: A Survey", Library & Archival Security, Volume 3, pp. 1-22, 1982.
- [2] Zhou Wei, Zhu Rue-de, Wang Jin-quant, "GSM based monitoring and control system against electricity stealing", Electric Power Automation Equipment, Vol. 24, No. 2, pp. 64-66. 2004.
- [3] G. L. Prashanthi, K. V. Prasad, "The power consumed by a model organization" International Journal of Engineering trends and Technology.
- [4] M. Singh and E. V. Sanduja, "Minimizing Electricity Theft by Internet-of-Things", International Journal of Advanced Research in Computer and Communication Engineering, vol. 4(8), pp. 326-329, 2015.
- [5] S. V. Anushree and T. Shanthi, "IoT Based Smart Energy Meter Monitoring and Theft Detection Using ATMEGA", International Journal of Innovative Research in Computer and Communication Engineering, vol. 4(11), pp. 19801-19805, 2016.
- [6] A. Astafari and N. Yamaina, "Electricity theft: A threat on power industry," International Journal of Electrical Engineering and Technology, vol. 8, pp. 172-177, Nov. 2016.
- [7] 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.
- [8] J. Atakari, S. SUTAR, V. Birajdar, and A. B. Kanwade, "Electrical Power Line Theft Detection," International Journal on Recent Innovation Trends in Computing and Communication., vol. 5, pp. 137-141, June 2017.
- [9] ThingSpeak, <https://www.thingspeak.com/channels>