International Journal of Scientific Research & Engineering Trends
Volume 11, Issue 2, Mar-Apr-2025, ISSN (Online): 2395-566X

IoT-Based Electricity Theft Detection System

Mohammad Gulrez Zaidi[1], Deepanshu Punj[2], Moseen Khan[3], Ms. Jyoshita Narang[4]
Department of Electronics and Communication Engineering
IMS Engineering College, Ghaziabad, Uttar Pradesh

Abstract- Innovative solutions for various industries have been developed as a result of the proliferation of Internet of Things (IoT) devices. IoT has the potential to completely change how electricity is produced, transmitted, and used in the electricity sector. The use of IoT for detecting and preventing electricity theft is one such application. Meter tampering, also known as electricity theft, is a significant problem that affects the revenue and profitability of electricity boards. It entails circumventing meters in an unlawful manner in order to use electricity without paying for it. This not only costs government's money, but also puts consumers and the electricity grid in danger of injury or damages. In this project, we propose creating an IoT-based system to track down and stop electricity theft. Smart meters with sensors and communication capabilities make up the system, along with a central server for data processing and analysis. Electricity consumption patterns are continuously monitored by smart meters, which also send data to a central cloud-based database. The database values are utilized by the authorities when it discovers anomalies or suspicious activity upon close monitoring of the data stored in real-time. The proposed system could significantly lower the number of instances of electricity theft, increasing revenue and profitability for the electricity providers while enhancing consumer safety. By offering real-time information on electricity consumption and billing, it can also assist utilities in streamlining their operations and enhancing customer service.

Index Terms- Internet Of Things, Meter Tampering, Smart Meters, Database, IoT Security, Real Time Information.

I. INTRODUCTION

Internet of Things is a term used for a system where devices are given IP addresses, and everybody makes the device recognizable 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) . IoT has the propensity to alter people's lifestyles. People prefer to monitor things through automatic systems in today's world rather than through any manual system together with the circuitry driving the system, which are the main elements of the IoT-based electricity theft detection system introduced in this project. An economy's production and consumption of electricity are key determinants of its size and development, electricity theft slows economic growth. Even though exporting electric power is rarely profitable, most of it is produced for domestic use. Even though only a few nations profit from the export of electric power, the majority of it is used for domestic consumption in developing nations.

Most developing countries have suffered undesirable economic consequences to meet the demands of electricity for real estate and industrialization 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 23% in 2014, gathered from officially recognized sources. Reducing transmission and distribution losses is the greatest challenge to power utility authorities.

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

Reports suggest 25 percent of Ghana's current annual average losses are due to electricity theft. However, the emergence of smart grid technologies has informed researchers to utilize the smart grid platform to detect and monitor electricity theft. Our research proposes a generalized IOT-based design using an ATMEGA328 microcontroller 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 database server, which is accessible in real-time.

II. METHODOLOGY

The block diagram is shown in figure 2.1. It consists of an AC line, energy meter, current sensor, voltage sensor, load 1, load 2, ATMEGA328, WI-FI module, LCD display, and cloud interface.

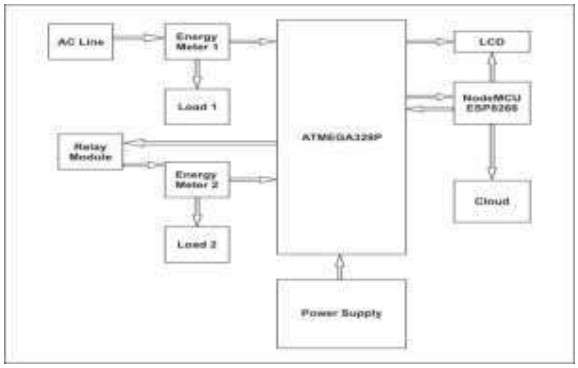

Figure 1 Block diagram

The AC power supply line is affixed with the current sensors and the voltage sensors, which passes through the power meter fixed. Each set of sensors and the power meter are treated as a node here. The single node represents an individual point of power supply which may be an individual unit of home or the point where theft occurs.

The current sensors start sensing power usage in the nodes whenever a load is operational. The various readings noted by the sensors in the presence of the operational loads are then passed on to the microcontroller, which gathers the information regarding power consumption in real-time.

The gathered information is then processed in user-understandable formats and they are displayed up in the LCD display after which the microcontroller checks for anomalies in the power consumption and the alert for power theft is given.

Information processed in the microcontroller is sent to the cloud, via the WI-FI module which is interfaced with a backend cloud storage space where the received data is maintained, the maintained data can be manipulated in a lot of ways which enables the authorities from the side of the electricity providers to remotely manage and control the power flow from the electricity grids.

Hardware Requirement

- Atmega 328-P Microcontroller
- Lcd Display
- Power Supply Module
- Electric Energy Meter
- Relay Module
- Wi-Fi Module

Atmega328-P Microcontroller

The ATmega328 IC is the brain of the Arduino board and is widely used in various projects. It is not suitable for industrial use, however, the standalone ATmega328 IC can be used as an alternative to the Arduino board. It can be programmed using the Arduino IDE, either using FTDI or the Arduino board.

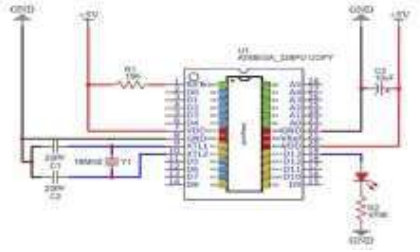

Figure 2. Atmega328-P Microcontroller

This microcontroller features three Timer/Counters with compare modes and internal/external interrupts, a USART with serial programming capability, a 2-wire serial interface, an SPI serial port, a 6-channel 10-bit ADC (8 channels on TQFP and QFN/MLF packages), a programmable watchdog timer with internal oscillator, and five software-selectable power saving modes. The idle mode conserves power by suspending the CPU, while allowing the SRAM, Timer/Counters, USART, 2-wire serial interface, SPI port and interrupt system to remain active. The power-down mode maintains the register contents, freezing all other chip functions until the next interrupt or hardware reset.

The Atmel ATmega328P is a powerful microcontroller that offers a cost-effective solution for many embedded control applications. The device combines an 8-bit RISC CPU with an in-system self-programmable flash on a monolithic chip. In standby mode, the crystal/resonator oscillator runs while the rest of the device is sleeping, allowing for fast start-up with low power consumption.

The on-chip ISP flash allows the program memory to be reprogrammed in-system through an SPI serial interface, with a conventional non-volatile memory programmer, or with an on-chip boot program running on the AVR core. The boot program can use any interface to download the application

program into the application's flash memory, and the software in the boot flash section will continue to run while the application flash section is being updated, providing true read-while-write operation..

The ATmega328P AVR is supported by a variety of development tools, including C compilers, macro assemblers, program debugger/simulators, in-circuit emulators, and evaluation kits.

Software in the boot flash section will continue to run while the application flash section is updated, providing true read-while-write operation. By combining an 8-bit RISC CPU with an in-system self-programmable flash on a monolithic chip, the Atmel ATmega328P is a powerful microcontroller that provides a highly flexible and costeffective solution to many embedded control applications. The ATmega328P AVR is supported with a full suite of program and system development tools including C compilers, macro assemblers, program debugger/ simulators, in-circuit emulators, and evaluation kits.

This register file contains 32 8-bit general purpose working registers with a single clock cycle access time. This allows for single-cycle arithmetic logic unit (ALU) operations. It is possible to perform arithmetic and logic operations between registers or between a constant and a register, as well as single register operations within the ALU.

Six of the 32 registers can be used as three 16-bit indirect address register pointers for data space addressing – enabling efficient address calculations. One of these address pointers can also be used as an address pointer for look up tables in flash program memory. The ALU supports arithmetic and logic operations between registers or between a constant and a register. Single register operations can also be executed in the ALU. After an arithmetic operation, the status register is updated to reflect information about the result of the operation. Program flow is provided by conditional and unconditional jump and call instructions, able to directly address the whole address space.

Lcd Display

The most commonly used Character based LCDs are based on Hitachi's HD44780 controller or other which are compatible with HD44580. LCDs found in the market today are 1 Line, 2 Line or 4 Line LCDs which have only 1 controller and support at most of 80 characters, whereas LCDs supporting more than 80 characters make use of 2 HD44780 controllers.

Most LCDs with 1 controller have 14 Pins and LCDs with 2 controllers has 16 Pins (two pins are extra in both for back-light LED connections). Pin description is shown in the figure 2.3.

The display gives out real time readings of the processed information from the microcontroller such as the power consumed from the individual units, total power consumed and power being theft, used for the monitoring of power from the hardware.

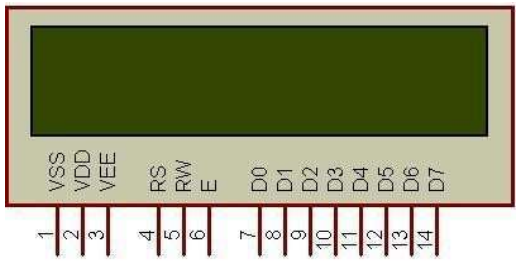

Figure.3. Character LCD type HD44780 Pin diagram (16*2) 3 Power Supply Module

Figure 4. Power module

The figure 2.4 shows various components of the power module and its interfacing ports which are to be connected with the AC power line and thus providing power for the various components which are used in the project.

Table 2.1 Power supply module specifications

Application	Electronic Instruments
Output Voltage	5-12 V DC
Input Voltage	110-240 V
Rated Power	32 Kw
Maximum Load	0.75 Amp

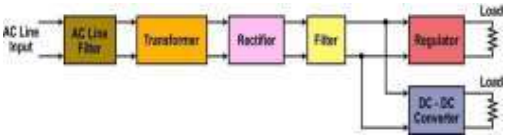

Figure 5. Components of a power supply

- A transformer is commonly used to step the input AC voltage level down or up. Most electronic circuits operate from voltages lower than the AC line voltage so the transformer normally steps the voltage down by its turns ratio to a desired lower level.

- For example, a transformer with a turns ratio of 10 to 1 would convert the 120 volt 60 Hz input sine wave into a 12 volt sine wave.
- Rectifier:
- The rectifier converts the AC sine wave into a pulsating DC wave.
- There are several forms of rectifiers used but all are made up of diodes.
- Filter:
- The rectifier produces a DC output but it is pulsating rather than a constant steady value over time like that from a battery.
- A filter is used to remove the pulsations and create a constant output.
- The most common filter is a large capacitor Regulator:
- The regulator is a circuit that helps maintain a fixed or constant output voltage.
- Changes in the load or the AC line voltage will cause the output voltage to vary.
- Most electronic circuits cannot withstand the variations since they are designed to work properly with a fixed voltage.
- The regulator fixes the output voltage to the desired level and then maintains that value despite any output or input variations.

Electric Energy Meter:
A.C. Single Phase, 2 Wire Solid State (Static) Fully Electronic Energy Meter, Accuracy Class 1.0 &Current Rating 5-30 Amp. with Backlit LCD Display for 240 Volt System fitted with Pilfer Proof Meter Box.

This specification covers design, engineering, manufacture, testing, inspection & supply of A.C. Single phase, two wire solid state (static) fully electronic energy meters of accuracy class 1.0 & current rating 5-30 A, with backlit LCD display for 240 Volt systems as per requirement in this specification and pilfer proof meter box

(PPMB) made of engineering plastic, FR grade with self-extinguishing property suitable for single phase meter.
The meter should be capable of recording & displaying energy in KWH & demand in KW for single phase two wire A.C. loads respectively for power factor range of Zero lag – unity – Zero lead. Meters should have facility/ capability of recording tamper information.

Figure 6. Energy meter

The meter shall conform in all respects to high standards of engineering, design and workmanship shall be capable of performing commercial operation continuously in a manner acceptable to WBSEDCL and shall have the right to reject any work or material which in its judgment is not in accordance therewith.

The offered meter must include all parts and accessories required for the system to function effectively and without errors for the aforementioned purpose. Whether or not these components are mentioned specifically in this specification and/or the commercial order, they will be considered to fall under the scope of the bidders' supply.

The original manufacturers of LT A.C. static energy meters shall only quote against this tender. In case of foreign manufacturers their authorized agent may also bid provided that they should be registered vendor and shall have all the testing facilities in India. They should also produce the documents authorizing them as agents, in India It is mandatory that in case of all manufacturers, the offered meter shall be ISI marked and bidder shall have to furnish valid BIS certification along with the offer.

Power Relay
Relay modules are simply circuit boards that house one or more relays. They come in a variety of shapes and sizes but are most commonly rectangular with 2, 4, or 8 relays mounted on them, sometimes even up to 16 relays.

Relay modules contain other components than the relay unit. These include indicator LEDs, protection diodes, transistors, resistors, and other parts. But what is the module relay, which makes the bulk of the device? You may ask. Here are facts to note about it:

- A relay is an electrical switch that can be used to control devices and systems that use higher voltages. In the case of module relay, the mechanism is typically an electromagnet.
- The relay module input voltage is usually DC. However, the electrical load that a relay will control can be either AC or DC, but essentially within the limit levels that the relay is designed for.
- A relay module is available in an array of input voltage ratings: It can be a 3.2V or 5V relay module for low power switching, or it can be a 12 or 24V relay module for heavy-duty systems.
- The relay module information is normally printed on the surface of the device for ready reference. This includes the input voltage rating, switch voltage, and current limit.

Relay Module Working:
How does a relay module work? The relay module's working principle is quite simple. It uses an electromagnet to open and

close a set of electrical contacts. Here is the sequential working of relay module devices for easier understanding:

- The typical relay module connection points include an input side that consists of 3 or 4 jumper pins, and an output side that has 3 screw terminals.
- When the control signal is applied to the input side of the relay, it activates the electromagnet, which attracts an armature.
- This in turn closes the switch contacts on the output (high voltage) side, allowing electricity to flow and power the device or system that is connected to it.
- To prevent flyback voltage from damaging the relay module circuit and the input device, a diode is often placed in parallel with the electromagnet coil. This diode is known as a flyback diode. It allows current to flow in only one direction.
- When a higher level of isolation is required, an optocoupler is used. An opto-isolated relay module has a photoelectric device on the input side, which is used to control the electromagnet's switching action.

Relay modules are available with either normally open (NO) or normally closed (NC) switch configurations.

- A NO switch is open when the electromagnet is not activated, and closed when it is activated.
- An NC relay switch, on the other hand, remains closed by default and only opens when the relay is activated.

Figure 7. Relay Module

Wi-Fi Module

The ESP8266 Wi-Fi Module is a self-contained SOC with an integrated TCP/IP protocol stack that can give any microcontroller access to the Wi-Fi network. The ESP8266 is capable of either hosting an application or offloading all Wi-Fi networking functions from another application processor.

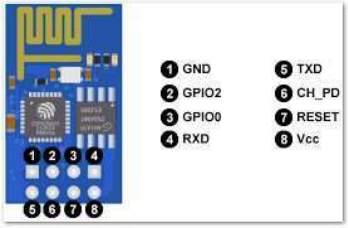

Figure 8. ESP8266

Each ESP8266 module comes pre-programmed with an AT command set firmware, meaning, it can be simply hooked up to the Arduino device and get about as much Wi-Fi-ability as a Wi-Fi Shield offers (and that's just out of the box)! The ESP8266 module is an extremely cost-effective board with a huge, and ever growing, community.

This module has a powerful enough on-board processing and storage capability that allows it to be integrated with the sensors and other application specific devices through its GPIOs with minimal development up-front and minimal loading during runtime.

Its high degree of on-chip integration allows for minimal external circuitry, including the front-end module, is designed to occupy minimal PCB area. The ESP8266 supports APSD for VoIP applications and Bluetooth coexistence interfaces, it contains a self-calibrated RF allowing it to work under all operating conditions, and requires no external RF parts.

There is an almost limitless fountain of information available for the ESP8266, all of which has been provided by amazing community support. Additional points to be considered in powering up the microcontroller and boot loading it are:

- The ESP8266 Module is not capable of 5-3V logic shifting and will require an external Logic Level Converter. Please do not power it directly from the 5V dev board.
- This new version of the ESP8266 Wi-Fi Module has increased the flash disk size from 512k to 1MB.
- Features:
- 802.11 b/g/n
- Wi-Fi Direct (P2P), soft-AP
- Integrated TCP/IP protocol stack
- Integrated TR switch, balun, LNA, power amplifier and matching network
- Integrated PLLs, regulators, DCXO and power management units
- +19.5dBm output power in 802.11b mode
- Power down leakage current of <10uA
- 1MB Flash Memory
- Integrated low power 32-bit CPU could be used as application processor
- SDIO 1.1 / 2.0, SPI, UART
- STBC, 1×1 MIMO, 2×1 MIMO
- A-MPDU & A-MSDU aggregation & 0.4ms guard interval
- Wake up and transmit packets in < 2ms

Standby power consumption of < 1.0mW (DTIM3)

Software Requirement

- Proteus
- Ccs Compiler/Arduino

Proteus
Proteus is a software tool for simulating electronic circuits and embedded systems. It allows users to design and test virtual prototypes of electronic circuits and devices, and can be used for a variety of applications, including education, training, and prototyping.

It is available in several versions, including Proteus Design Suite, Proteus VSM (Virtual System Modeling), and Proteus Lite. The software includes a library of components and devices, as well as a graphical user interface for creating and simulating circuits.

Proteus is widely used in industry and academia for a range of applications, including the development of microcontroller-based systems, simulation of analog and digital circuits, and the design and testing of printed circuit boards (PCBs). It can also be used to teach basic electronics and embedded systems concepts to students and beginners.

Overall, Proteus is a valuable tool for designing, testing, and simulating electronic circuits and systems, and is widely used in the fields of engineering and computer science.

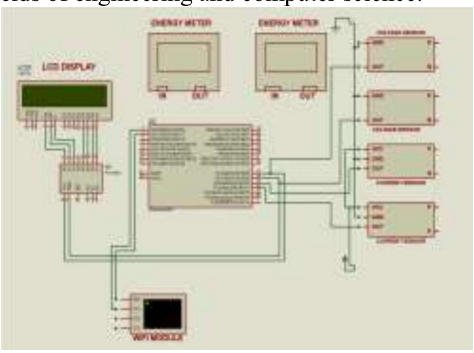

Figure 9. Proteus simulated circuit diagram

Figure 2.13 shows the interfacing of the microcontroller with various components, The ATMEGA328P controller's second pin is interfaced with transmitter side of WI-FI module and the third pin is interfaced to the receiver side of the W-IFI module. These connections helps to ensure the transmission and reception of the controller.

The 23rd and 24th pins are connected with the voltage sensor for monitoring the potential difference across the AC lines. The 25th and 26th pins are connected to current sensors for noting down the current from the respective nodes.

The pins of 23 and 24 connections are made with LCD interfacing component at serial clock and at serial data ports. The ports of 4, 5, 6 in LCD interfacing component gets connected with the LCD display ports of 4, 5, 6 respectively for register select, read/write enable functions. And the ports 10, 11, 12 of LCD interfacing component are connected to ports of 12, 13, 14 of LCD display which are used to send the data for display.

Css Compiler/Arduino
Boot loading is the process of uploading a program to a microprocessor (a small computer that is embedded in a device). The program, also known as a bootloader, is a special program that is used to load other programs or applications into the microprocessor's memory.

To bootload a microprocessor, you will need a computer and a programming tool, such as a programmer or debugger. The programmer or debugger is a device that connects to the microprocessor and allows you to upload a program to it.

The Arduino IDE is used here to bootload the Atmega328, this is done by keeping up the target microcontroller placed in the breadboard and the intstructions are provided from the actual Arduino UNO board that is being connected with the PC via an USB port of the system.

Once the required code along with the functionalities of the microcontroller are entered and debugged in the IDE then these are compiled and kept ready to be burned onto the microcontroller.

III. MODELING AND ANALYSIS

Thing Speak is an open data platform for the Internet of Things. The device or an application can communicate with Thing Speak using a RESTful API, and it keeps either the data private, or make it public. In addition, use Thing Speak to analyze and act on the data. Thing Speak provides an online text editor to perform data analysis and visualization using MATLAB®. Otherwise perform actions such as running regularly scheduled MATLAB code or sending a tweet when the data passes a defined threshold. Thing Speak is used for diverse applications ranging from weather data collection and analysis, to synchronizing the colour of lights across the world.

The heart of Thing Speak is a time-series database. Thing Speak provides users with free time-series data storage in channels. Each channel can include up to eight data fields.

Connect ESP8266 to ThingSpeak
The Hardware part of the IoT System and the ESP8266 provides the necessary API (or the user interface) for the system. The API is then embedded into the code in the microcontroller from which a remote connection is established to the ThingSpeak software interface.

Procedure of ThingSpeak
- Overview

- Creating ThingSpeak Account
- Prerequisites for the Project
- Connect ESP8266 to ThingSpeak using AT Commands

Overview

The ThingSpeak is special and different as it uses simple HTTP Protocol to transfer, store and retrieve information from different sensors.

Also, the ThingSpeak Application allows us to log the sensor data, track locations and even social networking of things.
Another important thing (or rather a unique feature) about ThingSpeak is its support from MATLAB. The close relationship between ThingSpeak and MATLAB has lead to integrate several key features of MATLAB into the ThingSpeak Application.

One such feature is to analyse and visualize the user data i.e. the sensor data in a graphical way without the MATLAB License.

Thus, the ThingSpeak Application is a great tool for IoT-related projects.

Creating ThingSpeak Account

An account is the major stepping stone in the interfacing of the hardware with the ThingSpeak. Since the collaboration with MATLAB, use the MathWorks credentials to log in to ThingSpeak. The steps in creating the account are as follows:

After logging in, create a new channel for the data to be stored. For this go to Channels–>My Channels and click on New Channel.

Figure 10. Thingspeak intro and channel creation

- Enter the name of the channel and name of Field 1 in the corresponding sections. Fields in a channel are used to hold the data and each channel can have up to 8 fields. After entering the details save the channel.
- In this case, the Channel called “Test Channel” is created and the Field 1 as “Random Number”.
- The next step is to prepare the hardware for the project, which includes ESP8266 WiFi Module, Arduino UNO Board and a few connecting wires.

Prerequisites for the Project

There are two ways to connect ESP8266 to ThingSpeak Application. For both the ways, make sure that the ESP8266 Module is loaded or flashed with AT Commands Firmware.

- For flashing the AT Commands firmware, enable the programming mode in ESP8266 by connecting GPIO0 to GND and resetting the module.
- But in this circuit (assume the firmware has been flashed already), the ESP Module is in Normal Mode i.e. GPIO0 can be left floating.

After flashing the ESP with AT Commands Firmware, proceed with connecting ESP8266 to ThingSpeak. As it is said before, it can be done in two ways: One is through AT Commands and the other way is through Arduino (even this way uses AT Commands but Arduino controls them).

The circuit diagram in order to connect ESP8266 to ThingSpeak is very simple. In fact, it might have already seen this connection before. The Arduino UNO Board is used just to transmit the data between the computer and the ESP8266 i.e. it acts as an USB-to-UART Converter.

Connect ESP8266 to ThingSpeak using AT Commands

Connect the Arduino board to the computer and open the serial monitor of Arduino and check for connectivity using the following command.

AT
Set the baud rate to 115200 and also select “Both NL & CR” option in the Serial Monitor. After receiving the response as “OK”, proceed with connecting the ESP Module to the WiFi Network using the following command.
AT+CWJAP=”SSID”,”PASSWORD”
Replace SSID with the name of the WiFi Network and enter the password in place of PASSWORD. Now the confirmation response will be received regarding the WiFi Connection as follows.

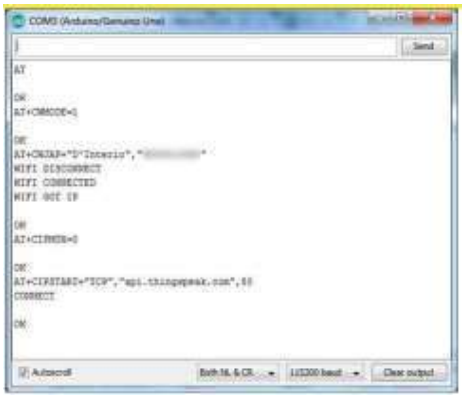

Figure 11 AT Commands of WIFI module testing

Now, set the single connection using the following command.

International Journal of Scientific Research & Engineering Trends
Volume 11, Issue 2, Mar-Apr-2025, ISSN (Online): 2395-566X

AT+CIPMUX=0
Next step is to connect to the ThingSpeak API using TCP Protocol. For this, use the following command.
AT+CIPSTART="TCP","api.thingspeak.com",80
Alternatively, the IP Address of the host api.thingspeak.com can be used i.e. 184.106.15349.
AT+CIPSTART="TCP","184.106.15349",80

After starting the TCP connection, if action is not performed, the connection will be closed automatically after some time, usually after 1 minute.

Now, the "TCP" connection between the ESP8266 and ThingSpeak has been successfully enabled. Next, any data can be sent through this TCP Connection.
For this, use the following commands one after the other. but trying it for a couple of times, the process is understandable.

In order to send the data, send three different information: One is the actual send command, next is the data along with the ThingSpeak Field Key and finally the close connection command.

Before sending the data, need to acquire the API Key. For this, go to the channel (the one have been just created) and click on "API Keys" Tab. Below that, it is found as Write API Key, which is an alphanumeric string of 16 characters. Make a note of this key.

Figure 12 ThingSpeak Write API key Now, use the following command to initialize the data transmission.

AT+CIPSEND=51
The value 51 is the length of the data to be transmitted. This includes the complete data including the API Key and the "\r" and "\n" values. For this command, the following response is got.

OK
Now type the following information and hit send. Here, "XXXXXXXXXXXXXXXX" is nothing but the 16 character Write API Key, which is just copied. And the number "143" is the actual data transmitted to field1.

GET
/update?api_key=XXXXXXXXXXXXXXXX&field1=143

After typing this text and hitting on send, there will be no response. It is actually waiting for the close command. Once hitting the send for the above text, immediately type the following command and again hit send.

Figure 13. Debugging of WIFI Module using Serial Monitor

Here, the number 5 intimates it is the 5th message to that Key. Now, Open the Thing Speak API and open the channel. In the "Private View" tab, the value '143' in the Field 1 Chart is seen.

If all these steps are executed, then the ESP8266 to ThingSpeak API connection can be successfully made. To send more data, repeat the steps from creating the TCP Connection.

Figure 14 Final output of ThingSpeak server

Since the ESP8266 is controlled through Arduino, the circuit diagram will be slightly different. But the components will be the same.

Typing all the AT Commands manually is not easier, so here comes Arduino to rescue the difficulty. Make all the connections as per the above circuit diagram and proceed with the code.

IV. RESULTS AND DISCUSSION

A Electricity Theft Detection and monitoring system has been designed and developed with proper integration of both the hardware and the software. Without any human interface, this system provides an effective and easy way to detect electrical theft. The use of IoT helps in achieving the numerous advantages of wireless network communications. Power theft is actually bypassing the energy meter, but in this project, the theft is detected if some unauthorized consumption is done on the main AC supply.

Figure 15. Full setup of the project

Using IOT, the illegal usage of power can be solved electronically without any human intervention and wirelessly. The WI-FI module regularly communicates with the cloud interfacing, sending readings of the power consumption.

Figure 16 Result from hardware

These readings gets continuously stored onto the remote database that is connected and the readings from the remote database collections are as shown below

Figure 17. Results from the cloud

V. CONCLUSION

A remote cloud-based Electricity Theft Detection and monitoring system has been designed and developed with proper integration of both the hardware and the software. Without any human interface, this system provides an effective and easy way to detect electrical theft. This main feature of theft detection is done seamlessly using the integrated cloud system, which is able to detect the theft of electricity that is being drawn from the main AC line and also maintain the statistical data of that theft power.

This system also helps to monitor the usage patterns of authorized power consumers over a period of time. These recorded data can be further used to study the power consumption under various sub-branches of power supply and would enable the electricity providers on the power grid upgrades and even help them to look for failure on the devices used for power transmission. The project as a whole helps to eradicate theft to a larger amount and lower the financial losses of the electricity providers, thus helping them in manifold ways.

REFERENCES

1. A. K. Gupta, A. Mukherjee, A. Routray and R. Biswas, “A novel power theft detection algorithm for low voltage distribution network,” IECON 2017 - 43rd Annual Conference of the IEEE Industrial Electronics Society, Beijing, 2017, pp. 3603-3608.
2. M. Golden, B. Min, “Theft and loss of electricity in an Indian Statetechnical report,” Int. Growth Centre 2012.
3. Navani JP, Sharma NK and Sapra S. “Technical and non-technical losses in power system and its economic consequence in Indian economy,” Int J Electron Comp Sci Eng, Vol 1, pp. 757–61, 2012.
4. W. Han and Y. Xiao, “NFD: A practical scheme to detect non-technical loss fraud in smart grid,” 2014 IEEE International Conference on Communications (ICC), Sydney, NSW, 2014, pp. 605-609.
5. ECI Telecom Ltd., Fighting Electricity Theft with Advanced Metering Infrastructure (March 2011) [Online] Available: http://www.ecitele.com
6. J. Nagi, K. S. Yap, S. K. Tiong, S. K. Ahmed and M. Mohamad, “Nontechnical Loss Detection for Metered Customers in Power Utility Using Support Vector Machines,” in IEEE Transactions on Power Delivery, vol. 25, no. 2, pp. 1162-1171, April 2010.
7. S.S.S.R. Depuru, “Modeling, Detection, and Prevention of Electricity Theft for Enhanced Performance and Security of Power Grid,” The University of Toledo, Aug. 2012.
8. J. Nagi, K.S. Yap, S.K. Tiong, S.K. Ahmed, and A.M. Mohammad, “Detection of abnormalities and electricity

theft using genetic support vector machines," Proc. IEEE Region 10 Conference TENCON, Hyderabad, India, Jan. 2009, pp. 1–6.
9. S. Sahoo, D. Nikovski, T. Muso, and K. Tsuru, "Electricity theft detection using smart meter data," in Innovative Smart Grid Technologies Conference (ISGT), IEEE Power and Energy Society, 2015.
10. S. A. Salinas and P. Li, "Privacy-Preserving Energy Theft Detection in Microgrids: A State Estimation Approach," IEEE Trans. Power Syst., vol. 31, no. 2, pp. 883 - 894, 2016.
11. Yip, Sook-Chin, KokSheik Wong, Wooi-Ping Hew, Ming-Tao Gan, Raphael C-W. Phan, and Su-Wei Tan. "Detection of energy theft and defective smart meters in smart grids using linear regression," International Journal of Electrical Power & Energy Systems 2017, vol 91, pp. 230- 240.
12. Yip, Sook-Chin, Chia-Kwang Tan, Wooi-Nee Tan, Ming-Tao Gan, and Ab-Halim Abu Bakar, "Energy theft and defective meters detection in AMI using linear regression," in 2017 IEEE International Conference on Environment and Electrical Engineering and 2017 IEEE Industrial and Commercial Power Systems Europe (EEEIC/I&CPS Europe), 2017, pp. 1-6.
13. 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), Pune, 2015, pp. 1424- 1428.
14. Y. Tawaragi, "Power theft inspection apparatus and method, and recording medium," U.S. Patent 14/593,160, 2015.
15. 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.
16. L. K. Lekha, G. Jegan and M. D. Ranganathan, "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.