Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 10, October : 2023

USING RASPBERRY PI TO DESIGN AN INTERNET OF THINGS-BASED METHOD FOR DETECTING ELECTRICITY THEFT

[#1]**Dr. M. GANESH,** ***Associate Professor,*** [#2]**Mr. R. SRINIVAS,** ***Associate Professor,***

[#3]**Mr. D. SAMPATH,** ***Associate Professor,*** [#4]**Ms. B. SRUJANA,** ***Associate Professor,***

[#1,2,3,4]**Department of Electronics and Communication Engineering,**

TRINITY COLLEGE OF ENGINEERING AND TECHNOLOGY, PEDDAPALLY

ABSTRACT: Energy production and consumption affect economic growth, hence power thievery slows it. Few countries profit from energy exports, even though most power is used locally. Utility companies lose a lot. Losses are technological and non-technical. The network avoids most technical losses, leaving wires and other devices to lose power. Measuring errors, unmetered energy, and electrical theft generate non-technical losses. Utility personnel struggle to spot electricity theft. This is addressed by our Raspberry Pi-based IoT electricity theft detection system. Researchers anticipate a rise in internet-connected things, in the coming years. This technology should improve utility efficiency and reduce losses. The research design architecture tries to discover illegal utility service provider-energy meter conduct on customer property. Due of internet connection, utility authorities can monitor the system live.

Keywords: *Internet of Things; Electricity Theft Detection; Raspberry Pi.*

1. INTRODUCTION

In the Internet of Things system, devices have IP addresses for online identification. Web growth from the internet, a computer network, continues. Researchers expect more internet-connected sensors, gadgets, and things in the future. Another name for IoT is product network. IoT can change lives. Today, event tracking automation is chosen over humans. This article's Internet of Things-based electrical theft detection system requires Raspberry Pi, relay, and system-powering hardware. Energy production and consumption affect economic growth, hence power thievery slows it. Few countries profit from energy exports, even though most power is used locally. Few countries profit from exporting power, although most growing countries generate electricity for internal use. Many emerging economies have suffered from energy stealing due to rising real estate and industrial electricity consumption. The World Bank's development indicator collection shows transmission caused 23% of Ghana's 2014 distribution and losses. Lower transmission and distribution losses are electric utility administrators' top priority. There are technological and non-technical losses. Technical losses are systematic but fixable. Power dissipation in transmission and distribution line equipment and conductors causes most residual losses. Untechnical losses result from energy meter misrecording, electricity theft, and poor metering. Energy theft occurs when electricity is used without permission and the meter is not monitored. Energy theft occurs when someone tamper with, avoid, or tap power lines to access residences. Customers have stolen power to avoid paying the correct price due to malfunctioning metering equipment and a lack of transparency and accountability in public utility billing. Electricity theft reduces utility and power distribution company investment. The ripple effect arises when theft-related losses are passed on to customers as inferior service or increased charges. Studies reveal energy theft accounts for 25% of Ghana's annual losses. Academics monitor and detect electricity theft using smart grid technologies. A Raspberry Pi and generalized IoT setup detect electricity theft in this study. Utility service entry and energy meter entrance currents are compared. Firebase stores and displays real-time comparisons. Several energy fraud detection systems are tested. Final section 5 reviews study implications and research ideas.

The detecting system we proposed covers the entire design. Conclusions and research proposals end chapter five.

2. RELATED WORKS

Current and prospective electricity theft detection designs are examined here. Academic rewriting is prohibited in user content. The theft detecting system has two current transformers at the energy meter's input and output. Power theft is suspected when current transformer input and output mismatch. Power line communication is used in system construction. Anti-theft energy metering system by Umar Hashmi and Jayesh G. Priolkar studies AMI and PLC technologies. Academics require a revised Md. Handshakes are used to exchange data between AMI residential meters M1 and M2. This method sends meter data to the energy provider's headquarters server. The reported value is 1 kWh. Comparing the two meters' consumption rates reveals the link. Programmable Logic Controller delivers server filtered signal frequency between M1 and M2. Signal changes indicate an unauthorized connection or intrusion. N. N Vinay. unknown background and identity. Shubham R explained ATmega32 architecture. The first current sensor measures source current, while the second measures the heavy load's current consumption. The master transceiver, coupled to the Atmega32, receives computerized data from the slave. CPUs continuously monitor sensor and LCD data. If any sensor detects an unwelcome burden, sensor one will measure more current than sensor two. Master microcontroller alerts operator via GSM modem when fault occurs. System to identify power theft was suggested. The embedded microprocessor compared two energy meters' consumption. Digital energy meter 1 determines distribution system energy delivery. A digital energy meter 2 simplifies home energy tracking. Digital energy meter 2 used eight units of energy, according to a smart hardware microcontroller. Digital meter 1's energy reading is compared to recorded data next.

Fig. 1. Cable for service distribution.

Plaintiff claims five two-way communication devices were stolen. Zig Bee electrical theft countermeasures technical document. An LCD panel displays energy meter resistance data from a microcontroller. Power theft control systems using WSNs have been extensively explored.

The authors suggest an Arduino-based billing and power theft detection system and an IoT-based monitoring and detection system. Power theft and automatic billing use current and voltage sensors.

3. METHODS EMPLOYED IN ELECTRICITY THEFT

Utility distribution service wires deliver electricity to energy meters. A typical distribution service line is shown in Figure 1. Ghana's largest electricity provider, the Electricity Company of Ghana (ECG), has placed energy meters to combat theft. Electricity consumption is measured by meters. Ghana uses mostly Whole Current (WC) and Transformer Operated (TO) energy meters. WC meter analysis is our main focus due of its widespread use. This section discusses power theft and meters.

Whole Current Meters

The client cargo acceptance facility receives these meters immediately. Low-energy residential and business consumers use them. WC meters use electromechanical or electrical technology.

Electrically conductive aluminum disks revolve at energy-related speeds, which the Electromechanical Meter counts. Revolutions imply energy utilization. The voltage coil's 2 volt energy usage is ignored by energy meters. Like the preceding coil, the current coil utilizes energy proportionate to the square of the current, usually a few watts at peak efficiency, according to the meter. The electromechanical energy measurement apparatus is shown in Figure 2. Fraudsters carefully installed enormous magnets on the meter's edges to control it. This motion slows aluminum disc rotation, saving electricity. The meter's plastic casing features holes for a magnetic needle to slow or halt disc spinning. Another way is circumventing utility meters and illegally connecting service lines to subscribers' homes. Power thieves attract ants by sugaring the meter's rotating disc. Slowing the disc's spinning speed slows electricity usage computation.

Electrical theft decreased after electronic meters were installed, but fraudsters found new tactics. Some meters can transmit data over long distances and display energy use on LEDs or LCDs. Manufacturer-specific impulse ratings per kWh are calculated by these meters. Electronic meters measure energy, reactive power, voltage, power factor, and maximum and minimum consumption rates. It supports time-of-night and day invoicing to estimate off-peak and peak energy use. Smart ZIGB and GPRS with utility system servers are used. The server sends the energy charge to the system server after meter transmission. Power customers receive a text message from the system server stating the charge. Using unique seals to lock out items boosts security. These meters can be bypassed and residential service connections compromised despite security measures. This is due to ECG/NEDCO field staff committing organized crime with clients. Unreliable electricians used contactors. Figure 3 shows how this strategy allows utility technicians to locate service lines undetected. Energy thieves often cut and disconnect neutral wires. The meter cannot monitor the voltage differential between the main and neutral wires and the consumer distribution board under these conditions. The meter's energy estimate will be off.

Fig.2. Electromechanical energy meters track power use.

This study was funded by the 5150 Spring Specialised (05492018012, 05762018039), the National Social Science Fund of China's Major Program (Grant No. 17ZDA092), Jiangxi Province's 333 High-level Talent Cultivation Project (BRA2018332), the Royal Society of Edinburgh, and the China Natural Science Foundation Council's joint International Projects Jiangsu Province's Basic Research Programs supported BK201913988.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 10, October : 2023

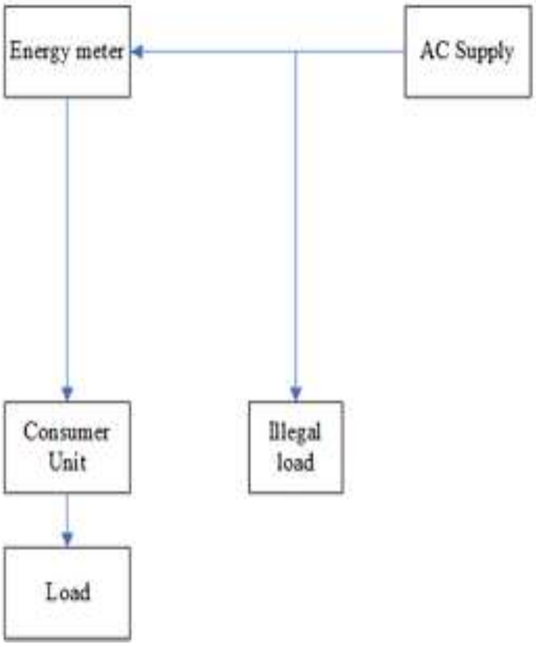

Fig.3. Illegal utility access is illegal.

4. THE PROPOSED SYSTEM

We advocate a Raspberry Pi-based IoT system to identify power theft in this study.

System Design

The Raspberry Pi foundation made minicomputers. UK firm promotes computer science and technology education. Free tools teach students how computers interact with sensors and other devices. First Raspberry Pi product released in 2006. Models A and B debuted February 19, 2012. A Model B+ was revealed in July 2014. On February 29, 2016, Raspberry Pi 3 Model B launched. Raspberry Pi is a cheap, tiny PC. Digital impulses can be converted to text. TVs and displays connect to Raspberry Pi. Raspberry Pis support mouse and keyboards. The CPU and GPU are Broadcom single-chip devices. Raspberry Pi 3 CPUs are 700–1200 MHz. Device RAM is 256–1 GB. SD media holds stable OS and app memory. Figure 4 displays Raspberry Pi parts.

Components

- We provide 2, 4, and 8 GB LPDDR4 3200 SDRAM.
- IEEE 802.11ac at 2.4 or 5 gigahertz offers wifi other than Bluetooth 5.0 and BLE.
- There are two USB 2.0 and two USB 3.0 ports.
- Fast networking gigabit Ethernet can transfer one gigabit per second.

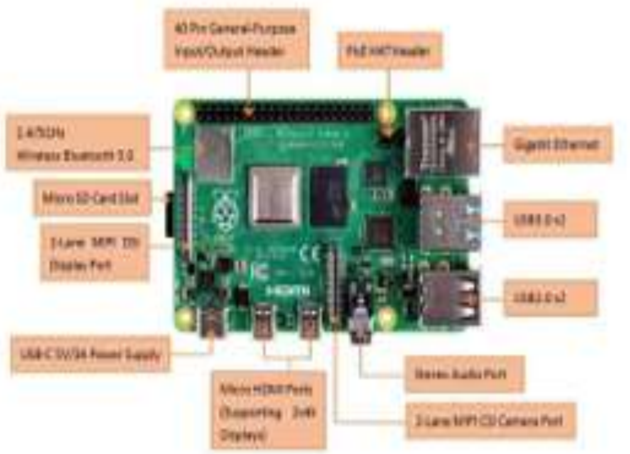

Fig.4. Single-board Raspberry Pi 4 computers appeal to academics.

- Full backward compatibility is provided by the 40-pin standard GPIO header.
- Two micro-HDMI ports support 4kp60.
- It has DSI display port and 2-channel MIPI CSI camera interface.
- Four-pole video and audio connectors transmit signals.
- It decodes H.265 at 4kp60, H.264 at 1080P60, and 1080p30.
- 3.0 OpenGL graphics
- The gadget stores and loads OS on micro-SD cards.
- USB-C supports 5V DC and 3A minimum current.
- The GPIO header supports 5VDC and 3A minimum current.
- Enable Ethernet PoE.

NodeMCU ESP8266:

Node MCU Development board firmware and kit are widely accessible. Short script lines in open-source firmware and developer kits build IoT apps. You may flash via USB with this feature. It employs a microcontroller and WIFI access point. The module's major component is the low-cost Wi-Fi microprocessor ESP8266, which features a full TCP/IP stack and microcontroller. These qualities make Node MCU WiFi networking popular. This technology can host web servers, download and publish data, and operate as an access point. This component allows Raspberry Pis to retrieve and publish data online.

Fig.5. The NodeMCU ESP8266 microcontroller board is popular.

Components

- Converters transform continuous analog impulses into discrete digital representations.
- Input and output GPIO pins are on the Node MCU. Digitally converting zeros and ones for LED control is simple. Additionally, it controls pulse width.
- The Node MCU-based ESP8266 has 4 SPI pins.
- HSPI links SPI. Devices connect to Quad-SPI via SPI. SPI facilitates adding devices to Node MCU-enabled devices, enhancing connectivity.
- I2C ports are on Node MCU GPIO pins.
- The universal asynchronous receiver transmitter connects UART 0 and 1. Onboard firmware and protocols are uploaded via UART0.

Relay Module:

The circuit board is a 4-channel relay interface with 5V and 15–20 mA per channel. Manage high-current home appliances and devices. A high-current relay can operate at 250 volts and 10 amps of alternating current or 30 volts and 10 amps of direct current. The microcontroller in Figure 6 operates the interface via protocols.

Components

- Relay outputs 250 volts AC and 10 amps DC.
- The 4-way relay module supports several electrical circuits using four relays.
- A standard interface can be controlled by Raspberry Pi.
- Safety and high-voltage ground protection necessitate isolation opto couplers.

Fig.6. This is the relay module block diagram.

Fig.7. Discussion is about Current Sensor.

Current Sensor:

A proportional signal is output by the ACS712 current sensor, which monitors wire or network current. Raspberry Pi comparators receive and send sensor signals. Use relay module to investigate observed current.

Firebase Server:

Firebase, a Back-End-as-a-Service (BaaS) platform from YC11 at Y Combinator, is now part of Google Cloud as a cutting-edge application development platform. Firebase lets developers focus on UI. Replace server hosting with Firebase. Firebase stores data, offers an API, and servers. Due to its generic nature, Firebase's data storage must be customized. This flexibility allows Google Cloud storage. Firebase storage platform security provides authenticated users access to the Google Cloud container.

Utility Service Box (USB):

Utility Service Boxes have current-sensor relay modules. This gadget on a utility pole is only accessible to authorized people.

System Architecture

The Utility Authority will monitor systems live. This architectural solution can recognize and convert illegal content into text Node MCU can save on Firebase.

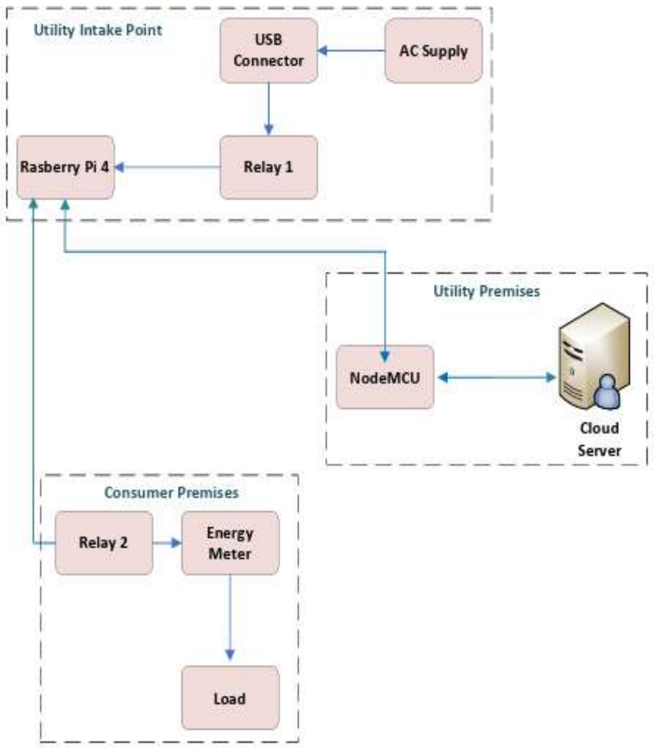

Fig.8. This graphic displays an IoT-based electricity detecting system's activity flow.

5. CONCLUSION

Raspberry Pi-based IoT detects power theft. Architecturally designed four-channel relay interface circuit boards with current sensors accurately detect and record current imbalances. Raspberry Pis allow utility regulators to monitor USB interface and energy meter thefts live. The design used Node MCU to access Firebase's G Cloud data. Future system use research will evaluate this design's viability.

REFERENCES

1. N. Donald, The Internet of Things: Do-It-Yourself at Home Projects for Arduino, Raspberry Piand Beagle Bone Black, London: McGraw- HillTABElectronics,2015
2. WORLD BANK, Electric power transmission and distribution losses(%of output) – Ghana, World Bank, Ghana, 2018.
3. J. Parmar, Total losses in power distribution and transmission lines, Electrical Notes, vol. 1, no. 2, pp. 33-47, 2013.
4. O. Eseosa and E. Promise, Economic Effects of Technical and NonTechnicalLossesinNigeriaPowerTransmissionSystem,IOSRJournalofElectricalandElectronicsEngineeringVer.I,vol.10,no.2,pp.2278-1676,2015.
5. P. Navani, N. K. Sharma and . S. Sonal, A Case Study Of Analysis OfTechnical And Non-Technical Losses In Power System And Its ImpactOn Power Sector, International Journal Of Advances In EngineeringScience And Technology (IJEAST), vol. 1, pp. 2319-1120, 2013.
6. T. B. Smith, Electricity theft: A comparative analysis, Energy Policy,vol. 32, no. 18, pp. 2067-2076, 2004.
7. Ghanaweb, ECG to fight power theft as it faults churches, Ghanaweb,the 2nd of March 2020. [Online]. Available:https://www.ghanaweb.com/GhanaHomePage/business/ECG-to-fight-power-theft-as-it-faults-churches-836506. [Accessed 06 08 2020].
8. K.B.Amal,T. G.AlphyandN. K. Fathima, HOME ENERGY MANAGEMENT SYSTEM BASEDON POWER LINE, International Research Journal of Engineering and Technology(IRJET),vol.4, no.4, p.2532,2017.
9. M. U. Hashmiand J. .G. Priolkar, Anti-theftenergy metering fosmart electrical distribution system, in 2015 International Conference on Industrial Instrumentation and Control, ICIC 2015, Maharashtra, 2015.

10. S.N.Vinayand M.R.Shubham, WSN-POWERTHEFTCONTROL, International Research Journal ofEngineering and Technology (IRJET),vol. 04, no. 01, p. 1984, 2018.