

Unplugging The Thieves Microcontroller Based Power Theft Detection

Prof. Balasaheb Jadhav¹, Roshan Madake², Aditya Madale³, Rajesh Madewar⁴, Rushikesh Lonkar⁵, M.S. Dawglinia Fanai⁶, Rahul Madhawani⁷

^{1,2,6,7}Dept. of Computer application Vishwakarma Institute and Technology, Pune-Bibwewadi

^{3,4}Dept. of mechanical engineering, Vishwakarma Institute of Technology, Pune-Bibwewadi

⁵Dept. of Instrumentation Engineering, Vishwakarma Institute of Technology, Pune-Bibwewadi

Abstract—As we all know the matter of electricity theft is a big problem in developing countries like India. Poor people who don't want to pay for the services of electricity often steal it and someone else has to pay for the service which he is not availing. This builds up for a huge need for electricity theft monitoring system in our country so that people can be aware of electricity theft and they don't have to pay for someone else's luxury.

Keywords— Arduino uno, GSM Module, IoT, Monitoring, Detection.

I. INTRODUCTION

The problem of electricity theft in developing countries cannot be overemphasized. According to a report by "The Tribune" as of 2021-22 in 1,81,078 meters checked, 45,470 cases of electricity theft were detected, that comes out as a 25% electricity theft ratio. It totalled to a value of 156.65 crores worth of stolen. For these 42,501 FIR'S have been filed in Police Station. It is not only that but people who risk their lives to hang onto live electricity transmission cables and poles so that they can hang wires on them for stealing electricity is a huge problem because this can lead to serious injuries in case of loss of balance and in some cases death either due to electrical shock from the live wires or due to physical shock from falling from the 120ft electricity pole. This is a big problem and it needs to be tackled with a solution that is not only accurate but also affordable and easy to use in slum areas. Microcontroller Based Power Theft Detector is a simple device that can be used to warn people about electricity being stolen. It is also not very big in size which in turn makes it portable and not very expensive too as we are targeting a middle class audience as that is where electricity is and will be stolen from. It will also send a message to the respective person when it detects electricity theft.

II. EASE OF USE

A power theft detector will let people know about electricity theft either from their circuit boards or from the directly overhead power transmission wires. It is such a device that can be used a lot in slum areas where it is common for people to hang live wires of power transmission cables to steal electricity.

This paper is a detailed study about power theft detectors. Our device uses components like Arduino uno, GSM module, etc for detection of power theft and thereby save people's hard earned money from being wrongly wasted. Some of the novelty features include:

1. Quick Detection: Our device can easily and hastily detect electricity theft in just a matter of seconds and can sound a buzzer whenever electricity theft is detected.
2. Communication with the owner: Our device will send a message to the mobile phone of the device owner informing about the theft so the person can take necessary action against the culprits.

III. COMPONENTS USED

1. Arduino Uno: The first and most important component of our device is the Arduino uno microcontroller. The Arduino uno is a commonly used microcontroller made by Arduino.cc. It is a single board microcontroller that is used for building digital devices. The CPU used on the Arduino Uno are Atmel AVR(8-Bit), ARM Cortex-M0+(32-Bit), ARM Cortex-M3(32-Bit) and Intel Quark(x86) (32-Bit).

It uses SRAM and Flash EEPROM Storage. A microcontroller board called Arduino UNO is based on the ATmega328P. It contains 6 analogue inputs, a 16 MHz ceramic resonator, 14 digital input/output pins (six of which can be used as PWM outputs), a USB port, a

power jack, an ICSP header, and a reset button. It comes with everything needed to support the microcontroller; to get started, just plug in a USB cable, an AC-to-DC adapter, or a battery. You can experiment with your UNO without being overly concerned that you'll make a mistake; in the worst case, you can replace the chip for a few dollars and start over. Due to the fact that it is not soldered to the board, the ATmega328P can be simply replaced. It consists of several input output pins and it can be programmed using the C and c++ languages in the Arduino IDE Software. The picture of a Arduino Uno is shown below.



Fig 1:Arduino Uno

2. GSM Module SIM900A: A GSM module or a GPRS module is a chip or circuit that will be used to establish communication between a mobile device or a computing machine and a GSM or GPRS system. The modem (modulator-demodulator) is a critical part here. A GSM OR A Global System for mobile communications is a device developed by the ETSI and is commonly used for enabling wireless communication between devices. They use SIM cards like we have in our mobile phones to identify their device to the network. It is a circuit switched system that divides each 200000 Hertz channel into multiple time slots. can be paired with the Arduino uno microcontroller and thus can be used for sending and receiving messages, internet connectivity, I the case of our device we will be using it for receiving messages in case of electricity theft. The different types are also gsm/gprs modem's, mobiles, etc. The picture of a GSM Module SIM900A is shown below.



Fig 2:GSM Module SIM900A

3. Relay Module: The relay is the device that open or closes the contacts to cause the operation of the other electric control. It detects the intolerable or undesirable condition with an assigned area and gives the commands to the circuit breaker to disconnect the affected area. Thus protects the system from damage. A relay is a electronically operated switch that can be switched on or off and can be used to allow current flow or restrict it with low voltages like the 5V we use in the Arduino Uno. the relay we are using has 2 channels and it is used to protect the other components from short circuit. The picture of a relay module is shown on the next page.



Fig 3:2-Relay Module

4. ACS 712 Current Sensor: Voltage drops as current flows across a conductor. Ohm's law specifies the relationship between current and voltage. An increase in current above what is required by an electronic equipment causes overload, which may result in device damage. Current measurement is required for the proper operation of equipment. Voltage measurement is a passive operation that can be carried out without influencing the system. As opposed to measuring voltage, which is an intrusive task

that cannot be observed directly. The ACS 712 is a linear current sensor based on the hall effect. While other sensors work on the principle of Ohm’s Law that is they measure the voltage drop between two ends and then multiply it by resistance to calculate the current, the ACS 712 works on the Hall Effect. The current flows through a onboard hall sensor circuit in its Integrated Circuit and the hall effect sensor then measures the current using magnetic field generation and the principle of magnetic effect of Electric Current. We are using the above said sensor in our project as a device to measure electric current. The picture of a ACS 712 Current Sensor is shown below.



Fig 4.ACS 712 Current Sensor

IV. METHODOLOGY

A microcontroller-based electricity theft detection system works in the following ways:

1.Hardware Installation: The system must contain a microcontroller, a power meter such as a power divider, a power meter such as a current transformer, and a communication module. (like GSM or Ethernet modules). In addition, the system must be connected to the distribution network.

2.Voltage and Current Detection: Voltage sensors are installed in power lines to measure voltage. It converts analog voltage signals into digital signals that can be processed by a microcontroller. Current sensors measure the current flowing through the power line and convert it into a digital signal.

3.Calibration: The system must be calibrated to produce a normal power reading before detecting power tampering. This calibration is done by measuring and recording voltage and current values when tampering does not occur.

4.Power Monitoring: The microcontroller continuously monitors voltage and current readings from sensors.

Calculates power consumption over time by multiplying voltage and current values. Compare the calculated power consumption with the reading on the bottom of the meter to determine if there is a difference.

5.Voltage Surge Analysis: Power theft is often associated with bypassing voltage meters or tampering with power lines. These activities lead to changes in the system. The microcontroller detects the change in voltage by comparing it with the previous counter. If the voltage fluctuation is above the threshold, it indicates a potential tampering.

6.Tamper Detection: Microcontrollers use various algorithms and techniques to detect power consumption patterns and voltage changes. If it detects a significant difference between the measured value and the presence of the abnormality, it may make a loud noise or require indication of discomfort.

7.Communication and Alarm Systems: When electricity theft is detected, the microcontroller informs the authorities or administrators. This can be done by various communication methods such as GSM or Ethernet. The system can also be designed to generate automated actions such as alerts, alerts, or even power off unauthorized users.

8.Data Logging and Analysis: The microcontroller can store data on power consumption, power changes and related events in memory for further analysis and storage. This information can be used to generate reports, analyze trends, and improve performance over time.

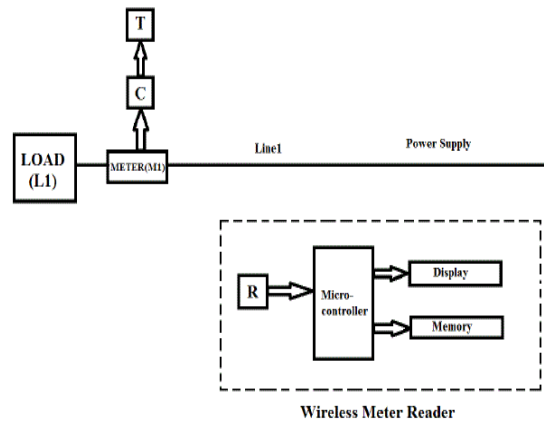


Figure 5: Wireless meter reading

Fig 5:Components,Connection and Working of the device

V.ADVANTAGES

Microcontroller based energy theft system has many advantages over traditional systems. Here are some key advantages:

1.Real Time Detection: Microcontroller based systems can monitor and analyze power consumption patterns in real time. The meter quickly detects unusual or unauthorized activities such as tampering or illegal connections.

2.Precision: Microcontrollers have high processing power and can perform complex calculations accurately. The system can accurately analyze the energy consumption data and distinguish between normal exchange and real energy theft.

3.Cost-effective:

Microcontrollers are relatively inexpensive and readily available. Using a microcontroller as a power thief is cost-effective compared to other complex systems. It requires minimal hardware and can be easily integrated into existing electronic devices.

4.Remote Monitoring and Control: The microcontroller can be connected to a central monitoring station or server via communication means such as Ethernet, Wi-Fi or GSM.

Take care of the remote control and control of the power distribution and facilitate rapid response to theft incidents.

5.Data Logging and Analysis: Microcontrollers can store utility data for analysis and reporting.

This information can be used to analyze spending patterns, investigate crime, and generate detailed information for further investigation or legal action.

6.Alarms and Warnings: Microcontroller based systems can generate alarms or warnings when power is detected. This allows for quick action, such as sending personnel to the site or notifying the police, to reduce theft and reduce loss of revenue.

7.Energy saving: The system can identify bad consumption patterns or waste products by accurately monitoring energy consumption. This information can be used to implement energy saving strategies and optimize energy distribution, resulting in overall energy

savings.

8.Deterrent Factor: The presence of an electronic anti-theft system creates a deterrent for criminals. Knowing that their activities can be caught and punished can deter people from trying to steal electricity, leading to a safe and equitable distribution of electricity.

VII.LIMITATIONS

Although microcontroller-based energy theft systems have many advantages, they also have some limitations. Below are some of the limitations associated with these systems:

1.Limited capabilities:

Microcontroller-based systems are generally designed for Specific applications or limited spaces. Scaling these systems to cover large deployments or multiple sites can be difficult. It will require additional hardware, communications infrastructure and data management capabilities.

2.Depending on the power supply:

The microcontroller needs a stable power supply to function properly. Power outages or blackouts can affect system performance. A redundant power solution or a reliable power supply should be considered for ongoing maintenance and operation.

3.Tamper Vulnerabilities:

Like all electronics, microcontroller-based systems are vulnerable to tampering or hacking. Advanced attackers may attempt to manipulate a system or corrupt its data to avoid detection. To mitigate these risks, strong security measures such as access, authentication and physical protection should be implemented.

4.Vulnerabilities and false negatives:

Microcontroller-based power theft detection systems rely on data analysis techniques to identify malicious patterns. However, these algorithms can produce false results (indicating legitimate use as theft) or negative results (inability to detect actual theft). There is a need for continuous development and improvement of search algorithms to minimize errors.

5.Maintenance and Calibration:

Microcontroller-based systems require regular maintenance and calibration to provide accurate and

reliable readings. Sensors, communication systems, and other physical components need to be analyzed and evaluated from time to time. Failure to do so may result in incorrect readings or poor performance.

6.Data management and privacy concerns: Microcontroller-based systems for generating and storing large amounts of data. Managing and analyzing this data can be a complex task that requires dedicated resources and data management. Additionally, privacy concerns arise when the system collects and processes data and must be carefully monitored by privacy laws and data protection.

7.Integration with Existing Systems:

Implementing microcontroller-based systems may require integration with existing distribution systems, including sensors, transformers, and circuits. Social problems, competition problems and complex integration may arise in the integration process.

8.Cost considerations:

While the microcontrollers themselves are relatively inexpensive, the total cost of using the power theft device includes other components such as sensors, communications infrastructure, software development, installation and maintenance. The cost of implementing and maintaining the system must be carefully considered to ensure its feasibility and return on investment.

VII.CONCLUSION

This method will greatly reduce the loss of energy and income from electricity theft. From this it can be concluded that there is a huge need for these products on both the customer home to home level and also on international business offices level. Our will not only help save money but will also be helpful in many other cases due to the use of microcontrollers. We can add another sensor and connect it with the Arduino like and Ultrasonic Sensor and use it to measure the amount of rainfall in that area.

REFERENCE

- [1]"Controlling electricity theft and improving revenue", World Bank report on reforming the power sector, 2010.
- [2]Annual report of power and energy division of planning commission,

government of India, New Delhi, 2011-12.

[3]"All India Electricity Statistics", Central Electricity Authority, Ministry of Power, Government of India, New Delhi, 2011-12.

[4]www.arduino.cc, March 31, 2017

[5] R. M. Mutupe, S. O. Osuri, M. J. Lencwe and S. P. Daniel Chowdhury, "Electricity theft detection system with RF communication between distribution and customer usage," IEEE PES PowerAfrica, Accra, 2017, pp. 566-572.

[6]M.Saad,M.F.Tariq,A.Nawaz and M.Y. Jamal,"Theft detectionbased GSM prepaid electricity system," IEEE International Conference on Control Science and Systems Engineering (ICCSSE), Beijing, 2017, pp. 435-438.

[7] R.E.Ogu and G.A.Chukwudebe,"Development of a cost-effective electricity theft detection and prevention system based on IoT technology," IEEE International Conference on Electro-Technology for National Development (NIGERCON), Owerri, 2017, pp. 756-760.

[8] A. S.Metering, S.Visalatchi and K. K. Sandeep, "Smart energy metering and power theft control using arduino & GSM," 2nd International Conference for Convergence in Technology (I2CT), Mumbai, 2017, pp. 858-961.