Abstract – Command to the GSM is the main objective of this paper. Also, to send a message in the event of energy meter being tampered. The alert message is sent via GSM modem to the concerned authority. As electricity consumption is increasing, so is the attempt for tampering the energy meter. Identifying a tampered meter is only possible when the electricity board’s authority manually checks it, which is a time consuming and costly method. This proposed system detailed in the paper is a possible solution to detect meter tampering. Energy meter is integrated with the system in such a way that if anybody opens the cover of the meter, an IR sensing arrangement sends a command to the microcontroller (8051 family). Microcontroller then senses a change in the logical input from IR sensor and gives modem to send an SMS to the designated mobile phone number stored in the controller’s memory. The project in future can be enhanced by having an added feature of disconnecting the supply to the load by electricity department through SMS in case of any tampering of energy meter.

Keywords – Tampering, GSM, Modem, Micro-controller, Meter.

I. INTRODUCTION

An electric meter is a device used for measuring the amount of electrical energy supplied to a residential or commercial building. Due to the increasing cost of electricity, tampering and security in electric meters has become a major concern for government agencies across the globe. Especially in populous countries like India tampering in electric meter and energy theft have become quite common.

Electric meters can be manipulated, thus causing them to stop, under-register or even bypassing the meter. Consumers, who tamper with electric meter, effectively use power without paying for it. This theft or fraud can be dangerous as well as dishonest. Electric meter security is looked upon as major issue in many countries today.

Today, many power companies are installing remote-reporting meters which are capable of detecting any tampering in electric meters, and discover energy theft. These smart power meters are particularly helpful in preventing energy theft and encouraging security in electric meters.

A large portion of a country’s revenue is lost due to the high density of tampering and security in electric meters. Hence it becomes very important to detect tampering in electric meters to ensure proper billing. Electric meter readers are trained to spot signs of tampering. The consumers who tamper with electric meter may be charged each billing period with the maximum rate until the tamper is removed, or in some cases the service may also be disconnected.

Rectified DC loads causes mechanical but not electronic meters to under-register. As the DC currents do not cause the coils to make eddy currents in the disk, thus causing reduced rotation and a lower bill. Other ways of tampering in electric meters and playing with the electric meter security is to use some combinations of capacitive and inductive load, which also result in reduced or reverse motion.

Today, many modern meters can easily detect all of these effects. The owner of the meter normally secures the meter against tampering. Newer computerized meters usually have counter-measures against tampering. In order to find and fix power distribution problems, power companies today normally investigate discrepancies between the total billed and the total generated. These investigations are an effective method of discovering tampering and security in electric meters.

Literature Survey reveals work of [10] which details collecting energy consumption during electricity stealing due to external tampering, partial earth, double feeding, magnetic interference, reverse polarity, missing potential bypass energy meter etc thus reducing losses. No tampering due to specific reason noted. [11] explains how GSM modem is used to intimate consumer about power shut down schedule, about their monthly bills or to inform area supervisor incase of emergency. Also [12] has described monitor consumption of power in order to improve the utility of power, wireless low work load, great quantity of data transmission, high veracity and low expenses using embedded system improves stability of wireless data transmission.

Paper discusses tampering detection of energy meter by GSM modem for different modes of tampering like (i) Energy meter case removal (ii) interruption by hand and (iii) disturbance of energymeter lay out (iv) under-register. No tampering due to specific reason noted. Also using a GSM modem interfaced with 8051 microcontroller using MAX232 IC to alert the customer in case the tampering is
done. Basically the IR sensor will detect the tampering which will send the data to a port of microcontroller. Now this microcontroller will send the GSM the signal to notify the customer whose meter is being tampered.

II. TAMPERING

Methods Of Tampering

![Diagram of Tampering Methods](image-url)
III. HARDWARE

Microcontroller

The AT89C51 is a low-power, high-performance CMOS 8-bit microcontroller with 4K Bytes of Flash programmable and erasable read-only memory (PEROM). The device is manufactured using Atmel’s high-density non-volatile memory technology and is compatible with the industry-standard MCS-51 instruction set and pin out. The on-chip Flash allows the program memory to be reprogrammed in-system or by a conventional non-volatile memory programmer. By combining a versatile 8-bit CPU with Flash on a monolithic chip, the Atmel AT89C51 is a powerful microcomputer which provides a highly-flexible and cost-effective solution to many embedded control applications.

In addition, the AT89C51 is designed with static logic for operation down to zero frequency and supports two software selectable power saving modes. The Idle Mode stops the CPU while allowing the RAM, timer/counters, serial port and interrupt system to continue functioning. The Power-down Mode saves the RAM contents but freezes the oscillator disabling all other chip functions until the next hardware reset.

MAX 232 IC

The MAX232 is a hardware layer protocol converter IC manufactured by the Maxim Corporation. It consists of a pair of drivers and receivers. Basically, a driver converts TTL & CMOS voltage levels to the voltage levels which are compatible for serial communication.

The MAX232 requires a voltage between -3 V to -15 V to represent binary 1, and a voltage between +3 V to +15 V to represent binary 0. For CMOS and TTL communication, this is incompatible since TTL uses 5 V to represent binary 1 and 0 V to represent binary 0. This chip therefore performs the necessary conversion of the electrical voltage levels in both directions.

It also contains a dual charge pump dc-dc voltage converters. It has two internal charge pumps that converts +5 V to +10 V & -10 V for RS-232 operations. The first converter uses capacitor C1 to double the +5 V to +10 V on C3 at the v+ output. The second converter uses capacitor C2 to invert +10 V to -10 V at C4 on v- output.

One particular application of MAX232 is that it eliminates the need of bipolar (+ or -) 12v supply.

GSM SIM300

GSM/GPRS RS232 Modem is built with SIMCOM Make SIM900 Quad-band GSM/GPRS engine, works on frequencies 850 MHz, 900 MHz, 1800 MHz and 1900 MHz. It is very compact in size and easy to use as plug in GSM Modem. The Modem is designed with RS232 Level converter circuitry, which allows you to directly interface PC Serial port. The baud rate can be configurable from 9600-115200 through AT command. The modem needed only 3 wires (Tx, Rx, GND) except Power supply to interface with microcontroller/Host PC. Using this modem, you will be able to send & Read SMS, connect to internet via GPRS through simple AT commands.
IV. Flow Chart for Operational Mode

Scan the output of IR Sensor @ P0.7
i.e. Mybit.

mybit=0?

Send AT Command to Sim800 to Send

NO

YES
V. BLOCK DIAGRAM AND SIMULATION

1. 12V/1A DC Supply
2. 7805 IC
3. AT89C51 MCU
4. MAX232 IC
5. SIM 300
LAYOUT AND OBSERVATIONS

1. REMOVAL OF CASE
2. OBSTACLE OF HAND

3. DISTURBANCE OF LAYOUT – IR SENSOR

4. RESULT
VI. CONCLUSION

Firstly the working of photo diode-IR LED transmitter receiver pair has been verified. Now as the cover is removed from the sensing arrangement it sends the data to p0.7 of microcontroller. Microcontroller loaded with the proper program sends GSM the command to send a message on a number which is provided in the program.

Thus paper has summarized realization of detection of tampering of energy meter and sending a message to a mobile, through software proteus and hardware configuration.

REFERENCES

[12] S Arun and Dr. Sidappa naidu,” Design and implementation of automatic meter reading system using GSM, zigbee through GPRS.” Int. journal of advanced research in computer science and software Engg., vol2,issue 5, May 2012

AUTHOR'S PROFILE

Patel Ishan
is a student of Final Year Graduation Studies at Department of Elect and Electronics Engg, Faculty of Technology & Engineering, The Maharaja Sayajirao University of Baroda, Vadodara, Gujarat, India.

Ansol Saini
is a student of Final Year Graduation Studies at Department of Elect and Electronics Engg, Faculty of Technology & Engineering, The Maharaja Sayajirao University of Baroda, Vadodara, Gujarat, India.

Axat Soni
is a student of Final Year Graduation Studies at Department of Elect and Electronics Engg, Faculty of Technology & Engineering, The Maharaja Sayajirao University of Baroda, Vadodara, Gujarat, India.

Anuradha S. Deshpande
is an Associate professor working with department of Elect and Electronics Engg, Faculty of technology & Engineering, M.S.University of Baroda, Vadodara 390001, Gujarat, India. She has obtained her ME in Electrical Engg from the same university where she is employed. She has many publications published in National and International Journals of repute. She has membership of ISTE, IEEE, Institution of Engineers India, Society for power engineers etc. She has obtained gold medals and awards at different stages of her career.