IoT Based Power Theft Detection

Suhail Bhat[1] Ms. Shalini Kashyap[2]
[1]M. Tech Student [2]Assistant Professor
[1,2]Department of Electronics and Communication Engineering
[1,2]Satya College of Engineering and Technology, Palwal

Abstract— The Internet of Things (IOT) is the network of physical objects—devices, vehicles, buildings and other items which are embedded with electronics, software, sensors, and network connectivity, which enables these objects to collect and exchange data. The IOT Based Power Theft Detection System is unique of its kind. It can detect power theft and electric meter tampering. Whenever meter tampering is done or overload is detected, the system senses it with the help of LDR and current sensors. Once it has detected the theft, it generates a log for theft type and timing with help of RTC and at the same time publishes this log info over internet website. It sends SMS to the subscriber reporting the type of theft.

Key words: LDR, IoT, RTC

I. INTRODUCTION

The Internet of Things (IOT) allows objects to be sensed and controlled remotely across existing network infrastructure, creating opportunities for more direct integration of the physical world into computer-based systems, and resulting in improved efficiency, accuracy and economic benefit. Driven by the popularity of gadgets empowered by wireless technological innovation such as Wireless Bluetooth, Radio Frequency Identification, Wireless-Fidelity, embedded sensor, IoT has moved out from its beginning stage and it is actually on the edge of changing the present fixed internet into a well featured upcoming Internet. Currently there are almost nine billion inter-connected gadgets and it is estimated to touch almost fifty billion gadgets by 2020.Today the world is facing such an environment that offers challenges. Energy crisis is the main problem faced by our society. There are two types of losses technical and Nontechnical losses. Every year the electricity companies fare the line losses at an average 20-30% according to power ministry WAPDA Company's loss is more than RS.125 billion.

Vidyut Upbhogta Sangh submitted the report in 2015 that in U.P. the losses at an average are 25.38% which results in the loss of around INR 10,000 Crores. Electricity theft is at the centre of focus all over the world, but electricity theft in India has a significant effect on the Indian economy. The loss on amount of theft is reflected in ARR of the electricity company. Thus these costs are routinely passed on to the customers in the form of the higher energy charges. Mr. R.K. Singh, Energy Manager, Indus Tower Ltd, submitted that Distribution Licensees inability to curtail losses is the main reason for tariff hikes in UP. The report of Vidut Upbhogta Kendra also states that the net revenue collected from the consumers is approximately INR 10,000 Crore in state of U.P. So, even if the losses are reduced by 5%, then it will result in equivalent tariff distribution by 25%. This paper discusses the problem of electricity theft as well as proposed new methods to reduce electric theft and catch the culprit red handed in case anyone tries to steal it away. Negative effects of electricity theft are severe and dangerous. Modes of Power Theft:-

1) Meter Tampering.
2) Overloading.

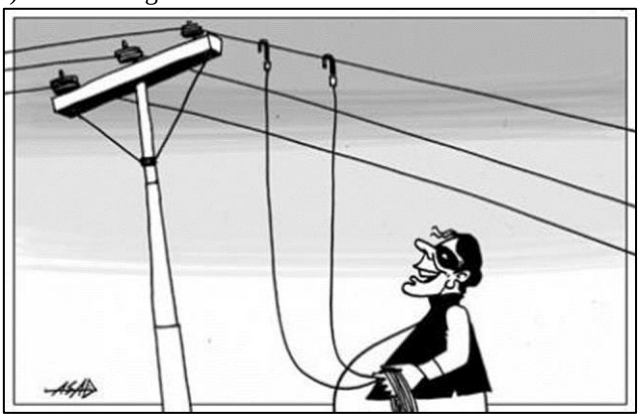

Fig. 1:

II. LITERATURE SURVEY

There are many factors that encourage people to steal electricity of which socio-economic factors influences people to a great extent in stealing electricity. A common notion in many people is that, it is dishonest to steal something from their neighbor but not from the state or public owned utility company. In addition, other factors that influence illegal consumers are:

- Higher energy prices deject consumers from buying electricity. In light of this, rich and highly educated communities also steal electricity to escape from huge utility bills.
- Growing unemployment rate show severe effect on the customer's economic situation.
- Lower illiteracy rate in under developed communities has greater impact on illegal consumers, as they might not be aware of the issues, laws and offenses related to the theft.
- Weak economic situation in many countries has implied its effect directly on common man.
- In view of socio economic conditions of the customer, electricity theft is proportional to the tariff of electricity utilization.
- Countries with weak enforcement of law against electricity theft have recorded high proportion of theft.

Negative effects of electricity theft are severe and dangerous. Primarily, electricity theft affects the utility company and then its customers. In addition, electricity theft overloads the generation unit. In energy market, utility companies expect their money back from the customers for the electricity supplied, most of which is lost by them due to not investing on measures to reduce the electricity theft. These economic losses affect the utility company's interest in development of the devices in view of improving the quality

of supply or for electrification process. Earlier theft was more common in villages because they need more power requirement for their field to drive water pump and for motor. But today it is not only limited to villages but also to industrial areas as well as consumer side comes under power theft. There are various modes of power theft such as Bogus seal and tampering of seals, Meter tampering, meter tilting, meter interface and meter bypassing, Changing connection etc.

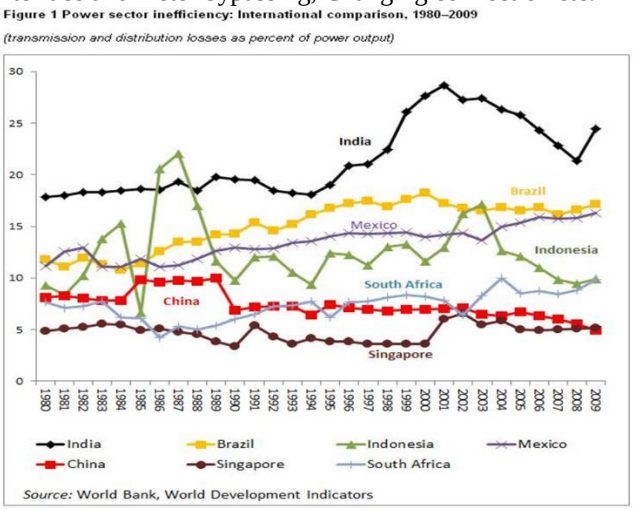

Fig. 2.1:

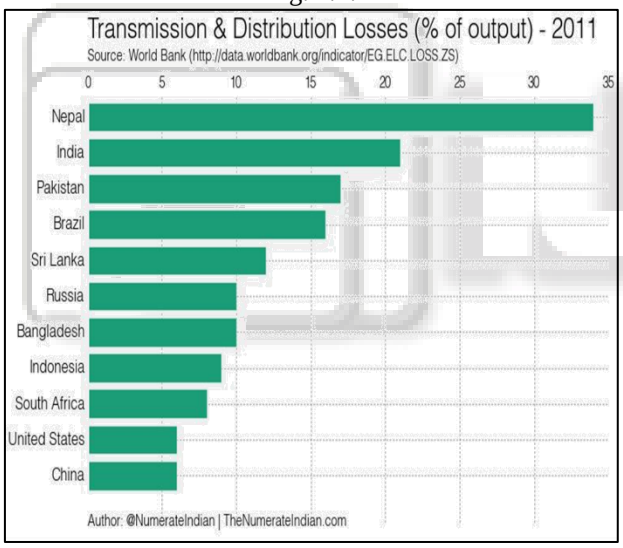

Fig. 2.2:

III. COMPONENTS USED

A. *GSM Module*

GSM (Global System for Mobile Communications, originally Groupe Spécial Mobile), is a standard developed by the European Telecommunications Standards Institute (ETSI) to describe the protocols for second-generation (2G) digital cellular networks used by mobile phones, first deployed in Finland in July 1991. As of 2014 it has become the default global standard for mobile communications - with over 90% market share, operating in over 219 countries and territories.
2G networks developed as a replacement for first generation (1G) analog cellular networks, and the GSM standard originally described a digital, circuit-switched network optimized for full duplex voice telephony. This expanded over time to include data communications, first by circuit-switched transport, then by packet data transport via GPRS (General Packet Radio Services) and EDGE (Enhanced Data rates for GSM Evolution or EGPRS).

Subsequently, the 3GPP developed third-generation (3G) UMTS standards followed by fourth-generation (4G) LTE Advanced standards, which do not form part of the ETSI GSM standard.

1) Technical Details

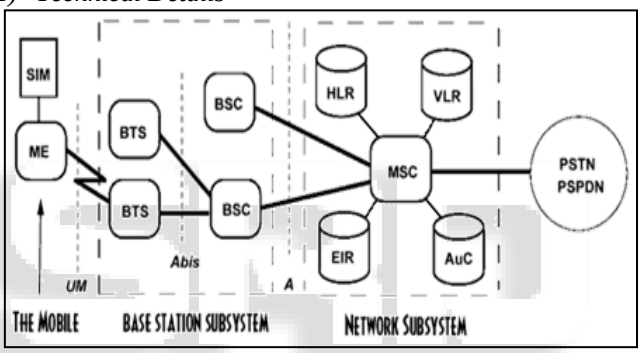

Fig. 3.1:

The network is structured into a number of discrete sections:

- Base Station Subsystem – the base stations and their controllers explained.
- Network and Switching Subsystem – the part of the network most similar to a fixed network, sometimes just called the "core network".
- GPRS Core Network – the optional part which allows packet-based Internet connections.
- Operations support system (OSS) – network maintenance.

2) Base Station Subsystem

Fig. 3.2:

3) GSM cell site antennas in the Deutsches Museum, Munich, Germany

GSM is a cellular network, which means that cell phones connect to it by searching for cells in the immediate vicinity. There are five different cell sizes in a GSM network—macro, micro, pico, femto, and umbrella cells. The coverage area of each cell varies according to the implementation environment. Macro cells can be regarded as cells where the base station antenna is installed on a mast or a building above average rooftop level. Micro cells are cells whose antenna height is under average rooftop level; they are typically used in urban areas. Pico cells are small cells whose coverage diameter is a few dozen meters; they are mainly used indoors. Femtocells are cells designed for use in residential or small business environments and connect to the service provider's network via a broadband internet connection. Umbrella cells are used to cover shadowed regions of smaller cells and fill in gaps in coverage between those cells.

Cell horizontal radius varies depending on antenna height, antenna gain, and propagation conditions from a couple of hundred meters to several tens of kilometers. The longest distance the GSM specification supports in practical use is 35 kilometers (22 mi). There are also several implementations of the concept of an extended cell, where the cell radius could be double or even more, depending on the antenna system, the type of terrain, and the timing advance.
Indoor coverage is also supported by GSM and may be achieved by using an indoor Pico cell base station, or an indoor repeater with distributed indoor antennas fed through power splitters, to deliver the radio signals from an antenna outdoors to the separate indoor distributed antenna system. These are typically deployed when significant call capacity is needed indoors, like in shopping centers or airports. However, this is not a prerequisite, since indoor coverage is also provided by in-building penetration of the radio signals from any nearby cell.

4) GSM carrier frequencies

GSM networks operate in a number of different carrier frequency ranges (separated into GSM frequency ranges for 2G and UMTS frequency bands for 3G), with most 2G GSM networks operating in the 900 MHz or 1800 MHz bands. Where these bands were already allocated, the 850 MHz and 1900 MHz bands were used instead (for example in Canada and the United States). In rare cases the 400 and 450 MHz frequency bands are assigned in some countries because they were previously used for first-generation systems.

Most 3G networks in Europe operate in the 2100 MHz frequency band. For more information on worldwide GSM frequency usage, see GSM frequency bands.

Regardless of the frequency selected by an operator, it is divided into timeslots for individual phones. This allows eight full-rate or sixteen half-rate speech channels per radio frequency. These eight radio timeslots (or burst periods) are grouped into a TDMA frame. Half-rate channels use alternate frames in the same timeslot. The channel data rate for all 8 channels is 270.833 kbit/s, and the frame duration is 4.615 ms.

The transmission power in the handset is limited to a maximum of 2 watts in GSM 850/900 and 1 watt in GSM 1800/1900.

5) Subscriber Identity Module (SIM)

One of the key features of GSM is the Subscriber Identity Module, commonly known as a SIM card. The SIM is a detachable smart card containing the user's subscription information and phone book. This allows the user to retain his or her information after switching handsets. Alternatively, the user can also change operators while retaining the handset simply by changing the SIM. Some operators will block this by allowing the phone to use only a single SIM, or only a SIM issued by them; this practice is known as SIM locking.

6) Phone Locking

Sometimes mobile network operators restrict handsets that they sell for use with their own network. This is called locking and is implemented by a software feature of the phone. A subscriber may usually contact the provider to remove the lock for a fee, utilize private services to remove the lock, or use software and websites to unlock the handset themselves.
In some countries (e.g., Bangladesh, Belgium, Brazil, Chile, Germany, Hong Kong, India, Iran, Lebanon, Malaysia, Nepal, Pakistan, Poland, Singapore, South Africa, Thailand) all phones are sold unlocked.

7) GSM Security

GSM was intended to be a secure wireless system. It has considered the user authentication using a pre-shared key and challenge-response, and over-the-air encryption. However, GSM is vulnerable to different types of attack, each of them aimed at a different part of the network.

The development of UMTS introduces an optional Universal Subscriber Identity Module (USIM), that uses a longer authentication key to give greater security, as well as mutually authenticating the network and the user, whereas GSM only authenticates the user to the network (and not vice versa). The security model therefore offers confidentiality and authentication, but limited authorization capabilities, and no non-repudiation.

GSM uses several cryptographic algorithms for security. The A5/1, A5/2, and A5/3 stream ciphers are used for ensuring over-the-air voice privacy. A5/1 was developed first and is a stronger algorithm used within Europe and the United States; A5/2 is weaker and used in other countries. Serious weaknesses have been found in both algorithms: it is possible to break A5/2 in real-time with a ciphertext-only attack, and in January 2007, The Hacker's Choice started the A5/1 cracking project with plans to use FPGAs that allow A5/1 to be broken with a rainbow table attack. The system supports multiple algorithms so operators may replace that cipher with a stronger one.

Since 2000, different efforts have been done in order to crack the A5 encryption algorithms. Both A5/1 and A5/2 algorithms are broken, and their cryptanalysis has been considered in the literature. As an example, Karsten Nohl developed a number of rainbow tables (static values which reduce the time needed to carry out an attack) and have found new sources for known plaintext attacks. He said that it is possible to build "a full GSM interceptor from open-source components" but that they had not done so because of legal concerns. Nohl claimed that he was able to intercept voice and text conversations by impersonating another user to listen to voicemail, make calls, or send text messages using a seven-year-old Motorola cellphone and decryption software available for free online.

New attacks have been observed that take advantage of poor security implementations, architecture, and development for smart phone applications. Some wiretapping and eavesdropping techniques hijack the audio input and output providing an opportunity for a third party to listen in to the conversation.

GSM uses General Packet Radio Service (GPRS) for data transmissions like browsing the web. The most commonly deployed GPRS ciphers were publicly broken in 2011.

The researchers revealed flaws in the commonly used GEA/1 and GEA/2 ciphers and published the open-source "gprs decode" software for sniffing GPRS networks. They also noted that some carriers do not encrypt the data (i.e., using GEA/0) in order to detect the use of traffic or protocols they do not like (e.g., Skype), leaving customers unprotected. GEA/3 seems to remain relatively hard to break and is said to be in use on some more modern networks. If used with USIM to prevent connections to fake base stations and downgrade attacks, users will be protected in the medium term, though migration to 128-bit GEA/4 is still recommended.

B. IOT Module

The Internet of Things (IoT) is the network of physical objects—devices, vehicles, buildings and other items—embedded with electronics, software, sensors, and network connectivity that enables these objects to collect and exchange data. The IoT allows objects to be sensed and controlled remotely across existing network infrastructure, creating opportunities for more direct integration of the physical world into computer-based systems, and resulting in improved efficiency, accuracy and economic benefit;[3][4][5][6][7][8] when IoT is augmented with sensors and actuators, the technology becomes an instance of the more general class of cyber-physical systems, which also encompasses technologies such as smart grids, smart homes, intelligent transportation and smart cities. Each thing is uniquely identifiable through its embedded computing system but is able to interoperate within the existing Internet infrastructure. Experts estimate that the IoT will consist of almost 50 billion objects by 2020. British entrepreneur Kevin Ashton first coined the term in 1999 while working at Auto-ID Labs (originally called Auto-ID centers, referring to a global network of objects connected to radio-frequency identification, or RFID). Typically, IoT is expected to offer advanced connectivity of devices, systems, and services that goes beyond machine-to-machine (M2M) communications and covers a variety of protocols, domains, and applications. The interconnection of these embedded devices (including smart objects), is expected to usher in automation in nearly all fields, while also enabling advanced applications like a smart grid, and expanding to the areas such as smart cities.

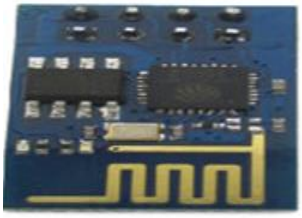

Fig. 4:

1) Trends and Characteristics

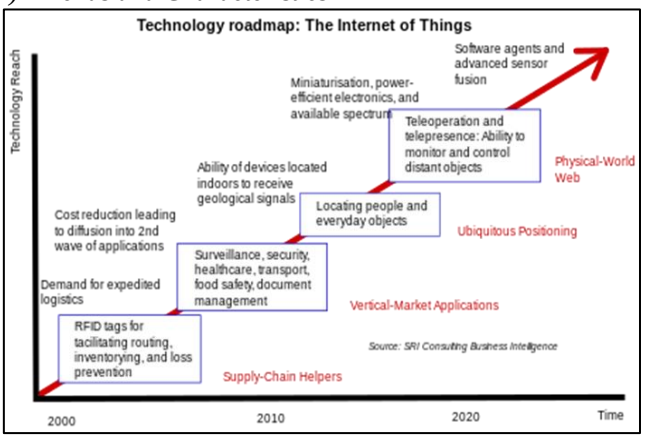

Fig. 4.1: Technology Roadmap: Internet of Things

2) Architecture

The system will likely be an example of event-driven architecture,[102] bottom-up made (based on the context of processes and operations, in real-time) and will consider any subsidiary level. Therefore, model driven and functional approaches will coexist with new ones able to treat exceptions and unusual evolution of processes (Multi-agent systems, B-ADSc, etc.).

In an Internet of Things, the meaning of an event will not necessarily be based on a deterministic or syntactic model but would instead be based on the context of the event itself: this will also be a semantic web.[103] Consequently, it will not necessarily need common standards that would not be able to address every context or use: some actors (services, components, avatars) will accordingly be self-referenced and, if ever needed, adaptive to existing common standards (predicting everything would be no more than defining a "global finality" for everything that is just not possible with any of the current top-down approaches and standardizations). Some researchers argue that sensor networks are the most essential components of the Internet of Things.[104]

Building on top of the Internet of Things, the Web of Things is an architecture for the application layer of the Internet of Things looking at the convergence of data from IoT devices into Web applications to create innovative use-cases. In order to program and control the flow of information in the Internet of Things, a predicted architectural direction is being called BPM Everywhere which is a blending of traditional process management with process mining and special capabilities to automate the control of large numbers of coordinated devices.

3) Enabling Technologies for the IOT

There are many technologies that enable IOT.

1) RFID and near-field communication – In the 2000s, RFID was the dominant technology. Later, NFC became dominant (NFC). NFC have become common in smartphones during the early 2010s, with uses such as reading NFC tags or for access to public transportation.[citation needed]
2) Optical tags and quick response codes – This is used for low cost tagging. Phone cameras decode QR code using image-processing techniques. In reality QR advertisement campaigns gives less turnout as users need to have another application to read QR codes.

3) Bluetooth low energy – This is one of the latest tech. All newly releasing smartphones have BLE hardware in them. Tags based on BLE can signal their presence at a power budget that enables them to operate for up to one year on a lithium coin cell battery.
4) Low energy wireless IP networks – embedded radio in system-on-a-chip designs, lower power WiFi, sub-GHz radio in an ISM band, often using a compressed version of IPv6 called 6LowPAN.
5) ZigBee – This communication technology is based on the IEEE 802.15.4 protocol to implement physical and MAC layer for low-rate wireless Private Area Networks. Some of its main characteristics like low power consumption, low data rate, low cost, and high message throughput make it an interesting IoT enabler technology.
6) Z-Wave – is a communication protocol that is mostly used in smart home applications.
7) LTE-Advanced – LTE-A is a high-speed communication specification for mobile networks. Compared to its original LTE, LTE-A has been improved to have extended coverage, higher throughput and lower latency. One important application of this technology is Vehicle-to-Vehicle (V2V) communications.
8) WiFi-Direct – It is essentially WiFi for peer-to-peer communication without needing to have an access point. This feature attracts IoT applications to be built on top of Wi-Fi-Direct to get benefit from the speed of Wi-Fi while they experience lower latency.

C. Microcontroller Atmega 328

1) Specifications

The Atmel 8-bit AVR RISC-based microcontroller combines 32 KB ISP flash memory with read-while-write capabilities, 1 KB EEPROM, 2 KB SRAM, 23 general purpose I/O lines, 32 general purpose working registers, three flexible timer/counters with compare modes, internal and external interrupts, serial programmable USART, a byte-oriented 2-wire serial interface, SPI serial port, 6-channel 10-bit A/D converter (8-channels in TQFP and QFN/MLF packages), programmable watchdog timer with internal oscillator, and five software selectable power saving modes. The device operates between 1.8-5.5 volts. The device achieves throughputs approaching 1 MIPS per Mhz.

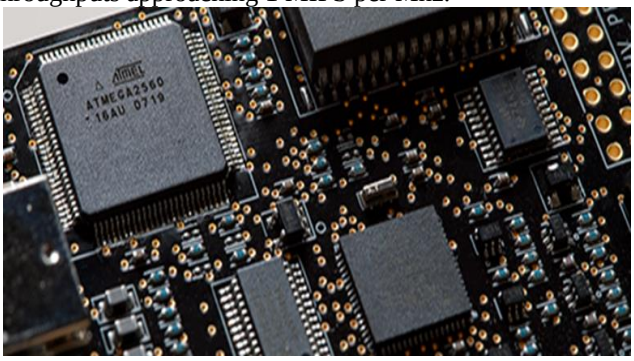

Fig. 4.2:

2) Applications

Today the ATmega328 is commonly used in many projects and autonomous systems where a simple, low-powered, low-cost micro-controller is needed. Perhaps the most common implementation of this chip is on the popular Arduino development platform, namely the Arduino Uno and Arduino Nano models.

3) Series Alternatives

A common alternative to the ATmega328 is the "picoPower" ATmega328P. A comprehensive list of all other member of the megaAVR series can be found on the Atmel website.

D. Real Time Clock (RTC)

A real-time clock (RTC) is a computer clock (most often in the form of an integrated circuit) that keeps track of the current time. Although the term often refers to the devices in personal computers, servers and embedded systems, RTCs are present in almost any electronic device which needs to keep accurate time.

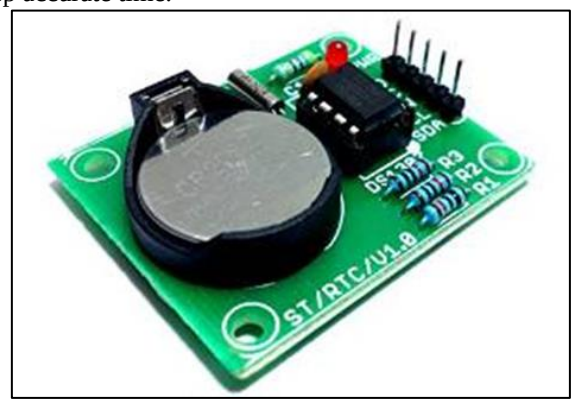

Fig. 5:

1) Terminology

The term is used to avoid confusion with ordinary hardware clocks which are only signals that govern digital electronics, and do not count time in human units. RTC should not be confused with real-time computing, which shares its three-letter acronym but does not directly relate to time of day.

2) Purpose

Although keeping time can be done without an RTC, using one has benefits:

- Low power consumption (important when running from alternate power)
- Frees the main system for time-critical tasks
- Sometimes more accurate than other methods

A GPS receiver can shorten its startup time by comparing the current time, according to its RTC, with the time at which it last had a valid signal.[3] If it has been less than a few hours, then the previous ephemeris is still usable.

3) Power Source

RTCs often have an alternate source of power, so they can continue to keep time while the primary source of power is off or unavailable. This alternate source of power is normally a lithium battery in older systems, but some newer systems use a supercapacitor,[4][5] because they are rechargeable and can be soldered. The alternate power source can also supply power to battery backed RAM.

4) Timing

Most RTCs use a crystal oscillator,[7][8] but some use the power line frequency.[9] In many cases, the oscillator's frequency is 32.768 kHz.[7] This is the same frequency used in quartz clocks and watches, and for the same reasons, namely that the frequency is exactly 215 cycles per second, which is a convenient rate to use with simple binary counter circuits.

E. Current Sensor

A current sensor is a device that detects electric current (AC or DC) in a wire, and generates a signal proportional to it. The generated signal could be analog voltage or current or even digital output. It can be then utilized to display the measured current in an ammeter or can be stored for further analysis in a data acquisition system or can be utilized for control purpose.

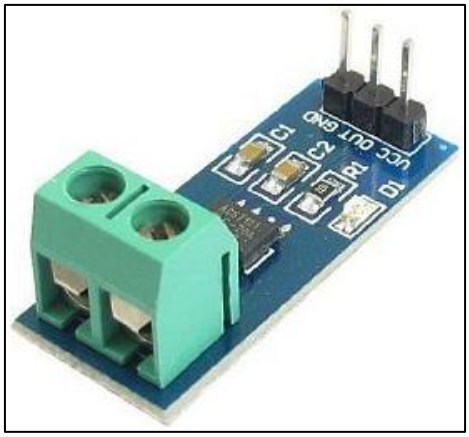

Fig. 6:

The sensed current and the output signal can be:

- Alternating current input,
- analog output, which duplicates the wave shape of the sensed current
- bipolar output, which duplicates the wave shape of the sensed current
- unipolar output, which is proportional to the average or RMS value of the sensed current
- Direct current input,
- unipolar, with a unipolar output, which duplicates the wave shape of the sensed current
- digital output, which switches when the sensed current exceeds a certain threshold

F. Light Dependent Resistor (LDR)

A photo resistor (or light-dependent resistor, LDR, or photocell) is a light-controlled variable resistor. The resistance of a photo resistor decreases with increasing incident light intensity; in other words, it exhibits photoconductivity. A photo resistor can be applied in light-sensitive detector circuits, and light- and dark-activated switching circuits.

A photo resistor is made of a high resistance semiconductor. In the dark, a photo resistor can have a resistance as high as several mega ohms (MΩ), while in the light, a photo resistor can have a resistance as low as a few hundred ohms. If incident light on a photo resistor exceeds a certain frequency, photons absorbed by the semiconductor give bound electrons enough energy to jump into the conduction band. The resulting free electrons (and their hole partners) conduct electricity, thereby lowering resistance. The resistance range and sensitivity of a photo resistor can substantially differ among dissimilar devices. Moreover, unique photo resistors may react substantially differently to photons within certain wavelength bands.

A photoelectric device can be either intrinsic or extrinsic. An intrinsic semiconductor has its own charge carriers and is not an efficient semiconductor, for example, silicon. In intrinsic devices the only available electrons are in the valence band, and hence the photon must have enough energy to excite the electron across the entire bandgap. Extrinsic devices have impurities, also called dopants, added whose ground state energy is closer to the conduction band; since the electrons do not have as far to jump, lower energy photons (that is, longer wavelengths and lower frequencies) are sufficient to trigger the device. If a sample of silicon has some of its atoms replaced by phosphorus atoms (impurities), there will be extra electrons available for conduction. This is an example of an extrinsic semiconductor.

1) Design Considerations

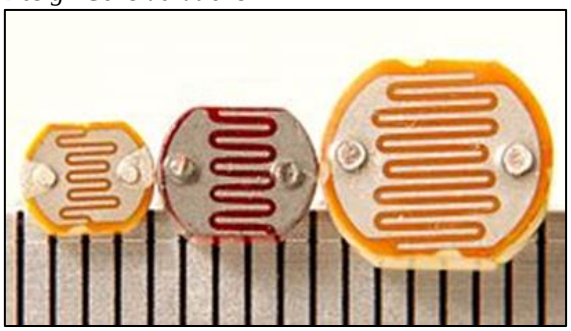

Fig. 6.1:

Three photo resistors

Photo resistors are less light-sensitive devices than photodiodes or phototransistors: the two latter components are true semiconductor devices, while a photo resistor is a passive component and does not have a PN-junction. The photo resistivity of any photo resistor may vary widely depending on ambient temperature, making them unsuitable for applications requiring precise measurement of or sensitivity to light.

Photo resistors also exhibit a certain degree of latency between exposure to light and the subsequent decrease in resistance, usually around 10 milliseconds. The lag time when going from lit to dark environments is even greater, often as long as one second. This property makes them unsuitable for sensing rapidly flashing lights, but is sometimes used to smooth the response of audio signal compression.[2]

2) Applications

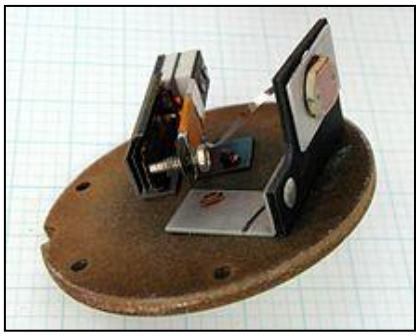

Fig. 6.2:

The internal components of a photoelectric control for a typical American streetlight. The photo resistor is facing rightwards, and controls whether current flows through the heater which opens the main power contacts. At night, the

heater cools, closing the power contacts, energizing the street light.

Photo resistors come in many types. Inexpensive cadmium sulphide cells can be found in many consumer items such as camera light meters, clock radios, alarm devices (as the detector for a light beam), nightlights, outdoor clocks, solar street lamps and solar road studs, etc.

Photo resistors can be placed in streetlights to control when the light is on. Ambient light falling on the photo resistor causes the streetlight to turn off. Thus energy is saved by ensuring the light is only on during hours of darkness.

They are also used in some dynamic compressors together with a small incandescent or neon lamp, or light-emitting diode to control gain reduction. A common usage of this application can be found in many guitar amplifiers that incorporate an onboard tremolo effect, as the oscillating light patterns control the level of signal running through the amp circuit.

The use of CdS and CdSe[3] photo resistors is severely restricted in Europe due to the RoHS ban on cadmium.

Lead sulphide (PbS) and indium antimonide (InSb) LDRs (light-dependent resistors) are used for the mid-infrared spectral region. Ge:Cu photoconductors are among the best far-infrared detectors available, and are used for infrared astronomy and infrared spectroscopy.

IV. CIRCUIT AND BLOCK DIAGRAM

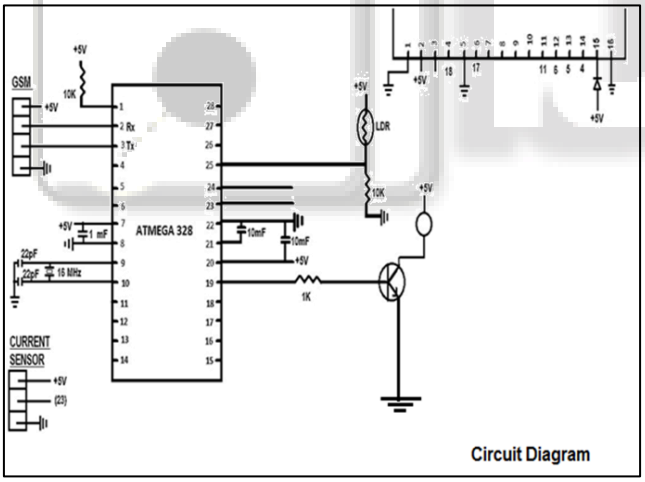

Fig. 7:

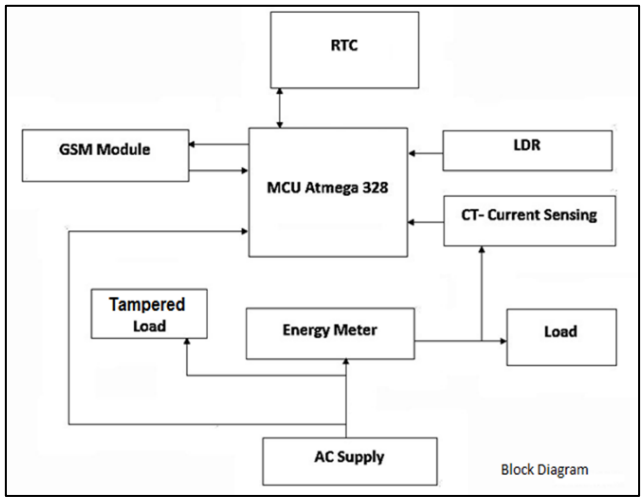

Fig. 8:

A. Coding

1) Program Code

```
#include <avr/io.h>
#include <util/delay.h>
#include <string.h>
#include <stdio.h>
#include "lcd.h"
#include "lcd.c"
#include "adc.h"
#include "adc.c"
#define bit(p) (1<<(p))
#define clear_bit(p,b) p&=~b
#define set_bit(p,b) p|=b
#define flip_bit(p,b) p^=b
#define check_bit(p,b) p&b
int main(void){
int ldrSensorPin = 23;
int currentPin = 24;
unsigned long sampleTime = 100000UL;
unsigned long numSamples = 250UL;
unsigned long sampleInterval = sampleTime/numSamples;
int adc_zero = 510;
int buzzerPin = 5;
int ldrValue = 6;
int ldrValue1 = 0,ldrValue2 = 0,ldrValue3 = 0,ldrValue4 =
0,ldrValue5 = 0;
set_bit(DDRB,bit(buzzerPin));  //Buzzer
clear_bit(DDRC,bit(ldrSensorPin));  //LDR
clear_bit(DDRC,bit(currentPin));  //Current
initLCD();
lcdxy(0, 0);
lcdwrite("  Power Theft  ");
lcdxy(0, 1);
lcdwrite("    System     ");
_delay_ms(2000);
lcdclear();
lcdwrite("Starting GSM...");
_delay_ms(10000);
lcdclear();
lcdwrite("GSM Started!");
_delay_ms(1000);
lcdclear();
lcdwrite("System Ready!");
```

```
_delay_ms(1000);
while(1){
unsigned long currentAcc = 0;
unsigned int count = 0;
while (count < numSamples)
{
if (micros() - prevMicros >= sampleInterval)
{
int adc_raw = adcRead(currentPin) - adc_zero;
currentAcc += (unsigned long)(adc_raw * adc_raw);
++count;
prevMicros += sampleInterval;
}
}
float rms = sqrt((float)currentAcc/(float)numSamples) *
(75.7576 / 1024.0);
lcdclear();
lcdxy(0, 0);
lcdwrite("RMS");
lcdxy(0, 1);
lcdwrite(rms,DEC);
delay(1000);
//Get LDR Value
ldrValue1 = adcRead(ldrSensorPin);
delay(100);
ldrValue2 = adcRead(ldrSensorPin);
delay(100);
ldrValue3 = adcRead(ldrSensorPin);
delay(100);
ldrValue4 = adcRead(ldrSensorPin);
delay(100);
ldrValue5 = adcRead(ldrSensorPin);
ldrValue = (ldrValue1 + ldrValue2 + ldrValue3 + ldrValue4
+ ldrValue5)/5;
lcdclear();
lcdxy(0, 0);
lcdwrite("LIGHT");
lcdxy(0, 1);
lcdwrite(ldrValue,DEC);
delay(1000);
if(ldrValue>300){  //Send SMS for Meter tampered
lcdclear();
lcdxy(0, 0);
lcdwrite("Meter Tampered");
delay(3000);
}
if(rms>=2.0 && rms<=3.0){  //Send SMS for Meter
tampered
lcdclear();
lcdxy(0, 0);
lcdwrite("Overload Detected!");
delay(3000);
}
}
}
```

V. CONCLUSION

The evidence points to the increasing levels of power theft in many countries and the financial losses for some systems are so immense that the utility is in financial turn over. Investment in improving the system and adding additional capacity cannot be undertaken, loans and payments cannot be met, and the consumer faces increased electricity charges. Even in efficient systems, theft losses can account for millions of dollars each year in lost revenue. Electricity theft in its various forms can be reduced and kept in check only by the strong and assertive action of power sector. The strategy and the action should be based upon a thorough understanding of the specific nature of the theft problem. Finally the proposed work is implemented on hardware.

REFERENCES

[1] Andrea Zanella, Senior Member, IEEE, Nicola Bui, Angelo Castellani, Lorenzo Vangelista, Senior Member, IEEE, and Michele Zorzi, Fellow,IEEE, "Internet of Things for Smart Cities", IEEE Internet of Things Journal, vol. 1, no. 1, pp. 22-32, February 2014.
[2] Poonam Borle, Ankitha Saswadhar, Deepali Hiwarkar, Rupali S Kali, "Automatic Meter Reading for Electricity",International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 2, no. 3,pp. 982-987, March 2013.
[3] IoT Based Electricity Energy Meter Reading, Theft Detection and Disconnection using PLC modem and Power optimization. International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering (An ISO 3297: 2007 Certified Organization) Vol. 4, Issue 7, July 2015. ISSN (Print) : 2320 – 3765.
[4] Amin S. Mehmood, T. Choudhry, M.A. Hanif, "A Reviewing the Technical Issues for the Effective Construction of Automatic Meter Reading System" in International Conference on Microelectronics, 2005 IEEE.
[5] Abdollahi, A. Dehghani, M. Zamanzadeh, "SMS-based Reconfigurable Automatic Meter Reading System" in Control Applications, 2007.
[6] Pal, Arpan. "Internet of Things- Making The Hype a Reality"(PDF).IEEE Computer Society.
[7] Want, Roy; Bill N. Schilit, Scott Jenson (2015). "Enabling The Internet of Things", Sponsored by IEEE Computer Society. IEEE. pp. 28-35.
[8] Sauter, Martin (21 Nov 2013). "The GSM Logo: The Mystery of the 4 Dots Solved". Retrieved 23 Nov 2013. [...] here's what [Yngve Zetterstrom, rapporteur of the Maketing and Planning (MP) group of the MoU (Memorandum of Understanding group, later to become the GSM Association (GSMA)) in 1989] had to say to solve the mystery: '[The dots symbolize] three [clients] in the home network and one roaming client.' There you go, an answer from the prime source!
[9] Anton A. Huurdeman, The Worldwide History of Telecommunications, John Wiley & Sons, 31 juli 2003, page 529

