# POWER THEFT PREVENTION SYSTEM USING IOT

Ashwitha K[1], Gracy A[2], Pooja sree M[3], Somashekar B[4], Dhayanand B R[5]
Ashwithaashwitha400@gmail.com[1], agracy021@gmail.com[2], poojasreem22@gmail.com[3]

**Abstract**

**These days with emerging developments in all sectors and growing demands, electricity has become priority for every individual and every organization. The basic procedure for power supply includes power generation, power transmission and power distribution to the destinations. Naturally owing to few technical faults, losses may occur due to power dissipation by some devices. These losses can be minimized using the fast developing technology, but what about the other kind of losses? These are the losses caused deliberately by human beings for the sake of illegal access to the power distribution. This is power theft.In developing countries like India, power theft is one of the most prevalent issues which not only cause economic losses but also irregular supply of electricity. It hampers functioning of industries and factories, due to shortage of power supplied to them. It causes shortage of power supply to homes. It leads to loss of revenue by Government as individual enterprises may opt to install their own power generators, increases corruption in form of bribes and many more. Ultimately it is the country's economy which suffers along with the country's political reputation.**

**In this paper a simple design for single phase power theft identification and alert system is proposed which employs real time comparison method to compare the current ($I_1$) at incoming side of the energy meter with that of the load side ($I_2$), if both the $I_1$ and $I_2$ are same it is considered that there is no power theft occurred, if $I_1$ is greater than $I_2$ then it is considered as power theft has been occurred which is immediately intimated to the Electricity Board via Internet in Real time. On getting the notification on smartphone the electricity board personal can disconnect the load remotely**.

**Index Terms: power theft, incoming side, outgoing side, controller, wifi adapter, sensors**.

## I. INTRODUCTION

The transmission as well as distribution of electricity induces the large amount of loss of power. The quantity of this loss is rising day by day due to it the power authorities are facing losses in their profits a new method to identify the fraud customers is proposed.

There is a huge demand for electricity and there is always a mismatch between supply and demand. Satisfactory operation of power systems requires overall coordination of all the power system components. Attention and focus are given for generating power using both renewable and conventional sources of energy. But the transmission of power also plays a vital role in conveying power with minimal loss to the consumers. Hence proper maintenance of transmission as well as distribution network is mandatory for efficient and effective distribution of power. Though the losses associated with generation can be exactly formulated, there is no proper and precise quantification of transmission and distribution losses. Many parameters are involved and hence more data is required in addition to the sending end data. Also it is not only the technical parameters that influence transmission and distribution losses, but also the non-technical parameters. Power theft is one such parameter in developing countries. In India, the power theft is highly significant and it is approximately 420MW accounting to heavy revenue loss to power utilities.

Often power theft is done during transmission by illegal tapping of power lines to divert the power to the required destination. It is also done by illegal connections to the power grid stations, which are cut at the time of billing. A real time comparison method is made which is used to compare the current at L.V (low voltage) side of the distribution transformer with that of the consumption of connected legal consumers. A wireless IOT module is employed for this purpose. A simple design for single phase distribution system is proposed for analysis and the same can be implemented for three phase system by adding relevant features.

Power theft occurs in two main ways: meter frauds i.e. manipulating the electricity usage data and, un-metered usage where the power is enjoyed for free. Political interference is a major reason promoting power theft in India. There are incidences when officials from the state-owned power sector companies are transferred, suspended or sometimes even killed if they try to expose the culprits. Another strange fact which confirms the politics of populism in the sector is that power theft increases during elections. This also shows that political leaders earn votes by allowing electricity theft. Farmers occupy a major chunk of voters in the country and the political leaders often promise them free or subsidized electricity to attract their votes. Moreover, most of the overhead electrical wires in India are still not insulated facilitating illegal hookups. The ineffective law enforcement system in the country regarding power theft further removes the fear among power thieves.

## II.Impact of power theft on the Indian economy:

According to the World Bank estimates, power theft reduces India’s GDP by around 1.5% (Smith, 2012). A recent study by NDTV also concluded that 40% of the electricity in India is unpaid (NDTV, 2012). Of all the power generated in the country, around 1/4th is either stolen or lost in transmission. This figure is 5 times the figures for China and one of the reasons why India is not developing at the same pace as China (Denyer, 2012). These data itself show the pathetic situation of power sector in the country. UP has the lowest growth rate across the country which in a way proves that level of electricity losses and the economic growth rate are inversely related.

There is definitely a need for strict regulations against power theft in the country but the situation can never improve unless the people themselves do not stop stealing power. This requires more of a moral awakening rather enforcement of legal penalties.Power theft occurs in two main ways: meter frauds i.e. manipulating the electricity usage data and, un-metered usage where the power is enjoyed for free. Political interference is a major reason promoting power theft in India. There are incidences when officials from the state-owned power sector companies are transferred, suspended or sometimes even killed if they try to expose the culprits. Another strange fact which confirms the politics of populism in the sector is that power theft increases during elections. This also shows that political leaders earn votes by allowing electricity theft.

### Injecting foreign element into energy meter

*Meters* are manipulated via a remote by installing a circuit *inside* the *meter* so that the *meter* can be slowed down at any time. This kind of modification can evade external inspection attempts because the *meter* is always correct unless the remote is turned on. Sometimes skilled individuals inject foreign elements such as transistors, resistors or IC chips into the energy meter.

## III PROBLEM OBJECTIVES

1. The main aim of our project is to detect an electrical power theft automatically and prevent it from occurring
2. Globally get information about power theft via internet on Smartphone's from anywhere in the world using IOT(Internet Of Things)
3. Make the system cost effective and very compact so as it can be added to existing energy meter system without much complexity

## IV. METHODOLOGIES ADOPTED

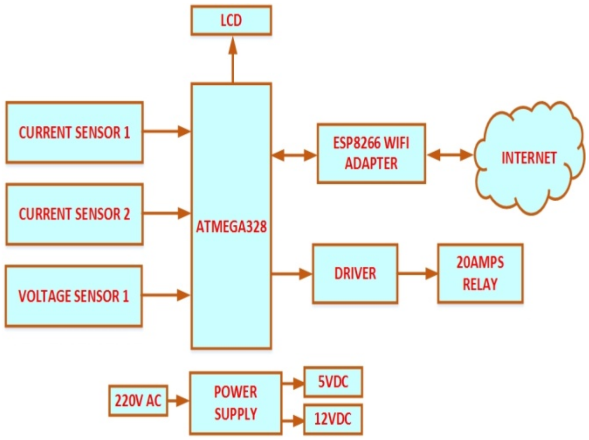
1. AVR ATmega328-8 bit Advanced Virtual RISC Microcontroller used as a real time high speed digital monitoring and control system

2. Customizing BLYNK Google play application for globally accessing of information
3. Interfacing ESP8266 to microcontroller for providing Wi-Fi link to access internet
4. Integration of Hall effect sensors for current measurement more effectively than conventional techniques

## V. SPECIFICATIONS

| Devices | Parameters | Values |
|---|---|---|
| Current sensor | $I_1$ (amps) | 30 |
| Current sensor | $I_2$ (amps) | 30 |
| Voltage sensor | V (volts) | 250 |
| Relay | R (amps) | 20 |

## VI.BLOCK DIAGRAM



## V.MICROCONTROLLER

A microcontroller (sometimes abbreviated µC, or MCU) is a small computer on a single integratedcircuit containing a processor core, memory, and programmable input/outputperipherals. Program memory in the form ofNOR flash or OTP ROM is also often included on chip, as well as a typically small amount of RAM. Microcontrollers are designed for embedded applications, in contrast to the microprocessors used in personal computersor other general purpose applications needed to control non-digital electronic systems.

Embedded design

A microcontroller can be considered a self-contained system with a processor, memory and peripherals and can be used as an embedded system. The majority of microcontrollers in use today are embedded in other machinery, such as automobiles, telephones, appliances, and peripherals for computer systems. These are called embedded systems. While some embedded systems are very sophisticated, many have minimal requirements for memory and program length, with no operating system, and low software complexity. Typical input and output devices include switches, relays, solenoids, LEDs, small or custom LCD displays, radio frequency devices, and sensors for data such as temperature, humidity, light level etc. Embedded systems usually have no keyboard, screen, disks, printers, or other recognizable I/O devices of a personal computer, and may lack human interaction devices of any kind.

History of AVR

The AVR is a modified Harvard architecture8-bitRISC single chip microcontroller which was developed by Atmel in 1996. The AVR was one of the first microcontroller families to use on-chip flash memory for program storage, as opposed to one-time programmable ROM, EPROM, or EEPROM used by other microcontrollers at the time.The AVR architecture was conceived by two students at the Norwegian Institute of Technology (NTH) Alf-Egil Bogen Blog (www.alfbogen.com) and Vegard Wollan. The original AVR MCU was developed at a local ASIC house in Trondheim, Norway called Nordic VLSI at the time, now Nordic Semiconductor, where Bogen and Wollan were working as students. It was known as a µRISC (Micro RISC) and was available as silicon IP/building block from Nordic VLSI.When the technology was sold to Atmel from Nordic VLSI, the internal architecture was further developed by Bogen and Wollan at Atmel Norway, a subsidiary of Atmel. The designers worked closely with compiler writers at IAR Systems to ensure that the instruction set provided for more efficient compilation of high-level languages. Atmel says that the name AVR is not an acronym and does not stand for anything in particular. The creators of the AVR give no definitive answer as to what the term "AVR" stands for. However, it is commonly accepted that AVR stands for Alf (Egil Bogen) and Vegard (Wollan)'s RISC processor.

Note that the use of "AVR" in this article generally refers to the 8-bit RISC line of Atmel AVR Microcontrollers.

AVR microcontrollers are available in three categories:

1. **TinyAVR** – Less memory, small size, suitable only for simpler applications
2. **MegaAVR** – These are the most popular ones having good amount of memory (upto 256 KB), higher number of inbuilt peripherals and suitable for moderate to complex applications
3. **XmegaAVR** – Used commercially for complex applications, which require large program memory and high speed

The following table compares the above mentioned AVR series of microcontrollers:

| Series Name | Pins | Flash Memory | Special Feature |
|---|---|---|---|
| TinyAVR | 6-32 | 0.5-8 KB | Small in size |
| MegaAVR | 28-100 | 4-256KB | Extended peripherals |
| XmegaAVR | 44-100 | 16-384KB | DMA , Event System included |

ATmega328 Microcontroller

ATmega328 is a low-power CMOS 8-bit microcontroller based on the AVR enhanced RISC architecture. By executing powerful instructions in a single clock cycle, the ATmega328 achieves throughputs approaching 1 MIPS per MHz allowing the system designed to optimize power consumption versus processing speed.

Features

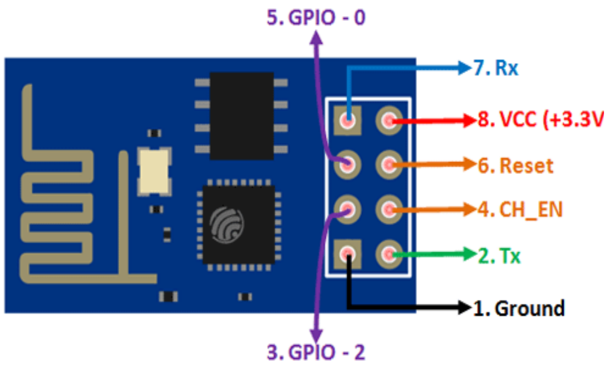
1. High Performance, Low Power AVR 8-Bit Microcontroller
2. Advanced RISC Architecture
3. 131 Powerful Instructions – Most Single Clock Cycle Execution
4. 32 x 8 General Purpose Working Registers
5. Fully Static Operation
6. Up to 20 MIPS Throughput at 20 MHz
7. High Endurance Non-volatile Memory Segments
8. 32K Bytes of In-System Self-Programmable Flash program memory
9. 1K Bytes EEPROM
10. 2K Bytes Internal SRAM
11. Write/Erase Cycles: 10,000 Flash/100,000 EEPROM
12. Data retention: 20 years at 85°C/100 years at 25°C

Special Features

1. Power-on Reset and Programmable Brown-out Detection
2. Internal Calibrated Oscillator
3. External and Internal Interrupt Sources
4. Six Sleep Modes: Idle, ADC Noise Reduction, Power-save, Power-down, Standby, and Extended Standby

VI.ESP8266

The ESP8266 is a low-cost Wi-Fi microchip with full TCP/IP stack and microcontroller capability produced by Shanghai-based Chinese manufacturer, Espressos Systems. The chip first came to the attention of western makers in August 2014 with the ESP-01 module, made by a third-party manufacturer, Ai-Thinker. This small module allows microcontrollers to connect to a Wi-Fi network and make simple TCP/IP connections.



ESP8266 delivers highly integrated Wi-Fi SoC solution to meet users' continuous demands for efficient power usage, compact design and reliable performance in the Internet of Things industry. With the complete and self-contained Wi-Fi networking capabilities, ESP8266 can perform either as a standalone application or as the slave to a host MCU. When ESP8266 hosts the application, it promptly boots up from the flash. The integrated high-speed cache helps to increase the system performance and optimize the system memory.

Also, ESP8266 can be applied to any microcontroller design as a Wi-Fi adaptor through SPI / SDIO or I2C / UART interfaces. ESP8266EX integrates antenna switches, RF balun, power amplifier, low noise receive amplifier, filters and power management modules. The compact design minimizes the PCB size and requires minimal external circuitries

Features

1. Processor: L106 32-bit RISC microprocessor core based on the Ten silica Xtensa Diamond Standard 106Micro running at 80 MHz
2. Memory:
    a. 32 KB instruction RAM
    b. 32 KB instruction cache RAM
    c. 80 KB user data RAM
    d. 16 KB ETS system data RAM
3. External QSPI flash: up to 16 MB is supported (512 KB to 4 MB typically included)
4. IEEE 802.11 b/g/n Wi-Fi
    a. Integrated TR switch, balun, LNA, power amplifier and matching network
    b. WEP or WPA/WPA2 authentication, or open networks
5. 16 GPIO pins
6. SPI
7. I²C (software implementation)
8. 10-bit ADC

Applications

1. Home appliances
2. Home automation
3. Smart plugs and lights
4. Mesh network
5. Industrial wireless control
6. Baby monitors

Current sensor

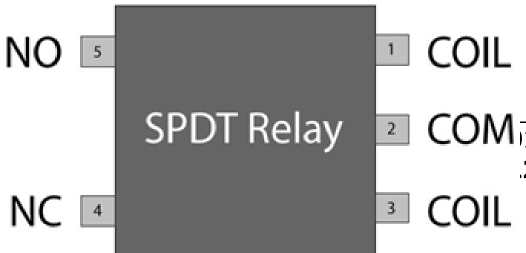
Measuring a voltage in any system is a "passive" activity as it can be done easily at any point in the system without affecting the system performance. However, current measurement is "intrusive" as it demands insertion of some type of sensor which introduces a risk of affecting system performance.

Current measurement is of vital importance in many power and instrumentation systems. Traditionally, current sensing was primarily for circuit protection and control. However, with the advancement in technology, current sensing has emerged as a method to monitor and enhance performance.

Knowing the amount of current being delivered to the load can be useful for wide variety of applications. Current sensing is used in wide range of electronic systems, viz., Battery life indicators and chargers, 4-20 mA systems, over-current protection and supervising circuits, current and voltage regulators, DC/DC converters, ground fault detectors, programmable current sources, linear and switch-mode power supplies, communications devices , automotive power electronics, motor speed controls and overload protection, etc.

RELAY

The term relay generally refers to a device that provides an electrical connection between two or more points in response to the application of a control signal. The most common and widely used type of electrical relay is the electromechanical relay or EMR.



Why to use a Darlington Pair?

In some application the amount of input current available to switch on a transistor is very low. This may mean that a single transistor may not be able to pass sufficient current required by the load.

As stated earlier this equals the input current x the gain of the transistor (hFE). If it is not be possible to increase the input current then we need to increase the gain of the transistor. This can be achieved by using a Darlington Pair. A Darlington Pair acts as one transistor but with a current gain that equals:

Total current gain (hFE total) =

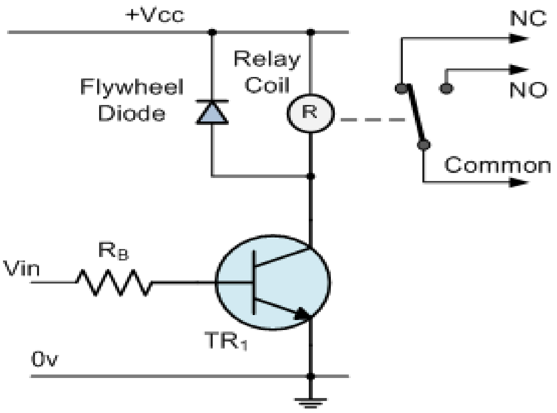
Current gain of transistor 1 (hFE t1) x current gain of transistor 2 (hFE t2)

So for example if you had two transistors with a current gain (hFE) = 100

(HFE total) = 100 x 100

(HFE total) = 10,000

You can see that this gives a vastly increased current gain when compared to a single transistor. Therefore this will allow a very low input current to switch a much bigger load current.



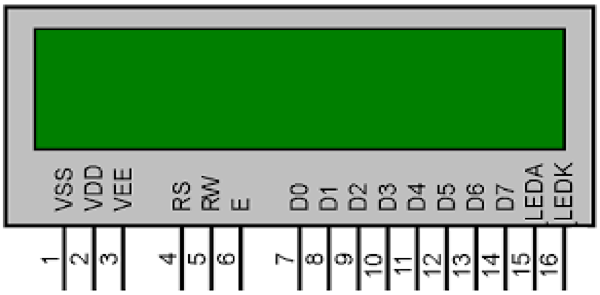
16X2 LCD:

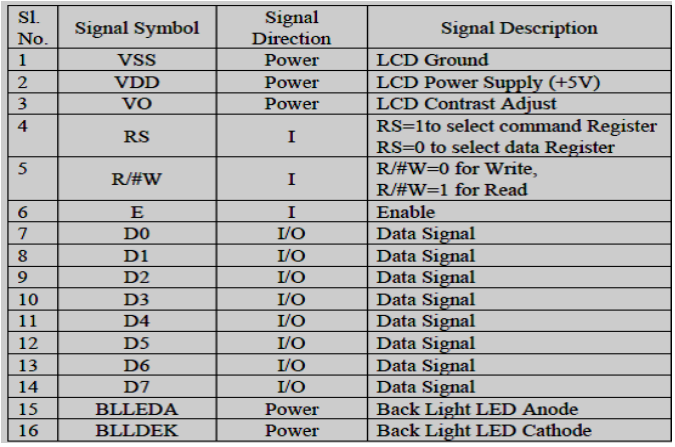
A Liquid Crystal Display (LCD) is a low cost, low-power device capable of displaying text and images. LCDs are extremely common in embedded systems, since such systems often do not have video monitors like those that come standard with desktop systems. It can be found in numerous common devices like watches, fax and copy, machines and calculators.

The backlight feature of the LCD makes it readable even in low light conditions.

The LCD is used here in 4-bit mode to save the microcontroller's port pins. Usually the 8-bit mode of interfacing with a microcontroller requires eleven

Pins, but in 4-bit mode the LCD can be interfaced to the microcontroller using only six pins.





| Sl. No. | Signal Symbol | Signal Direction | Signal Description |
|---|---|---|---|
| 1 | VSS | Power | LCD Ground |
| 2 | VDD | Power | LCD Power Supply (+5V) |
| 3 | VO | Power | LCD Contrast Adjust |
| 4 | RS | I | RS=1to select command Register<br>RS=0 to select data Register |
| 5 | R/#W | I | R/#W=0 for Write,<br>R/#W=1 for Read |
| 6 | E | I | Enable |
| 7 | D0 | I/O | Data Signal |
| 8 | D1 | I/O | Data Signal |
| 9 | D2 | I/O | Data Signal |
| 10 | D3 | I/O | Data Signal |
| 11 | D4 | I/O | Data Signal |
| 12 | D5 | I/O | Data Signal |
| 13 | D6 | I/O | Data Signal |
| 14 | D7 | I/O | Data Signal |
| 15 | BLLEDA | Power | Back Light LED Anode |
| 16 | BLLDEK | Power | Back Light LED Cathode |

SKETCH

The Sketch IDE (Integrated Development Environment) is a special program running on your computer that allows you to write sketches for the Arduino board in a simple language modelled after the Processing language. The magic happens when you press the button that uploads the sketch to the board: the code that you have written is translated into the C language, and is passed to the AVR-GCC compiler, an important piece of open source software that makes the final translation into the language understood by the microcontroller. This last step is quite important, because it's where Arduino makes your life simple by hiding away as much as possible of the complexities of programming microcontrollers.

The programming cycle on Arduino is basically as follows:

1. Plug your board into a USB port on your computer.

2. Write a sketch that will bring the board to life.

3. Upload this sketch to the board through the USB connection and wait a couple of seconds for the board to restart.

4. The board executes the sketch that you wrote.

The idea of sketching in code is a way of thinking about writing code as a simple intuitive process, just like drawing in a sketchbook. In this way, an Arduino program is called a sketch and is saved in a folder called a sketchbook. Sketching means we can get our hands dirty and quickly try out a new idea. It is a skill available to all of us.

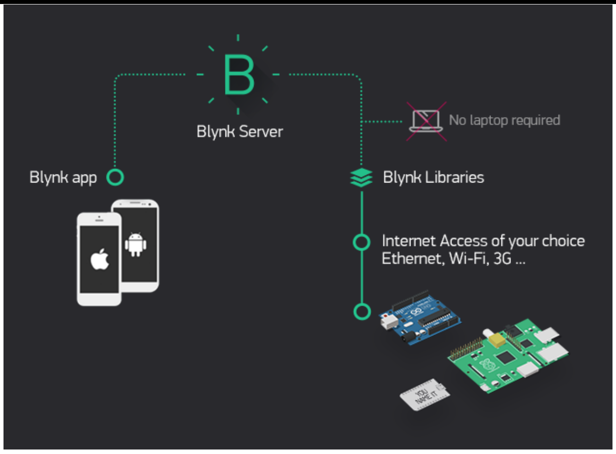
BLYNK

Blynk is designed for the Internet of Things. It can control hardware remotely, it can display sensor data, and it can store data, visualize it and do many other cool things.

There are three major components in the platform:

1. Blynk App - allows to you create amazing interfaces for your projects using various widgets we provide.
2. Blynk Server - responsible for all the communications between the smartphone and hardware. You can use our Blynk Cloud or run your private Blynk server locally. It's open-source, could easily handle thousands of devices and can even be launched on a Raspberry Pi.
3. Blynk Libraries - for all the popular hardware platforms - enable communication with the server and process all the incoming and out coming commands.

Now imagine: every time you press a Button in the Blynk app, the message travels to space the Blynk Cloud, where it magically finds its way to your hardware. It works the same in the opposite direction and everything happens in a blynk of an eye.



Blynk works over the Internet: This means that the hardware you choose should be able to connect to the internet. Some of the boards, like Arduino Uno will need an Ethernet or Wi-Fi Shield to communicate, others are already Internet-enabled: like the ESP8266, Raspberry Pi with Wi-Fi dongle, Particle Photon or Spark Fun Blynk Board. But even if you don't have a shield, you can connect it over USB to your laptop or desktop (it's a bit more complicated for newbies, but we got you covered). What's cool is that the list of hardware that works with Blynk is huge and will keep on growing.

## ADVANTAGES:

- This system would provide a simple way to detect an electrical power theft without any human interface wirelessly via Internet
- Maximize the profit margin of power utility company
- Monitor voltage, current and make disconnections and reconnection remotely without employing manpower

## DISADVANTAGES:

- Requires internet facility

## CONCLUSION

Since power theft is one of the major problem that is taking place in the present scenario we require an effective method to protect the power theft. By using the simple devices like microcontroller, current sensors and internet of things we have implemented the model. This is economically low cost and can be easily fitted to the energy meter very compact in size, and man power is not required. This model can also be used for industrial purpose.

The study of various techniques is done to propose the new technique which is expected to have higher accuracy to detect theft in electricity. Thus technique would be helpful for the power authorities to further minimize the non-technical losses in electricity distribution.

## FUTURE SCOPE:

This is a potable model which is used to determine power theft and disconnection of unpaid bills. Due to day by day increase in the technology by using the same model we can also implement the following in the software part.

- Over load notification can be added in the software part.
- Short circuit notification can be implemented

## REFERENCES

Christopher, A.V., PravinThangaraj, “Distribution Line Monitoring System for the Detection of Power Theft using Power Line Communication”, Energy Conversion (CENCON), 2014 IEEE Conference on 13-14 Oct. 2014.

[2] D.Dangar, S.K.Joshi, “Electricity Theft Detection Techniques for Distribution System in GUVNL”, IJREDR 2014.

[3] D.Dangar, S.K.Joshi, “Normalization based K means Clustering Algorithm” IJREDR 2014.

[4] Eduardo Werley S. dos Angelos, Osvaldo R. Saavedra, “Detection and Identification of Abnormalities in Customer Consumptions in Power Distribution Systems”, IEEE, October 2011.

[5] Glenn Sheriff, Kelly Maguire, “Ranking Distribution of Environmental Outcomes Across Population Groups”, National Center for environmental economics August 2013.

[6] Harshit Saxena1, Dr. VineetRichariya, “Intrusion Detection System using K- means, PSO with SVM Classifier: A Survey”, International Journal of Emerging Technology and Advanced Engineering February 2014.

[7] John Creedy, “Interpreting Inequality Measures and Changes in Inequality”, Working Paper September 2014.

[8] J. Nagi, K.S. Yap, F. Nagi, etal, “NTL Detection of Electricity Theft and Abnormalities for Large Power Consumers in TNB Malaysia”, Proceedings of 2010IEEE Student Conference on Research and Development (scored 2010), 13 -14 Dec 2010, Putrajaya, Malaysi.

[9] Kanaan EL. Bhissy, Fadi EL. Faleet and WesamAshour, “Spectral Clustering Using Optimized Gaussian Kernel Function” ,International Journal of Artificial Intelligence and Applications for Smart Devices (2014).

[10] M. Gunasekaran, K .S .Ramaswami, “Portfolio optimization using neuro fuzzy system in Indian stock market”, Journal of Global Research in Computer Science, April 2012.

[11] http://www.google.com/search?tbm=isch&sa=1&ei=4ef

[12]http://www.google.com/imgres?imgurl=https%3A%2F%2Fbusinesshilights.com.ng%2Fwp-content%2Fuploads%2F2016% (Google)

[13] http://www.google.com/search?q=power+theft&source=lnms&tbm=isch&sa=X&ved=0ahU