*Chapter 1*

*introduction*

**Electricity Pilferage Detection, Monitoring & Controlling**

* 1. **INTRODUCTION**

Theft of electricity increases the costs paid by customers and can have serious safety consequences. It leads to misallocation of costs among suppliers that can distort competition and hamper the efficient functioning of the market. The costs faced by an electricity supplier in detecting electricity theft by its customers may be greater than the costs to the industry as a whole. In particular, when it detects electricity theft by one of its customers, the supplier may incur liabilities relating to generation, network and balancing costs associated with the entry to the settlement system of estimates of the volume of electricity stolen by that customer.

On the other hand, this action does not lead to an increase in costs at the level of the industry as a whole.

Detecting electricity theft has been traditionally addressed by physical checks of tamper-evident seals by field

Personal and by using balance meters. Although these techniques reduce unmeasured and unbilled consumption of electricity, they are insufficient. Indeed, tamper- evident seals can be easily defeated, and although balance meters can detect that some customers are fraudulent, they cannot identify the culprits exactly. Despite the security vulnerabilities of smart meters, the higher-resolution data collected by them is seen as a promising technology that will complement traditional detection tools. They have clear potential to improve metering, billing and collection processes, and the detection of fraud and unmetered connections. Common methods of theft range from compromising the physical security of meters to directly connecting loads to electricity distribution lines. Default of payments has been a major problem, due to suboptimal levels of monitoring and enforcement.

The lack of technology and insufficient distributor incentives were the major contributors to this problem.

* 1. **OBJECTIVE**

This project of ours is aimed at reducing the illegal power usage in homes.

The main objective of this project is to develop the portable electricity pilferage detection system.

* To detect the pilferage using Hall sensor .
* To monitor the pilferage using IOT and separate web site of the project.
* To control the pilferage using microcontroller.

1.3Outline of project

**1.3.1 Project Overview**

In India electricity generation is less and demand is more. In industrial, rural, agriculture areas the available electricity is also less. And the customer is utilizing power illegally. So that power losses increases.

It consists of overview of the project, the project aim, objectives and scopes of the project. This project is about to develop and fabricate the circuit that can detect the electricity pilferage by using IOT. In this proposed system there are three sections, detection, monitoring &controlling. The detection is done by Hall sensor. The monitoring is done through IOT (Internet Of Things) and separate web site for project. Controlling section consist of microcontroller.

The Web site used here display the pilferage is detected or not. Microcontroller gives the order of suggestions received to all network & sensible factor. The meter 1 & meter 2 is at home. Microcontroller reads energy pulses & current signals. If current is drawing & energy pulses are normal, then no power pilferage is being done. If balanced is finished and load is operating, then it indicates power pilferage. Microcontroller is communicating with IOT. When power pilferage is done then it displays ‘**PILFERAGE IS DETECTED**’ in IOT & also on Web site.

**Uniqueness of the project:-**

The IOT Based Power Theft Detection System is unique of its kind. It can detect power theft and electric meter tampering. Whenever a meter tampering is done or direct load is connected before meter in the supply, the system senses it with the help of Hall sensors. Once it has detected the theft, it generates a log for theft type and timing with help of microcontroller and stores it on IOT platform for the backup and at the same time publishes this log info over internet website. When the number of theft attempts exceeds, It sends an Signal to web site.

**Scope of the Project:-**

* It requires only one time installation cost after installation this can be used for life time.
* It will completely eliminate the power theft and will increase revenue for the Government. And saves electricity.
* We can make this project more users friendly by introducing a system.

**Types of Power Theft**

**Theft of electricity** is the criminal practice of stealing [electrical power](https://en.wikipedia.org/wiki/Electrical_power). It is a crime and is punishable by fines and/or [incarceration](https://en.wikipedia.org/wiki/Incarceration). It belongs to the [non-technical losses](https://en.wikipedia.org/wiki/Losses_in_electrical_systems).

There are various types of electrical power theft, including Tapping a line or bypassing the [energy meter](https://en.wikipedia.org/wiki/Energy_meter). According to a study, 80% of worldwide theft occurs in private dwellings and 20% on commercial and industrial premises. The various types of electrical power theft include:

### Direct hooking from line

Hooking is the most used method. 80% of global power theft is by direct tapping from the line. The consumer taps into a power line from a point ahead of the [energy meter](https://en.wikipedia.org/wiki/Energy_meter). This [energy](https://en.wikipedia.org/wiki/Energy) consumption is unmeasured and procured with or without switches.

### Bypassing the energy meter

In this method, the input terminal and output terminal of the energy meter is short-circuited, preventing the energy from registration in the energy meter.

### Injecting foreign element into the 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.

### Physical obstruction

This type of tampering is done to [electromechanical](https://en.wikipedia.org/wiki/Electromechanical) meters with a rotating element. Foreign material is placed inside the meter to obstruct the free movement of the disc. A slower rotating disk signals less energy consumption.

### ESD attack on electronic meter

This type of tampering is done on electronic meter to make it either latent damage or permanent damage. Detection can be done correctly in high end meters only.

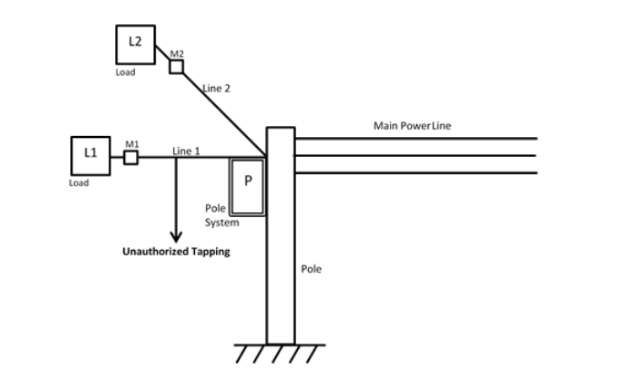
**Problems in electricity pilferage**

Mainly the electricity theft happens at two places, household energy meter and pole side distribution line.

Our project is depends on the power tapping.

Theft detection for pole site tapping in order to detect pole site tapping following method is proposed. Consider a distribution system shown in Fig. as a conceptual diagram. Two single phase loads L1 and L2 are supplied from two different phases. M1 and M2 are the energy meters that measure power consumed by these loads over a period. Pole based system (P) have been installed to detect power theft. Suppose there is tapping done illegally on the line to connect his usage. Over a certain period there will be difference between meter reading and pole based reading. Microcontroller will compare these two values and if the measured value on pole is more than value send by meter by some tolerance then power theft is happening on line. This theft signal generated on pole system can be transmitted to substation by power line communication technique, Tolerance should be provided for losses of line. Because over a long period there will be difference in reading of meter on load side and pole side due to loss of line between pole and load. Therefore tolerance should be provided through programming of micro-controller.

* L1, L2 - Single phase loads
* M1, M2 - Digital energy meters
* P - Pole based system (installed on a distribution pole)

****

**Literature Survey**

[1] ZHOU Wei, “GSM based monitoring and control system against electricity stealing” electricity-stealing prevention became a big problem to the electricity board. Based on the kind of electricity-stealing and actual demand of prevention of stealing electricity, realizes the behaviour of electricity-stealing with remote monitoring. Objective of this system is to design a system in order to avoid the displeasure for the users from pilferage bill irrespective of the use of the electricity due to pilferage using GSM module.

[2] Louis J. Romeo, “Electronic Pilferage Detection Systems: A Survey”, Library & Archival Security, they said that wireless electricity pilferage detection system using ZigBee technology present inefficient and less costly way to adulterate the wireless technique used in this research paper. This wireless system is used to overcome the pilferage of electricity via bypassing the energy meter and hence it also controls the revenue losses and utility of the electricity authorized agency. Mainly the electricity is being stolen via bypassing the energy meter therefore this wireless system is utilizes to overcome this type of the pilferage of the electricity and is very beneficial for the authorized agency to control its revenue loss as all of us know that the cost of fuel is increasing day by day hence the intensity of stealing the electricity and using it as a substitute is also increasing therefore it is needed much to design a system that can detect the pilferage of the electricity.

[3] H .G .Rodney, this system presents of design and development of Automatic meter reading (AMR) system. AMR system is a boom for remote monitoring and control. Controller reads energy pulses & current signals. If current is drawing &energy pulses are normal, then no power pilferage is being done & buzzer is off. If balanced is finished and load is operating, then it indicates power pilferage. Whenever power pilferage is detected, then ARM7 will send this meter information to buzzer circuit through buzzer driver. And this controller also disconnects power to the loads to avoid power pilferage.

[4] P. Kadurek, Student member, J. Blom, J. F. G. Cobben, W. L. Kling, Member they provide insight into the illegal use or abstraction of electricity in the Netherlands. The importance and the economic aspects of pilferage detection are presented and the current practices and experiences are discussed. The paper also proposes a novel methodology for automated detection of illegal utilization of electricity in the future distribution networks equipped with smart metering infrastructure. The necessary data requirements for smart meters and distribution substations are defined, in order to unlock this feature in distribution network.

[5] G. L. Prashanthi, K. V. Prasad, researched to record the power consumed by a model organization such a household consumers from a commonly located point. Recording the power means measuring the power consumed exactly by the user at a given time. The energy used by the user is measured and the records are sent to the controlling substation whenever needed by the person at the nearest substation. The feedback from any of the consumers helps in analyzing the usages between legal and illegal users which helps in controlling the power theft. Communication between the house hold meters and the substation is done with the means of wireless communication. The scope of this study is limited with the detection of power theft and not identifying the exact location.

[6] Soma ShekaraSreenadh Reddy Depuru, LingfengWang, Vijay Devabhaktuni focused on the factors that provoke the consumers to steal electricity. In view of these ill effects, various methods for detection and estimation of theft are discussed. This paper proposes an architectural design of smart meter circuit. Motivation of this work is to detect illegal consumers, and conserve and effectively utilize energy. As well as smart meters are designed to provide data for various parameters related to instantaneous power consumption

**methodology**

**METHODOLOGY**

**STAGE 1:**

**Selection of topic**: In this primary stage we have gone through many topics on that we can work. Finally we have selected this topic because we can solve electricity theft problem. At the same time we can increase the efficiency and accuracy of their system.

**STAGE 2:**

**Block diagram selection:** After finalising of our project topic we started working on block diagram. After working on this we have made the selection of block diagram.

**STAGE 3:**

**Selection of components:** After selection of block diagram we will select the sensors, microcontroller and Wi-Fi module. Serial communication done between wifi module, Hall sensor used for current sensing, microcontroller used for control the pilferage, IOT used for displaying the data.

**STAGE 4:**

**Preparation of circuit diagram:** we will prepare circuit diagram and its layout.

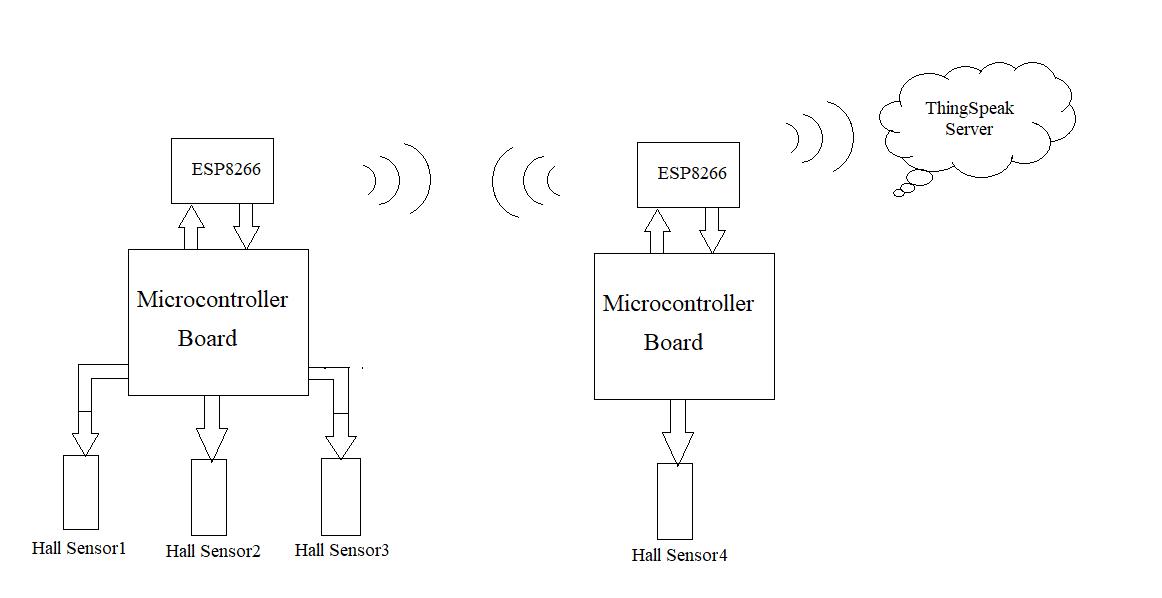
**STAGE 5:**

**Software selection:** we will write the program on arduino uno for controller. And also we will use separate web site for monitoring the parameter.

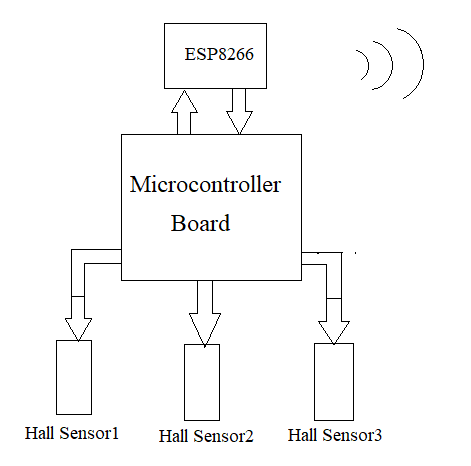
**STAGE 6:**

**Testing of system:** After completion of programming and simulation we will start system implementation. We will divide the work of implementation in stages. The system implementation follows the block diagram. After the successful implementation of system we will have test on it and then after we will give the demo.

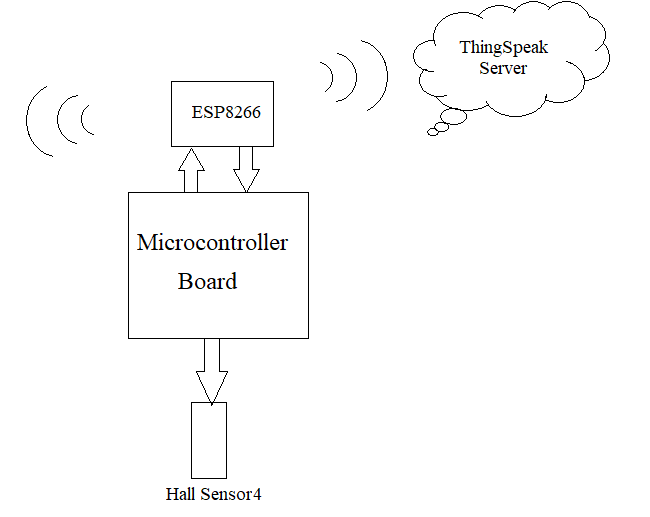
**Proposed work:**

****

**Fig. Block diagram of****Electricity Pilferage Detection, Monitoring & Controlling**

****

**Fig. Block diagram at client side**

****

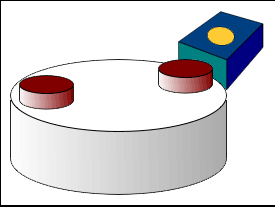
**Fig. Block diagram at server side**

**Hall sensor:**

A **Hall effect sensor** is a [transducer](https://en.wikipedia.org/wiki/Transducer) that varies its output [voltage](https://en.wikipedia.org/wiki/Voltage) in response to a [magnetic field](https://en.wikipedia.org/wiki/Magnetic_field). [Hall effect](https://en.wikipedia.org/wiki/Hall_effect) sensors are used for [proximity](https://en.wikipedia.org/wiki/Distance) switching, positioning, speed detection, and current sensing applications. In a Hall effect sensor a thin strip of metal has a current applied along it, in the presence of a magnetic field the electrons are deflected towards one edge of the metal strip, producing a voltage gradient across the short-side of the strip (perpendicular to the feed current). Inductive sensors are just a coil of wire, in the presence of a changing magnetic field a current will be induced in the coil, producing a voltage at its output. Hall effect sensors have the advantage that they can detect static (non-changing) magnetic fields.

In its simplest form, the sensor operates as an [analog](https://en.wikipedia.org/wiki/Analog_(signal)) transducer, directly returning a voltage. With a known magnetic field, its distance from the Hall plate can be determined. Using groups of sensors, the relative position of the magnet can be deduced.

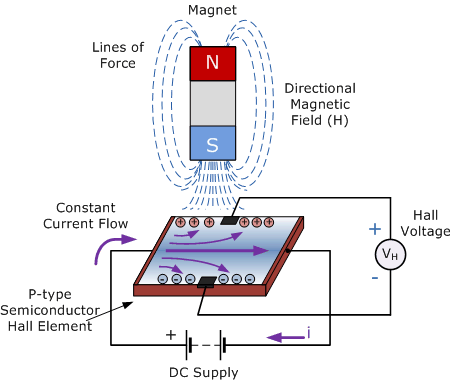
Frequently, a Hall sensor is combined with threshold detection so that it acts as and is called a [switch](https://en.wikipedia.org/wiki/Switch).



**Working principle**:

When a beam of charged particles passes through a magnetic field, forces act on the particles and the beam is deflected from a straight path. The flow of electrons through a conductor is known as a beam of charged carriers. When a conductor is placed in a magnetic field perpendicular to the direction of the electrons, they will be deflected from a straight path. As a consequence, one plane of the conductor will become negatively charged and the opposite side will become positively charged. The voltage between these planes is called the Hall voltage.

When the force on the charged particles from the electric field balances the force produced by magnetic field, the separation of them will stop. If the current is not changing, then the Hall voltage is a measure of the magnetic flux density. Basically, there are two kinds of Hall effect sensors. One is linear which means the output of voltage linearly depends on magnetic flux density; the other is called threshold which means there will be a sharp decrease of output voltage at each magnetic flux density.



**Features and Benefits**

▪ Low-noise analog signal path

▪ Device bandwidth is set via the new FILTER pin

▪ 5 μs output rise time in response to step input current

▪ 80 kHz bandwidth

▪ Total output error 1.5% at TA = 25°C

▪ Small footprint, low-profile SOIC8 package

▪ 1.2 mΩ internal conductor resistance

▪ 2.1 kVRMS minimum isolation voltage from pins 1-4 to pins 5-8

▪ 5.0 V, single supply operation

▪ 66 to 185 mV/A output sensitivity

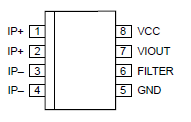
▪ Output voltage proportional to AC or DC currents

▪ Factory-trimmed for accuracy

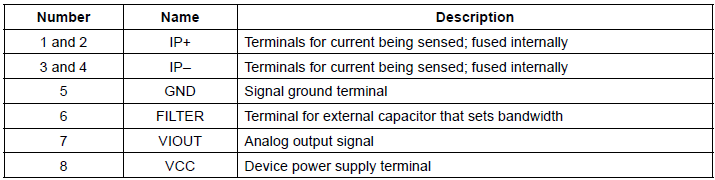
▪ Extremely stable output offset voltage

▪ Nearly zero magnetic hysteresis

▪ Ratiometric output from supply voltage



**Fig.Pin-out Diagram**



**Fig.Terminal List Table**

**Advantages:**

A Hall effect sensor may operate as an electronic switch.

* Such a switch costs less than a [mechanical switch](https://en.wikipedia.org/wiki/Reed_switch) and is much more reliable.
* It can be operated up to 100 kHz.
* It does not suffer from contact bounce because a solid state switch with hysteresis is used rather than a mechanical contact.
* It will not be affected by environmental contaminants since the sensor is in a sealed package. Therefore, it can be used under severe conditions.

In the case of linear sensor (for the magnetic field strength measurements), a Hall effect sensor:

* can measure a wide range of magnetic fields
* is available that can measure either North or South pole magnetic fields
* Can be flat.

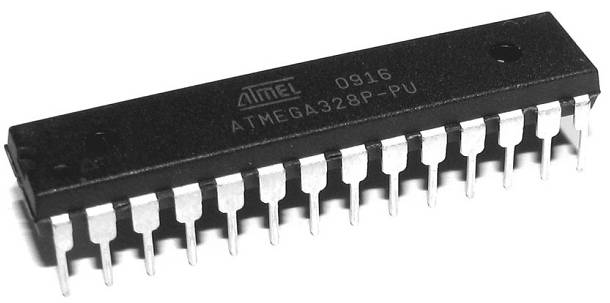
### Application:

### Direct current (DC) transformers

Hall effect sensors may be utilized for contactless measurements of [DC current](https://en.wikipedia.org/wiki/DC_current) in [current transformers](https://en.wikipedia.org/wiki/Current_transformer). In such a case the Hall effect sensor is mounted in the gap in magnetic core around the current conductor. As a result, the DC [magnetic flux](https://en.wikipedia.org/wiki/Magnetic_flux) can be measured, and the DC current in the conductor can be calculated.

**Microcontroller ATmega328P:**

The Atmel picoPower ATmega328/P 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/P achieves throughputs close to 1MIPS per MHz. This empowers system designed to optimize the device for power consumption versus processing speed.



**Feature:**

High Performance, Low Power Atmel AVR 8-Bit Microcontroller Family

• Advanced RISC Architecture

– 131 Powerful Instructions

– Most Single Clock Cycle Execution

– 32 x 8 General Purpose Working Registers

– Fully Static Operation

– Up to 20 MIPS Throughput at 20MHz

– On-chip 2-cycle Multiplier

• High Endurance Non-volatile Memory Segments

– 32KBytes of In-System Self-Programmable Flash program Memory

– 1KBytes EEPROM

– 2KBytes Internal SRAM

– Write/Erase Cycles: 10,000 Flash/100,000 EEPROM

– Data Retention: 20 years at 85°C/100 years at 25°C(1)

– Optional Boot Code Section with Independent Lock Bits

• In-System Programming by On-chip Boot Program

• True Read-While-Write Operation

Peripheral Features

– Two 8-bit Timer/Counters with Separate Prescaler and Compare Mode

– One 16-bit Timer/Counter with Separate Prescaler, Compare Mode, and Capture Mode

– Real Time Counter with Separate Oscillator

– Six PWM Channels

– 8-channel 10-bit ADC in TQFP and QFN/MLF package

• Temperature Measurement

– 6-channel 10-bit ADC in PDIP Package

• Temperature Measurement

– Two Master/Slave SPI Serial Interface

– One Programmable Serial USART

– One Byte-oriented 2-wire Serial Interface (Philips I2C compatible)

– Programmable Watchdog Timer with Separate On-chip Oscillator

– One On-chip Analog Comparator

– Interrupt and Wake-up on Pin Change

• Special Microcontroller Features

– Power-on Reset and Programmable Brown-out Detection

– Internal Calibrated Oscillator

– External and Internal Interrupt Sources

– Six Sleep Modes: Idle, ADC Noise Reduction, Power-save, Power-down, Standby, and Extended Standby

• I/O and Packages

– 23 Programmable I/O Lines

– 28-pin PDIP, 32-lead TQFP, 28-pad QFN/MLF and 32-pad QFN/MLF

• Operating Voltage: – 1.8 - 5.5V

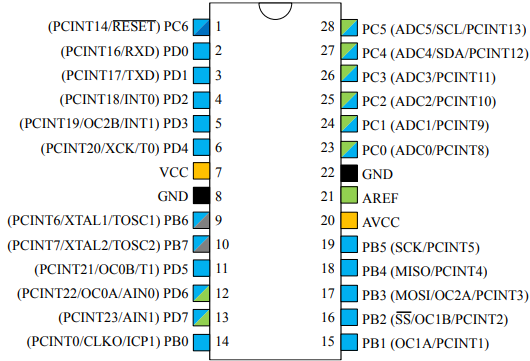
• Temperature Range: – -40°C to 105°C

• Speed Grade: – 0 - 4MHz @ 1.8 - 5.5V – 0 - 10MHz @ 2.7 - 5.5V – 0 - 20MHz @ 4.5 - 5.5V

• Power Consumption at 1MHz, 1.8V, 25°C

– Active Mode: 0.2mA – Power-down Mode: 0.1μA

– Power-save Mode: 0.75μA (Including 32kHz RTC)



Pin Descriptions:

* VCC Digital supply voltage.
* GND Ground.
* Port B (PB[7:0]) XTAL1/XTAL2/TOSC1/TOSC2 Port B is an 8-bit bi-directional I/O port with internal pull-up resistors (selected for each bit). The Port B output buffers have symmetrical drive characteristics with both high sink and source capability. As inputs, Port B pins that are externally pulled low will source current if the pull-up resistors are activated. The Port B pins are tri-stated when a reset condition becomes active, even if the clock is not running. Depending on the clock selection fuse settings, PB6 can be used as input to the inverting Oscillator amplifier and input to the internal clock operating circuit. Depending on the clock selection fuse settings, PB7 can be used as output from the inverting Oscillator amplifier. If the Internal Calibrated RC Oscillator is used as chip clock source, PB[7:6] is used as TOSC[2:1] input for the Asynchronous Timer/Counter2 if the AS2 bit in ASSR is set.
* Port C (PC[5:0]) Port C is a 7-bit bi-directional I/O port with internal pull-up resistors (selected for each bit). The PC[5:0] output buffers have symmetrical drive characteristics with both high sink and source capability. As inputs, Port C pins that are externally pulled low will source current if the pull-up resistors are activated. The Port C pins are tri-stated when a reset condition becomes active, even if the clock is not running.
* PC6/RESET If the RSTDISBL Fuse is programmed, PC6 is used as an I/O pin. Note that the electrical characteristics of PC6 differ from those of the other pins of Port C. If the RSTDISBL Fuse is unprogrammed, PC6 is used as a Reset input. A low level on this pin for longer than the minimum pulse length will generate a Reset, even if the clock is not running. Shorter pulses are not guaranteed to generate a Reset. The various special features of Port C are elaborated in the Alternate Functions of Port C section.
* Port D (PD[7:0]) Port D is an 8-bit bi-directional I/O port with internal pull-up resistors (selected for each bit). The Port D output buffers have symmetrical drive characteristics with both high sink and source capability. As inputs, Port D pins that are externally pulled low will source current if the pull-up resistors are activated. The Port D pins are tri-stated when a reset condition becomes active, even if the clock is not running.
* AVCC AVCC is the supply voltage pin for the A/D Converter, PC[3:0], and PE[3:2]. It should be externally connected to VCC, even if the ADC is not used. If the ADC is used, it should be connected to VCC through a low-pass filter. Note that PC[6:4] use digital supply voltage, VCC.
* AREF AREF is the analog reference pin for the A/D Converter.
* ADC[7:6] (TQFP and VFQFN Package Only) In the TQFP and VFQFN package, ADC[7:6] serve as analog inputs to the A/D converter. These pins are powered from the analog supply and serve as 10-bit ADC channels.

**Application:**

As of 2013 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](https://en.wikipedia.org/wiki/Arduino" \o "Arduino) development platform, namely the [Arduino Uno](https://en.wikipedia.org/wiki/Arduino_Uno" \o "Arduino Uno) and [Arduino Nano](https://en.wikipedia.org/wiki/Arduino_Nano" \o "Arduino Nano) models.

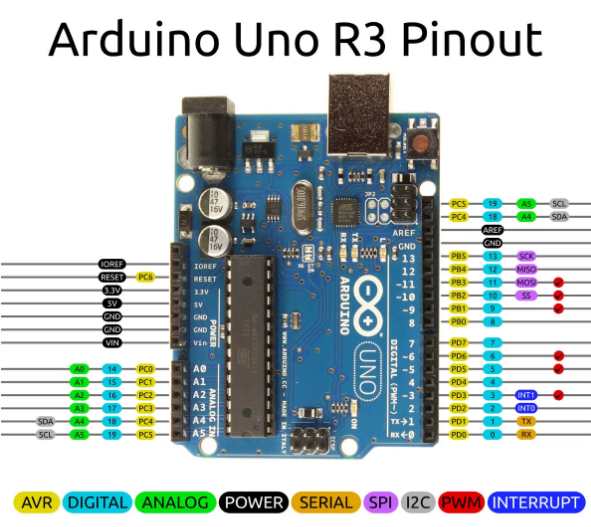
### The Microcontroller Arduino UNO

It is important to understand that the Arduino board includes a microcontroller, and this microcontroller is what executes the instructions in your program. If you know this, you won't use the common nonsense phrase "Arduino is a microcontroller" ever again.

The ATmega328 microcontroller is the MCU used in Arduino UNO R3 as a main controller. ATmega328 is an MCU from the AVR family; it is an 8-bit device, which means that its data-bus architecture and internal registers are designed to handle 8 parallel data signals.

ATmega328 has three types of memory:

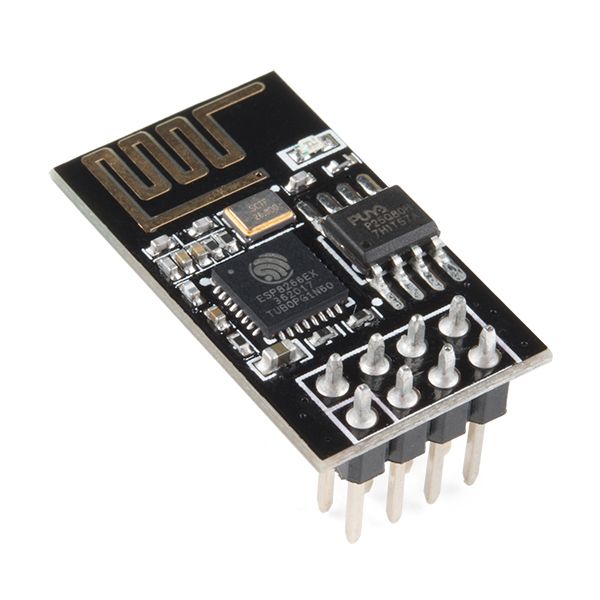
* **Flash memory:** 32KB nonvolatile memory. This is used for storing application, which explains why you don't need to upload your application every time you unplug arduino from its power source.
* **SRAM memory:** 2KB volatile memory. This is used for storing variables used by the application while it's running.
* **EEPROM memory:** 1KB nonvolatile memory. This can be used to store data that must be available even after the board is powered down and then powered up again.

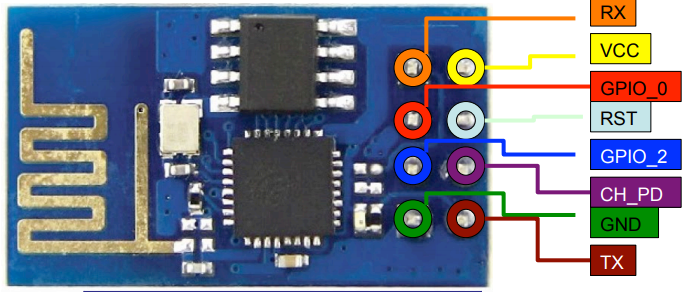


**Advantages**

1. Still runs on 5 V, so legacy 5 V stuff interfaces cleaner
2. Even though it's 5 V capable, newer parts can run to 1.8 V. This wide range is very rare.
3. Nice instruction set, very good instruction throughput compared to other processors (HCS08, PIC12/16/18).
4. High quality GCC port (no proprietary crappy compilers!)
5. "PA" variants have good sleep mode capabilities, in micro-amperes.
6. Well rounded peripheral set
7. QTouch capability

**Wifi module:**





The **ESP8266** is a low-cost [Wi-Fi](https://en.wikipedia.org/wiki/Wi-Fi) microchip with full [TCP/IP stack](https://en.wikipedia.org/wiki/TCP/IP_stack) and [microcontroller](https://en.wikipedia.org/wiki/Microcontroller) capability produced by Shanghai-based Chinese manufacturer, Espressif Systems.[[1]](https://en.wikipedia.org/wiki/ESP8266#cite_note-Espressif_ESP8266-1)

The chip first came to the attention of western [makers](https://en.wikipedia.org/wiki/Maker_culture) 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 using [Hayes](https://en.wikipedia.org/wiki/Hayes_command_set)-style commands. However, at the time there was almost no English-language documentation on the chip and the commands it accepted.[[2]](https://en.wikipedia.org/wiki/ESP8266#cite_note-2) The very low price and the fact that there were very few external components on the module which suggested that it could eventually be very inexpensive in volume, attracted many hackers to explore the module, chip, and the software on it, as well as to translate the Chinese documentation.[[3]](https://en.wikipedia.org/wiki/ESP8266#cite_note-3)

The **ESP8285** is an ESP8266 with 1 MiB of built-in flash, allowing for single-chip devices capable of connecting to Wi-Fi.[[4]](https://en.wikipedia.org/wiki/ESP8266#cite_note-esp8285-4)

The successor to these microcontroller chips is the [ESP32](https://en.wikipedia.org/wiki/ESP32).

**features**

* Processor: L106 32-bit [RISC](https://en.wikipedia.org/wiki/Reduced_instruction_set_computing) microprocessor core based on the [Tensilica](https://en.wikipedia.org/wiki/Tensilica" \o "Tensilica) Xtensa Diamond Standard 106Micro running at 80 MHz†
* Memory:
  + 32 KiB instruction RAM
  + 32 KiB instruction cache RAM
  + 80 KiB user data RAM
  + 16 KiB ETS system data RAM
* External QSPI flash: up to 16 MiB is supported (512 KiB to 4 MiB typically included)
* [IEEE 802.11](https://en.wikipedia.org/wiki/IEEE_802.11) b/g/n [Wi-Fi](https://en.wikipedia.org/wiki/Wi-Fi)
  + Integrated [TR switch](https://en.wikipedia.org/wiki/Duplexer#Transmit-receive_switch), [balun](https://en.wikipedia.org/wiki/Balun" \o "Balun), [LNA](https://en.wikipedia.org/wiki/Low-noise_amplifier), [power amplifier](https://en.wikipedia.org/wiki/RF_power_amplifier) and [matching network](https://en.wikipedia.org/wiki/Matching_network)
  + [WEP](https://en.wikipedia.org/wiki/Wired_Equivalent_Privacy) or [WPA/WPA2](https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access) authentication, or open networks
* 16 [GPIO](https://en.wikipedia.org/wiki/General-purpose_input/output) pins
* [SPI](https://en.wikipedia.org/wiki/Serial_Peripheral_Interface_Bus)
* [I²C](https://en.wikipedia.org/wiki/I%C2%B2C) (software implementation)[[5]](https://en.wikipedia.org/wiki/ESP8266#cite_note-EspressifBBS_I2C-5)
* [I²S](https://en.wikipedia.org/wiki/I%C2%B2S) interfaces with DMA (sharing pins with GPIO)
* [UART](https://en.wikipedia.org/wiki/Universal_asynchronous_receiver/transmitter) on dedicated pins, plus a transmit-only UART can be enabled on GPIO2
* 10-bit [ADC](https://en.wikipedia.org/wiki/Analog-to-digital_converter) ([successive approximation ADC](https://en.wikipedia.org/wiki/Successive_approximation_ADC))

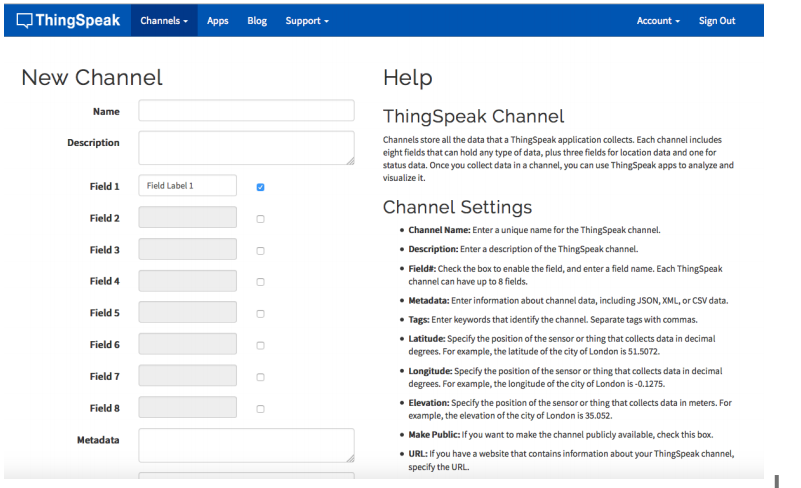
**ThingSpeak:**

According to its developers, "**ThingSpeak** is an [open source](https://en.wikipedia.org/wiki/Open_source) [Internet of Things](https://en.wikipedia.org/wiki/Internet_of_Things) (IoT) application and [API](https://en.wikipedia.org/wiki/API) to store and retrieve data from things using the [HTTP](https://en.wikipedia.org/wiki/HTTP) protocol over the Internet or via a Local Area Network. ThingSpeak enables the creation of sensor logging applications, location tracking applications, and a social network of things with status updates".[[2]](https://en.wikipedia.org/wiki/ThingSpeak#cite_note-2)

ThingSpeak was originally launched by ioBridge in 2010 as a service in support of IoT applications.[[3]](https://en.wikipedia.org/wiki/ThingSpeak#cite_note-3)

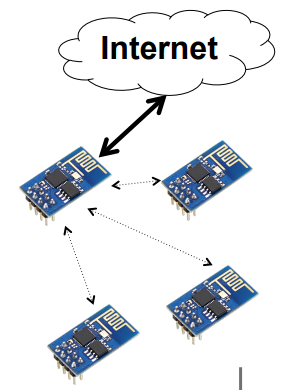
ThingSpeak has integrated support from the numerical computing software [MATLAB](https://en.wikipedia.org/wiki/MATLAB) from [MathWorks](https://en.wikipedia.org/wiki/MathWorks" \o "MathWorks),[[4]](https://en.wikipedia.org/wiki/ThingSpeak" \l "cite_note-4) allowing ThingSpeak users to analyze and visualize uploaded data using Matlab without requiring the purchase of a Matlab license from Mathworks.

ThingSpeak has a close relationship with [Mathworks](https://en.wikipedia.org/wiki/Mathworks" \o "Mathworks), Inc. In fact, all of the ThingSpeak documentation is incorporated into the Mathworks' Matlab documentation [site](https://www.mathworks.com/help/thingspeak/) and even enabling registered Mathworks user accounts as valid login credentials on the ThingSpeak website.[[5]](https://en.wikipedia.org/wiki/ThingSpeak#cite_note-5) The terms of service[[6]](https://en.wikipedia.org/wiki/ThingSpeak" \l "cite_note-6) and privacy policy[[7]](https://en.wikipedia.org/wiki/ThingSpeak#cite_note-7) of ThingSpeak.com are between the agreeing user and Mathworks, Inc.



**Fig. thingspeak channel**

**Autonomous network**

****

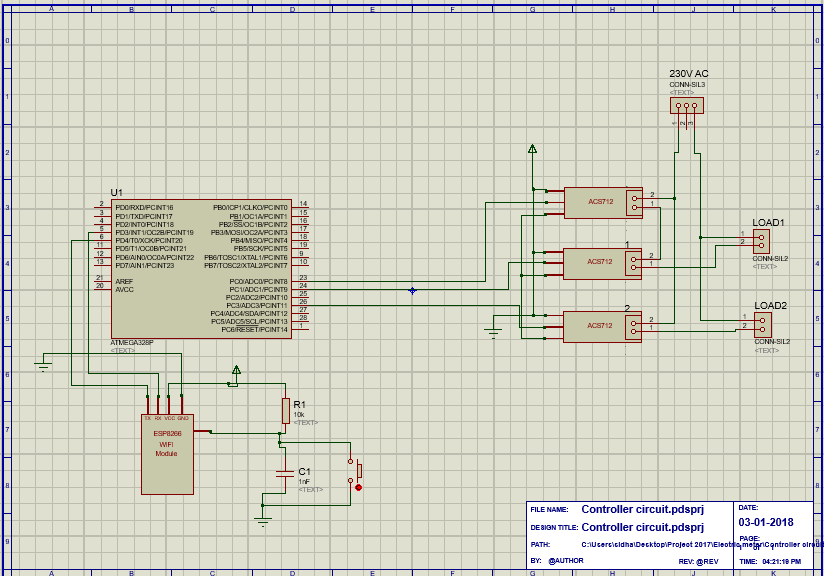
* Multiple ESP8266

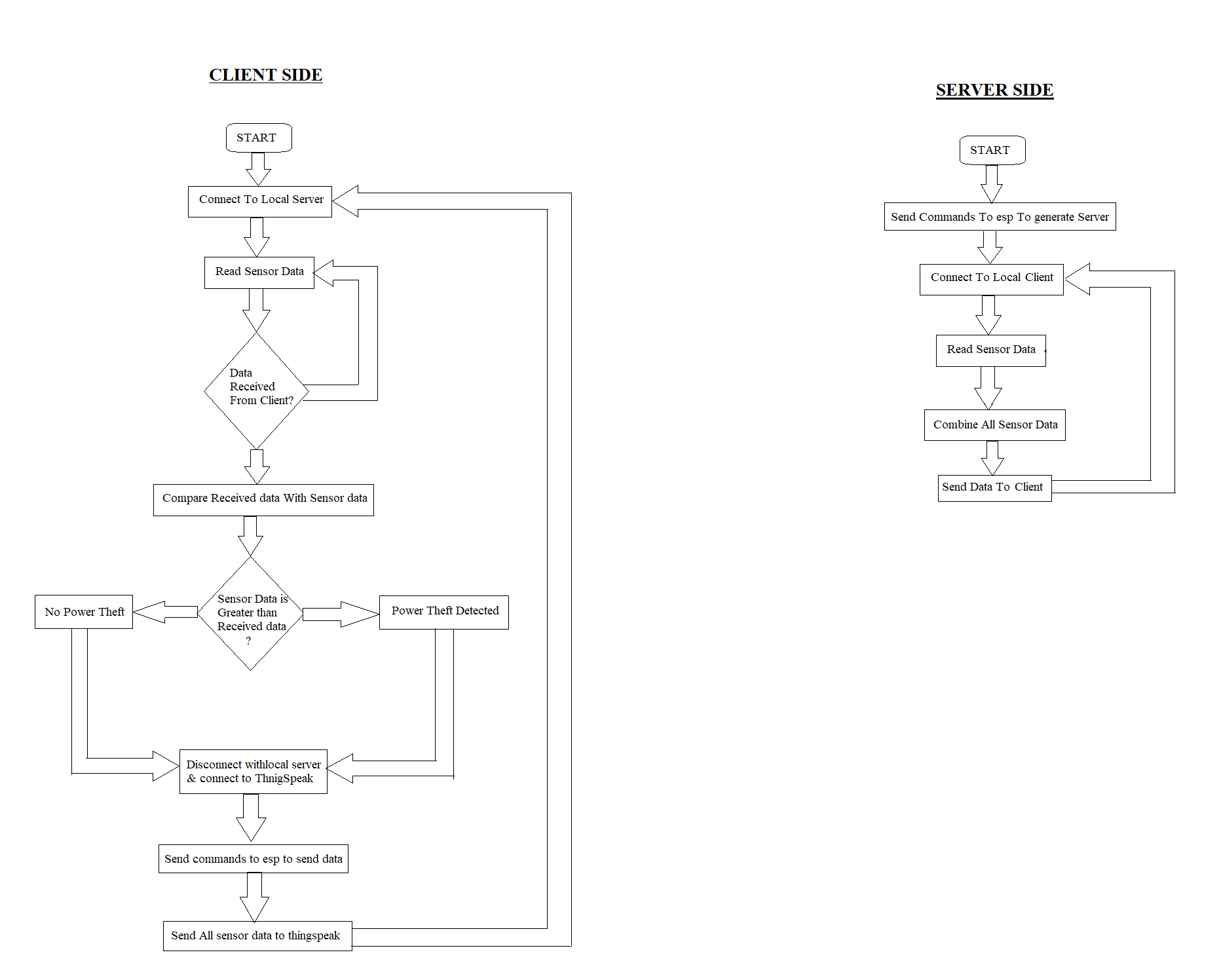
• The first one will serve as access point and send data to ThingSpeak

• Others will connect to the first ESP8266 and send data to him

• The first one will also display a page showing the devices connected

• If the first one dies, another one will replace it.

****

****

**First Commands**

1. Ensure AT commands are received correctly (the AT seems not to be case sensitive but the

rest of any command *is* case sensitive):

AT

Response:

OK

If you don’t get this response check:

* Hardware connections (the blue LED on the board should flash). Try swapping RX & TX.
* Correct baudrate–should be 115200 on the default firmware version (00160901).
* Correct line endings–should be Carriage Return only for default firmware version (00160901).

If it still doesn’t work, give up, you’ve probably got better things to do with your life…

2. Ensure the module is in a known state by issuing a reset command:

AT+RST

Response:

ets Jan 8 2013,rst cause:4, boot mode:(3,6)

wdt reset

load 0x40100000, len 24444, room 16

tail 12

chksum 0xe0

ho 0 tail 12 room 4

load 0x3ffe8000, len 3168, room 12

tail 4

chksum 0x93

load 0x3ffe8c60, len 4956, room 4

tail 8

chksum 0xbd

csum 0xbd

ready

Or similar. The important part is the ready on the last line.

3. Check the firmware version:

AT+GMR

The stock firmware produces this output:

00160901

4. Enable the module to act as both a “Station” and an “Access Point”:

AT+CWMODE=3

Response:

OK

(You *may* need to perform another reset after changing this setting.)

5. List surrounding WiFi networks.

First, if you’re on (at least) the 00160901 firmware you need to work around an apparent

firmware bug that hangs on listing WiFi networks if the last joined network is no longer available.

The following command ensures no network details are stored for connection (you should get an

OK ) response:

AT+CWJAP="",""

(You can check to see what the currently stored network details are with:

AT+CWJAP?

which should generate the following output if no network details are stored:

+CWJAP:""

With a later firmware or if the last joined network is still in the vicinity you shouldn’t need to do this

pre-step.)

Now you send the *actual* command to list networks in the vicinity:

AT+CWLAP

You should get a response like:

+CWLAP:(0,"",0)

+CWLAP:(3,"WiFiArtThouRomeo",-80)

+CWLAP:(3,"Free Public WiFi",-51)

+CWLAP:(3,"Guest",-91)

OK

Sometimes you might get ERROR or no response–in which case you’ll have to try doing the USB

plug/unplug cycle and try again. (Or the same with the ground jumper.)

6. Join a suitable WiFi access point:

AT+CWJAP="<access\_point\_name>","<password>"

You should get an OK response.

For example, with the above list of access points you might use:

AT+CWJAP="Guest","MyVoiceIsMyPasswordSoWhyDoINeedThis?"

You can check if the module has been allocated a IP address with:

AT+CIFSR

You should get your current IP address in response, e.g:

192.168.1.2

**Acting as a TCP Client**

You can connect to an internet server (e.g. a web server) with the following method:

1. Enable multiple connections (you need an OK response):

AT+CIPMUX=1

2. Specify which connection channel you wish to connect on ( 0 - 4 ), the protocol type (TCP/UDP),

the IP address (or domain if you have DNS access) and the port number using the CIPSTART

command:

AT+CIPSTART=4,"TCP","google.com",80

You should receive the response OK followed by Linked when the connection is open:

OK

Linked

3. Next you need to specify how much data you wish to send (after specifying which channel). In this

example we’re going to send “ GET / HTTP/1.0\r\n\r\n ” which is 18 bytes:

AT+CIPSEND=4,18

This time, instead of an “OK” response your will get a > prompt:

>

This indicates the module is waiting for you to send the 18 bytes of data.

Here it gets a bit messy if you’re using the Arduino serial monitor as you have to swap between the

line ending the module requires (“Carriage return” only) and what the HTTP server is expecting

(“Both NL & CR”). Change the setting to *Both NL & CR* and send the following (you will need to

press Send a second time to send the empty line the HTTP server expects):

GET / HTTP/1.0

The module should respond with:

SEND OK

Now you should change the line ending setting to *Carriage return* only so you can send additional

commands.

The module should provide a second response once the web server responds:

+IPD,4,530:

The 4 indicates it’s data from connection channel 4 and the 530 indicates there’s 530 bytes of

data. You should now see the data:

HTTP/1.0 302 Found

Cache-Control: private

Content-Type: ...

Woo! You just put a thing on the internet…time to go find a VC!

You’ll likely get an OK response or two and then eventually an indication that the server has

closed the connection:

Unlink

**Acting as a TCP Server:**

You can enable the module to *accept* TCP connections (i.e. act as a server) in the following manner:

1. Connect to a WiFi access point.

2. Enable multiple connections.

AT+CIPMUX=1

3. Find out the IP address of the module:

AT+CIFSR

Note the response, e.g.:

192.168.1.2

4. Set the module to listen (first parameter, mode is set to 1 ) for a connection on a specific port

(in this case port 1336):

AT+CIPSERVER=1,1336

5. From another device on the same network connect to the listening port, e.g. with telnet:

telnet 192.168.1.2 1336

The module should display:

Link

Type some text into the telnet session, e.g.:

KiwiconAte!

The module should display the following ( 0 being the connection channel, 13 being the length

of the data received:

+IPD,0,13:KiwiconAte!

OK

You can send data in response with the CIPSEND command as used previously, e.g. ( 0 is the

channel, 8 is the length of the data):

AT+CIPSEND=0,8

The module will display the prompt:

>

Then you can send the data, e.g.:

WhatEvs

And then the module will respond with:

SEND OK

The telnet session should now display:

WhatEvs

You can then end the telnet session with by pressing Ctrl-] and q<enter> , the module will

display:

Unlink

**Acting as a WiFi Access Point:**

In addition to connecting to WiFi Access Points the module can also act *as* an Access Point–this means

you can connect devices to the module without any other network infrastructure in place. Ideal for a

local private shared “drop box” perhaps…

1. The module comes with an access point pre-defined (SSID of “ESP\_…”) but you can define your

own with:

AT+CWSAP="NoWorriESSID","password",3,0

The first parameter is the SSID name; the second parameter is the password; the third the WiFi

channel–pick one not used in your area; and, the final parameter is the encryption standard to use.

An encryption value of 0 turns encryption off which means the password is ignored–but it still

can’t be an empty value. I couldn’t get any encryption to work though (it would always create an

unencrypted network) you might have more luck–possibly with a more recent firmware…

2. To actually enable the network to be created you need to set the “WiFi mode” of the module to “AP”

( 2 ) or “Both” ( 3 ):

AT+CWMODE=3

Now you will be able to connect to your module as an access point from another device (e.g. a

laptop or a phone).

3. You can list the IP address etc of any device connected to the network with:

AT+CWLIF

Which generates the response:

192.168.4.100, [...]

4. Now you can run the server example from above and connect–note that the module always has the

IP 192.168.4.1 when acting as an AP.

**Conclusion**

In this section we design the “Electricity pilferage detection system” which avoids the illegal use of electricity. It mainly focused on industrial purpose. The similar idea can be implemented for domestic areas for avoiding the illegal usage of electricity. This system is aimed at reducing the heavy power and revenue losses that occur due to power theft by the customers. By this design it can be concluded that power theft can be effectively curbed by detecting where the power theft occurs and informing the authorities. Also an automatic circuit breaker may be integrated to the unit so as to remotely cut off the power supply to the house or consumer who tries to indulge in power theft.

**References**

[1] ZHOU Wei, ZHU Rue-de, WANG Jin-quant. GSM based monitoring and control system against electricity stealing. Electric Power Automation Equipment, 2004, Vol.24, No.2: pp.64-66.

[2]Louis J. Romeo, “Electronic Pilferage Detection Systems: A Survey”, Library & Archival Security, Volume 3, Issue 3 & 4 January 1982 , pages 1 – 22. [LJR 1982]

[3] HE Xiao-rong, DONG Ch. UN, LIU Shu-xi. The new Technology and application of single phase electric Energy meter defense electricity stealing. Power Supply,2007, Vol.24, No.2: pp.70-71, 74.

[4] “Pilferage detection and smart metering practices and expectations in the Netherlands” P.Kadurek, Student member, IEEE, J. Blom, J. F. G. Cobben, W. L. Kling, Member, IEEE1

[5] G. L. Prashanthi, K. V. Prasad, researched to record the power consumed by a model organization such a household consumers from a commonly located point. Recording the power means measuring the power consumed exactly by the user at a given time.

[6] D. Dangar and S. K .Joshi, *Electricity pilferage detection techniques for distribution system in GUVNL* ,*International journal of Engineering development and research,* 2014, 11-18.

[7] R. Kalaivani, M. Gowthami , S .Savitha, N .Karthick.,S. Mohanvel, *GSM Based Electricity Pilferage Identification in Distribution Systems, International Journal of Engineering trends and Technology, volume 8,*2014,512-516.

[8] T. B. Smith, *Electricity pilferage: a comparative analysis, Elsevier Journal Energy Policy, vol. 32, no. 18*, 2004, 2067-2076.

[9] Nabil Mohammad and Anomadarshi Barua and Muhammad Abdullah Arafat, *A Smart Prepaid Energy Metering System to Control Electricity Pilferage, International Conference on Power, Energy and Control (ICPEC),*2013,562-565.

[10] A. J. Dick, *Pilferage of electricity-how UK electricity companies detect and deter, in proceedings of European Convention on Security and Detection*, may1995, 90-95.

[11] A. Barua, N. Mohammad, A. I. Abbas, and M. A. Arafat, Single phase SMS prepaid digital energy meter, unpublished.

[12] A. Barua, N. Mohammad, M. A. Arafat, K. Khan, A. I. Abbas, and R. Chaudhary Three phase SMS prepaid digital energy meter, International Conference on Electrical and Computer Engineering, 2012, in press.

[13] Mr. Sudheer , K. Reddy, Mr. Musthafa.P, Mr. K Sakthidhasan *Equipment for Anti - Electricity Stealing with Remote Monitoring, International journal of engineering research and applications, volume 1,*241-245.

[14] Irfan Quazi1 , Sachin Kumar Gupta2 and Rajendra Prasad, *Pre-paid Energy Meter based on AVR Microcontroller, International journal of Engineering research and applications, volume 1,issue 4,*1879-1884.

[15] S.S.S.R. Depuru, L. Wang, V. Devabhaktuni, and N. Gudi, *Measures and setbacks for controlling electricity pilferage, in proceedings of North American Power Symposium,* Sept. 2010,1-8.

[16] Fourie J.W and Calmeyer J.E, A statistical method to minimize electrical energy losses in a local electricity distribution network, in Proc. of the 7th IEEE AFRICON Conference Africa, Technology Innovation, Gaborone, Botswana, 2004.