

IOT Based Vehicle Tracking and Security System

**1.Sudarsanam Deepika 2.SK.Hepsibha Hussain 3.SK.Nasar Hassain
4.Rahul.CH 5.Dr.N.Chaitanya(Associate Professor)**

ABSTRACT

In highly populated Countries, everyday people lose their lives because of accidents and poor emergency facilities. These lives could have been saved if medical facilities are provided at the right time. This project implies a system which is a solution to this drawback, when a vehicle meets with an accident.

The proposed systems have been simulated and practically design by the use of hardware components and the results are satisfied with the expectation. Accelerometer detects the sudden change in the axes of vehicle and GSM module sends the alert message on your Mobile Phone with the location of the accident. Location of accident is sent in the form of Google Map link, derived from the latitude and longitude from GPS module. There is a SOS button (switch) present to trigger the buzzer if anyone needs help immediately or if the person is feeling sick. A Reset button (switch) is also provided in order to terminate the sending of a message in rare case where there is no casualty, this can save the precious time of the ambulance.

At monitoring center various software's are used to plot the Vehicle on a map. In this way the Vehicle owners are able to track their vehicle on a real-time basis. Due to real time tracking facility, vehicle tracking systems are becoming increasingly popular among owners of expensive vehicles.

So smart vehicle using an Internet of Things (IoT) technology is the solution to reduce the number of accidents and also to prevent theft. This paper presents a smart system design to detect the accident immediately. This system always monitors the gap between the vehicles using ultrasonic sensor. The proposed design is cognizant with GPS/GPRS and GSM that automatically send an alert message to family members and nearest rescue team. The GPS/GPRS system continuously keeps the track of vehicle location and can be used during an accident and theft.

Architecture of IoT:

Currently, the IT market is full of new concepts such as data science, analytics, artificial intelligence, and the internet of things (IoT), but the question is what do these actually mean? The Internet of Things refers to the widespread interconnection of various devices, such as wearables, watches, tablets, remote controls, sensors, home appliances, and more, with people who utilize them. Specifically, the solution gathers data from a large number of devices, which is then sent to data centers and servers for further analysis which drives automation and actions. However, between your command and the achievement of your tasks, there remains an extensive and largely invisible architectural framework that relies on multiple elements and interactions.



Different Layers of IoT Architecture.

To do any project or research about IoT having knowledge of architecture of IoT is required. There are four layers of IoT architecture. They are Interface layer, Service layer, Networking layer, Service layer.[13]

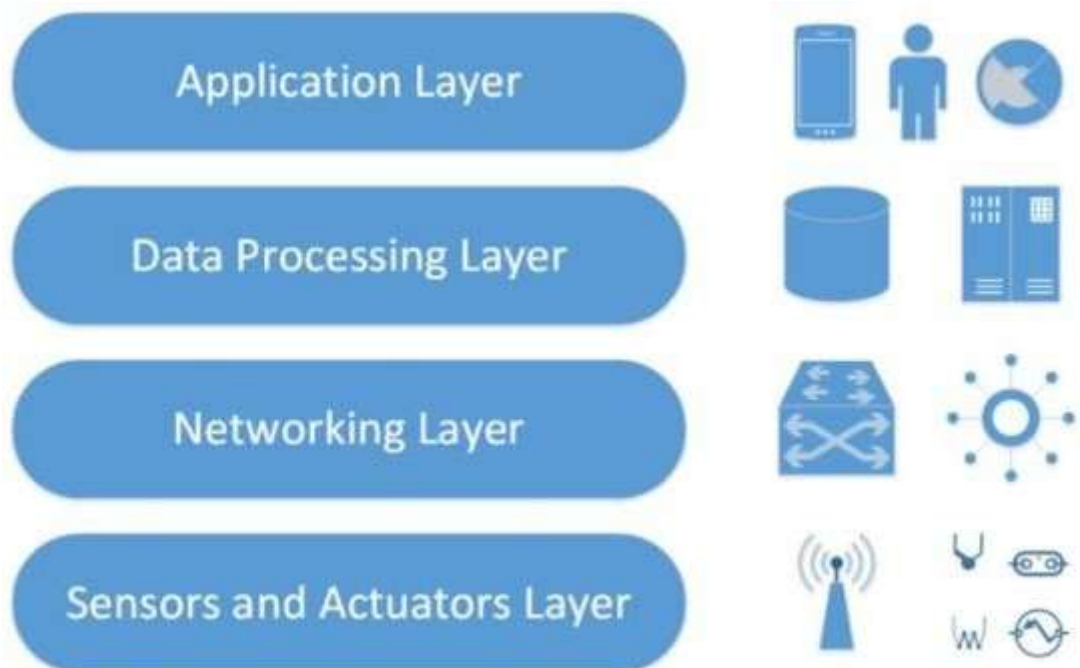


Fig : Four layers of IoT architecture

Application Layer

The first layer of IoT is application layer. This layer provides the interaction methods between users and application. The application layer defines all applications in which IoT has deployed. It is the interface between the end IoT devices and the network. IoT Applications such as smart homes, smart health, smart cities, etc. It has the authority to provide services to the applications. The services may be different for each application because of services based on the information collected by sensors.

It is applied through a dedicated application at the device end. Such as for a computer, the application layer is applied by the browser. It is the browser that executes application layer protocols like HTTP, HTTPS, SMTP, and FTP. There are many concerns in the application layer out of which security is the key issue.[13]

Common issues and threats of application layers:

- **Cross-site scripting:**

It is a type of computer security infirmities that typically found in web applications. It enables attackers to inject client-side scripts such as JavaScript into web pages viewed by other users. By doing so, an attacker can completely change the contents of the application as per his needs and use original information in an illegal way.

The first method you can use to prevent cross-site scripting from appearing in your applications is by escaping user input. Escaping input means taking the data from an application has received and ensured it's secure before supplying it for the end-user. Validating input is another process of ensuring an application is providing the correct data and protecting harmful data from doing harm to the site, database, and users.

- **Malicious Code Attack:**

It is a particular code in any part of the software system or script that is considered to cause undesired effects, security threats or damage to the system. It is that threat that may not be blocked or controlled by the use of anti-virus software.

Static Code Analysis (SCA) is an effective method to protect the malicious code from successfully causing any damage to computers. SCA is a debugging method of a computer program that is done by analyzing the code without performing the program. The process

supplies an understanding of the code structure and can help to ensure that the code should match with industry standards.

Today's superior scanners can easily detect malicious code such as a Data Leakage, Time Bombs, Anti Debugging techniques, backdoor Threats, etc.

Data Processing Layer

In three-layer architecture, the data were directly sent to the network layer. Due to sending data directly the chances of getting damages increase. In four-layer architecture, data is sent to this layer that is obtained from a perception layer. Data Processing Layer has two responsibilities it confirms that data is forwarded by the authentic users and prevented from threats.

Authentication is the most commonly used method to verify the users and the data. It is applied by using pre-shared, keys and passwords to the concerned user. The second responsibility of the layer is to send information to the network layer. The medium through which data is transferred from the Data Processing Layer to the network layer can be wireless and wire-based.

Common issues and threats of the Data Processing layer are:

- **DoSAttack :**

An attacker sends a huge amount of data to make network traffic overloaded. Thus, the huge consumption of system resources exhausts the IoT and makes the user unable to access the system.

Deploy an antivirus program and firewall will restrict the bandwidth usage to authenticated users only. Server Configuration is another method that can help reduce the probability of being attacked.

- **Malicious Insider Attack:**

It comes from the inside of an IoT environment to access private information. It is conducted by an authorized user to access the information of another user.

The practices such as an encryption of data, implementing proper password management practices, installing antivirus will helps to keep data safe from such threats.

Communication with web server and sending notification.

The proposed IoT (and Wireless Sensor Network) based system contains the following three classes of components: master nodes, probe nodes and web server. The module uses IEEE 802.15.4 protocol and also equipped with GSM, Wi-Fi and Bluetooth. The master is the control center that is responsible for communication with the probe nodes, other master nodes and web server for vehicle traffic monitoring purpose. In this system drivers, will be notified of a motorcycle around them in four stages.



Figure: Stages of vehicle alert system

Vehicle Identification:

Vehicles will be identified by identifying smartphones of the vehicle users. For the success of this project, it is very important to identify motorcycle and other vehicles separately. Wi-Fi and Bluetooth module of a smartphone have unique MAC address. Once a vehicle comes near to a probe, an Android application of the smartphone user will send custom beacon to the probe nodes changing the length of MAC address. For a motorcycle, the length of the MAC address will be shorter and for other vehicles, that length will be longer. This way user privacy is reserved and the whole system will deal with only two types of vehicles [14].

Vehicle Registration:

Once the vehicle is identified, the vehicle will be registered in the system. The probe will send registration data such as smartphones' MAC address, GPS data (if available) and the location of the probe that registered the phone to the master node for processing purpose.

3.4.5: ESP8266 Wi-Fi Module:

The ESP8266 Wi-Fi Module is a self-contained SOC with integrated TCP/IP protocol stack that can give any microcontroller access to your Wi-Fi network. The ESP8266 is capable of either hosting an application or offloading all Wi-Fi networking functions from another application processor. Each ESP8266 module comes pre-programmed with an AT command set firmware, meaning, you can simply hook this up to your Arduino device and get about as much Wi-Fi-ability as a Wi-Fi Shield offers (and that's just out of the box)! The ESP8266 module is an extremely cost-effective board with a huge, and ever growing, community.

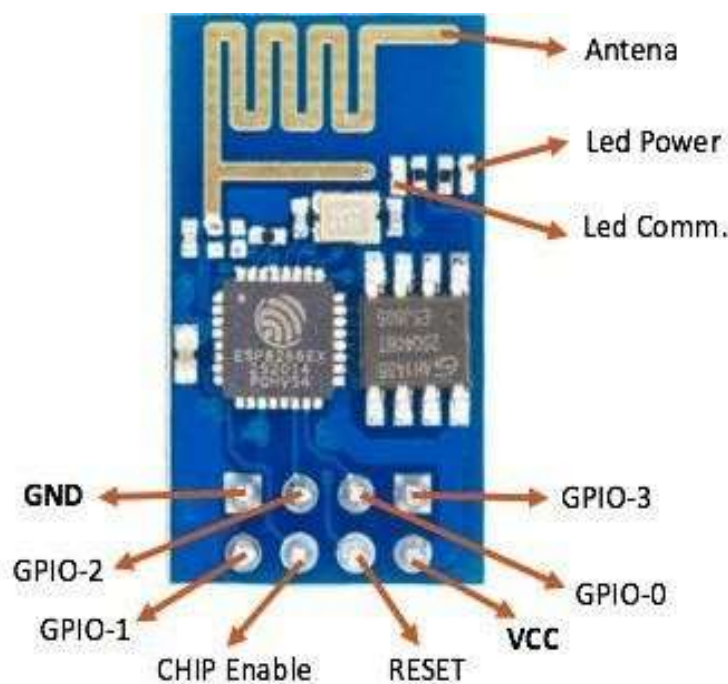


Figure : ESP8266 Wi-Fi Module

ESP8266 Wi-Fi Module Specifications:

The ESP8266 Wi-Fi module specifications or features are given below.

- It is a powerful Wi-Fi module available in a compact size at a very low price.
- It is based on the L106 RISC 32-bit microprocessor core and runs at 80 MHz
- It requires only 3.3 Volts power supply and maximum Input/Output voltage is 3.6 Volts
- The current consumption is 100m Amp.
- The maximum Input/Output source current is 12 mA
- The frequency of built-in low power 32-bit MCU is 80 MHz
- The size of flash memory is 513 kb
- It is used as either an access point or station or both
- It supports less than 10 micro-Amps deep sleep
- It is programmed using either AT commands, Arduino IDE, or Lua script
- It is a 2.4 GHz Wi-Fi module and supports WPA/WPA2, WEP authentication, and open networks.
- It uses two serial communication protocols like I2C (Inter-Integrated Circuit) and SPI (Serial Peripheral Interface).
- It provides 10-bit analogue to digital conversion
- The type of modulation is PWM (Pulse Width Modulation)
- UART is enabled on dedicated pins and for only transmission, it can be enabled on GPIO2.
- It is an IEEE 802.11 b/g/n Wi-Fi module with LNA, power amplifier, balun, integrated TR switch, and matching networks.
- GPIO pins – 17
- Memory Size of instruction RAM – 32 KB
- The memory size of instruction cache RAM – 32 KB
- Size of User-data RAM- 80 KB
- Size of ETS systems-data RAM – 16 KB

3.4.6: 16*2 LCD Display Module:

An LCD (Liquid Crystal Display) screen is an electronic display module and has a wide range of applications. A 16x2 LCD display is very basic module and is very commonly used

in various devices and circuits. A 16x2 LCD means it can display 16 characters per line and there are 2 such lines.



Figure: 16*2 LCD Display Module

Features LCD display module:

- LCD display module with blue backlight.
- Wide viewing angle and high contrast.
- Built-in industry standard HD44780 equivalent LCD controller.
- Commonly used in: copiers, fax machines, laser printers, industrial test equipment, networking equipment such as routers and storage devices.
- Can display 2-lines X 16-characters.
- Voltage: 5V DC.
- Module dimension: 80mm x 35mm x 11mm.
- Viewing area size: 64.5mm x 16mm

I²C 16X2 LCD MODULE:

This 2×16-character LCD Module with BLUE Backlight uses an I2C interface to communicate with the host microcontroller. This budget-conscious LCD is used on projects requiring the display of text, data, or ASCII characters of all types. Connect to Vcc, Gnd, SDA (serial data line), and SCL (serial clock line).



Figure : I²C 16X2 LCD Module

16×2 I2C LCD Display Module with Blue Backlight Specifications:

- Display capacity: 16character x 2row
- Display colour: Blue backlit
- Character size: 2.95 mm wide x 4.35 mm high
- Character pixels: 5 W x 7 H
- Voltage requirements: 5 VDC +/- 0.5V Current
- requirements: 2 mA @ 5 VDC
- Connection: 4-pin male header with 0.1": spacing
- Communication: I2C
- Overall dimensions: 3.15 x 1.42 x 0.51 in (80 x 36 x 13 mm)
- Operating temperature range: 32 to +131 °F (0 to +55 °C)

SW-520D Tilt Sensor:

The tilt sensor is a component (switch) that can detect the orientation of an object (upright or not). It is equivalent to a pushbutton activated through its physical orientation. It contains a metallic ball inside that will commute the two pins of the device from CLOSED to OPEN if the sensor exceeds a certain angle and vice versa. Only when the tilt sensor is in its upright position, metallic balls inside the tilt sensor bridges the two contacts, completing the circuit. When the sensor is tilted beyond the sensitivity range, the contacts move away, and thus opens the circuit.

Table : Power Consumption:

Modes	Frequency	Current Consumption
Power down		60 μ A
Sleep mode		1 mA
Stand by		18 mA
Call	GSM850	199 mA
	EGSM900	216 mA
	DCS1800	146 mA
	PCS1900	131 mA
GPRS		453 mA
Transmission burst		2 A

GPS Module neo6m:

The NEO-6M GPS module is a well-performing complete GPS receiver with a built-in 25 x 25 x 4mm ceramic antenna, which provides a strong satellite search capability. With the power and signal indicators, you can monitor the status of the module.

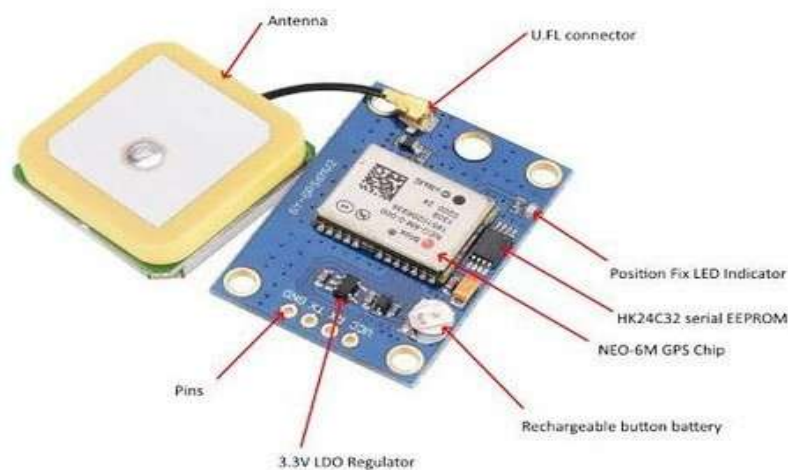


Figure : GPS Module neo6m

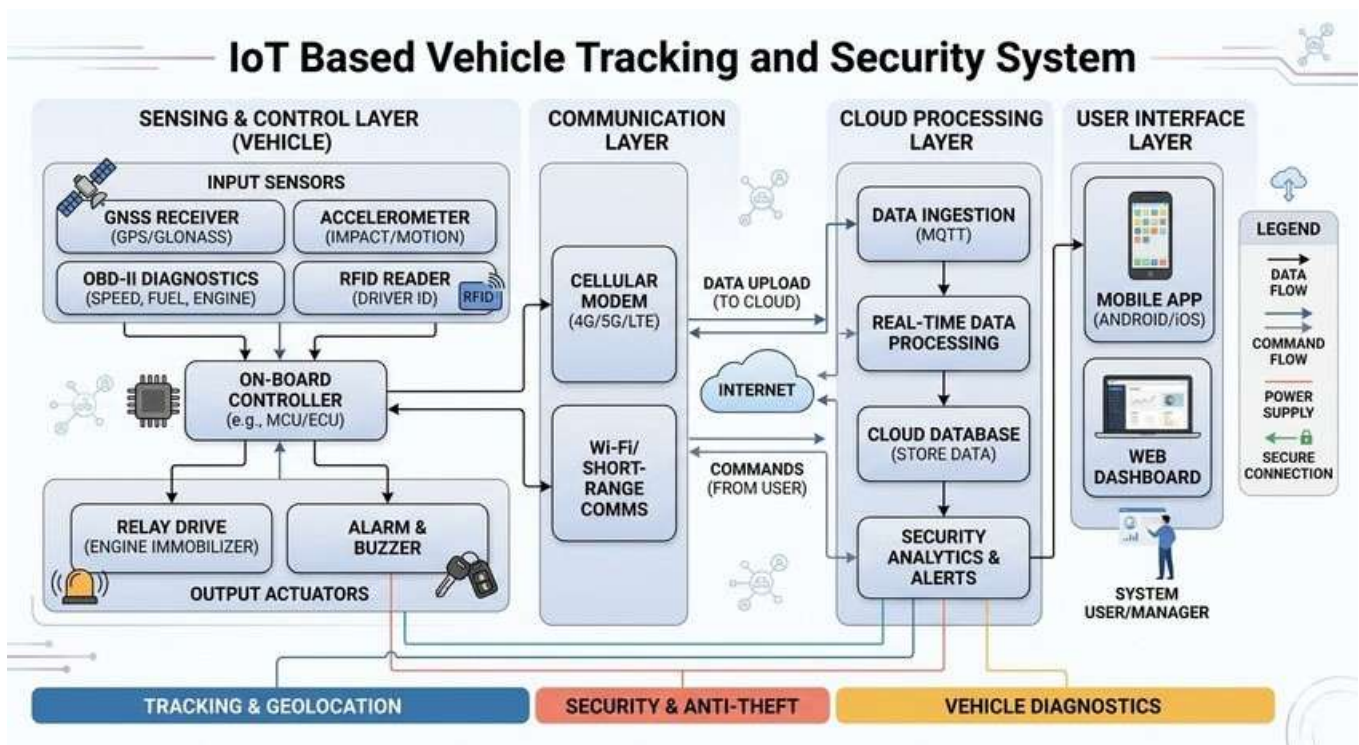


Figure : Block Diagram of the Hardware.

3.5.2 Web services:

To interact with users, a website has been developed where a user with the hardware can create an account and monitor all the vehicle installed this system. User will get notification if any vehicle gets into accident through the website account, mobile application and mobile SMS with the exact GPS location of accident. Also, any police station and hospital can open an account from the website and will get notification through website and mobile SMS about an accident with the accident location and direction towards the accident location using google map.