Journal of Data Acquisition and Processing
ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.7778496

DESIGN AND IMPLEMENTATION OF INTERNET OF THINGS BASED SECURED APPLICATION FOR SELF-DRIVEN VEHICLES

[1]Dr. Basavaraj Patil, [2]Pushpa G, [3]Dr. Dattatreya P. Mankame
[1,2,3]Department of Computer Science and Business Systems, Dayananda Sagar College of Engineering, Bangalore
[1]bbpatilcs@gmail.com, [2]pushpa2817@gmail.com, [3]dpmankame@gmail.com

Abstract— Vehicle theft is now a common problem for all citizens as the number of urban Self-Driven vehicles increases quickly. For the urban inhabitants, safety and security have always been essential. The current anti-theft system, however, is deficient in tracking and monitoring capabilities. Electronics have been ruled by the Internet of Things (IOT), and cloud services have been dominating the rapidly expanding electronics product market. For the safety of cars and their occupants, needs to build a system that uses IOT to protect the vehicle from issues like theft and tugging. The proposed methodology suggests a cutting-edge security system built on wireless medium with a Bluetooth module. The paper presents a message-sending model that takes advantage of the GSM. The owner can manage the engine's ignition and, if necessary, switch it off. The system additionally uses a keypad password (with a maximum of three tries) to regulate the opening of a safety locker door and seatbelt. The IR module/sensor detects any window intruders or other obstacles and alerts the microcontroller if they are present. An alarm system and a Bluetooth module are both connected to the controller. The technology sends a signal of alert to the owner's mobile device. To control the security system, the system uses Bluetooth module of owner's mobile phone.
Keywords— Android, Arduino, GSM, GPS, Micro-controller

I. INTRODUCTION

The internet of things (IOT) corresponds to a physical network of things or objects—devices, buildings, cars, and other elements—embedded with software, sensors, electronic components, and network connectivity. This network lets these entities or objects collect and share data. An anti-theft system used to prevent or detect valuables objects from theft. IoT components are predicted to deliver a higher level of human-to-machine communication as well as machine-to-machine communication [1]. The major aim is to reduce the human intervention. Automation has long been a significant component of security systems.

The motivation of the work is to adopt a security solution which is IoT-enabled, provides control via a hand-held mobile phone. In today's world, there are numerous luxurious and costly vehicles equips with their own security systems. Despite massive investments in vehicle security, vehicle theft continues to rise. This situation guides the need for research to incorporate security precautions and actions to prevent vehicle thefts [2].

The finding is to focus on improving vehicle security and safety to reduce thefts. The owner may keep an eye on their car, its travels, and its arrival thanks to the vehicle tracking

technology. There is still a problem. Many people now choose to travel in their own vehicle thanks to recent advancements in the auto industry [3]. The impact on car ownership is growing. However, parking all these Self-Driven vehicles in major metropolises is a time-consuming and challenging task. There is currently no remedy for problems like towing that result from incorrect parking. The concept thereby addresses the issue of parking and consequent towing. The proposed work includes features like keyless automobile door unlocking, ignition control via both keypads, and seat belt use to address all the issues mentioned above. The concept also addresses difficulties with car window intruders and even locating a vehicle after it has been towed. The car should be more secure thanks to these features.

II. LITERATURE SURVEY

With the use of cutting-edge technology to unlock the car's door and the use of seatbelts, this concept increases vehicle security. The owner can start the car's ignition with these two requirements satisfied. Similarly, protecting the valuables from intruders breaking in via the window and the issue of towing.

Pathak et.al [4] planned to build a model with the least number of circuits conceivable. The SBBSS has different benefits, counting making automobiles more secure, making strides treatment for collision casualties, helping protections companies with crash examinations, and improving street conditions to diminish the passing rate. Vehicle robbery could be a common issue as for Self-Driven vehicles on the street increments, and current anti-theft frameworks need following and observing capabilities. The rise of the Web of Things (IOT) has led to a requirement that ensure security and store vehicle information. The model utilizes IOT to secure cars and their inhabitants from issues like burglary and towing. Clients can control the engine's start and turn it off remotely in case essential. The framework incorporates a Bluetooth module and controller to permit the client to oversee the security framework from their mobile phone or any gadget with a web association. It also offers 24-hour vehicle following utilizing Google Maps, which can be accommodating within the occasion of tow or burglary. The SVBBS framework has appeared guarantee in precisely recognizing mischances, evaluating their reality, and finding Self-Driven vehicles.

Authors proposed [5] system for tracking Self-Driven vehicles and locating using GPS and GSM devices. To shed light on several issues, a tracking and positioning system for vehicle burglaries has used face recognition technology. For real-time face-to-face distinguishing proof and discovery, the framework uses the Open CV Python Module. A locking and recognizing structure have also been added to the vehicle. A portable application recognizes the owner's face and assesses it against data to determine whether they are the owner. If all the conditions are satisfied, the car is unlocked; otherwise, it is left fastened. When someone tries to damage or break the device, the framework not only calls the offender but also sends an alarm. It saves burglary data on a USB drive, allowing clients to investigate the circumstances of the robbery. The framework moreover incorporates a concealed car track framework that activates a buzzer and notifies the client if an unauthorized individual tries to compromise it.

The development of a low-cost antitheft system that uses a platform based in the community to trace stolen goods is examined [6]. Members use their smartphones to look for these devices and report their locations to help owners find their stolen property. The system uses a Bluetooth device as a guide to trace stolen items. The paper also highlights the development of a test mechanism to improve the next handle.

The usage of wireless communication and an inexpensive Wi-Fi module is being proposed for a new security system for automobiles [7]. With the help of IoT technology, this system seeks to safeguard Self-Driven vehicles from theft and towing. Owners may control the engine and ignition with the assistance of the system, which uses the ESP8266 module to send messages and even give them choice to turn them off. In addition, a safety locker's opening is regulated by a keypad with a password. Vehicle theft has become a problem due to the increase in urban automobiles, and current anti-theft systems lack tracking and monitoring capabilities. The creation of this new security system has been influenced by the growth of IoT and cloud services in the electronics sector. This system offers a keyless locking and unlocking method to stop car theft and maintain owner safety. It is cutting-edge, reasonably priced, and provides increased security for car owners. The owner will automatically receive an SMS message and a call to inform them if someone attempts to tamper with the system.

Urban automobiles are becoming more prevalent, and mobility is becoming increasingly important. All vehicle owners are concerned about vehicle theft, yet current anti-theft technologies are unable to stop theft before it occurs. This study suggests a smart vehicle security system that works using an Android app linked to the ignition system of the car. If the ignition key is stolen or lost, this technology prohibits unauthorized access to the vehicle's operational system. Only authorized owners can start the vehicle with the ignition key or the smartphone app, and the technology enables drivers to stay connected to their vehicle. It [2] employs various components, including an Android smartphone, a node MCU, Bluetooth low energy, transistors, and power relays. Once built, it is inexpensive and needs minimal upkeep. The phone app manages the ignition system and guards against unauthorized entry. In case someone tries to begin the vehicle using only the ignition key, the device also has an alarm to warn the car owner. Experiments have revealed that this technology is reliable and hard to breach.

The GSM and GPS tracking capabilities of the microcontroller-based vehicle security system can be utilized to increase vehicle safety as recommended. It can locate a missing vehicle, provide confidence that it is solid proof that it was stolen. It uses GPS and GSM technologies as collection modules[8].

The planning and creation of an automated security framework utilizing GSM technology is shown in this framework. The warming flag and direction are communicated using GSM portable communication. The use of the short message service (SMS) protocol [9], the client and the framework are given control and communication. When an alarm flag is launched or when the auto-access route vibrates or opens illegally, SMS is stolen.

The existing techniques sometime fails to track Self-Driven vehicles by using GPS. They lack with facilities like password system, fingerprint reader and face recognition and lack of integrating smart alert for system protection.

III. PROBLEM STATEMENT

Develop a system that uses the IOT to provide self-driven vehicle security. The system must be capable of performing owner authorization as well as providing access to regulate and supervise the self-driven motor vehicle for any suspicious behaviour. It must keep the car secure by sending an SMS alert to the owner in case of unauthorized access, theft, incursion, or towing.

IV. METHODOLOGY

The procedure of the anticipated method is illustrated in fig 1. The owner must input a password using the keypad to start the ignition or unlock the door; if the password is entered correctly, just the car door will unlock; the owner has only 3 efforts to give valid password; if the password is consistently incorrect, the system must be reset by pressing the reset button.

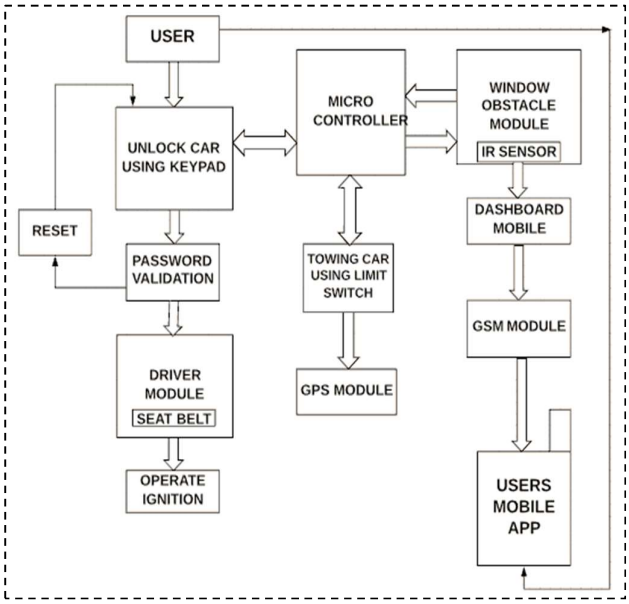

Fig.1 System Design

The owner controls over the ignition or engine of the vehicle, provided they are secured up and the password is put right. A limit switch will automatically be hit if we park our automobile close to an unapproved area and if it is towed. This transmits a command to the controller, which then uses a Bluetooth module to send a signal to the dashboard (the mobile device on the dashboard). The owner is then alerted with the same constant beeping sound and information is sent to them through SMS along with a GPS location from the dashboard.

An IR sensor notices when something moves in front of a window or if someone tries to steal something valuable through a window. The controller then uses Bluetooth to transmit signals to the dashboard (mobile device on the dashboard) after receiving a command from the sensor.

The owner then receives information from the dashboard side mobile through SMS with GPS position.

The diverse hardware and sensors can be integrated, connecting to the internet, and enabling remote monitoring and control, the IoT presents several opportunities for enhancing security. Here is a simple breakdown of the elements and features you could include in such a system:

a. Automotive sensors: Install a variety of sensors on the car to look for unauthorized entry, tampering, or strange activity. Potential sensors could be:
    - Sensors for doors and windows: These sensors can identify unauthorized door or window openings.
    - Motion sensors: When the car isn't supposed to be inhabited, they can detect movement inside.
    - Glass break sensors: Activated when they hear glass breaking. Sensors that detect vibrations, look for attempts at forced entry.
b. GPS Tracking: Integrate a GPS module into the vehicle to track the vehicle's location instantaneously. This might facilitate the swift recovery of stolen Self-Driven vehicles.
c. Cameras: Install cameras both inside and outside the car to record any security breaches with pictures or videos. These can be used as proof and to find the offenders.
d. Using a remote to lock and unlock the door: Use a web or a mobile app to provide remote control of the vehicle's locking and unlocking mechanisms. The lock and unlock the car from any location makes sure as it is secured when parked.
e. Alarm Device: Integrate a warning system that can go off in response to unauthorized entry or dubious activity. The alarm can send notifications to your mobile device and be audible.
f. Web interface or mobile app: Create a owner-friendly app or web interface that enables the vehicle owner to keep an eye on the security situation, get notifications, manage locking and unlocking, and see live camera feeds.
g. Connectivity to the cloud: To store and process the information gathered from sensors and cameras, connect the system to a cloud platform. This enables remote system management, alarm delivery, and access to historical data.
h. Security Protocols :To prevent hacking or unauthorized access to the system, put strong security measures in place for data transfer and storage.
i. Geofencing: Create virtual boundaries for the vehicle by setting up geofences. You can get warnings if the car violates these lines without permission.
j. Power management: Ensure that none of the system's parts—particularly the sensors and tracking equipment—drain the car's battery. To increase the system's battery life, employ effective power management strategies.
k. Integration with Vehicle Systems: To establish a comprehensive security solution, integrate the security system with the vehicle's already-installed security elements, such as the central locking system.
l. Apply machine learning techniques to analyze data patterns and spot potential dangers. AI can assist in improving alarm trigger intelligence and minimizing false positives.

V. HARDWARE AND SOFTWARE COMPONENTS

a. Arduino

The Arduino Mega 2560 is a microcontroller board that has a bunch of cool features as in fig 2. It's got a ton of pins, both digital and analogue, UARTs, a crystal oscillator, and a USB connection. You can power it up by plugging it into your computer or using an AC-to-DC adapter or battery. It's also compatible with most shields made for the Arduino decimal. The ATmega2560 chip inside has plenty of memory for storing code, and you can even use it to interact with your computer. Plus, you can power the Arduino Mega with either USB or an external power supply.

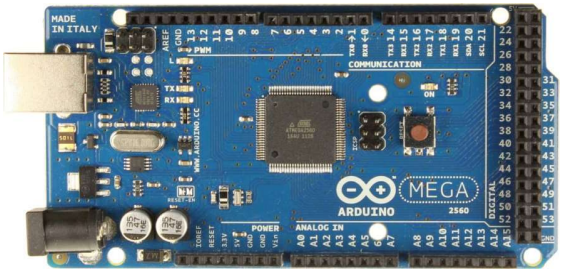

Fig.2 Arduino Mega 2560

b. GPS(Global positioning System)

A satellite navigation system in space, the GPS as in fig 3 offers position and timing data in any weather. The owner's additional position is verified by the GPS receiver using triangulation and the information provided.

Fig.3 GPS Module

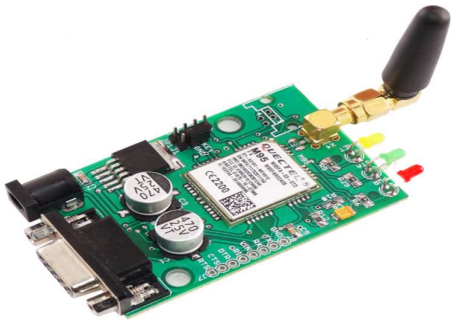

Fig.4 GSM Module

The GPS receiver can calculate the distance to the satellite using the time difference. The receiver can now pinpoint the owner's location and show it on the device's electronic map after receiving distance measurements from a few additional satellites. To determine a 20 position and track movements, a GPS receiver must be situated on the signal of at least three satellites. When four or more satellites are visible, the receiver can calculate various data such as speed, bearing, track, travel distance to destination, sunrise, and sunset times, and so on.

c. GSM (Global System for Mobile System)

GSM is used by over 2 billion individuals in 212 nations and regions. GSM utilized a framework based on direct prescient coding as in fig 4. These codecs made strides in the

capacity of the air interface layer to distinguish between the more basic sound components, permitting it to donate them higher need and way better assurance. They were moreover successful when it came to bit rates.

d. LCD(Liquid Crystal Display)

LCD is the display technology used in laptops and other tiny parts as shown in fig 5 and 6. Like gas plasma and light-emitting diode technologies. It is the 16 X 2 lines LCD display, display with 16 characters per line is translated into two lines using the 16 X 2 algorithm. Each character on this LCD is presented in a 5 × 7-pixel matrix.

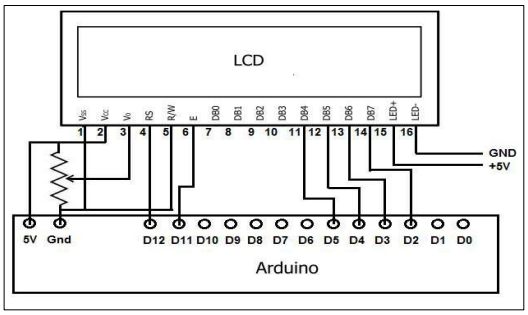

Fig.5 Pin Diagram of LCD

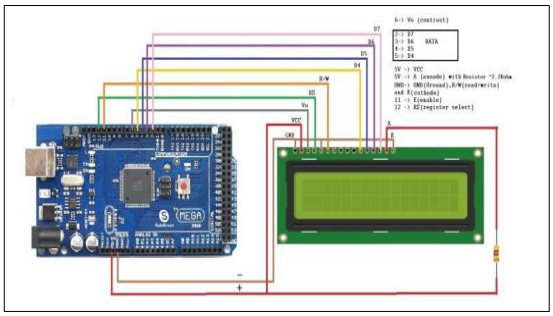

Fig.6 LCD interfacing with Arduino mega

e. IR Sensor

A digital device that has an IR sensor emits light to detect nearby objects as in fig 7. An IR sensor can monitor an object's heat while also spotting movement. An IR LED serves as the emitter, while an IR photodiode serves as the detector.

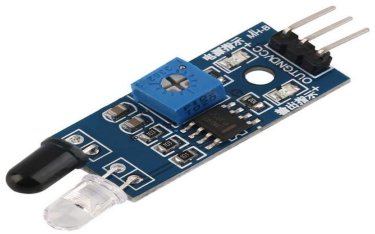

Fig. 7 IR Sensor

Fig.8 Limit Switch

f. Limit switch

Limit switches tracks an object's mobility constraints and detect its presence. They were initially employed to calculate the furthest an object could travel before coming to a stop. These switches have a mechanical actuator and are electromechanical devices with electrical connections. The electrical connection in the switch is opened or closed when the actuator touches an object.

g. Kiel µ version3

The µ Version3 IDE is a software development environment for Windows. It has an editor, project management features, and can generate code. In Version 3, it combined the C compiler, assembler, linker/locator, and HEX file generator.

VI. RESULTS AND DISCUSSIONS

In this work, a prototype represents a car as shown in fig 9.

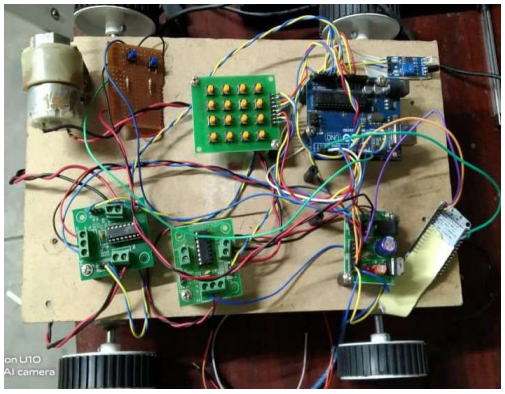

Fig. 9 Circuit Connection for Car prototype.

To start the ignition, the owner must input the password via the keypad, PIN is then validated as seen in fig 10. The owner is the sole person responsible to have access to if the password is true. The owner is allowed to start the car only after that if they are wearing seatbelts and the password is accurate. Through an IR sensor, any intrusion can be found. This uses a Bluetooth module to send commands to a mobile device on the dashboard and sends the owner's information via SMS combined with GPS location.

Fig.10 PIN Validation

Fig.11 Alert message for valid PIN

A command is sent to the controller while towing when the limit switch is depressed, and the controller then sends a command to the dashboard through Bluetooth module as in fig 10.

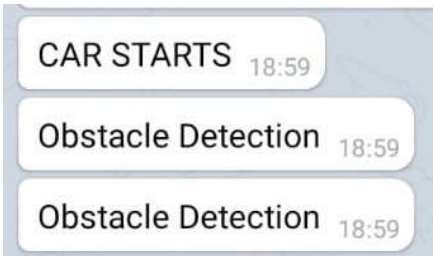

Fig.12 Alert message for intrusion or towing

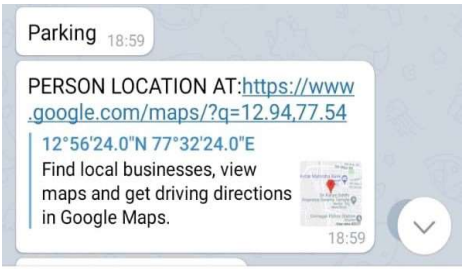

Fig.13 Location on owner's mobile on Google maps

The owner gets the details via SMS and with GPS location. If the password is incorrect every time, the system must be reset by pressing the reset button as shown in fig 12 and 13.

VII. CONCLUSIONS

The quality of life is improved by continued research in IOT and its sphere, whether it is fully or partially implemented. To fulfill the needs of security systems with technology, the proposed IOT based advanced vehicle system provides efficient safekeeping. Experimental results demonstrate that the advanced car system is viable, and theft can be automatically curbed. The advanced secured monitoring vehicle system is IOT enabled and has a secured locking/unlocking mechanism in addition with seat belt alerts for owner safety with lesser response time. In addition, it gives security against auto theft and other unauthorized activities. The components and modules utilized in this work can also be used for any kind of Self-Driven vehicles achieving excellence for automobiles. The advanced vehicle system provides improved efficiency, convenience, and safety.

VIII. REFERENCES

[1] M. M. N. Assistant, S. M. Suresh, V. Vaishnavi, and S. Yashaswini, "' An IoT Based Vehicle Theft Detection and Remote Engine Locking System ,'" vol. 7, no. 6, pp. 1037–1042, 2020.

[2] T. J. Claude, I. Viviane, I. J. Paul, and M. Didacienne, "Development of Security Starting System for Self-Driven vehicles Based on IoT," *2021 International Conference on Information Technology, ICIT 2021 - Proceedings*, pp. 505–510, 2021, doi: 10.1109/ICIT52682.2021.9491637.

[3] Z. Liu, A. Zhang, and S. Li, "Vehicle anti-theft tracking system based on Internet of Things," *Proceedings of 2013 IEEE International Conference on Vehicular Electronics and Safety, ICVES 2013*, pp. 48–52, 2013, doi: 10.1109/ICVES.2013.6619601.

[4] U. K. A. Pathak, "IOT BASED SMART VEHICLE BLACK BOX WITH SECURITY SYSTEM," pp. 1–4, 2022, doi: 10.55041/IJSREM14785.

[5] S. Mohanasundaram, V. Krishnan, and V. Madhubala, "Vehicle Theft Tracking, Detecting and Locking System Using Open CV," *2019 5th International Conference on Advanced Computing and Communication Systems, ICACCS 2019*, pp. 1075–1078, 2019, doi: 10.1109/ICACCS.2019.8728460.

[6] N. Papadakis, N. Koukoulas, I. Christakis, I. Stavrakas, and D. Kandris, "An iot-based participatory antitheft system for public safety enhancement in smart cities," *Smart Cities*, vol. 4, no. 2, pp. 919–937, 2021, doi: 10.3390/smartcities4020047.

[7] K. Sneha, S. Shankari, K. Priyanka, and M. Vijayshree, "Iot Based Real Time Vehicle Theft Control System," pp. 5094–5096, 2020.

[8] D. Mukhopadhyay, M. Gupta, T. Attar, P. Chavan, and V. Patel, "An attempt to develop an IOT based vehicle security system," *Proceedings - 2018 IEEE 4th International Symposium on Smart Electronic Systems, iSES 2018*, pp. 195–198, 2018, doi: 10.1109/iSES.2018.00050.

[9] A. Verma, S. Seth, A. Kumar, and V. Sarada, "Vehicle Theft Identification and License Authentication Using IoT," *Journal of Physics: Conference Series*, vol. 1964, no. 6, pp. 0–12, 2021, doi: 10.1088/1742-6596/1964/6/062068.

[10] Zhigang liu, Anqi Zhang and shaojun Li, " Vehicle Anti-theft Tracking system based on Internet of Things", International conference on computer and communication Engineering (ICCCE 2010), pp.15,May 2010.

[11] H. song, S. Zhu, and G. Cao, "Svats: A sensor-network-based vehicle anti-theft system," IEEE INFOCOM 2008, pp.2128-2136, April.2008.

[12] Shiqing Liu, "Integration and Application Design of GPS and GSM system." Heilongjiang Science and Technology Information, vol.23, no. 12, pp.85, Dec.2010.

[13] Tapas Kumar Kundu and Kolin Paul, " Android on Mobile Device: An Energy Perspective," 2010 10th IEEE International Conference on Computer and Information technology (CIT 2010), pp.2421-2426, Jun.2010.

[14] Shihab A. Hameed, Othman Khalifa, "Car Monitoring, Alerting and tracking Model Enhancement with Mobility and Database Facilities," International Conference on Computer and Communication Engineering (ICCCE 2010), pp. 1-5, May 2010.

[15] Seok Ju Lee, Tewolde, G, Jaerock Kwon, "Design and implementation of vehicle tracking system using GPS/GSM/GPR technology and smartphone application," Internet of Things(WF-IoT), 2014 IEEE World Forum on, vol., no., pp.353, 358, 6-8 March 2014.

[16] Zhigang Shang, Wenli; He, cho; Zhou, Xiofeng; Han, Zhonghua; Peng, Hui; Shi, Haibo, "Advanced vehicle monitoring system based on arcgis Silverlight," Modelling, Identification & control (ICMIC), 2012 procesedings of International Conference on, vol., no.,pp.832,836, 24-26 June 2012.

[17] Kumar, R; Kumar, H., "Availability and handling of data Received through GPS device: In tracking a vehicle," advance Computing conference (IACC), 2014 IEEE International, vol., no., pp.245, 249, 21-22 Feb. 2010.