International Journal of
Advanced Technology and Innovative Research

ISSN 2348–2370
Vol.07,Issue.07,
July-2015,
Pages:1190-1193

www.ijatir.org

Anti Theft Control System Design using Embedded System

KOMPALLI SUPRIYA[1], M. VENKATESHWARLU[2]

[1]PG Scholar, Sri KS Raju Institute of Technology and Sciences, Hyderabad, Telangana, India.
[2]Associate Professor, Sri KS Raju Institute of Technology and Sciences, Hyderabad, Telangana, India.

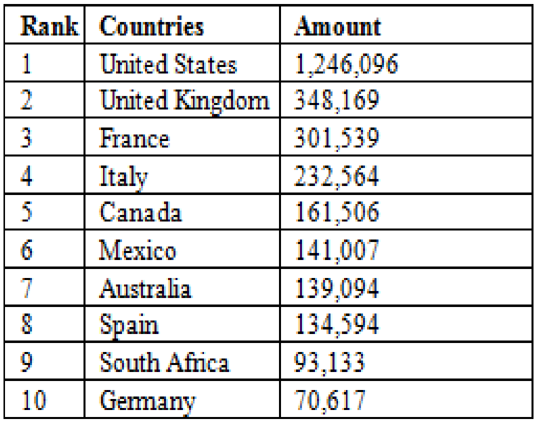
Abstract: In modern day vehicles, vehicle anti-theft system is of prime importance. The vehicle anti-theft system presented here consists of multiple layers of protection with one complementing the other, rather than the conventional anti-theft system where a particular system is only being used. The first layer of protection in the system is a Key recognition, based on which the doors are opened. The Key matching is done by utilizing the Minutiae based Key recognition scheme. Also to prevent thieves from breaking the glass and getting inside the vehicle, vibration sensors are used in all the windows with a threshold level to prevent false alarms. Once inside, the vehicle is turned on only with the mechanical keys along with correct key number entry on the combination keypad present, failing to do so for three successive times will result in vehicle getting immobilized by cutting the fuel supply and an alert message is sent to the mobile number of the owner. Further to prevent the seizure of the vehicle, Tyre pressure sensor is also being used which also alerts the owner through a mobile message. The seized vehicle can be tracked using a GPS tracker which is also being attached. The different layers of protection defined are controlled by an ARM 7 based controller acting as the central node. The whole system was tested using a test set up by mimicking the vehicle door, vehicle immobilizer etc. with equivalent motors whereas Key data was received from Matlab based GUI application. The experimental results proved the functionality of the anti-theft system in working environment.

Keywords: GSM, GPS, Electronic Lock, Embedded System, Anti Theft Mechanism.

I. INTRODUCTION

In recent years, vehicle thefts are increasing at an alarming rate around the world. People have started to use the theft control systems installed in their vehicles. The commercially available anti-theft vehicular systems are very expensive. Here, we make a modest attempt to design & develop a simple, low cost vehicle theft control scheme using an inbuilt microcontroller. This scheme involves a microcontroller & a mobile for the communication purposes [1]. The Global System for Mobile communications (GSM) is the most popular standard for mobile phones in the world. Over billion people use GSM service across the world. The usability of the GSM standard makes international roaming very common between mobile phone operators, enabling subscribers to use their phones in many parts of the world. GSM differs significantly from its predecessors in that both signaling and speech channels are digital, which means that it is considered a second generation (2G) mobile phone system. This fact has also meant that data communication was built into the system from very early on [2]. The recent statistics on vehicle theft in various countries are shown below.

TableI. No of Car Thefts



Rank	Countries	Amount
1	United States	1,246,096
2	United Kingdom	348,169
3	France	301,539
4	Italy	232,564
5	Canada	161,506
6	Mexico	141,007
7	Australia	139,094
8	Spain	134,594
9	South Africa	93,133
10	Germany	70,617

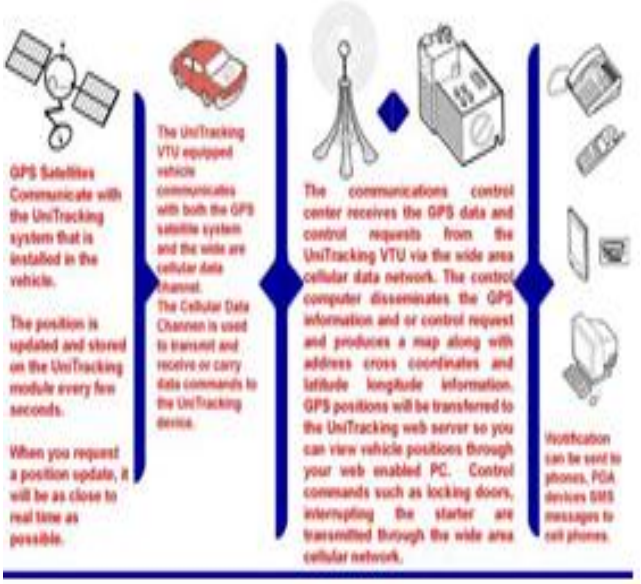
We start off exploring the existing scenarios and later we move towards the proposed architecture, describing the various modules in detail and the working methodology. Finally we present the simulation results and the various component details. The concept of this paper has been implemented as a small prototype model

II. EXISTING SCENARIOS

Various anti-theft control systems have developed over the past few years. An integrated Info-Security Circuit Board [3] that communicates with ECUs and sensors inside a vehicle through CAN bus, LIN bus, Flex Ray and MOST Bus communicates with other vehicles, road-side infrastructure and mobile phones with wireless interfaces. The main drawback with the system is the data timeliness and network delays to realize reliable secure car communications. Other systems include an invehicle anti-theft component [4] that will not enable the functions of the appliances if it should find itself is illegally moved to another car. The limitation here is that it requires a secure processor and smart card chips to store in the Group Identification Number. There are many remote controlled security systems that disables an automobile and its key auto systems through remote control when it is stolen. This requires secure vehicle-vehicle communications.

A. The Available Control System in the Market

Data such as global position, speed and velocity of the vehicle is transmitted over the cellular network to the users confidential account. The user can get to know about the vehicle and can give command to the vehicle such as stopping the vehicle, door lock …etc through the PDA devices or mobile phones.



GPS Satellites Communicate with the UniTracking system that is installed in the vehicle.

The position is updated and stored on the UniTracking module every few seconds.

When you request a position update, it will be as close to real time as possible.

The UniTracking VTU equipped vehicle communicates with both the GPS satellite system and the wide are cellular data channel.

The Cellular Data Channen is used to transmit and receive or carry data commands to the UniTracking device.

The communications control center receives the GPS data and control requests from the UniTracking VTU via the wide area cellular data network. The control computer disseminates the GPS information and or control request and produces a map along with address cross coordinates and latitude longitude information. GPS positions will be transferred to the UniTracking web server so you can view vehicle positions through your web enabled PC. Control commands such as locking doors, interrupting the starter are transmitted through the wide area cellular network.

Notification can be sent to phones, PDA devices SMS messages to cell phones.

Fig1. Control System.

B. Disadvantages of the Existing System

The cellular network is not available in all places throughout the country such as forests deserts and uninhabited areas. The cost of this system is exorbitant and to implement this system it costs nearly half the cost of the car. We will work on a full-fledged two lock security system that completely eliminates the theft of automobiles taking into consideration the disadvantages of existing systems.

III. PRINCIPLE AND METHODS

First let us have an overview about the inductive proximity sensor and then we will look into its usability in first lock system. Inductive proximity sensors operate under the electrical principle of inductance. Inductance is the phenomenon where a fluctuating current, which by definition has a magnetic component, induces an electromotive force (emf) in a target object. To amplify a device's inductance effect, a sensor manufacturer twists wire into a tight coil and runs a current through it. magnetic field the shape of a doughnut around the winding of the coil that locates in the device's sensing face. When a metal object moves into the inductive proximity sensor's field of detection, Eddy circuits build up in the metallic object, magnetically push back, and finally reduce the Inductive sensor's own oscillation field.

Fig 2. A Typical Inductive proximity sensor.

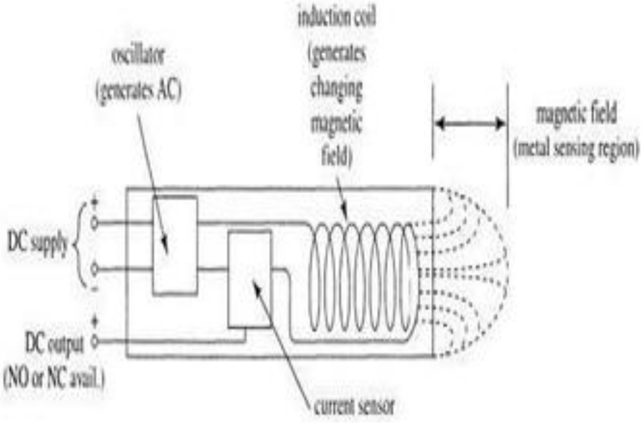


Fig3. Cross-section view of inductive proximity sensor.

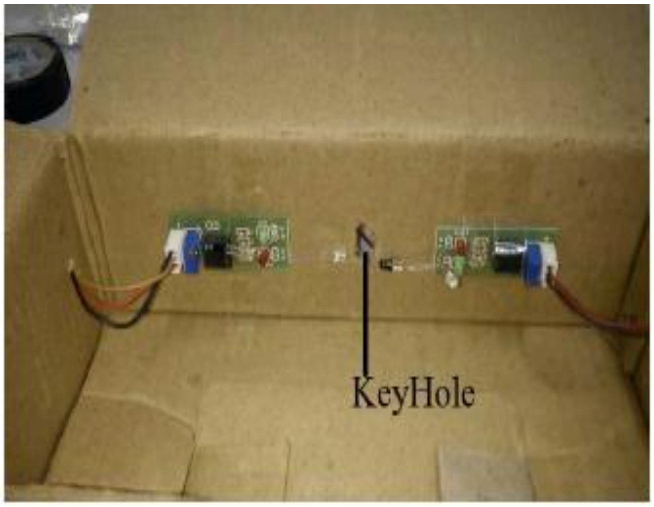


Fig4. The real time prototype of the system.

The sensor's detection circuit monitors the oscillator's strength and triggers an output from the output circuitry when the oscillator becomes reduced to a sufficient level. The inductance of the loop changes according to the material inside it and since metals are much more effective inductors than other materials the presence of metal increases the current flowing through the loop. This change can be detected by sensing circuitry, which can signal to some other device whenever metal is detected. The inductance of the loop changes according to the material inside it and since metals are much more effective inductors than other materials the presence of metal increases the current flowing through the loop. This change can be detected by sensing circuitry, which can signal to some other device whenever metal is detected.

IV. PROPOSED SYSTEM

A. Architecture of the Proposed System

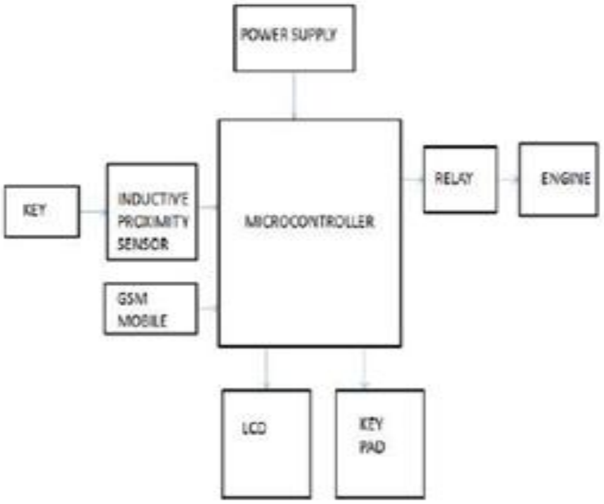


Fig5. A Sample Block diagram explaining the principle of anti-theft control system.

When the key is inserted inside the keyhole, the proximity sensor detects the obstacle and triggers the microcontroller. A message is displayed on the LCD screen asking to enter the password. At the same time intimation about the usage of the car is sent to the owner's mobile with the help of a GSM module. The password is entered in the numeric keypad. Totally three chances would be given for the user to enter the correct password. If the password entered incorrect, a second lock system placed in the door will be activated. And again through the GSM module a message is sent to the owner about the unauthorised usage of his/her car.

V. MODULES USED

A. Microcontroller Used

Our prototype employs Arduino ATMEGA 328 which is very simple and compact. An Arduino board consists of an 8-bit Atmel AVR microcontroller with complementary components to facilitate programming and incorporation into other circuits. An important aspect of the Arduino is the standard way that connectors are exposed, allowing the CPU board to be connected to a variety of interchangeable add-on modules (known as shields). Official Arduinos have used the megaAVR series of chips, specifically the ATmega8, ATmega168, ATmega328, and ATmega1280. A handful of other processors have been used by Arduino compatibles. Most boards include a 5 volt linear regulator and a 16 MHz crystal oscillator (or ceramic resonator in some variants), although some designs such as the LilyPad run at 8 MHz and dispense with the on-board voltage regulator due to specific form-factor restrictions. An Arduino's microcontroller is also preprogrammed with a boot loader that simplifies uploading of programs to the on-chip flash memory, compared with other devices that typically need an external chip programmer.

B. Global System for Mobile Communication (GSM) Model

GSM modem is a specialized type of modem which accepts a SIM card, and operates over a subscription to a mobile operator, just like a mobile phone. From the mobile operator perspective, a GSM modem looks just like a mobile phone. When a GSM modem is connected to a computer, this allows the computer to use the GSM modem to communicate over the mobile network. While these GSM modems are most frequently used to provide mobile internet connectivity, many of them can also be used for sending and receiving SMS and MMS messages.

Fig6. Mobile Communication (GSM) Model.

C. Keypad

Keypad used here for inputting the data is of the form (4 × 3) matrix board, which is used to connect to the microcontroller (From P3.0 to P3.3 row wise & from P1.3 to P1.5 column wise). It is used to input the password for validation purposes. The Fig. 2 shows a (4 × 3) matrix connected to two ports. The rows are connected to an output port and the columns are connected to an input port. If no key has been pressed, reading the input port will yield 1's for all columns since they are all connected to high (Vcc). If all the rows are grounded and a key is pressed, one of the columns will have 0 since the key pressed provides the path to ground. It is the function of the microcontroller to scan the keyboard continuously to detect and identify the key pressed.

D. LCD (Liquid Crystalsplay)

Here, the LCD is connected to Port2 (P2.0 to P2.7) of the microcontroller. It is used to display messages (either error or accepted). Variable resistor connected to Pin3 of LCD, is used to control the brightness of LCD. A liquid crystal display is a low cost, low power device capable of displaying text and images. LCD’s are extremely common in embedded systems; since such systems often do not have video monitors like those that Come standard with desktop systems.

E. Relay

The relay we are using in this is an electromechanical relay. The excitation voltage that is required is +12V DC. It is driven using the relay driver IC ULN2003 /VLN 2003A. The device is connected to the electro mechanical relay. When the relay is excited by applying the 12V DC the relay gets activated and in the process turns ON the device and when the excited voltage is stopped, the relay gets deactivated and in the process turns OFF the devices. In magnetic relay, insulated copper wire coil is used to magnetize and attract the plunger. The plunger is normally connected to N/C terminal. A spring is connected to attract the plunger upper side. When output is received by the relay, the plunger is attracted and the bulb glows.

VI. RESULTS

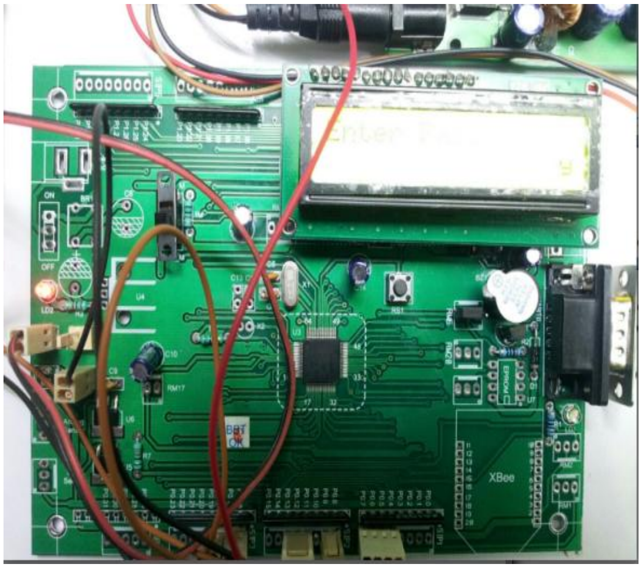


Fig7. Hardware under off State.

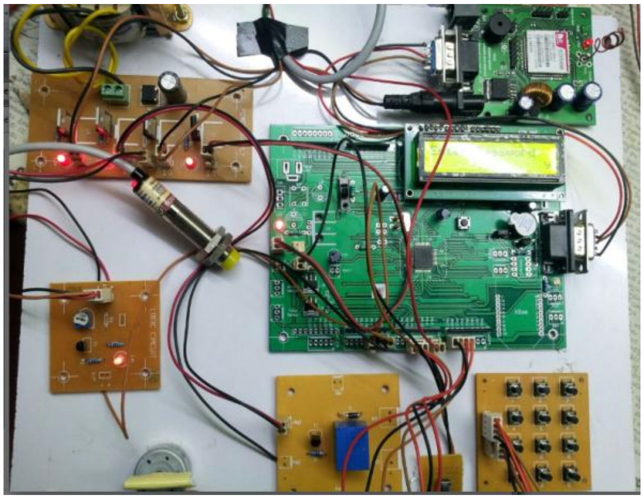


Fig8. Hardware in Testing.

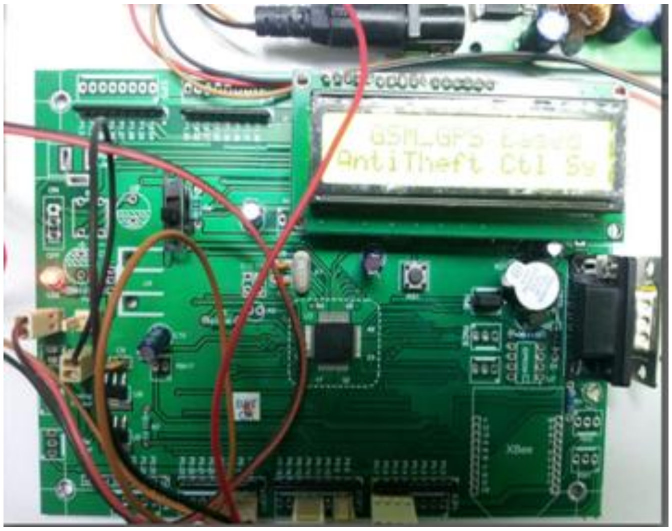


Fig9. GSM –GPS based Anti theft System.

VII. CONCLUSION

Hence a modest attempt is made to bring in a lowcost and effective vehicle theft control system. The major advantage of this system is that the whole work can be made with a meagre amount of investment and can be used in any automobiles and thus bringing in less sophisticated and simple technology. Being Students of Technology we strongly feel that ANTI-THEFT CONTROL SYSTEM would be a landmark of both Technological as well as Social excellence .If our project could help control the theft rate of automobiles , then the success of our project would have been achieved.

A. Future Enhancement

The whole system can be made more compact and flexible. All the modules and sensing system can be brought under a single chip and System-On- Chip (SOC) for anti-theft control can be designed.

VIII. REFERENCES

[1] B.G.Nagaraja, Ravi Rayappa, M.Mahesh, Chandrasekhar M Patil, Dr TC Manjunath:’Design and Development of GSM based vehicle theft control system’ Advanced Computer Control ICACC ’09 International conference.pp148.

[2] Islam,S.Ajmal,F.Ali,S.Zahid,J.Rashdi,A..: ‘Secure end-to-end communication over GSM and PSTN networks’, IEEE International Conference on Electro/Information Technology, 2009, pp-323.

[3] Huaqun Guo Lek Heng Ngoh Yong Dong Wu Teo, J.C.M: ‘Secure wireless Vechile Monitoring and control’, IEEE Asia-Pacific Conference on Services Computing APSCC 2009, pp-81.

[4] Jung-Hsuan Wu Chien-Chuan Kung Jhan-Hao Rao Pang-Chieh Wang Cheng-Liang Lin Ting-Wei Hou Y.: ‘Design of an In-Vehicle Anti-Theft Component’, International Conference on Intelligent Systems Design and Applications IDSA 2008 , pp-566.