RFID BASED AUTOMOBILE SECURITY SYSTEM

Abhinav Matharoo[1], Dr. Sukhwinder Singh[2]

[1]UG Student, [2]Supervisor, Assistant Professor,

Department of Electronics & Communication Engineering, PEC University of Technology,
Chandigarh, (India)

ABSTRACT

In this document a RFID based engine immobiliser is elaborated. RFID (Radio Frequency Identification) is used to deactivate the engine immobiliser via a LabVIEW interface. The LabVIEW program reads the 17 bytes and compares it to the 17 byte value stored in it initially. If both codes match our system send a signal to the engine control unit else silently sends an email to your email id.

Keywords: **RFID, LabVIEW, VISA**

I. INTRODUCTION

Automobile security has always been a major concern of automobile manufactures. Continuous research is being carried out to prevent the cars from being stolen. RFID is a technology which can be used for the same. Each RFID tag has a unique code stored in it. This code can be read and interpreted by LabVIEW and further operations can be carried out depending on value read

II. RELATED WORKS

Intelligent Computerized Anti-theft System or iCATS is a system installed in almost every car manufactured by Maruti Suzuki India Limited. This system has an electronic chip embedded in the key of the car. This chip sends a signal to the engine control unit every time the key is inserted. Once the engine control unit verifies the code received is genuine it starts the engine. If the key code doesn’t match the engine control units cut of power to the ignition and as claimed there is virtually no way to start the car. This ensures that only the person who possesses the original key will be able to start the car. Merely making a copy of the key won’t suffice.

III. RFID

Radio Frequency Identification or RFID is a technology that uses electromagnetic field to transfer a unique code that is stored in a device called RFID tag. There are two types of RFID tags that are commonly used namely active tag and passive tag. An active tag has a power source and it constantly keeps sending the code for the reader to read. A passive tag on the other hand used the power emitted by RFID reader to transmit the code stored in it. As a result active RFID tags provide better range than passive RFID tags. The range of passive RFID tags depends on the frequency of RFID reader. Low range RFID reader works on 125KHz and prove a working range of 5 to 10 cm. UHF or Ultra High Frequency RFID readers can read tags from a distance of up to 1m. Long range RFID readers are usually expensive and are very bulky. They are not suitable for our application. So in this project we will be using 125Khz RFID reader which will read passive tag embedded in a key chain as shown in Fig. 1

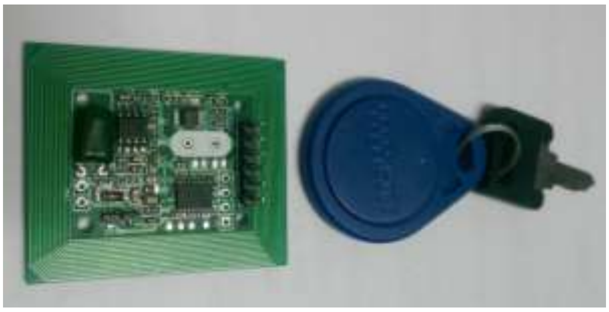

Fig. 1 RFID Tag and Reader

IV. LABVIEW

LabVIEW stands for Laboratory Virtual Instrument Engineering Workbench. It is graphical programming software developed by National instruments. We will be using this software to implement Virtual instrumentation i.e. controlling hardware virtually using software. The RFID reader send the RFID code via serial UART communication. This serial data can be read by LabVIEW using Virtual Instrument Software Architecture (VISA). A USB to TTL convertor is attached as a peripheral to the PC. The PC identifies it as a standard COMM port. VISA libraries can then be used to read the tag id and send commands to the micro controller

V. HARDWARE

The major hardware components used to implement this system are:

1. 125 Khz RFID reader
2. Atmega8
3. PL2303
4. Key switch

Fig.2 shows the usage of above hardware in form of a flow chart

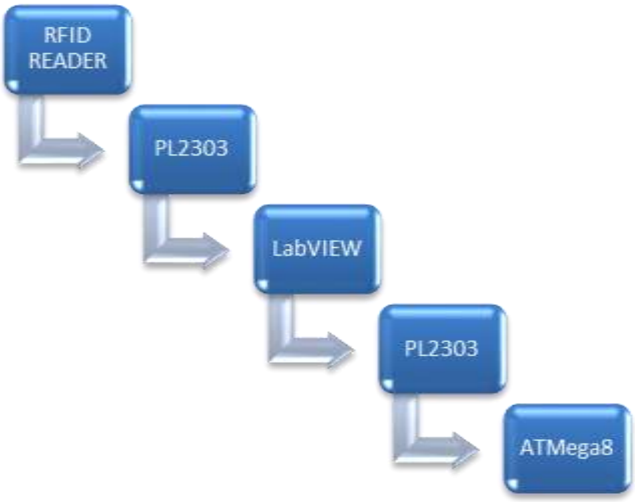

Fig 2. Block Diagram

VI. IMPLEMENTATION

The RFID reader is connected to the Rx to PL2303 and Tx of PL2303 is connected to Atmega8. The bytes received by PL2303 are read by LabView and displayed in hex and string format in the boxes shown in Fig. 3

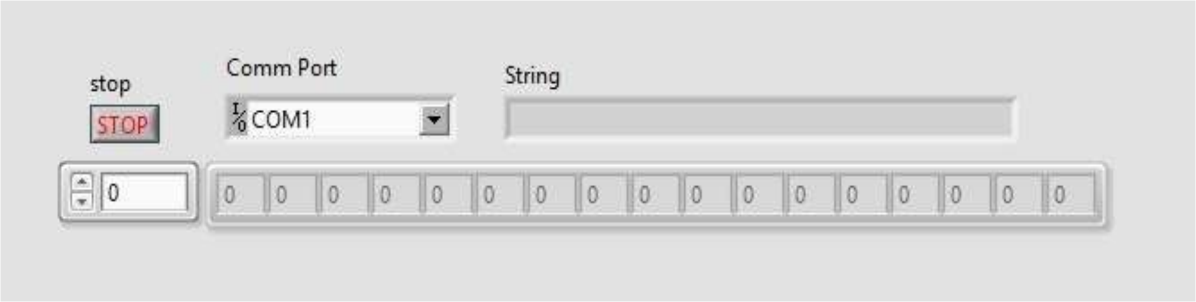

Fig. 3 Front Panel of VI

This information is visible due to the block diagram shown in the Fig. 4. This block diagram specifies the characteristics of received data ie 9600 baud rate and 1 stop bit. It also stores the data into a string and an array of unsigned 8 bit numbers.

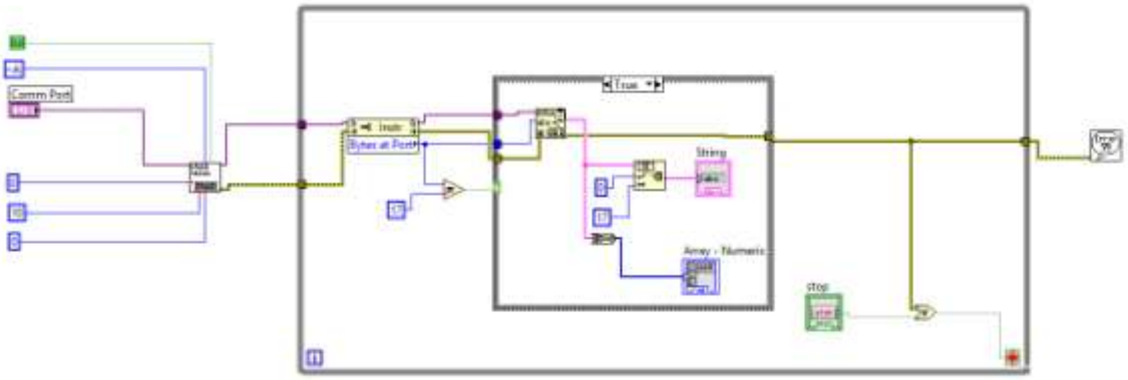

Fig. 4 Block Diagram of VI

The final component of implementation of this system is a VI which generates and sends an email every time wrong key tag is used on this system. This alerts the user in case of theft. Fig. 5 is the block diagram of the final VI which generates a email and sends it to a user from a system defined email id on gmail.

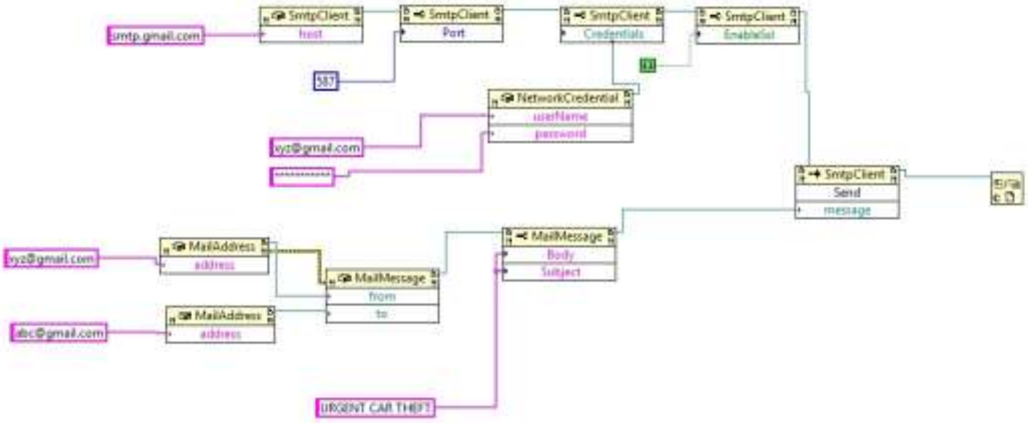

Fig. 5 Block Diagram which Send Email

VII. CONCLUSION

As technology is growing rapidly its use for malicious purposes is also growing. This system provides a very safe and cheap method to protect your car from theft. RFID tags are almost impossible to replicate without knowing the tag id. Using LabVIEW for virtual instrumentation further cuts down the cost of the entire system as actual hardware is very less. This also reduces the chances of hardware failure. Therefore in present scenario our system provides a failsafe method of protecting your car from theft.

VIII. FUTURE SCOPE

This system can further be improved by using safer RFID tags with longer key codes. Further break-in warnings can be sent to the user's phone using a GSM module. A in car camera can click photos of the thief and store it so that the thief can be identified. The location of the car can be uploaded using GPS technology to track the car. As cars are getting smarter and smarter more and more features can be added to make the system even more secure than it already is.

REFRENCES

[1]. http://www.theautomotiveindia.com/forums/technical-zone/2037-how-marutis-icats-system-works.html
[2]. https://www.ni.com/visa/
[3]. http://www.ni.com/labview/
[4]. http://www.ni.com/community/
[5]. https://labviewhacker.com