

THREE TIER AUTO SECURITY SYSTEM

Prateek Gambhir¹, Dr. Sukhwinder Singh²

*¹Student (U.G), ²Supervisor, Department of Electronics and Electrical Communication Engineering
PEC University of Technology, Chandigarh, (India)*

ABSTRACT

Enclosed in this document is the detailed description of the working of an auto security system using RF (Radio Frequency) for locking and unlocking and an RFID (Radio Frequency Identification) based engine immobilizer using National Instruments' LabVIEW.

Keywords: *RFID, RF, LabVIEW, VISA*

I. INTRODUCTION

Security is an important aspect to be considered in automobile design. Here, an attempt has been made to enhance the already existing methods and designs of auto security. RF is used to send bits of continuously changing code to the receiver in the automobile, further, an RFID system is used as an appendage to the engine immobilizer.

II. RELATED WORKS

Maruti cars are equipped with iCAT - Intelligent Computerized Anti-theft System - essentially a device which communicates with the ECU (electronic Control Unit) of the car to disable the ignition and render the car immobilized if you fail to use the factory supplied keys. Your car keys use a RFID (Radio Frequency Identification Device) which transmits a unique factory assigned code to the key fob of the car which in turn, enables the ECU. Any other key or locally made key will not have the RFID and the unique code which will disable the ECU. KeeLoq is a proprietary hardware-dedicated block cipher in which "code hopping" encoders encrypt a 0-filled 32-bit block with KeeLoq cipher to produce a 32-bit hopping code.

III. RF

Radio frequency (RF) is a rate of oscillation in the range of around 3 kHz to 300 GHz, which corresponds to the frequency of radio waves, and the alternating currents which carry radio signals. RF usually refers to electrical rather than mechanical oscillations.

IV. RFID

Radio-frequency identification (RFID) is the wireless use of electromagnetic fields to transfer data, for the purposes of automatically identifying and tracking tags attached to objects. The tags contain electronically stored information. Some tags are powered by electromagnetic induction from magnetic fields produced near the reader. Some types collect energy from the interrogating radio waves and act as a passive transponder. Other types have a local power source such as a battery and may operate at hundreds of meters from the reader.

V. HARDWARE

1. 433MHz RF Module
2. 125KHz RFID Reader
3. PL 2303
4. Keyswitch

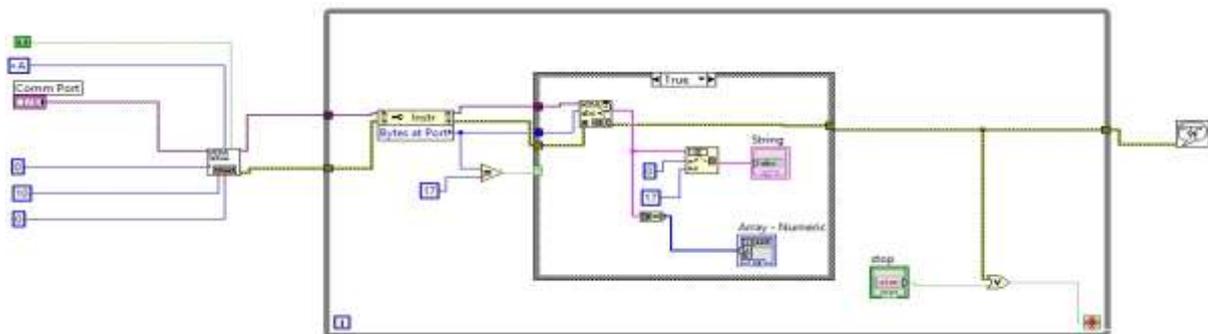
VI. WORKING

RF transmitter is used to send a 5 byte rolling code to the transmitter fitted in the automobile, a 433MHz module is used. This is the first tier. Further an RFID tag and reader combined with a keyswitch is used in conjunction with the engine immobilizer, this is the second tier. Finally, the third tier is LabVIEW interfacing i.e a master key is embedded in the receiver of the RF module for unlocking the automobile.

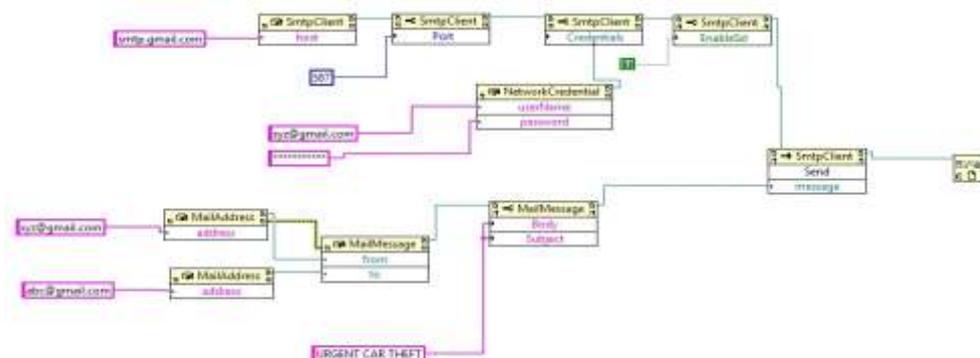
The RFID reader is connected to the Rx to PL2303 and Tx of PL2303 is connected to Atmega8. The bytes received by PL2303 are read by LabVIEW



This is the block diagram and 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.



Finally, this is the block diagram of a VI which generates a email and sends it to a user from a system defined email id on gmail if a wrong keytag is used:



VII. CONCLUSION

In this modern world of rapidly changing technology, it is imperative for one to have a sound and highly secure auto security system. The cost of installing such a system is a small price to pay for the safety and security of your automobile. The three tiers of automobile security illustrated here provide a fail safe mechanism for automobile security and also alert the owner of the automobile to any attempts at break-ins.

VIII. FUTURE SCOPE

This system can further be improved by using better hardware and faster processors to enable the designer to increase the encryption and complexity of the code so as to further reduce chances of jacking. In case of false keytags being used, a bluetooth and wifi module can be placed in the automobile so as to obtain the bluetooth or MAC address of the phone of the thief so as to implicate him.

REFERENCES

- [1]. <https://www.ni.com/visa/>
- [2]. <http://www.ni.com/labview/>
- [3]. <http://www.theautomotiveindia.com/forums/technical-zone/2037-how-marutis-icats-system-works.html>
- [4]. <http://en.wikipedia.org/wiki/KeeLoq>