Gen-X of Vehicle Anti-Theft System

Vinston Raja R[1], KrishnaRaj M [2,] SathisKumar. R[3]

Assistant Professor, Panimalar Institute of Technology, Anna University, Chennai, India[1]

Assistant Professor, Panimalar Institute of Technology, Anna University, Chennai, India[2]

Assistant Professor, Panimalar Institute of Technology, Anna University, Chennai, India[3]

ABSTRACT: The main scope of this project is to stamp out the threat caused by theft. This perception is implemented by using a RFID [Radio Frequency Identification] tag inside the engine of a vehicle [i.e., inside carburettor, the fuel injector], which is to be protected. RFID tag is given a super heat resistant coating, which can withstand heat up to 400°F (i.e., 204°C) .A RFID reader, is coupled with a traffic light signals across the city. When a vehicle is lost, the owner of the vehicle file a complaint over the theft in the nearby Police Station .The Corp register the complaint by assimilating your personal details, vehicle detail's etc. .,which in turn is stored into the database used by RFID reader through authorization .The RFID reader keeps track of all the vehicles passing by checking their respective RFID tag id installed within the engine, when the vehicle with respective RFID id reaches the traffic signal, RFID reader detects the theft vehicle and inform to the police station in which the case has been filed. Thus making it promising for us to detect our lost vehicle even when it is reassembled.

KEYWORDS: RFID, Bio-metric

I. INTRODUCTION

The substantial increase in vehicle theft has created the pressurizing environment in creation of anti- theft systems. This Technique can be adopted for both medium and high cost vehicles, which is compromised in the previous anti-theft works. This vehicle anti-theft system performs the following functions (1) detect the lost vehicle (2) provide details about the vehicle to the user. The ultimate focus while developing this anti-theft system was to satisfy the above features coequally. The most vital need in the field of anti-theft system is to provide security at affordable price which is gratified by the above approach .There are different levels of surveillance measures employed in this system. The first level of surveillance mechanism is performed by the traditional Password system and the second level is performed using the Fingerprint scanning mechanism, which is given by the authorized person (Corps).

The Third level is to provide security using the MAC address of the system, which should be send in same packet .These three security measures will provide the security at first level (we can also afford using Biometric scheme).The Password ,Fingerprint of the proposed persons will be hoarded in the Government Database beforehand with the coterminous value of the MAC address of the Computer System inside the station and at the time of entry of Password and Fingerprint it will be paired with the corresponding entry in the Government Database .The Next level of security mechanism can be materialized using the Encryption techniques in the Database. Encryption techniques such as SHA (Secure Hash Algorithm), MD-5(Message Digest) are used to accomplish the goal of Information Security.

The paper has been organized in the following manner
1.Introduction section
2.Allied works
3. Design section
4. Implementation section
5. Conclusion

II. ALLIED WORKS

The vehicle Anti-theft Systems proposed earlier has been discussed to provide the evolution of security systems. A lot of work has been done on recovering the lost vehicle [1] where the user can send a GSM message to the vehicle and thereby immobilize it and can also determine the exact location of the vehicle. These are commonly spoken as Vehicle Tracking System and are effective in controlling as well as discovering the location of the vehicle. Similarly, a Vehicle Tracking System is defined as a strategy which allows the user to gain control over the lost vehicle from a remote location (i.e.) the user can even release the pressure from the tire and immobilize the vehicle. Numbers of developments were based on RFID technology, which are useful in alerting the owner in case of forceful entry to the vehicle .But these approaches, will not be a cost- effective one and cannot be applied by everyone in the society. A core microcontroller will pay a way for meeting all the requirements stated above as discussed in the following Figure
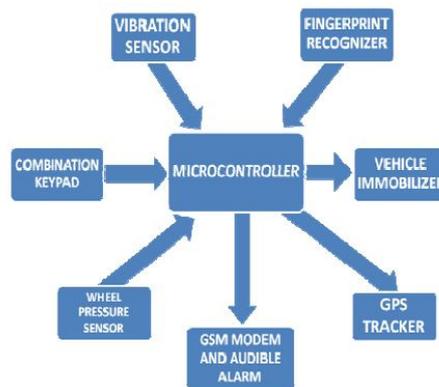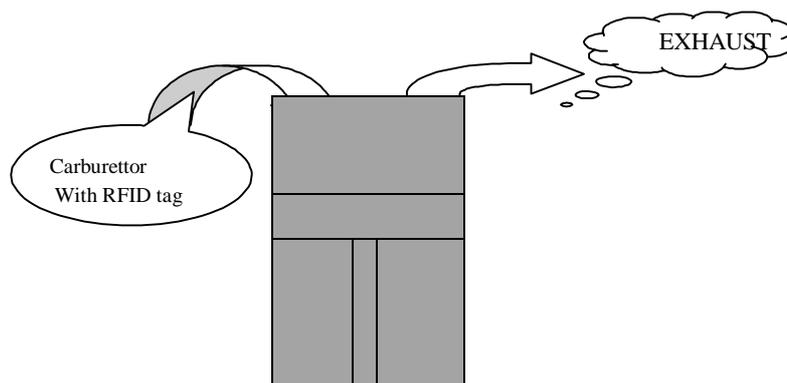

Fig -1: Vehicle Anti-Theft system

Thus a thought to satisfy all these needs has paid a way to the development of the proposed Anti-theft System

III. DESIGN APPROACH

This design approach results in complete satisfaction of the user

A. *PIONEER STRUCTURE:*

This Anti-theft design is implemented with the view to provide cost-effectiveness as well as the effective security mechanism to the customers. Every design of the module is given detailed description in this facet. The Project module begins with embedding RFID [Radio Frequency Identification tag] inside the carburettor of the vehicle by the respective manufacturing Company. In addition to placing it in the carburettor the RFID tag is given super heat resistant coating, which can withstand heat up to 400°F (i.e., 204°C). The RFID is imprinted in the Insurance and other important papers and also behind the key of the user. When the vehicle is lost the user uses his RFID value has an important component to identify the vehicle. Our first level of security earn wings by the [1] MAC address, which is a physical address residing in the corps system provided by the NIC [Network Interface Card]. After which our next level of security Password and Fingerprint Scanner comes into the phase of Access- Security. [2]The Password mechanism is realized by using traditional Strategies to prevent the Centralized Database from unauthorized access.[3]Fingerprint Scanner which scans the fingerprint of the authorized personnel and transfer it to the database(using cloud or isolated database).These security standards helps in realizing the security goals of our System effectively.

B. MINUTIAE BASED FINGERPRINT EVALUATION SCHEME:

We use separate TMS320 SERIES DSP Processor for Fingerprint Recognition .A separate DSP Processor preferred to a single processor because the Fingerprint Recognition is highly resource consuming. Minutiae based Fingerprint evaluation Scheme is used, which is one of the most accurate Fingerprint recognition Schemes. The Human Fingerprints are rich in details and also differ from person to person, which make it useful for many Biometric Schemes. The Fingerprint sample is shown in the left side, whereas the Minutiae that are extracted from the sample Fingerprint is shown in the right hand side. Minutiae refer to various terminations and bifurcations on the human Fingerprint Pattern, locations of which are unique for each and every individual. The database design plays a most vital role in the field of Anti-theft Programme. An alignment based elastic matching algorithm is used for Minutiae matching .This Algorithm will provide a way for comparison between the received Fingerprint Pattern and the Fingerprint which have been stored in the database at a earlier stage before using it for the intended purpose.
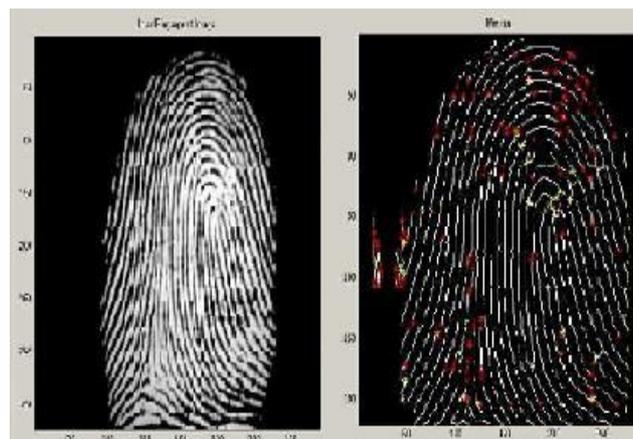
C. DATABASE STRUCTURE:

The database structure is realized in following manner(1)first attribute of the database is the MAC address to provide initial level of security(2)the Password of the authorized user[the password is stored in the backend in Encrypted format by using security algorithm such SHA,MD-4,MD-5 or PGP] (3) the Fingerprint attribute ,which stores the Fingerprint of the authorized personnel. All the requirements stated in the database (MAC, Password and Fingerprint) are entered at an earlier stage by the Database Administrator. A change in system MAC address, Password of the legitimate personnel or even the change in official must be informed to the database admin as early as possible because all three plays a crucial role in field of Information Security making it unavailable to pirated user. The accredited user Password, MAC address, Fingerprint will be compared with the data residing in the database. If the values are valid the corresponding RFID

datum will be enrolled inside the database that will be utilized by the terminal structure. The RFID reader will provide a Hexa- Decimal value that will be encoded to corresponding Binary data and then decoded to URI representation as shown in the Figure .After Decoding each fields

Will indicate separate divisions of the required fields.

MAC Address	Password (SHA or MD5)	Fingerprint Pattern (Minutiae)	RFID value
132.147.184.99	Sajdfjasiiyia dfykohfdssw		96-bit hex value
132.147.184.65	Fuasditdlfmh Giototptiuyu		96-bit hex value

For e.g., consider in a Company loading several products from several companies will be using following technique as follows.
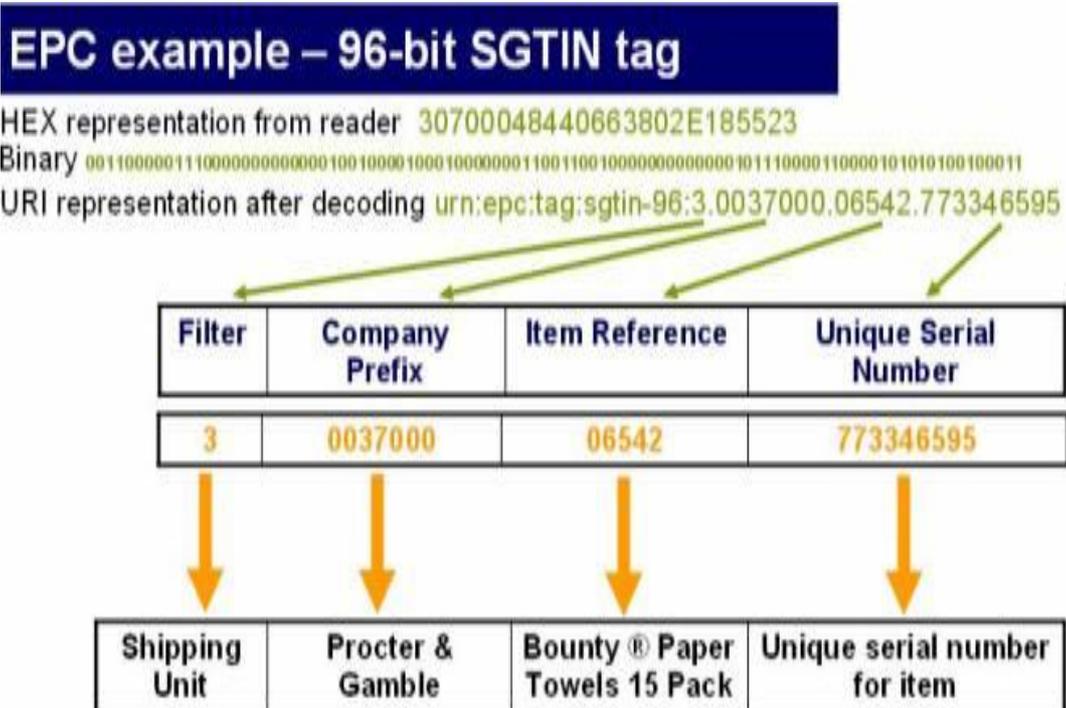
D. TERMINAL DESIGN:

The RFID reader, which is used to identify the Radio Frequency of the requested tag, is embedded on the Traffic Lights

The RFID reader has the capacity to detect device at the range approximately 100 meters (300 feet) or more. This RFID reader is anchored on the Traffic Lights, so that RFID value of the solicitated vehicle will be steadily monitored and if the vehicle found, the location of the vehicle will be prompted to the requesting MAC address. Thereby the thefted vehicle is blocked at a faster rate.

The example database structure is defined as follows:

```
Connection connection = null; String dburl = "jdbc: mysql://314159265:3306/Db_Name";String username =
"user";
String password = "password";
String macaddress ="macaddress";

   try { Class.forName("com.mysql.jdbc.Driver");
 connection = DriverManager.getConnection(dburl, userName, password, macaddress);
 Statement st = connection.createStatement();
if(macaddress)
   String query = "INSERT INTO DB VALUES(“132.147.184.99”,”xxxx”,”imgfin”,”96-bit hex”);
   int rsI = st.executeUpdate(query); System.out.println("value entered");
   }

   Exception e) {
   out.println(e);

   connection != null) {
   try {
   connection.close ();
   System.out.println ("Database connection ated");
} catch (Exception e) { /* ignore close errors
```

IV. IMPLEMENTATION

The implementation of the Anti-theft system is done by following the design approach as discussed earlier. The Fingerprint Recognition algorithm based on Minutiae based Fingerprint recognition technique is loaded into the DSP Processor.TMS320X series of Processor is used and the corresponding MATLAB code will be written and is transformed onto the Processor using Code Compressor Studio. When the victim loses his vehicle, he should register a compliant in a nearby Police Station. The Corps, while enrolling the compliant get information about the vehicle information with the RFID value (which will be imprinted on the Vehicle Key and also in other important papers such as Insurance…etc).After drawing satisfactory information from the user the Corps enter into Database, which maintains the RFID value of all lost vehicle. But the Corps also has some restriction while accessing the Database. He must provide authorized Password and the Password that he enters should be passed from the registered MAC address user, thereby arriving at first level Security. Our Second level Security is provided by the Fingerprint of the legitimate personnel, which also must be pre-entered in the Database before accessing.
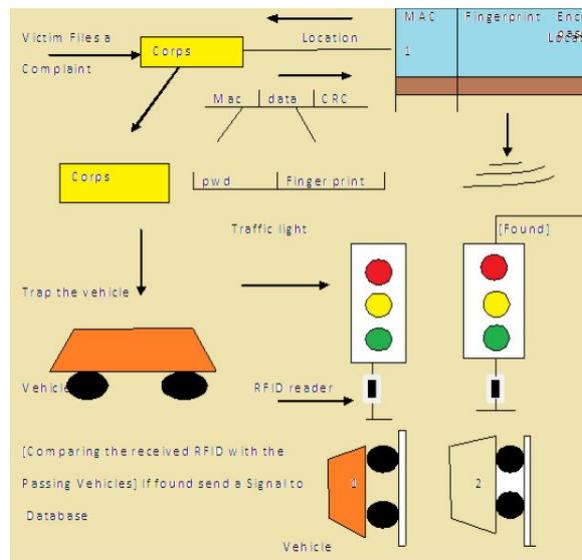
After providing trustworthy information, the Database inserts the RFID value in the Row corresponding to MAC address, Password and Fingerprint. This RFID value will be broadcasted to all the RFID reader adhered to the Traffic Lights within the city limit and also to the small proportion of lights, which are at the closest distance from the registered area. When the Vehicle is identified in the registered area, the RFID reader will provide a signal to the database and therefore corresponding location of the Vehicle will be transmitted to the source MAC address (Corps System).But when the burglar drives the vehicle to another area without passing through any Traffic lights(by shortcuts) there arise the fallacy. To satisfy this purpose, during broadcasting there is need to transmit the RFID value to the Traffic Lights, which are in closer proximity to the registered location.

V. CONCLUSION

The Vehicle Anti-theft System has been successfully designed and it would definitely provide a way to minimize Vehicle- Theft to major extent. Moreover this scheme will lend Vehicle user with greater simplicity and cost effectiveness, since the role of user is limited and number of tasks has been contributed as an automated service.

REFERENCES

[1] R Nair," Vehicle Anti-Theft ed Platform" published in search in Engineering and 163 p I S S N : 2 3 2 1 -7308.

[2] Land Vehicle Tracking Application on Android Platform Ramesh Chandra Gadri, Ankita Chavan, Reema Sonawane, Sujata Kamble. Guide: Bhagyashree Alhat, Kavitha S Nair. Department of Computer Engineering, MAE Alandi, University of Pune, Maharashtra, India. ISSN: 2248-9622

[3] Real Time Vehicle Tracking System using GSM and GPS Technology- An Anti-theft Tracking System Kunal Maurya 1, Mandeep Singh 2, Neelu Jain 3 1,3Department of Electronics, 1,3PEC University of Technology Chandigarh- 160012, India1kunalmaurya@gmail.com, 3neelujain@pec.ac.in 2 Department of E.P.D.T., 2C-DAC , Mohali 2cdac_mandep@yahoo.co.in
  Mohali-160071, India

[4] A New Method For GPS-Based Urban Vehicle Tracking Using Pareto Frontier and Fuzzy Comprehensive Judgment Yikai Chen, Yuncai Liu Research Center of Intelligent Transportation Systems Shanghai Jiao Tong University, Shanghai, 200240, China Email: {chenyikai83, whomliu}@sjtu.edu.cn

[5] Design and development of gps-gsmbased tracking system with googlemap based monitoring pankaj verma 1, j.s bhatia 2 centre for development of advanced computing, mohali, punjab, india pankajvermab35@yahoo.comjsbhatia.*cdac@gmail.com*

BIOGRAPHY

Mr.R.Vinston Raja received M.Tech in SathyaBama University Chennai, B.Tech Information Technology in Noorul Islam College of Engineering Anna University Chennai. He is working as an Assistant professor in Department of Information Technology at Panimalar Institute of Technology Chennai.

Mr.M.Krishna Raj. received M.Tech in SathyaBama University Chennai, B.E Computer Science Engineering in Narayanaguru College of Engineering Anna University Chennai. He is working as an Assistant professor in Department of Information Technology at Panimalar Institute of Technology Chennai.

 Mr.R.Sathiskumar doing research in Mobile Ad Hoc Networks at Sathyabama University. He received M.Tech in Sathyabama University Chennai, M.Sc Information Technology in Nehru Memorial College Of Arts And Science Bhrathidasan University Trichy. He is working as an Assistant professor in Department of Information Technology at Panimalar Institute of Technology Chennai.