A Survey on Anti Theft Control System

Ms.Padmaja Adgulwar[1], Prof. Nilesh Chaubey[2], Prof.Shyam Dube[3]
1(Dept. of Computer science & Engineering, NuvaCollege of Engineering & Technology , Nagpur, India)
2(Lecturer, Dept. of Electronics & Communication, Manoharbhai Patel Institute of Engg. &Technology,Gondia , India)
3(Lecture, Dept. of Computer science & Engineering, NuvaCollegeOfEngineering & Technology, Nagpur,India)

Abstract— Now a days the use of vehicle is must for everyone. At the same time, the ratio of vehicle theft increasing day by day rapidly as vehical theft is universal problem so this will lead to an increase in the vehicle insurance premium which has to be paid by consumers. Therefore we can say that the security systems installed by the vehicle manufacturer are not effective enough.

In this proposed system we can prevent the vehicle theft by using embedded platform. The projected security system for smart cars used to avoid them from theft using AVR microcontroller. The aim of this system is to provide the locking and unlocking system through OTP sent to user through GSM technology.

This method makes use of an embedded chip that has an sensor, which senses the key through insertion and sends an OTP to the owner's mobile the user have to enter the identical password which is sent to the authorized mobile number then vehicle will be started.

If the user be unsuccessful to enter the correct password in three trials, then it is treated as theft situation a text message is sent to the owner, a close relative or friend and police with the vehicle number. Further the fuel injector of the car disabled so that the user cannot start the car by any means. In addition it can also helpful in detecting fuel theft from the vehicle by monitoring fuel level in the vehicle.

Keywords*-Anti theft mechanism , Password Protected , GSM, Microcontroller based, embedded , electronic lock ,OTP.*

*****

I. INTRODUCTION

In recent years, vehicle thefts are increasing at an alarming rate around the world. The automobile manufacturers are trying to improve the security features of their products by presenting advanced technologies to avoid the thefts particularly in the case of cars.

Usually, biometric and non - biometric methods are widely used to provide security. In non–biometric method

- Password
- Personal ID are used to recognize the authorized person ,

while in biometric methods employ techniques such as follows

- Voice recognition
- Finger print recognition
- Signature recognition
- Eye retina recognition
- Iris recognition
- Face recognition.

II. LITERATURE REVIEW

Below are several of the best Products considered as security measure as Anti Theft Device .

- **Gear Locks** : Considered one of the best protection, a car thief would in a very rare circumstance puts up time to break gear lock in the car - which may use energy and time, rather is always on viewpoint of models which are parked without gear lock in it..
- **Ignition Cut Off** : A key-operated or hidden manual switch that interrupts the power supply from the battery to the ignition. This monitor switch can be taken out by the driver once the car is locked.
- **Car Alarms** : There are several alarm systems that will support to deter or depress vehicle thefts, and alert others of enforced entry into the car. You must need to make certain that these noise speakers should be installed in such a way as not to be easily able to reached on glance, else will be first disabled by them
- **Steering Lock** : A long metal bar with a lock that fits on the steering wheel and is intended to prevent the steering wheel from turning. Steering wheel locks are effective when using in combination with Gear Lock.
- **ICAT** : ICAT means Intelligent Computerized Anti-Theft system. Though, most of the models come with I-cat feature, still for those which don't have, under this system, The car starts only when the sensor in the vehicle receives the chip in the key (wherein that secret code is matched of the key with the chip). Even, sensors creates alarms buzz when somebody try to insert a fake key in a car .
- **Gps Tracker** : A GPS facility can help tracking a stolen car. Infact, can also alert you for misuse of your car by any Service Station.

2.1 Existing Systems

Several anti-theft control systems have developed over the previous few years. An integrated Info-Security Circuit Board [13]that communicates with ECUs and sensors inside a vehicle through LIN bus ,CAN bus, Flex Ray and MOST Bus communicates with other vehicles, road-side structures and mobile phones with wireless interfaces. The main disadvantage with the system is the data timeliness and network delays to understand reliable safe car communications. The existing car antitheft system are flashing light techniques, Car alarm which makes use of different type of sensors which can be pressure, door & tilt and shock sensors.

Other systems include an in vehicle anti-theft component [17]that will not enable the functions of the applications if it should find itself is illegally moved to one more car. The restriction here is that it needs a secure processor and smart card chips to store in the Group Identification Number. There are numerous remote controlled security systems that restricts key auto systems of automobile through remote control when it is stolen.

This needs secure vehicle-vehicle communications.

Apart from above devices there are different methodology to implement security in the system Such as

- **Single level Security**
- **Multilevel Security**

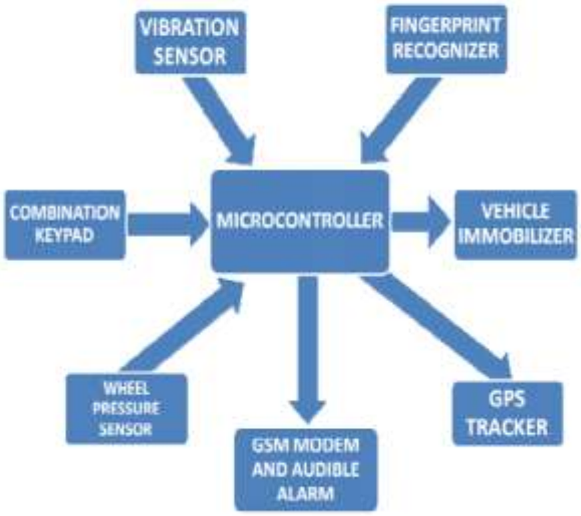

Fig 1.Antitheft Control System

2.2 Advantages and Disadvantages Of The Existing System

In 1997 B Webb present wheel and steering lock system, to prevent car from theft, but they are visible from outside the car and prevent the wheel from being turned more than a few degrees[1]. The next system was projected on Security Module for Car Appliances by Pang-Chieh Wang,et.al. This system prevents car appliances from stealing and unlawful use on other cars. If illegal moving and use a car appliance with the security module without approval occur that will lead the appliance to useless. But it does not prevent vehicle from theft [12]. In 2008 Lili Wan, et.al. implemented new system based on GSM in which owner can obtain the alarm message rapidly and if necessary, also it can monitor the car by phone[14] .The subsequent system was a sensor network created vehicle anti theft System (SVATS). In this method, first step is to form a sensor network by using the sensors in the vehicles that are parked within the same parking area, then identify and monitor possible vehicle thefts by detecting illegal vehicle movement. An alert will be reported to a base station in the parking area if an illegal movement is detected. As the sensor cannot link with the base station directly in the extreme case, automobile cannot receive any safety when no neighbors can be found even if a sensor has tried its extreme power level[15] . In [16]authors describe an automotive security system to disable an key auto systems of automobile through remote control when it is stolen. But it does not help to identify the theft.

An effective automotive safety system is implemented for anti-theft by an embedded system occupied with a Global Positioning System (GPS) and a Global System of mobile (GSM) by Montaser N. Ramadan et.al. to monitor and track vehicles that are used via certain party for particular purposes, likewise to stop the automobile if stolen and to track it online for recovery[18]. The subsequent system was projected in 2013 on real time automobile theft identity and control system created on ARM 9. It achieves the real time user verification using face recognition, using the Principle Component Analysis (PCA) algorithm if the outcome is not accurate then ARM produces the signal to block the car access and the car owner will informed about the illegal access with the help Multimedia Message Services (MMS) via GSM modem . But in this technique the camera captures owner's image only. If the owner's friends or relatives want to start the car it will not start [19]. Newly innovative system proposed on vehicle anti-theft system based on an embedded platform comprises of multiple layers of security .The first layer of security in the system is a fingerprint recognition, created on which the doors are opened. Also to avoid thieves from breaking the glass and getting inside the vehicle, vibration sensors are used in all the windows with a threshold level to avoid wrong alarms. 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 stopped by cutting the fuel supply and an alert message is lead to the mobile number of the owner. Additional to prevent the capture of the vehicle, tyre pressure sensor is also being used which also alerts the owner via a mobile message[20].

In circumstances of vehicle accident detection new system projected by Varsha Goud et.al. on vehicle accident automatic detection and remote alarm device. This system can sense accidents in significantly less time and sends the basic info to first aid center within short time covering geographical coordinates, the time and angle in which a vehicle accident had happened. This attentive message is sent to the rescue team in a short time, which will benefit in saving the valuable lives . Spotting an accident previously occurring it can save human life. To implement this new system was projected in which a car will try to avoid hurdle after avoiding animal or human if there is any. Driver will also be informed with red lights specifying that obstacles are in front. But, if the system would not be incapable to avoid accident then this system will habitually generate a tweet in tweeter. For further safety, this system also comprises buzzer and relay where relay helps to protect the car from battery ignition and buzzer will make noise to notify people surrounded[21].

In 2000 paper recommended on An Introduction to Face Recognition Technology which covers topics such as the generic framework for face recognition, several state of the art face recognition algorithms[4] and factors that may affect the performance of the recognizer. New system has been proposed in 2004 thru Jian Yang, et.al. is two-dimensional principal component analysis (2DPCA) aimed at image representation. As contrasting to PCA, 2DPCA is based on 2D image matrices rather than 1D vector so there is no necessity to change image matrix into a vector prior to feature extraction. Because of this an image covariance matrix is constructed openly by means of the original image matrices and its eigenvectors are resulting for image feature extraction[11] . The succeeding paper projected on image-based face detection and recognition to assess various face detection and recognition methods, which offer complete solution for image based face recognition and detection with higher accuracy, better response rate as an early step for video surveillance.

III. Techniques Elaborated in creation of One Time Password

Following are the two techniques for creation of one time password:

- **Time-synchronized One time password**: In time-synchronized OTPs the operator should enter the password within a assured period of time else it becomes expired and one more OTP must be created.
- **A counter-synchronized One Time Password**: With counter-synchronized One Time Passwords, a counter is synchronized among the client device and server. The device counter is incremented each time an OTP is demanded.

consider example of hash-based OTPs wherein we use hash algorithms like SHA-1 and MD5 that can be used to calculate the OTP. A cryptographic hash function also kown as one-way function maps message of random length to a fixed-length digest. So hash-based One Time Password requires input parameters (username, synchronization value, password), runs them through the cryptographic hash function, produces the fixed-length password, i.e., One Time Password.

3.1 Methods of One Time Password Delivery

- Text messaging: It is the most simple and common method always used for sending OTP.
- Email and Instant Message Services: These services are almost common and the cost effective .

3.2Recognition Based Techniques

Perrig and Dhamija [3] suggested a graphical authentication scheme built on the Hash Visualization method [2].In this method, the user is requested to select a definite number of images from a set of casual pictures produced by a program. Then the user will be valid by means of recognizing the preselected images. This method flops to influence since the server has to accumulate the seeds of the portfolio images of every user in plain text.

Akula and Devisetty’s algorithm [8] is like to the method proposed by Perrig and Dhamija [3]. The change is that by means of hash algorithm SHA-1, which creates a 20 byte output, the authentication is more secure which leads to less memory. The writers recommended a conceivable future development by providing persistent storage and this could be installed on the Internet, cell phones and PDAs. Kirkpatrick and Weinshall [9] sketched several authentication schemes, such as object recognition ,picture recognition and pseudo word recognition, showed a number of user studies. In the picture recognition study, a user is skilled to recognize a large set of images (100 –200 images) particular from a database of 20,000 images. This learning shown that pictures are the most effective between the three schemes discussed. Pseudo codes can also be used as an substitute but require proper setting and training.

Jansen et al. [10-6] suggested a graphical password procedure for mobile devices. During the enrolment stage, a user chooses a theme (e.g. sea, cat, etc.) which contains thumbnail photos and then registers a order of images as a password. During the verification, the user must enter the registered images in the correct sequence. One problem of this technique is that as the number of thumbnail images is inadequate to 30, the password space is not as much . Every thumbnail image is allocated a numerical value,the order of choice will generate a numerical password.

The outcome depicted that the image order length is usually smaller than the textual password length. To solve this problem, two pictures can be joint to compose a new alphabet component, thus increasing the image alphabet size.

Koike and Takada argued a similar graphical password method for mobile devices. This method lets users to use their favorite image for verification [7]. The users first register their preferred images (pass-images) with the server. During verification, a user has to go through several rounds of verification. At every round, the user either chooses a pass-image among several decoy-images or chooses nothing if no pass-image is existing. The program approves a user only if all verifications are successful. Allowing users to register their own images marks it easier for user to recall their password images. This method is a secure authentication method in contrast with text-based passwords. Letting users to use their own pictures would make the password even more expectable, particularly if the attacker is aware with the user.

3.3 Projected Resolution

The projected solution involves two methods: image based verification and an OTP generation
method.

- Image Based Password Verification
- HMAC-Based One-Time Password

3.3.1 Image Based Password Verification

The Image-based verification is based on Recognition Methods. When the user enrolls for first time in a web site they select fixed images that are easy to recollect, such as automobiles, natural scenery etc. Every time the user login into the site, they are provided through a grid of images that is casually produced. The user can recognize the images that were earlier selected by him. It is meaningfully easier for the user since they need to recollect a few simple images.Image Based Verification is based on a user’s successful identification of his set of images. After the user logins for the first time, website shows a grid of images, which consists of images after the users password set mixed with other images. The user is genuine if identifying the password images. Performing brute force attacks otherwise further attacks on such systems is very hard. A set of dissimilar images are carefully chosen to validate the user. The Image Identification Set , for all user is then stored at the Verification System. When a user logins, the IIS for that user is saved and also used to validate that particular user. The scheme does not store the images but the set of the images are put in storage as images are big files. This method is also extra secure and involves fewer memory. If this step is positive, next OTP is produced and pass on to the user email-id.

3.3.2 HMAC-Based One-Time Password Algorithm

Time-synchronized OTP values, based on SHA-1 based Hash Message Authentication Code (HMAC). This is known as the HMAC-Based One-Time Password since here OTP is produced based on HMAC. One-Time Password is visibly one of the easiest and most common forms of two-factor authentication that can be used for make safe entree to accounts. One-Time Passwords remain often referred to as a stronger and secure forms of authentication, allowing them to installed across multiple machines including mobile phones ,home computers, etc.When the user selects the pre-selected images to login an OTP is generated and sent to the user’s e-mail id. The user is then directed to next page where the user is asked to enter the OTP. The user gets the OTP using the email account and enters it. If the OTP is verified the user succeeds in logging in the system.

Also in case of numeric password random password key is generated if the user fails to enter correct password in 30 seconds then next OTP is generated and send to mobile.Every user given three chance if unable to enter correct password in three attempts then system is locked otherwise free to enter.

3.4 OTP Applications

Google is presently using one time password.RBI made OTP compulsory for transaction made with credit card. Hotmail is also using one time password to provide high security to usersAll banking systems are using OTP. E.g.:- Citi Bank ,ICICI Bank, HDFC, Axis, SBI etc

IV. GSM Module:

GSM module in our proposed system is used for establishing the communication between the vehicle and the user.Global System for Mobile communication (GSM) is a wireless modem that works with a GSM wireless network for mobile communication.

GSM has become the world's fastest growing communications technology of all time and the leading global mobile standard, spanning 218 countries. The GSM platform is a enormously positive wireless technology and an extraordinary story of global achievement and cooperation. GSM is an open, digital cellular technology intended for transmitting mobile voice and data services. GSM operates in the 900MHz and 1.8GHz bands GSM backings data transfer speeds of up to 9.6 kbps, permitting the transmission of basic data services such as SMS.

V. CONCLUSION

When associated with the existing system the advantage of proposed system is it’s very simple and cost effective. The major advantage of this system is that the whole work can be made with a small amount of investment and can be used in any vehicles and thus carrying in less refined and simple technology.

If this proposed work help to control the theft rate of automobiles , then the success of our project would have been attained. Being Students of Technology we intensely feel that ANTITHEFT CONTROL SYSTEM would be a milestone of both Social excellence and Technological

REFERENCES

[1] B Webb “Steering Column Locks and Motor Vehicle Theft: Evaluations From Three Countries” Situational crime prevention: Successful case studies, 1997

[2] A. Perrig and D. Song, "Hash Visualization: A New Technique to Improve Real-World Security," in Proceedings of the 1999 International Workshop on Cryptographic Techniques and E-Commerce,1999.

[3] R. Dhamija and A. Perrig, "Deja Vu: A User Study Using Images for Authentication," in Proceedings of 9th USENIX Security Symposium, 2000.

[4] Shang-Hung Lin, “An Introduction to Face Recognition Technology”, Informing Science special issue on multimedia Informing technology-Part 2, volume 3, No 1,2000

[5] W. Jansen, S. Gavrila, V. Korolev, R. Ayers, and R. Swanstrom, "Picture Password: A Visual Login Technique for Mobile Devices," National Institute of Standards and Technology Interagency Report NISTIR 7030, 2003.

[6] W. A. Jansen, "Authenticating Users on Handheld Devices," in Proceedings of Canadian Information Technology Security Symposium, 2003.

[7] T. Takada and H. Koike, "Awase-E: Image-based Authentication for Mobile Phones using User’s Favorite Images," in Human-Computer Interaction with Mobile Devices and Services, vol. 2795 /2003: Springer-Verlag GmbH, 2003, pp. pp. 347 - 351.

[8] S. Akula and V. Devisetty, "Image Based Registration and Authentication System," in Proceedings of Midwest Instruction and Computing Symposium, 2004.

[9] D. Weinshall and S. Kirkpatrick, "Passwords You’ll Never Forget, but Can’t Recall," in Proceedings of Conference on Human Factors in Computing Systems (CHI). Vienna, Austria: ACM, 2004, pp.1399-1402.

[10] W. Jansen, "Authenticating Mobile Device Users Through Image Selection," in Data Security, 2004.

[11] Yang, David Zhang, Alejandro F. Frangi, and Jing-yu Yang “Two-Dimensional PCA: A New Approach to Appearance-Based Face Representation and Recognition”IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 26, no. 1, January 2004

[12] Chieh Wang, Ting-Wei Hou, Jung-Hsuan Wu, and Bo-Chiuan Chen “A Security Module for Car Appliances” International Journal of Aerospace and Mechanical Engineering 2007

[13] 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

[14] Lili Wan, Tiejun Chen “Automobile Anti-theft System Design based on GSM” International Conference on Advanced Computer Control 2008

[15] H Song, S Zhu, G Cao “ SVATS: A Sensor network based Vehicle” INFOCOM The 27th Conference on Computer Communications. 2008

[16] H Guo, HS Cheng, YD Wu, JJ Ang “An Automotive Security System for Anti-Theft " International Conference on networks 2009

[17] 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

[18] Montaser N. Ramadan, Mohammad A. Al-Khedher, and Sharaf A. Al-Khede “Intelligent Anti-Theft and Tracking

System for Automobiles" International Journal Machine Learning and Computing, Vol. 2, No. 1, February 2012

[19] D.Narendar Singh, K.Tejaswi, "Real Time Vehicle Theft Identity and Control System Based on ARM 9" International Journal of Latest Trends in Engineering an Technology (IJLTET),Vol. 2 ,Issue 1, January 2013

[20] Arun Sasi, Lakshmi Nair " Vehicle Anti-theft System Based on an Embedded Platform" IJRET Volume: 02 Issue: 09 Sep-2013

[21] Maminul Islam, Rabiul Hasan, Imran Chowdhury, Towhid Chowdhury "Internet of Car: Accident Sensing, Indication and Safety with Alert system" American Journal of Engineering Research (AJER) Volume-02, 2013