Volume 8, No. 5, May-June 2017
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
RESEARCH PAPER
Available Online at www.ijarcs.info

Auto motive refuge concept using Embedded and computing approches

Suraj U. Rasal
Assistant Professor
Department of Computer Engineering, Bharati Vidyapeeth University College of Engineering Pune, MS, India

Kratika Gupta
Department of Computer Engineering, Bharati Vidyapeeth University College of Engineering Pune MS, India

Varsha Rasal
Department of Computer science & Engineering, Nehru College of Engineering & Research Centre, Thrissur, India

Shraddha Shelar
Assistant Professor
Department of Information Technology, D Y Patil College of Engineering Akurdi, Pune, MS, India

Abstract: Traditional approaches are non smart and easy to intrude. In proposed approach, automotive components like steering, brakes, engine starter and door locks are controlled by computing approaches. Mobile is considered as unlocking key where global system for mobile services is used. Proposed system activation is done by online system through internet technology. Cryptographically imposed techniques are applied to securely store and access sensitive data. Multi locality approach is applied to avoid disaster and unauthorized ownership using randomizing algorithm. Computing and embedded with existing mechanical locking approaches are applied through Global System for Mobile service, internet technology, Engine Control Unit and applied cryptography.

Keywords: Antilock Braking System (ABS), Central ECU , Computing Vehicle Locking System (CVLS), Device Drivers, Engine Control Unit (ECU), Input Output drivers, JAVA,JVM, Mobile Engine Control Unit (MECU), , One Time Password (OTP), Raspberry Pi.

I. INTRODUCTION

Embedded Systems is a electronic approach which performs varied or dedicated functions. It is a combinational unit of hardware and software which act as control unit now days. Embedded system and software solutions are used to good advantages in surfeit areas today. Automotive systems highlight the effective and evolutionary use of both the technologies. ICT (information and communication technology) plays an important role in wireless and wired communication between various components of car. Main challenge is the lagging of ICT architectures in cars with respect to technological advances. As the number of ECU (Engine Control Unit) increases i.e. 70-100 ECU's, which

are worked by complex mesh of cables, the outdated ICT provide a hindrance to innovation. And Software Challenges [1]. A very handy feature of automotive is the Digital lock.

Digital locks provide a keypad which may be a touchpad to store his security key to open doors. The owner just has to enter his security code to open the car doors. If match is found between the stored security key and entered security key then the door opens. But such technology still comes with some drawbacks: If the owner shares his security code with many people there is a possibility that intruder may access his car. Spoofing can allow unauthorized access to car. OTP is a One Time Password which allows access for just one full session [2]. OTP thus provides relief from static passwords. Thus if an intruder gets access to the OTP he cannot use that to ingress the system [3]. To manage all car components sensors are used. For example for Engine Maintenance crank position sensor, intake temperature sensor, throttle sensor are used. These sensors help to calculate the RPMS (revolutions per minute), fuel injection timing with respect to position of crankshaft. Other example to support statement is ABS (anti-lock braking system), Wheel sensors are connected to control module thus speed of the car and the rotational speed of the wheel are monitored, and a skid is detected, this information is given to ABS computer. This computer sends signals to Hydraulic unit and booster which then apply hydraulic pressure to the wheel to avoid further skidding. The Airbag Control unit has crush zone remote accelerator sensors, occupant sensing system, side impact acceleration sensor, also seat belt buckle sensor which works with Air bag control unit to detect impact and thus ignition of a gas generator propellant is triggered to inflate a bag [4]. The vehicle locking system consist of various security aspects, some of them are: The steering will lock anyway should anyone try to move the car without the key in the ignition. Any movement of the steering mechanism, whether at the wheel or the front tires when the key has been removed, will release a spring-loaded lever – causing it to engage a slot and lock the mechanism. Second: Ignition Interlock device is a breath analyzer. The driver is made to blow in an analyzing device which analyses the blood alcohol concentration. If the alcohol level is greater than the permissible level then the ignition interrupts the signal from the ignition to the starter until a valid breath sample is provided [5].

II. EXISTING APPROACHES

A. Vehicle Communication Mechanism

Cars come with various different control units and ample of sensors, communication between all these components is crucial. Integrate protocols are used for this like. SAE J1850 PWM (Standard of Ford Motors): It uses Pulse Width Modulation. SAE J1850 VPW (Standard of General Motor): It uses Variable Pulse Width. ISO 91412-2:

Asynchronous serial data is sent at 10.4kbps [6]. Bidirectional and single line is used for different communication by using UART signaling reference to the ISO14230 (Keyword Protocol) [6]. It incorporates the OSI model communication layers in it. 14230-1 Physical layer, 14230-2 Data link layer are14230-4 are requirements for emission-related systems. ISO 15765-4: CAN (Control Area Network) developed by Bosch includes Bus is the most important protocol, allows all the internal components to communicate without host computer. It is MESSAGE based protocol developed for interconnected wiring within automotive [6]. The idea of maximum effective development and reusability gives leap to improvise the embedded system architecture. With user specified hardware and software requirements it adds to more cost, increase in development time and wastage of many resources. It has two major drawbacks: first is the reusability of solutions in different project demanding same specifications cannot be supported by present architecture. Second, resources tend to oversize. Thus there is need to characterize universal embedded components and define parameters for reusable ones. A general architecture of Engine Control Unit is proposed and implemented. Based on it, cryptographic approach is proposed.

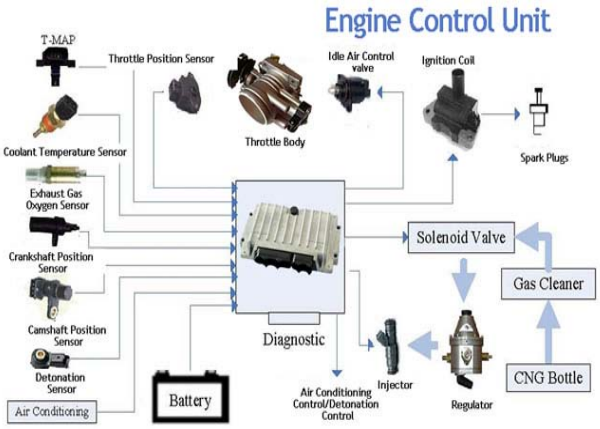

Fig.1. Engine Control Unit Architecture [7]

These components are ECU independent and hence can be reused or replaced as per requirement. To capture the signal processing, devices, sensors and actuators (hardware components) and software components (Local Device Manager) are implanted. An embedded application independent software component is also used as application software. Inter Component Exchange Manager plays the role of a middleware, in particular by providing transparent communication services. Whereas ECU dependent components like Input/Output drivers, the Software Components processes the operating System (OS) or the Communication Services are placed. Initially functionalities are specified by user and their implementations are checked independently. This step gives clear definition of Software Architecture and Software Architecture. Then allocation is used for mapping the functions to the ECU components. This is done via communication through hardware. Finally the task execution and the signal transmissions are minimized. For all the above task to be completed successfully synchronization points have to be developed which would provide connected and matched communication of information. Further universal syntax has to implement for understandable information transmission end to end [7].

B. Computing Platform for Car embedded system

Java has been a platform for embedded systems for more than a decade. The amalgam of JAVA tech and ARM processor provide powerful resource. JAVA ME(Micro edition) embedded provides: a robust, flexible environment for applications running on embedded systems: micro-controllers, sensors, gateways, mobile phones, personal digital assistants (PDAs), TV set-top boxes, printers and more.

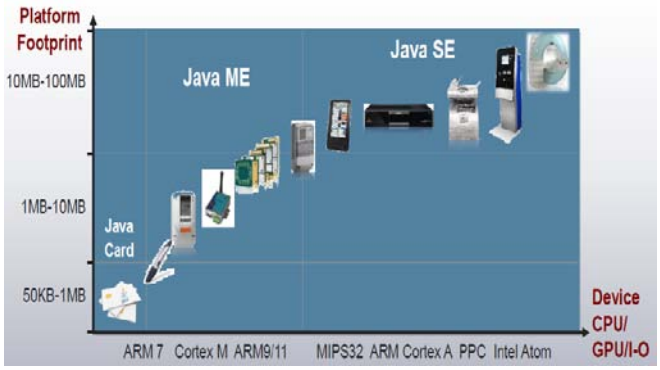

Fig.2. Java Technology for embedded system [6]

It has some key features like reduction in footprint JVM and core libraries & device Access API which is standard library for accessing GPIO-UART-I2C/SPI modules. JAVA SE (Standard Edition) lets you develop and deploy Java applications for systems that demand embedded environments. Java offers the rich user interface, performance, versatility, portability, and security. It has key features like Compatible with Raspberry Pi, ARM6 architecture independent of hardware, Raspberry Pi has JAVA one where JVM needs specific compiler options, includes JavaFX and recently added to standard build platforms.

III. PROPOSED APPROACH AND RESEARCH METHODOLOGY

As time is changing, computing environment has to be improved. Personal life and sensitive obstacles relies on automotive to comfort their life. Automotive environment needs to enhance the security level. Existing smart and computing approaches also have some drawbacks which need to be overcome [8]. In proposed approach, computing is applied to enhance the security level in automotive. Cryptographic approach of computing and automotive framework is used to improve vehicle locking system. Based on case studies, research materials and surveys, proposed approach is defined.

A. Identified risks in existing smart vehicle locking system

The ELM327 is a microcontroller that provides an easy access to a car's information using OBD (On Board

Diagnostic). It translates the data acquired from OBD to the display screen.OBD collects all the information from the sensors and control unit (ex: oil level, engine rpm, tire pressure etc).

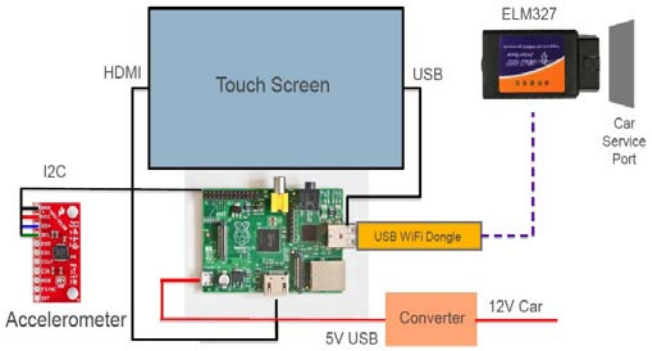

Fig.3. ELM327 Connectivity with ECU [6]

ELM 327 can provide connection via Bluetooth, USB or WiFi. By this connectivity, car's ECU is directly connected to user's screen. This is in turn connected by USB WiFi dongle to Raspberry Pi controller. It provides system on chip (SOC) which provides ARM compatible Central Processing Unit, with Graphic Processing Unit. Secure Digital SD cards are used to store the operating system. HDMI (High Definition Multimedia Interface) and composite video output, Ethernet port and power supply is provided. The accelerometer measures acceleration. It considers only dynamic acceleration. Assume no rotation of the sensor nearly correct, car will roll in corners and pitch under braking/acceleration. From this torque is calculated [6].

Torque (Nm) = Mass x Wheel Radius x Acceleration (in G)
The I2c is a standard which allow the chip to interact with other chips. It allows various devices to be attached to raspberry pi. In proposed approach, it is defined the various ways to represent data. There are basic displays like advance display and graph display. All display provide with different data. Some benefits are basic display gives car details, advanced display, torque graph display gives engine performance & Gforce display gives accelerometer reading.

B. Door locking system

In the proposed approach, there will be a mechanical key to unlock the fixed cover on SALS (Smart Automotive Lock System). Door locking system is added to access steps to overcome physical damage to the SALS. By using physical mechanical key, user can unlock the first layered physical lock to access the SALS.

C. Smart Automotive Locking System

SAL (Smart Automotive Locking System) is a smart device installed on car door properly. Computing platform is installed inside the vehicle cabin safely. It has four main layers. Application platform provides user interface to manually control the system. Service layer and Kernel layer interact with each other with respect to the inputs received from door device. It supports all services comes under GSM (Global System for Mobile) network such as SMS (Short Messaging Service) and others [9].

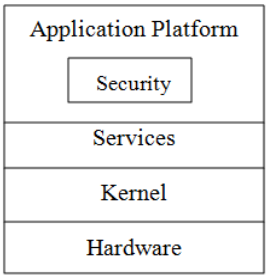

Fig.4. Mobile component

SALS is the device, provides UI (User interface) to enter or retrieve user credentials and details. Both Kernel and hardware layers are connected to the hardware layer which indirectly interacts with (VECU) Vehicle Engine Control Unit.

D. Vehicle Engine Control Unit

VECU (Vehicle Engine Control Unit) is the central processing system which manages all security system. It has three main components viz. Central ECU (Engine Control Unit), Car components & Mobile ECU.

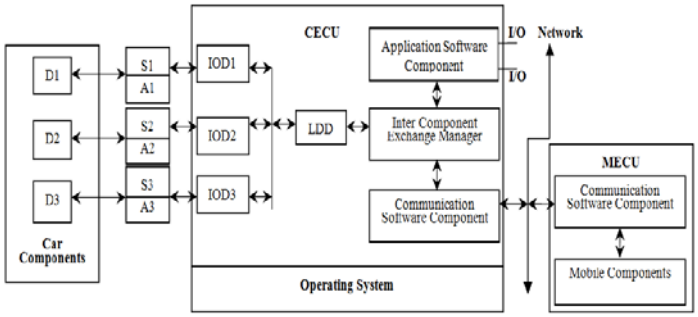

Fig.5. Vehicle Engine Control configured with Smart embedded System

VECU is central system which acts as middleware between SALS and vehicle parts.

1) Central Engine Control Unit

Central Engine Control Unit (CECU) manages the actual smart processing components of the system.

a) Local Device Driver & Input Output Driver

It is installed with LDD (Local Device Driver) and IOD (Input Output Driver). LDD is a software program designed to synchronize application environment with IOD. LDD is developed uniquely to control devices and sensors through IODs further. All information in terms of input and output is passed and understands through IOD to the LDD. LDD understands all possible meanings provided by IODs. LDD is developed in that manner so that application environment can control and access physical devices and sensors. Sensors and actuators reflect the devices information to the IOD. IOD only knows, what is meaning behind gathered information. Accordingly, IOD passes information to the LDD. Sensors and actuators can be related to the devices like engine starter, door locks & brakes.

b) Application Software Component

All logical operations are applied in the application software component. It includes coding platforms, executable engines

and user interfaces. It can be managed using regular application development platforms like editors and compilers. All values can be managed through proposed component.

c) Inter component Exchange Manager

It acts as middleware between application software and LDD. Application software component knows the information passed through inter component exchange manager. It is a short platform provided to execute and generate output provided from LDD. It can generate two kinds of computing information, one for application layer and another for communication software component.

d) Communication Software Component

Communication software component connects two ECUs. It provides inter device support between two different environments. Further, mobile environment is installed. So it is necessary to make reliable data understand by Mobile Engine Control Unit.

2) Mobile Engine Control Unit

Mobile Engine Control Unit (MECU) is further connected to the SALS. Communication software component of MECU interacts with communication software component of CECU.

a) Mobile components

In networking point of view, mobile components are installed in MECU where network related services are processed through this device.

- Global System for Mobile network

GSM service is necessary and important aspect of the computational security system. SMS is one of the preferable services used under GSM network. MECU installed with two layers viz. communication software to interact with CECU and Mobile components to interact with outside world.

- SMS service

Short Message Service (SMS) is accessed and delivered through installed device. CECU provides necessary data related to the user input to authorize and validate the user. Provided data is delivered through network using SMS service.

3) Car components

Car has various parts. In vehicle locking system, three parts are considered as devices. D1, D2 & D3 are considered devices as steering lock, engine starter & door device respectively. These devices are managed by actuators and sensors. Devices are designed with hardware in a way that respective device drivers are installed as IOD and LDD which understands the information meaning. Here, actuators and sensors are designed separately according to the devices. If engine starter is to be unlocked, synchronized sensor and actuator has to pass information to the specially designed hardware to the starter. This information will be based on CECU where it gets input from SALS.

E. Smart automotive lock system

Smart automotive lock system (SALS) is a smart device attached on door externally. In proposed concept, it is covered with physical safety lock to prevent physical damage unknowingly. It has two visible components as digital display and keyboard. Four possible user input components are available as keypad with numbers from 0 to 9, Cancel/Backspace & Enter key.

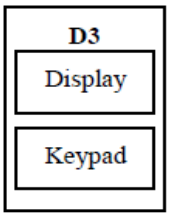

Fig.6. Door device with components

With respect to the input given by the user, information will be passed to the CECU where application software component does logical check method to validate & authenticate the user.

F. Application Software Component

Application software component implements actual logical and computing approach. Outcomes and decisions are based on algorithmic approach. Possibilities are defined based on which actual output is decided. Logical approach is included with mobile computing where one time password has to be retrieved, generate and manually registered Personal Identification Number (PIN) password for SALS. In this era, PIN for SALs cab be activated and deactivated as per user's requirement.

1) One Time Password

When user unlocks the first level which is actual key based physical lock, SALs activates automatically. SALS requires Personal Identity Number (PIN) to generate One Time Password (OTP) request [10], [11]. This step is important to enter into next security level. Logical approach is applied to generate OTP. Proposed algorithm is applied based on which OTP is generated. It is valid for predefined time. OTP is delivered through MECU. GSM network is used in MECU. Through SMS, OTP is delivered on registered user's mobile number. After entering correct required credentials, rests of the components are unlocked [2],[3].

2) Personal Identity Number

When user will be registered first time, he or she will get one time password via SMS to set new password for secure system. This password will be four digit personal Identity Number (PIN). It is kept as four digits because it can be remembered easily. SMS service is used as preferable service rather than increasing complexity in the system registry and reset. PIN is used as important credentials to identify user. PIN can be regenerated or changed as per user's requirement. But first time entered PIN is important to access central system.

3) Secure system logic with CVLS online portal

Application software is a component unit through which vehicle locking system can be managed and controlled. To access its layer, two I/O ports are given to connect it to the actual application. Application module includes, registering user credentials in online database provided by Vehicle Locking system module dealer. When Computing Vehicle locking system is installed in vehicle while initiating, first time user has to be register in online record. It will be one time registration process to register this unique locking product on the name of owner or purchaser. User credentials

will be name, surname, mobile number, email and password to access or modify it next time. But name and surname are non editable and one time registered identities.

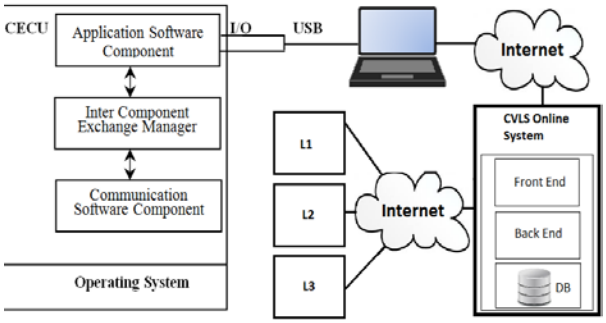

Fig.7. Online Vehicle Locking System Portal Access

User credentials are considered as the user attributes. Cryptographically imposed approach has been applied on the application software component which is interlinked with platform operating system. All logical part is applied in application software component. After installing security kit on vehicle, its first online synchronization process has to be completed after only which SMS service will be initiated to start the computing vehicle locking system. First time registration process will be initiated where CECU connected to the MECU has to be initialized. I/O USB (Universal Serial Bus) cable can be used and connect to computing device [12]. All interaction is done by Application Software Component layer. Local device driver will have all hardware running packages to run it in different platforms like Linux based, windows based or other. After installing Computing Vehicle Locking System (CVLS) driver, user has to login to the online mentioned or proposed portal to initiate CVLS [13]. Internet is the measure requirement to initiate the online registration process. While developing each individual CVLS systems, unique ID will be given to the systems. When CVLS web portal will be accessed through computing device, it will fetch and check for unique ID from system installed in vehicle. Considering unique ID, other user credentials will be asked like name, surname, city, mobile umber and email id where name, surname, email id and mobile number are mandatory fields. Using mandatory fields, PIN can be changed and online line account credentials can be accessed. Name and surname are one time entries which will denote ownership of the product. Based on user credentials, cryptographic logic is applied.

a) Attribute Based Encryption approach for Securely data storage Attribute based encryption approach is applied in proposed approach to securely access and store sensitive database. PIN is important aspect to proceed for next step in unlocking segment. Even online portal is also important aspect to modify user details. User details are considered as elements to which attributes are considered and allocated.
Data attributes are considered for user data entities like CVLS systems unique ID, name, surname, mobile number, email id and PIN number.
CVLS online portal database maintains all users affiliated to product safely by applying attribute based encryption approach. While allocating attributes to the elements, simple logic is applied based on which attribute set elements are allocated.
Attribute sets considered as N, S, UID, M,E & C for Name, Surname, Unique ProductID, Mobile number, Email ID & city respectively [14],[15]. While fetching the data based on attribute is stored in different location.

TABLE I. Attribute sets and attribute

User details component	Attribute set Name	Attributes
Unique Product ID	UID	$\{u_1, u_2, u_3, u_4, u_5, u_6, u_7,.....\}$
Mobile Number	M	$\{m_1, m_2, m_3, m_4, m_5, m_6, m_7,.....\}$
Email ID	E	$\{e_1, e_2, e_3, e_4, e_5, e_6, e_7,.....\}$
Name	N	$\{n_1, n_2, n_3, n_4, n_5, n_6, n_7,.....\}$
Surname	S	$\{s_1, s_2, s_3, s_4, s_5, s_6, s_7,.....\}$
City	C	$\{c_1, c_2, c_3, c_4, c_5, c_6, c_7,.....\}$

Attributes are specially used to reference the actual data. Example can be considered as if person has details as following,

TABLE II. Attribute set and actual attribute element values

User details component	Attribute set Name	Attributes
CVLS_7779	UID	u_1=' CVLS_7779'
+918793000079	M	m_1='+918793000079'
surasal@bvu coep. edu.in	E	e_1='surasal@bvucoep.edu.in'
Suraj	N	n_1='Suraj'
Rasal	S	s_1='Rasal'
City	C	c_1='Pune'

Central file is created by applying logical approach on all attribute sets randomly. Central file includes the information related to the actual allocated attributes.

Multi locality approach

TABLE III. Actual Data reference in CVLS database

File Name	Logic	Attribute	Value	Store_ ID	Location
F79	R_7	u_1	CVLS_7779	F79u1x	L1
		m_1	+918793000079	F79m1x	L2
		e_1	surasal@bvucoep.edu.in	F79e1x	L1
		n_1	Suraj	F79n1x	L1

		s_1	Rasal	F79s1x	L2
		c_1	Pune	F79c1x	L3

Similarly, other data is stored and fetched with reference to the file name and store_ID. When data is travelled on internet, file name and stored ids are travelled. When main database access is granted, it looks for actual stored values through file names, stored IDs in different locations. While accessing respective servers at different locations, different cryptographic approached are applied [15]. Proposed cryptographic approach is used to safely store and access user data in CVLS portal database only. For above file 'F79', data has to be fetched from location L1, L2 & L3. User details set 'D' is a set of attributes.

b) Randomized logical approach

D= F79

D $\xrightarrow{R_n \text{ Logic}}$ **L**

L = {L1, L2, L1, L1, L2, L3**}**

D= **{**L1, L2, L1, L1, L2, L3**}**

D= { F79u1x , F79m1x, F79e1x, F79n1x, F79s1x, F79c1x }

D= $\{u_1, m_1, e_1, n_1, s_1, c_1\}$

D={'CVLS_7779','+918793000079','surasal@bvucoep.edu .in',' Suraj','Rasal';'Pune'}

Here R_n denotes Random logic applied on 'L' location set values. Random logic depends on the sequential sorting algorithm where random sequence is generated. Based on it only location values are decided according to what attribute values are stored. In online communication through internet, attributes are travelled rather than travelling values. Even if unauthorized person try to access details, multi locality approach is applied due to which actual values can't be accessed. When data is stored in CVLS database, it is deleted immediately after processing is done. When data is fetched first time in the database, logical approach is applied after which actual data is stored in different locations. Main file 'F' is stored in the database. Based on applied logic, file is stored. Based on logic, stored_ID are generated. Stored_ID denote the attributes applied and data is fetched from randomized location where data is stored [16].

G. Power Failure Options

This option is given by considering power failure in the system. Power supply can be end up due to any physical condition. System will be restarted automatically to reset itself with all situations even though car is unlocked. Car will be locked if power failure occurs. If car is in running state, all components will be remain in the same state like if car is in running state. But message will be delivered through SMS service. Engine starter and cabin will be locked if power failure occurred in running state. System will start PIN reset option. After power failure, system will send one time PIN to reset your new PIN through SMS service on registered mobile. After entering new PIN only, OTP system will be initiated through GSM network to access next car components. Online process is to modify and edit details of product owner which doesn't need to be accessed on power failure. Only SMS service is sufficient on power failure to reset PIN [9]. If user forgets previously registered PIN, he or she has to change it via accessing online module which can be possible by official online process.

IV. CONCLUSION

Mechanical locking is provided to safely preserve smart locking system environment. Personal Identity Number enhances the security level to access smart system. One time Password approach improves credential storage gap. OTP denotes the present access system even though unauthorized person knows the first level PIN. Online Vehicle Locking System shows multi location and reliable approach to convey advanced smart locking system. Cryptographically imposed approach and online features improves the security level. Security is focused in automotive obstacles, because transportation is one of the reliable parameter in human activities. Online database security methods are applied to improve online computing. Secure logic and algorithms with multi locality approach are applied to enhance the security level. Importance is given to the security of the vehicle components and cabin. Computing Vehicle Locking System works in smart way to upgrade itself to the current computing approaches. All together forms multilevel advanced secured locking system.

V. REFERENCES

[1] Chakraborty, Samarjit, et al. "Embedded systems and software challenges in electric vehicles." Proceedings of the Conference on Design, Automation and Test in Europe. EDA Consortium, 2012.

[2] S U Rasal, S T Shelar, V S Rasal. (2016). "Securing Internet Banking Using Multiple Attributes Scheme And OTP". Institute of Integrative Omics and Applied Biotechnology (IIOAB). 7 (10), P26-30.

[3] Varsha S Rasal, Suraj Rasal, Shraddha T Shelar. (2016). "Enhancing Privacy And Security Through Mediator Using DCP-ABE With OTP". Institute of Integrative Omics and Applied Biotechnology (IIOAB). 7 (1), p277-283.

[4] Liang, Yew-Wen, et al. "Nonlinear reliable control with application to a vehicle antilock brake system." IEEE Transactions on Industrial Informatics 9.4 (2013): 2114-2123.

[5] Nalina, V., et al. "Cloud based multiple vehicle tracking and locking system." Advance Computing Conference (IACC), 2015 IEEE International. IEEE, 2015.

[6] Simon Ritter. (2012). White paper on "Is It A Car? Is It A Computer? No, It's The Raspberry Pi Java Carputer". Oracle . 1 (1), p15-46.

[7] Vivek Bhardwaj. (August 2014). ECU (Engine Control Unit) Cars,ECM,Parts,Functioning. Available: http://aermech.com/ecu-engine- control-unit-carsecmpartsfunctioning/. Last accessed 21st Sept 2016.

[8] Ramaiah, Chandra Shekar, et al. "Smart vehicle security system for defending against collaborative attacks by

malware". 2016 3rd MEC International Conference on Big Data and Smart City (ICBDSC). IEEE, 2016.

[9] Teymourzadeh, R., Ahmed, S.A., Chan, K.W. and Hoong, M.V., 2013, December. Smart GSM based home automation system. In Systems, Process & Control (ICSPC), 2013 IEEE Conference on (pp. 306-309). IEEE.

[10] Cong, S., 2013. A One-time Password System Based on Script of the Research and Implementation [J]. Information Security and Technology, 6, p.008.

[11] Suraj U Rasal,Megha Matta,Karan Saxena, [2016] OTP system with third party trusted authority as a mediator. International Journal of Engineering and Computer Science. 5 (5), (pp16566-16568).

[12] Szeremeta, W. and Trinh, M.N., Western Digital Technologies, Inc., 2014. Universal test connector for connecting a SATA or USB data storage device to a data storage device tester. U.S. Patent 8,753,146.

[13] Kadav, A. and Swift, M.M., 2012. Understanding modern device drivers. ACM SIGARCH Computer Architecture News, 40(1), pp.87-98.

[14] Shraddha U. Rasal, Bharat Tidke, (March 2014). Improving Revocation Scheme to Enhance the Performance in Multi-Authority ABE. International Journal of Computer Applications (0975 – 8887). 90(18):5-10).

[15] Jinguang Han, Willy Susilo, Yi Mu,Jianying Zhou,Man Ho Allen Au.(March 2015). Improving Privacy And Security In Decentralized Ciphertext-Policy Attribute-Based Encryption. IEEE transactions on information forensics and security. vol. 10, no. 3 (1), p665-678.

[16] Suraj U Rasal,Raghav Agarwal, Shraddha T Shelar,Varsha S Rasal. (2016). IOT appliance access structure using ABE based OTP technique. Institute of Integrative Omics and Applied Biotechnology. 7 (1), p180-186.