International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-10 Issue-3, September 2021

Cyber Intelligence in Smart Vehicles

Varun Chopra

Abstract*: *In the embryonic stage, the usage of vehicle tracking systems were primarily restricted to getting the geographical location of the vehicular units. This scenario, however, was not perennial and with the escalation from a rudimentary stage to a highly complex archi- tecture for vehicular administration that we witness today, the standards for the vehicles security have also become monumental. With the development of V2X communications, the gamut of facilities provided by smart vehicle services has expanded prodigiously. These technological advancements, however have come at a cost. The gargantuan transition that has taken place over the recent years exacts a lot of security and safety mechanisms to be implemented, adjunct to the products and services it comes equipped with. In this paper, after a comprehensive study in the domain, we imply a security system model comprising of a Microcontroller Unit (MCU), as a part of the Vehicle TracingMechanism (VTM), well connected with a Management Hub. The communications be- tween the Vehicular Unit(s), Management Hub and the system Vehicle Tracing Mecha- nism (VTM) are made viable via V2X communications with conducive aid from technolo- gies like Global Positioning System, Radio Frequency Identifications and GPRS network. The paper aims to ameliorate the extant security protocols and improve the security and safety standards of smart vehicles by broaching cyber intelligence in smart vehicles.

Keywords: About four key words or phrases in alphabetical order, separated by commas.

I. INTRODUCTION

In the recent years, there has been a drastic change in how the domain of vehicles or automobiles is perceived. In contrast to how it used to be, that was solely in the capable hands of mechanical engineers, now the vehicles also entail computers to contribute vitally to their existence. This conspicuously makes it manifest that computer no longer have a circumscribed domain; their versatility and gamut of applications have made them a cardinal element even in inchoate stages of any industrial project. This entailment of computers engendered smart vehicles and VANet(s). Smart Vehi- cles are intelligent vehicles having an array of attributes by incorporating technologies such as Artificial Intelligence, Machine Learning (ML), Internet of Things (IoT), and Cloud Services. This extraordinary application of computers was presaged fundamen- tally by suggesting a 5.8GHz Dedicated Short Range Communication (DSRC) System by Philips in the last decade of the 20th century. Since then, the industry has aggrandized exponentially. Vehicular Adhoc Networks or simply VANet(s) are vehicular networks deployed to ensure and administer interaction between smart vehicles and their smart surroundings. Each vehicle or smart device acts a node in the network and interacts with another node to communicate important data as speed, distance, routing, traffic update etc. For instance, consider two vehicles, A and B. Vehicle A is moving right ahead ofVehicle B, at a speed of 50km/h while Vehicle B is at moving a speed 55 km/h and accelerating, intending to overtake Vehicle A. Suddenly, the driver of Vehicle B receivesa phone call and is distracted for a few seconds intermittent his overtaking process. On the other hand, the driver of Vehicle A intends to turn right and flashes on his rightturning indicator and starts retarding his vehicle, which the driver of Vehicle B missesdue to lax driving. At this moment, considering both vehicles not to be smart ones,this probably would result in an accident. But, if they are smart vehicles, Vehicle A cansignal Vehicle B that it is slowing down and as an exigency safety protocol, Vehicle Bcan instigate a fail-safe and start slowing down on its own, in turn shunting the accident.The incessant range of advantages and features of these vehicles include reduced traffic congestion, sparing use of energy, fuel husbandry, escalated lane capacity, decline in incident of accidents and so on. Exigency braking helps shunting accidents and collisions with other road entities. Unfortunately, there's no light without darkness and with these enticing features come boding evils of security and safety threats that tend to not only thwart the escalation in this domain but also assail and iterate these attacks to have a detrimental impact on the industry. A sundry of challenges cumulatively add fuel to this fire. Privacy and Authentication tend to refuse to go hand in hand and hence pose a major threat to smart vehicles. In addition to this, to make these features available and key distribution also tend to add to the complications. This imbroglio is exacerbated by bootstrap issues and by the disparity in interests of covet manufacturers and ever exacting consumers. Pertinacious to overcome these obstacles, this paper focuses on a comprehensive study of existing security practices and ways to improve them by begetting a lucid model which uses extant services like V2X communication, GPS, GSM and GPRS network to ensure security, safety and apposite administration of Vehicular Unit(s) and the VANet they are a ramification of.

II. BACKGROUND

Emerging technologies are fostering modernisation in connected as well as autonomous vehicles industry.

Manuscript received on September 14, 2021.
Revised Manuscript received on September 16, 2021.
Manuscript published on September 30, 2021.
* Correspondence Author
Varun Chopra*, School of Computing Sciences and Engineering, Vellore Institute of Technology, Bhopal, (M.P.) India. Email: varunchopra1730@gmail.com

These encompass domains like Artificial Intelligence and its sub- domains, Machine Learning(ML), Computer Vision, Internet of Things(IoT), CloudTechnologies, Smart Robotics and Mobility. There is a transcending momentum in this field, with a compound annual growth rate (CAGR) anticipated to be more than what it was in the recent years, being a concomitantof this evolution.

III. I SMART VEHICLES

A Smart Vehicle is a conflation of existing equipment such as sensors, navigator, chip, Network Interface Card(NIC), Auto Braking System etc. with the vehicles, interconnected with each other via a server.

These can broadly be stratified into 2 categories: -

1. **Semi-Autonomous Vehicles:-** These Smart Vehicles are massively automated and are accoutered with multitude sensors in order to be capable of performing all functions without human intrusion, under certain circumstances.
2. **Autonomous Vehicles: -** These Smart Vehicles are monumentally automated and come with multitude sensors in order to be worthy of executing all the functions under all circumstances, with any human intrusion, autonomously.

IV. V2X COMMUNICATIONS

Interactions with the help of data exchanges between two vehicles or between vehicles and other establishments enroute, that may affect or may be affected by the vehicle, pertains to V2X communications.

V2V or Vehicle-to-Vehicle communications help vehicles interact with each other.

V2I or Vehicle-to-Infrastructure communications refer to interaction of vehicles with road infrastructure such as traffic signals, street lamps etc.

V2N or Vehicle-to-Network communications refer to interaction of vehicles with other networks.

V2P or Vehicle-to-Pedestrian communications refer to interaction of vehicles with other pedestrians on the road via their smart devices.

V2C or Vehicle-to-Cloud communications refer to interaction of vehicles with cloud services/platforms.

V2D or Vehicle-to-Device's communications refer to interaction of vehicles with other smart devices.

They subsume technologies like Dedicated Short Range Communications (DSRC), Wifi or Cellular Technologies (like 3G,4G,5G), Image Sensor Communication (ISC), Visible Light Communication(VLC) etc.

V2X Communications are conducive in escalating: -

1. Road Safety
2. Traffic Efficiency
3. Energy Savings

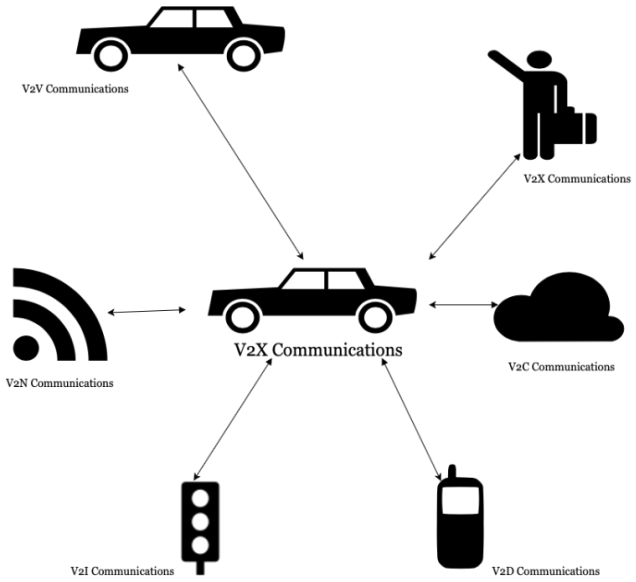

Figure 1: V2X Communications

V. ARTRIBUTES OF SMART VEHICLES

The key attributes of Smart Vehicles are as follows: -

- **Adaptive Cruise Control: -**Adaptive Cruise Control helps in increasing driver's comfort and reduces driver's efforts, in turn facilitating a comfortable and relaxed driving experience.
- **Emergency Braking: -** Many a times, the driver is distracted and this leads to accidents. This can be avoided with the help of emergency braking where in the smart vehicle automatically triggers braking when senses distance lesser than threshold proximity to avoid collisions via V2X communications.
- **Pedestrian Detection: -** This feature helps in saving lives by enabling the smart vehicle to detect pedestrians via interactions with their smart devices.
- **Collision Avoidance: -** Collisions can be avoided with the help of emergency breaking by using sensors enabling V2X communications.
- **Lane Departure Warning: -** V2V communications help in facilitating lane change/departure warnings from one vehicle to another over a VANET, thus reducing the risk of accidents.
- **Cross Traffic Alert: - Smart** Vehicles subsume a cross traffic alert mechanism to restrain accidents due to cross traffic. This is facilitated with the help of V2X communications via which one vehicle informs the other about the incoming cross traffic to prohibit any catastrophe.
- **Park Assistance: -** Park Assistance helps in saving a lot of time and space. This enables a smart vehicle to park itself in a suitable location even when it has dropped the driver at the destination. Handsfree parking reduces human effort and scope for human error.

- **Surround View:** - Surround or Ambient View is conducive to the driver to moon- it or surrounding traffic and environment and respond to it with apposite braking and acceleration adjustments.

VI. ADVANTAGES OF SMART VEHICLES

Smart Autonomous Vehicles have various advantages. A few of them are listed below: -

- **Decline in Accidents: - Due** to less or negligible human intervention, accidents are less likely to take place because autonomous vehicles are capable of providing a safer travelling experience.
- **Reduction in Traffic Congestion:** - Smart vehicles smooth out the traffic flow. Human drivers generally follow a stop-and-go mechanism which results in disruptions and congestion in traffic. This problem is unraveled by smart vehicles and hence, it also helps in reduction of transportation costs and saves time.
- **Energy Conservation: -** Energy can be husbanded by the use of smart vehicles since they are more fuel efficient. In this way, they are also conducive to sustainable development. This will also help in less CO2 emissions making smart vehicles eco-friendly.
- **Better Parking:** - Parking can at times be tedious for human drivers. Moreover, parking a normal vehicle requires adequate space between two vehicles for the drivers and passengers to enter and exit the vehicle. This, at times,
  instigates space issues. According to a census, smart vehicles require about 17 percent lesser space since the eliminate the need for the driver to get in or get out if the vehicle, by parking themselves. It also makes the job easier by dropping the driver at his destination and then finding an opposite place for it to park itself, even if it is farfrom the dropping point.
  - **Increased Accessibility to Transportation: -** Many aged and/or disabled pea- plex find it difficult to drive normal vehicles. With smart vehicles, getting errands done will become much easier and more feasible for people with disabilities or for the ones, who's age bars them from doing such petty jobs.
  - **Increased Efficiency of Taxis:** - Smart Taxis are considered to be more efficient and cost effective than normal taxis. This is because smart taxis have lower waiting time and are much more economic due to lesser fuel consumption and decreased traffic congestion.
  - **Escalated Lane Capacity:** - The lane capacity is increased significantly because of the ability to consistently keep a vigil at the ambient traffic and greet it with adequate braking and acceleration adjustments. This enables a safe travel at relatively higher speeds and reduces headway between vehicles, in turn, increasing lane capacity.

VII. PROBLEM STATEMENT

It is quite lucid to understand and presage that in the coming times, most smart vehicles will be equipped with the stipulated technology for inter-vehicular as well as communications between smart vehicles and other entities like road infrastructure, other smart devices, networks etc. This will facilitate anything and nigh everything for the suavity in driving experience and allow a breakthrough in the industry by allowing applications to provide a wide range for services ranging from traffic updates to warning signals to automated decision making in perilous or fatal circumstances. However, it is also a reputed fact that there are two sides of a coin and various security threats are also concomitants of these facilities and services that mesmerize us. In orderto assure the security of the users is not jeopardized, this paper attempts to review the basic security prerequisites for smart vehicles and their communications over vehicular networks and propose ways to ameliorate and implement better solutions.

VIII. CHALLENGES IN SECURING SMART VEHICLES

Today, almost all aspects of automotive industry have been revolutionized by the ever- developing technology. However, as it is rightly said that everything has both pros and cons, this revolution also has some limitations. For this reason, smart vehicle manufacturers must imperatively go for a holistic method for protecting their smart vehicles against cyber threats. Technical obstacles such as key distribution and some non-technical obstacles such as the need to appeal simultaneously to three very different markets contribute to Smart Vehicle challenges.

Some of the major challenges faced today while securing Smart Vehicles are mentioned below: -

Privacy Vs Authentication: - Binding each driver to a unique identity helps in preventing cyber-attacks germane to spoofing. However, many drivers find their privacy more valuable and hence refrain themselves from adopting practices that might results in intrusion of their privacy or practices that have forsaking of anonymity as a prerequisite.

Availability Concerns: - Many applications exact real-time or near real-time re- sponge mechanisms from smart vehicular networks in addition to hard-time guar- antes. In attempt to meet this demand, the manufacturer might also make the smart vehicle vulnerable to attacks like DoS (Denial of Service) which might ex- acerbate the situation. On the other hand, if there's even a diminutive delay of seconds in the messages, it might result in their futility. The predicament stunts the security of smart vehicles in a monumental way.

Key Distribution Feature: - The building block of vehicular networks is Key Distribution. Sundry vehicles are manufactured by different companies and hence at different places, so in order to install the key at the factory itself, the Manu- factures will have to work in sync, which isn't as easy as it seems. Moreover, a delay at one step would vitiate the next steps of the process, resulting in chaos. But this problem cannot be countenanced as without proper key distribution, the vehicles will become vulnerable to spoofing attacks.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Bootstrap Issues: - Since only a trivial percentage of vehicles are equipped with the requisite infrastructure and technology to bolster smart application, Applica- ton need to be developed considering this fact and benefiting vehicles with limited adaptability as well.

Market and Incentives: - **Vehicle** manufacturers, consumers and government, all have to be taken care of for this venture to be successful. This stunts the deployment since all three often have disparities in their interests and opinions.

IX. PROPOSED SOLUTION

This paper, after a comprehensive study of the problem statement and challenges thwart- ing the security of smart vehicles, proposes an opposite solution to triumph over such hurdles.

X. ADHERENT OF SECURITY

Some of the major attributes that act as the supporters of security in smart vehicles areas follows: -

- **Quotidian Scrutinizing:** - The smart vehicles must go through regular security checks which are categorically conducive in ratifying the software integrity on the processor of the vehicle. Moreover, this will be also facilitating updating/patching of the current software versions and renewal of the certificates.
- **Auxiliary Inputs:** - Nodes in a vehicular network have a predefined intelligent characteristic inane while in conventional sensors, the scenario is quite opposite. This enables the vehicles to extract and use even the most diminutive Information (for instance, drivers' facial expressions or demeanor in cases of accidents to enable collision avoidance) and take decisions and adapt discreetly to the circumstances.
- **Subdued Ingress:** - Access Control mechanisms have been schisms of majority of the ramifications of transportation infrastructure. This can be advantageous in facilitating roads and bridges with the stimulated technology that allows them to disseminate keys to vehicles lying the controlled domain. This, in turn, will allow inter-vehicular communications between vehicles in the restrained domain, making it mandatory for each vehicle to pass through a limited set of entry/exit point(s).
- **Invigorating Protocols:** - Prevailing set of laws and protocols are eternally conducive to inhibiting security attacks on vehicles. It is often noticed that the attacker tends to be in the proximity of the victim at the time of the attack to ascertain that the attack was effectual. If at that moment, the victim somehow manages to distinctly identify the attacker and apprise the law enforcement bodies responsible, the victim might be able to eschew the attack. Also, it is quite tritethat the manufacturers are considered to have higher standards than software Ven- doors and therefore, manufacturers have a monumental impetus to install security primitives in the vehicles.

XI. VEHICLE TRACING MECHANISM (VTM)

A sundry of technologies come in handy while facilitating this feature, such as: -

- Global Positioning System engenders the ability to get the geographic position and velocity of the vehicle.
- V2X communications enables interaction between the vehicular units and the man- agreement hub. Technologies like Global System for Mobile Communications (GSM)also play a cardinal role.
- Radio Frequency Identifications prove to be conducive in ratifying authorized ingress.

The integral element of VTM is an MCU or micro controller unit which concocts all the technologies involved and facilitates interaction between them. It is responsible for process of reconnaissance and impels the data agglomerated to the management hub for further processing. There is also a status check feature which helps in the intimation of current status of door lock/unlock, ignition active/inactive, fuel check, vehicle service check, all systems functioning check etc. This mechanism is completely automated and hence languishes the probability of error.

XII. MANAGEMENT HUB

Management Hub can function majorly in 3 distinct ways:

- Cellular Station

In this mode of operation, the user can send and receive information about the vehicular unit(s) on the user's cellular station/cell phone via a cellular network. The user can also administer the vehicles key features in times of exigencies and catastrophes, both virtual and physical debacles.

- PC Station

The GSM modem adjunct to the management hub, is very contributory because it learns data from the VTM's package and impels it to the PC station via theserial port. This enables us to keep a track of the historic developments in the vehicular units since this data is finally stored onto a database, each time after being welcomed via the serial port by the PC station.

- Web Server

This method of operation is similar to that of a PC station and has GSM or GPRS modem adjunct to the management hub, is very contributory because it learns data from the VTM's package and impels it to the PC station through the serial port via the GPRS network or V2X communications. This data collected is then stored onto a database for future reference and monitoring the transitions or developments the vehicular unit(s) undergo(es) over time. Only authorized users have ingress to this central database, taking its its security to the zenith of import. To showcase this data to the authorized users, a front-end software with a web user-friendly interface is used, functioning over the internet, thus being secure yet handy.

- Data Exchange Via V2X Communications

The data, distilled and processed, is channelised to a secluded management hub to makeit visible to the end user. This is a vital step to ensure safety and security and proprietyof geographical position of the vehicular units. Any vulnerabilities can emaciate the network and lead to a compromise/breach of security of vehicular units. This mode of communication, hence, must highly safe and immaculate.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

- In order to ascertain this, we use existing V2X communications. These communica- tions are safe and prove out to be much more pocket-friendly in contrast to deployment of a separate singular network for data transmission and communications. GSM tech- nology can also provide a vital contribution because of its gargantuan expanse. GSM prerequisites a modem and transmits data in form of messages via General Packet Radio Service(GPRS) and its network.

XIII. IMPLEMENTATION

The MCU acts as the central part of the system. Its major role is to accumulate and impel information from the Vehicular Unit(s) to the Management Hub. It agglomerates the gamut of data from the Vehicular Unit(s) ranging from door lock/unlock status, ignition active/inactive status, fuel status, vehicle service check, all systems functioning check etc. Furthermore, it interacts with various smart devices via V2X communications and other services like GSM, GPS and RFID, that constitute the ultimate part of the system. It is manifest that MCU plays a cardinal role in the whole set up.MCU is enjoined by a program written onto its flash memory (to make sure the mem-ory is non-volatile). The consummate program is severed into further ramifications or into smaller schisms. These schisms are regarded as modules. MCU reads the programs commands and executes them schism by schism until the designated job is completed.

XIV. ALGORITHM

The MCU acts as the central part of the system. Its major role is to accumulate and impel information from the Vehicular Unit(s) to

- Instigate the MCU.
- Activate V2X communications and other communication services.
- Agglomerate information from all connected Vehicular Units via V2X communi-cations.
- Assemble all data from GPS, GSM and RFID communication Services.
- Ratify the validity of instruction.
- If instruction is valid, proceed ahead.
- If instruction is invalid, send an alert to the end user.
- Identify ilk of instruction from the list given below:-
- Vehicle Embezzlement Alert
- Vehicle Status Notification
- Vehicle Service Due
- Vehicle System Override Alert
- System Malfunction Alert
- Stratify the required data according to the circumstances.
- Transfer the stipulated information to the Management Hub for further processingvia V2X communications or GPRS network.
- Management Hub takes the appropriate action based on the information received.
- The information or instruction is disseminated to the vehicular unit(s) under con- sideration via V2X communications or GPRS network.

XV. RELATED WORKS

Raya et al. [15] address the problem that how Vehicular Communications (VC) are stymied by potential security threats. The author aims to foster safer and more efficient driving conditions by recommending a lot of traffic safety and data security measures. Vehicular networking protocols will allow nodes or vehicles or roadside infrastructure units, to interact with each other over single or multiple hops. The author aims to encourage building vehicular communication protocols and systems that try to nullify any scope for misuse and abuse and simultaneously, remain resilient to ongoing and upcoming attacks. The author also describes the obstacles that stratify the security of vehicular networks and recommends possible solutions. A well-coordinated effort of allparties involved makes it feasible to come up with a solution that is compliant withthe exacting requirements of unique challenges of high speed and sporadic connectivity, based on their geographic location, the tension between liability and privacy and the humongous scale and very slow deployment of network. Raya and Humax [14] address the security of Vehicular Ashco Networks (VANETs) in the cyberspace. They aim to consign a detailed analysis and succinct security Archi- texture. The author delivers a set of security protocols, and shows that they protect privacy and we analyse their robustness, and we carry out a quantitative essay of the proposed solution. They talk about the state of the art and how this domain is emerging in these times of technological transcend. The paper gives a system model with some system assumptions. They also address some specific attacks that pose a challenge and how they can be tackled. In addition to this, the paper states that how digital signaturesand cryptography can be the building blocks of this grotesque domain. In a nutshell, this paper, construes why vehicular networks need to be secured, and why this problem requires a specific approach. Although technological advancements in the field of Information Technology have paved a way for better traffic management, road safety and driver convenience, it has seemed to have overlooked the repercussions that lead to security and privacy being com- promised. This paper by Humax et al. [7] aims to address the issues germane to the above-mentioned subject. It talks about various features constituting Vehicular Com- medication (VC) such as Event Data Recorder (EDR), GPS receiver, front end Radaretc. It also emboldens the use of electronic franchise plates or electronic license plates, tamperproof GPS, verifiable multi alteration etc., for better security and privacy. It discusses how bootstrapping and adoption of necessary hardware stymies a business ob.- stale and how to tackle this problem. Lu et al. [9] introduces an Efficient Conditional Privacy Preservation Protocol for Secure Vehicular Communications (VCs) to facilitate a solution to anonymous authentic- cation for safety with authority traceability.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

A VANET mainly comprises of On-Board Units (OBUs) and Roadside Units (RSUs), where OBUs are installed on vehicles to facilitate wireless communication capability, while RSUs are deployed to support wireless interfaces to vehicles within their radio coverages. This paper proposes a fresh and efficient conditional privacy preservation (ECPP) protocol for communications between vehicles secure. The ECPP protocol can tractably deal with the emerging revocation list while achieving conditional traceability by the authorities. It proposes a system model with succinct system roles, channels and system assumptions. It also depicts some creep- to graphic operations and contrasts their execution time. It also compares this model with GSB and HAB models through extensive performance analysis and prevails over them by being more efficient.

Garg et al. [6] discusses about UAV (Unmanned Aerial Vehicles) empowered edge com- putting environment for cyber threat detection in smart vehicles keeping in mind features like surveillance in ITS and transportation being the backbone of every city. It contrasts edge computing and cloud computing and talks about transportation challenges in the era of 5G and the role of ITS in-edge computing. It suggests how UAVs can be used in smart transportation and proposes various techniques to overcome challenges.

Paro and Perrigo [12] see short range radios as a future mode of communicationof smart vehicles with other smart vehicles or with highway infrastructure and how todeal with stymied problems to finally achieve this proposition

. They stratify various challenges into categories like authentication, privacy, availability, mobility, key district-button, low tolerance etc. and addresses each one of them profoundly. The paper also talks about adversities, attacks and some properties supporting security pertaining to the subject. Some security primitives such as Authenticated Localization of Message Origin, Anonymization Service, Secure Aggregation Techniques etc. are also taken into account in this paper. Conjuring vehicular networks that are viable and conformable to consumers, establishment of security protocols that satiate the stringent requirementsof this application space is mandatory. Luckily, the characteristics of vehicular net- works facilitate new approaches for these challenges, allowing the development of new primordial based on, for instance, the entanglement of vehicle trajectories and the useof simple deanonymizes.

Kaur et al. [8] discusses the importance of blockchain in facilitating information con- identicality, integrity, authenticity, privacy and anonymity. It also bolsters on the fact that records must be kept and maintained in a distributive manner and how blockchain can be conducive in achieving this. It proposes a system model based on blockchain and ECC to achieve the subject and some of the its key factors and features like region, Road Side Unit (RSU), On-board Unit (OBU), Audit Department etc.

It also limns cross data center authentication in Vehicular Fog Computing (VFC). With the advance- mints in this field, it also imperative to keep in mind the security risks and safeguard the network with all due precautions. Thus, to make this possible, the paper proposes a model designed to allow unrestrained access VFS for smart vehicles which is based onBlockchain and ECC.

Martinez-Fernandez et al. [10] limns AUTOSAR. AUTOSAR (Automotive Open Systeem Architecture) was established in 2003 and was first launched in 2005. AUTOSAR is a software reference architecture that has ingratiated over the years. This paper talks about the background of AUTOSAR and depicts a research methodology of its empirical study. It also discusses the outcomes and limitations of this survey. It depicts RQ2 and validity (both internal and external). Moreover, it says that the software facilitates an outline for conjuring automotive applications' software architectures.

An evaluation by AUTOSAR showed that the new requirements of smart vehicles cannot be fulfilled by software architectures wherein almost all vehicle internal comma- nictation is done via a profoundly embedded controller to meet OEM requirements suchas startup times or functional safety and where the communication can be limned by AUTOSAR means. First and Becher [5] discuss the key aspects of the E/E architect- true, the

AUTOSAR adaptive platform, support for the integration of the heterogenous platforms and AUTOSAR standards and timelines.

QuickChek helps perform manually conjured tests in effort and fault-finding cap- abilities with QuickChek models and automatic test case generation. Arts et al. [3] highlights the problems in essaying loftily configurable AUTOSAR software and con- strews how to overcome these hurdles. Arts et al. [3] also contrasts QuickChek method-ology with the manually created conventional test sets and makes it quite evident that QuickChek method is more efficient and correct/accurate.

Information sharing between smart vehicles poses security and privacy issues pertain- Ing to confidentiality, integrity and attacks. The proposed solution by Allowably et al. [2] adopts a 3-stage security mechanism concomitant within the participants. A system setup and performance evaluation are also done by the authors. The paper suggested a new hybrid method called D2H-IDS which is used for intrusion detection in smart con- nested vehicle cloud environments after being inspired by the necessity to inhibit such attacks and improve security.

Qu et al. [13] limns the threats, challenges and requirements in VANETs and basic ideas and solutions to such problems and challenges. The authors give a security art- echotexture and suggest some technological improvements in security. The paper also discusses some digital signature algorithms and recommends some privacy preserving solutions. In addition to this, it also limns a tradeoff between privacy and security which is inevitable. This paper proves to be conducive to the field by facilitating the general authentication processes in V2V and V2I communication scenarios and pointing out algorithms involved in these mechanisms.

Ogham et al. [11] describes B-FERL; a blockchain based framework for securing smart vehicles and elucidates a threat model with its architecture overview and network model. The aim of B-FERL is to recognize when an ECU of a smart vehicle has been compo- missed or attacked and take imperative measures to inhibit destruction in such scenarios.

The B-FERL framework constitutes mechanisms to bolster various forms of information
transactions and operations. In addition to this, there's also a performance evaluation done which is discussed in the later section of the paper.
Intrusion Detection Systems (IDS) are security systems that vigil the incoming and outgoing traffic in a missed and missed [4] discuss the challenges faced to secure network-controlled systems and possible solutions incorporating adaptive cruise control.
They limn intelligent intrusion detection systems and discusses various attack scenarios with apposite solutions. A mechanism for using adaptive cruise control to detect and compensate attacks is suggested by them. Two scenarios to covert attacks on ACC also elucidate the importance of the subject. The ACC system was learnt by an apocryphal neural network identifier and the outcomes were predicted.

Ahmad et al. [1] introduces a double security layer. To start with, it safeguards the PKES system from reputed relay attacks with the help of key fob features. Moreover, it complements the mechanism by adding a driver identification method which utilizes driving characteristics. It extracts a set of key fobs and driving traits. Driving features are inclusive of accelerator pedal positions, brake pedal positions and following distance. The introduced security layer employs machine learning techniques for identification ofa key fob signal follows the pattern of relayed signals. For better rate of detection ace-racy, a tenfold cross validation can be used. It limns various security features pertaining to the subject and also discusses CART algorithm. Based on experiments and evaluate- ton, it gives conclusive results post describing the testing environment which also works on real world data. The proposed solution has a relay attack detection accuracy rate of 99.8/100, and 81/100 accuracy rate for identification of legitimate drivers.

Table 1: A comparison of existing research (R1,R2,R3,R4,R5,R6,R7,R8)

Research Paper	Key Contributions	R1	R2	R3	R4	R5	R6	R7	R8
Inter Ve-hicular Communi-cation. [15]	Revocation protocol ofthe tamper-proof de-vice (RTPD)	YES	YES	YES	NO	YES	YES	YES	NO
Security in Vehicular Adhoc NETworks (VANETs). [14]	A System Model that identifies the most rel-evant communication aspects	YES	YES	YES	YES	YES	YES	YES	YES
The Secu-rity andPrivacy of Smart Ve-hicles. [7]	A smart vehicle's on-board instrumentation for supervising proto-col execution	NO	YES	YES	YES	YES	YES	NO	NO
ECPP: Efficient Condi- tional Privacy Preser-vation Protocol for Secure Vehicular Communi-cations. [9]	(ECPP) protocol for securing vehicular communications.	YES	YES	YES	NO	YES	YES	YES	YES
UAV-EmpoweredEdge Com-puting Environ-ment forCyber- Threat Detec-tion in Smart Ve-hicles. [6]	A System model us-ing a triple bloom fil-ter for tracking abnor-mal behaviour in real time and to keep a vigil on public vehicles	YES	NO	YES	YES	YES	YES	YES	YES

XVI. RESULT AND DISCUSSION

The proposed system tends to facilitate vehicle management, security, vigilance and administration. It is quite manifest that the smarts devices play a cardinal role in this undertaking and have been conducive at multiple steps of the process. The MCU, in the VTM, works well and majorly agglomerates the data and identifies the kind of requirement discreetly. It, quite efficiently, passes this on to the Management Hub for further processing and completion of task.

XVII. CONCLUSION

The illustrations above entail a comprehensive study on smart vehicles with their as- sorted attributes. They discuss V2X communications and their import in the ever tran-scending and enduring world of technology. They also throw light upon a sundry of advantages of Smart Vehicles and the challenges that impede their development and rife status. They undertake an imminent hurdle and propose a viable solution to resolve the shortcoming. The rife work tends to work on its limitations and is sanguine to incorporate more security attributes and mechanisms to ensure better safety of smart vehicles and to overcome hurdles that obstruct developments in the domain and aims to go hand in hand with the technological advancements in this field.

REFERENCES

1. Usman Ahmad, Hong Song, Awais Bilal, Mamoun Alazab, and Alireza Jolfaei. Securing smart vehicles from relay attacks using machine learning. *The Journal of Supercomputing*, 76(4):2665–2682, 2020.

2. Moayad Aloqaily, Safa Otoum, Ismaeel Al Ridhawi, and Yaser Jararweh. An in- trusion detection system for connected vehicles in smart cities. *Ad Hoc Networks*, 90:101842, 2019.
3. Thomas Arts, John Hughes, Ulf Norell, and Hans Svensson. Testing autosar soft-ware with quickcheck. In *2015 IEEE Eighth International Conference on Software Testing, Verification and Validation Workshops (ICSTW)*, pages 1–4. IEEE, 2015.
4. Faezeh Farivar, Mohammad Sayad Haghighi, Alireza Jolfaei, and Sheng Wen. On the security of networked control systems in smart vehicle and its adaptive cruise control. *IEEE Transactions on Intelligent Transportation Systems*, 2021.
5. Simon Fürst and Markus Bechter. Autosar for connected and autonomous vehicles: The autosar adaptive platform. In *2016 46th annual IEEE/IFIP international conference on Dependable Systems and Networks Workshop (DSN-W)*, pages 215–
6. 217. IEEE, 2016.
7. Sahil Garg, Amritpal Singh, Shalini Batra, Neeraj Kumar, and Laurence T Yang. Uav-empowered edge computing environment for cyber-threat detection in smart vehicles. *IEEE network*, 32(3):42–51, 2018.
8. Jean-Pierre Hubaux, Srdjan Capkun, and Jun Luo. The security and privacy of smart vehicles. *IEEE Security & Privacy*, 2(3):49–55, 2004.
9. Kuljeet Kaur, Sahil Garg, Georges Kaddoum, François Gagnon, and Syed Hassan Ahmed. Blockchain-based lightweight authentication mechanism for vehicular fog infrastructure. In *2019 IEEE International Conference on Communications Workshops (ICC Workshops)*, pages 1–6. IEEE, 2019.
10. Rongxing Lu, Xiaodong Lin, Haojin Zhu, P-H Ho, and Xuemin Shen. Ecpp: Ef- ficient conditional privacy preservation protocol for secure vehicular communica- tions. In *IEEE INFOCOM 2008-The 27th Conference on Computer Communica- tions*, pages 1229–1237. IEEE, 2008.
11. Silverio Martínez-Fernández, Claudia P Ayala, Xavier Franch, and Elisa Y Naka- gawa. A survey on the benefits and drawbacks of autosar. In *Proceedings of the First International Workshop on Automotive Software Architecture*, pages 19–26, 2015.
12. Chuka Oham, Regio A Michelin, Raja Jurdak, Salil S Kanhere, and Sanjay Jha.B-ferl: Blockchain based framework for securing smart vehicles. *Information Pro- cessing & Management*, 58(1):102426, 2021.
13. Bryan Parno and Adrian Perrig. Challenges in securing vehicular networks. In *Workshop on hot topics in networks (HotNets-IV)*, pages 1–6. Maryland, USA,2005.
14. F. Qu, Z. Wu, F. Wang, and W. Cho. A security and privacy review of vanets. *IEEE Transactions on Intelligent Transportation Systems*, 16(6):2985–2996, 2015.
15. Maxim Raya and Jean-Pierre Hubaux. Securing vehicular ad hoc networks. *Journal of computer security*, 15(1):39–68, 2007.
16. Maxim Raya, Panos Papadimitratos, and Jean-Pierre Hubaux. Securing vehicular communications. *IEEE wireless communications*, 13(5):8–15, 2006.

AUTHORS PROFILE

Varun Chopra, is a prospective computer science engineer. He is currently pursuing BTech. in Computer Science and Engineering with Specialization in Cyber Security and Digital Forensics from Vellore Institute of Technol- ogy (VIT), Bhopal, Madhya Pradesh. He is the Vice Chair of Association of Computing Machinery (ACM) Student Chapter at VIT. He also quite deservedly holds the positionof Head of Marketing for his department and has performed outstandingly well in the domain. His alacrity to learn and assiduity in his sedulous efforts justify his persevered nature. It's not amiss to surmise that not only is he a brilliant team player but also a terrific team leader. This topic kindles his innate interest towards the automobile industry and his proclivity in the domain of cyber security and enables him to concoct his interests and channelize his ebullient enthusiasm with propriety. His domains of interest include Vehicular Adhoc Networks, Machine Learning (ML), Artificial Intelligence (AI), Cyber Security, Digital Forensics, Internet of Things (IOT), Front-end Development, Management and Marketing. (varunchopra1730@gmail.com)