A LITERATURE REVIEW OF CYBER SECURITY ADOPTION IN AUTOMOBILE SECTOR: WITH SPECIAL REFERENCE TO CONNECTED AUTONOMOUS VEHICLES INDIAN CONTEXT

Prof. Pradnya Kashikar Research Scholar
MIT ADT University, Loni-Kalbhor, Pune- India
pradnyakashikar@gmail.com

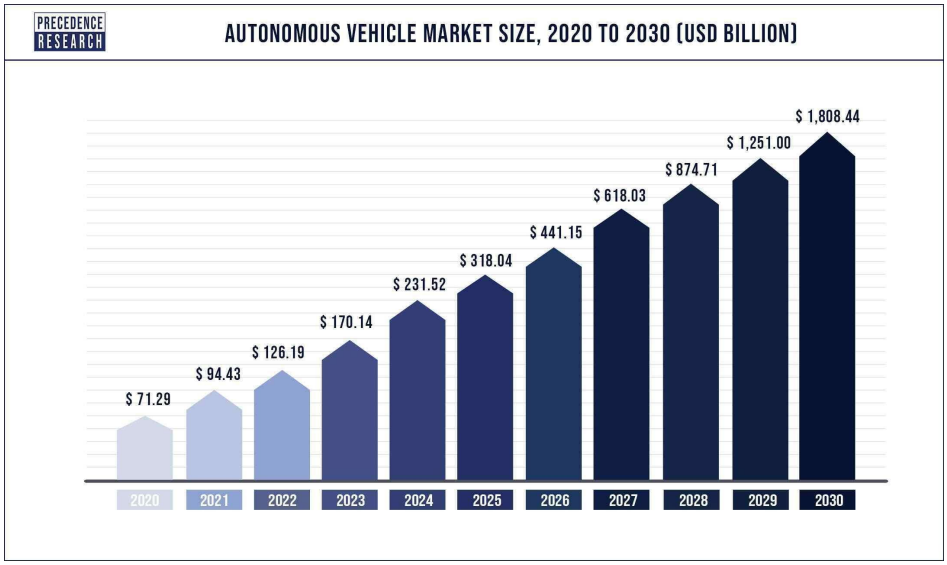
Dr. Samita Mahapatra Ph.D. Guide & Assistant Professor
MIT ADT University, Loni-Kalbhor, Pune- India
samita.mahapatra@mituniversity.edu.in

Dr. Rachana Shikhare Coach, Consultant and Associate
Samshodhan Trust, Pune-India
rachana.savita@gmail.com

ABSTRACT
Technology is progressing rapidly with the intent to have higher performance, scalability, and accuracy. Security which often used to take a back seat now has become prevalent in terms of maintaining integrity, confidentiality, and authentication of the information. An automobile sector is also adopting exponential and transformational technologies and vehicular networks. Cyber security in this sector is becoming challenging for the organizations to come up with optimal solutions. The growing emphasis on OEMs [Original Equipment Manufacturers] on autonomous driving and connected car systems have increased the risk of data breaching, thus augmenting the demand for cybersecurity solutions in the automotive market.
The researchers attempted to explore the connotation of decision models for cyber security implementation in automobile sector. The literature study undertaken revealed that; while positioning and fostering the technology-equipped integrated solutions for the cyber security implementation in the automobile sector, the decision models will play a vital role. The study of cyber challenges becomes more evident, predominantly when vehicular networks are used in autonomous vehicles. Furthermore, in the current scenario, the inevitable impact of cyber attacks, upcoming known and unidentified threats will imply the necessity of application of appropriate cyber security measures and controls is the major scope of the study.
Keywords: Cyber Security, Automobile Sector, Vehicular Networks, Autonomous Vehicles, Decision Models

Introduction

The automobile sector in India is one of the largest industries in the world although autonomous vehicular technology is recently evolving but with a promising future. An autonomous vehicle or a self-driving vehicle is self-operated, technology-controlled owing to its ability to sense its surrounding. Such vehicles use strategic decision models based on advanced exponential and transformational technologies. According to the study by McKinsey (2017), consumers across the globe have expressed interest in hybrid and electrified vehicles equipped using technological evolutions. The public consciousness is impacting the use of high-end vehicles with inbuilt features such as automation and digitization etc. The newer ways of mobility using AI and algorithm-led systems to drive innovations such as self-driving cars and drones are revolutionizing the automobile sector across the globe.



Graph 1: Autonomous vehicle market size
(Source: https://www.precedenceresearch.com/autonomous-vehicle-market)

The global autonomous vehicle market was estimated USD 94.43 billion in 2021 and it is projected to **hit around USD 1808.44 billion by 2030**, poised to grow at a compound annual growth rate **(CAGR) of 38.8% from 2021 to 2030. Autonomous vehicle market is being evolved gradually with technological advancement may be at a rapid pace, yet mass deployment not gained the desired momentum as on today.** (Rajasekhar and Jaswal, 2015).

A developing country like India, is witnessing a shift in mobility trends with technological innovations and the consumer expectations from automobile manufacturing companies. Nevertheless, in Indian context the application of automation and digitization in vehicular networks is gradually gearing up.

As modern vehicles can establish communication between the vehicles that is vehicle-to-vehicle and vehicle-to everything; automotive security threats must be well-thought-out and addressed. Vehicular networks are largely susceptible to cyberattacks such as eavesdropping, jamming, spoofing, man-in-the-middle attacks, compromising the security of control layer and navigation related aspects. (El-ewini, Sadatsharan, Selvaraj, Plathottam, Ranganathan, 2020)

To provide a better cyber security to autonomous vehicles, it is imperative to follow certain strategic process in terms of implementation as design decisions or decision models for strategy building or policy making. There are challenges as technology is evolving with an exponential speed and consumers are in a great demand of evolutionary autonomous vehicles. (Li and Liu, 2021). The world-wide organizations like Tesla Inc, Volkswagen AG, ABB, Magna International, General Motors, Uber, Waymo are some of the famous autonomous vehicles driving companies. In Indian context Tata motors, Mahindra & Mahindra, Hindustan Aeronautics Ltd. Are some of the key players working on the functionalities of autonomous vehicles and vehicular network in coordination with components makers such as Bosch, Continental, and Delphi. The start-up such as minus zero is coming up as first company building affordable fully Self Driving Cars in India.

Objectives of the study

1. To review the available secondary information related to the cyber security implementation and threats in vehicular networks.
2. To identify the challenges in making strategic decisions related to cyber security adoption in autonomous vehicles in Indian context.

Scope of the study

The chosen area of research being critical, sensitive, and complex, it is having vast scope beyond this paper leading to the doctoral research work undertaken.

The scope of this research paper has been kept limited for carrying out the literature review thereby, identifying the gaps and problem statement; that led to confirmation of the title of the research study. The geographical scope of the research work has been confined to the Indian context.

Literature Review

Cyber security adoption in autonomous vehicles is one of the upcoming research areas. A thorough literature review has been the strongest base considered by the researchers for exploring the context of the study undertaken. This being one of the key areas among various technological innovations in autonomous vehicles.

Cyber Security Adoption in Automobile sector

While positioning and fostering the technology-equipped integrated solutions for the cyber security implementation in the automobile sector, the decision models will play a vital role. Decision science utilizes a variety of tools which include models for decision-making. Establishing the criteria for evaluating and adopting appropriate and best alternatives will aid in implementation of the strategic decisions to be made for vehicular cyber security. The decision models based on hardware, software and services which are an integral part of upcoming automobiles will help in making technology management related strategic decisions and the impact can be studied. (Wang, Qin, Wang, Ji, Zhang, Wang, 2021).

Autonomous Vehicles in Indian context

Yadav, Kumar, Kumar, Yadav, (2022), proposed that; Indian automobile industry has historically been one of the prominent indicators of the growing economy along with the technological advancements. However, in context with autonomous vehicles and related networks developing globally at a rapid pace, the Indian counterpart has been a little sluggish. Wherein, until recently where Minus Zero got introduced as India's first startup, building affordable fully Self Driving Cars in the country in 2021. The new era of Autonomous vehicles is giving rise to a concept for an integration of self-driving vehicles into Industry 4.0 revolution leading to industry 5.0 technology evolution.

According to the study done by Technvaglobal about what is new for the Automotive Industry, India is gradually on the path of becoming a global automotive industry hub with more than 30 automotive R&D centres. As a result of the increase in R&D services in India, the connected car market is projected to grow exponentially by 2025. The in-vehicle connectivity and cyber security adoption in autonomous vehicles will become the default demand for car drivers in the coming years, which will lead to an increase in the number of connected cars to 250 million by 2022.

With the aggressive global automobile market rising, there has been a massive growth in the consumer market giving thrust for innovative solutions to the cyber threats in vehicular networks specific to self-driving vehicles. In this context, cyber security of such vehicles that are imitating human capabilities becomes inevitable.

Gupta, Iyer (2018) revealed that in India, the market for autonomous and connected vehicles is just coming into existence and beginning to display signs of future potential. Soon, most automobile manufacturers will have to consider the advanced features leading to embedding software in their vehicles to manage the complex system of hardware such as sensors, processors, and storage devices. It is important to develop a clear and time-driven strategy for embracing digitization, big data analytics, and connectivity to build and manage the integration of new technologies. Ensuring cyber security mechanisms for secure communication between connected vehicles is essential for the predicted growth in this sector.

Bimbraw (2015) investigated that Autonomous vehicles should be developed as efficient and practical vision guided vehicles. Indian Car buyers top the list when it comes to being open to increased vehicle connectivity. The research has claimed that 80% of Indian customers think that increased vehicle connectivity will be beneficial in the long-term. One of the largest car markets in the world, India ranks first in data collection related to connected vehicles.

Kim, Kim, Jeong, Park, and Kim (2021) deliberated that the Indian connected car market is expected to grow at a CAGR [Compound Annual Growth Rate] of 20% during the period 2020-2025. Since the connected car requires access to the internet for smooth functioning, many players are planning to launch their connected cars in India, and have collaborated with telecom companies to make their connected cars a reality in the Indian market. India is targeting of becoming an all-electric nation by 2030, where a mass production of connected cars is being considered. The Indian Government has mandated the presence of connected services for public transport that came into effect in April 2018. Industry 4.0 revolution leading to Industry 5.0 has expanded the possibilities of digital transformation in automotive and Research and Development is becoming an important aspect for the hybrid and electric vehicles, connected as well as autonomous cars.

Bernardini, Asghar, and Crispo (2017) explored that, the digitized world today, which is established on network of internet-enabled systems, is vulnerable to the risk of losing data integrity in the cyberspace. As a strong

protective shield, Cyber threat management demands an integrated cyber risk identification and management approach to address and mitigate the cyber security risks and threats in the cyberspace. Configuring an effective threat defence mechanism also deals with data acquisition and leveraging automation. Also, depending on the domain in which organization is working, relevant analytics and cross correlation across the vast domains of Cyber security can be analysed in context to technological advancements. Since it is nearly impossible to guarantee that there are no logic errors in any complex computing system, every vehicle is likely to contain at least some vulnerabilities that a skilled attacker may be able to discover and exploit. Based on the deterministic nature of these systems, understanding the possible permutations in advance, and blocking any instruction calls that were not projected can prevent in-memory attacks.

Martínez-Díaz, Soriguera (2018) studied that, as managing upcoming threats dynamically have become very much challenging, data analytics and algorithms helps in generating better solutions to provide safe communication and connected environment in the autonomous vehicles. Identifying appropriate decision models aligning them for the implementation of cyber security solutions, in the context of cyber threat management thereby bridging the gaps between challenges faced in cyber space in context with autonomous vehicles and vehicular networks in an automobile sector. and implementable realistic solutions.

Li, Shu, Chen, and Cao (2021) proposed that all organisation's strategic-level decision making processes are highly based on its domain specific environment. It became imperative to address the ever-changing cyber security challenges in the context of the business environment as well as technological advancements in an automobile sector. The alternatives available in decision models which can assist in provide secure communication among the autonomous vehicles play an important role in providing sustainable growth in these perspectives to optimally utilise and align decision making models in adopting cyber security solutions, there is a need to consider relevant tools and techniques for making effective decision making; in the context of computer security, data management, also legal and risk management. The researchers have further attempted to explore how decision-making models can be an enabler in identifying challenges and solutions in implementing effective cyber security and in building better and cyber secure infrastructures in autonomous vehicles. To sustain in this hyper competitive and data sensitive digital era, securing wealth of data gets vital precedence, using decision science Capabilities through advanced proven analytics have acknowledged the case.

The diagram below depicts the key touchpoints for connected car security. The future of mobility systems will majorly include the infotainment systems, integrated vehicle security, connected vehicles services, vehicle communication busses and use of mobile applications, firmware, and wireless communications.

The ever-expanding cyber security issues must be addressed which can further cause availability, integrity and confidentiality problems leading to vulnerabilities and cyber attacks on vehicular networks.

Figure 1 : Connected car security touchpoints
Image source: Deloitte analysis (https://www2.deloitte.com)

Following are the examples of possible cyber threats in autonomous vehicles:

1. **Insider's threats**
   Attacker uses their authorized access to an organization's data and resources to impair the vehicle's information, networks, equipment, and systems. Insider's threats include unauthorized information disclosure, industrial espionage, degradation of resources, sabotage, introducing malware or ransomware attacks and cyber terrorism, etc. Connected and self-driving vehicles are more susceptible to such kind of attacks. (Masike, 2023).
2. **Dumpster diving for data**
   Organizations are not keen about discarding the documents and other media without shredding or properly destroying them. A sensitive information can be retrieved from searching through such discarded dump which can be used to carry out attacks such as malicious attacks, identity theft and phishing in vehicular networks. (Dibaei, Zheng, Jiang, Abbas, Liu, Zhang, Xiang Yu, 2020).
3. **Hacking into manufacturer-to-vehicle communications**
   Hackers can break into the vehicles and using Remote Code Execution (RCE), a vehicle can be accessed from a remote server by executing arbitrary commands by the attacker. Cloning and Denial of Service (DoS) attacks are also possible with the help of intruding into manufacturer-to-vehicle communications. (Bharati, Podder, Mondal, Md. Robiul, 2020)
4. **Hijacking vehicle controls and sensors**
   In this, the hackers can acquire unauthorised access to the car with the help of, Bluetooth channels, USB, monitoring systems, navigation consoles and wireless and cellular signals. The main concern is a huge data can be collected by the vehicle while in motion using GPS, sensors, cameras, radars, and the overall system components. (Naughton, 2018).
5. **Distributed Denial of Service**
   In Vehicular Networks, there are many vehicles communicating with each other. The attackers can initiate attacks the victim from different locations and at different times. As a result, the victim cannot access the resources of the vehicular network. Such kinds of attack difficult to detect. (Zwilling, Klien, Lesjak, and Wiechetek, Sklodowska, 2022)
6. **Jamming**
   In context with the wireless communications and wireless networks, the intentional or even unintentional Wireless Radio Frequency (RF) jamming causes serious threats in Vehicular ad-hoc networks (VANET). Modern vehicular networks having safety-critical applications are vulnerable to such jamming attacks. (Kim, Chung, 2021)

7. **Impersonation**
   A false information can be injected in order to mislead the target vehicles or impersonation attack can be implemented by tampering the on-board unit. Attackers may collect the confidential information about the vehicle, track the vehicle's location through compromised navigation systems and may record the messages and communication between the target vehicle and the other connected vehicles. By divulging the authentication details of a vehicle, the authentication information can be used to access classified information or even as verification or validation with other parties. Attackers could also impersonate other vehicles to gain an advantage. (Dibaei, Zheng, Jiang, Abbas, Liu, Zhang, Xiang Yu, 2020).
8. **Black hole**
   This attack severely affects the availability attribute of CIA triad (Confidentiality, Integrity, and Availability Triad) in which data packets as well as the control packets are dropped by the malicious vehicle. This may prevent communication between vehicles entirely and can significantly reduce the accessibility of Vehicular Ad Hoc Networks (VANETs). We propose a solution to help secure these networks against this vulnerability by detecting the attack and removing the malicious node from the network. Dropping of data packets has a stern impact on a security, interoperability and performance of the vehicular networks which may lead to accidents, traffic jams and fatalities. (Tobin, Thorpe, Murphy, 2017)
9. **Masquerading**
   It is nothing but; by using other vehicle's identity. the attacker pretends to be another vehicle to carry out the frauds and malicious activities. For example, attacker's car may masquerade as a Police vehicle to trick with other vehicle to stop the vehicle or slow down their speed. (Upadhyaya, Shah, 2018)
10. **Global Positioning System Spoofing**
    In the self-driving vehicles, the navigation through the Global Positioning System (GPS) must be secure. In case, when the security mechanisms, cryptographic controls mechanisms and authentication techniques are not appropriately developed and implemented, the satellite signals can be easily replicated and GPS spoofing attacks can be launched by the attackers. With the help of such attacks, the spoofers can manipulate the navigation data and cheat or misguide the vehicle. (Krayani, Barabino, Marcenaro, Regazzoni, 2023).
11. **Threats in Protocol Layer of VANETs**
    The network and the transport layer in case of data transmission and communication may suffer from inappropriate routing and intentional delays and man-in-the-middle attacks in VANETs. The vehicle's location, network topology, vehicle's velocity, and distance between two or more connected vehicles may affect the QoS (Quality of Service). Stealing od bandwidth allocated for the communication between the autonomous vehicles may lead to delay in delivering the messages as well as congestion and collision resulting in environmental impact. The cyber attacks in the protocol layers of VANETS may cause problems related to mobility, security, authentication, network management and scalability, etc. (Kugali , Kadadevar, 2020).

The ever-dynamic technological advancements globally are fast paced and so are the new challenges that threaten the precious knowledge becoming more susceptible to cyber attacks. Thus, such vulnerable data and network communications would need stringent mechanism to address and resolve not only the anomalies but as well defend the cyber-attacks. Traditional model may form a basis of any solution that is being proposed. Newer and better routes need to be evaluated and verified complimenting the legacy systems; to address the invading threats to knowledge in the cyber space.

Gaps Analysis and problem description

Till date, there have been many decision models identified, proposed, and implemented in various sectors applying various business logic. Thereby, facilitating decision making process through some workflow or pattern or model. In context of cyber security implementation as well, such decision-making models has been already proposed (Aitor, 2019).

For the first time in a century, the nature of how we use motor vehicles is on the verge of a

fundamental technological change. In the coming decade, an increasing number of travelers will go from; directly manipulating vehicle control inputs for accelerating, braking, and steering to simply entering a destination and sitting back for the ride. These people using connected and automated vehicles beforehand, must have assurance about their vehicles being adequately protected from malicious actors, trying to do physical or financial harm via cyber-attacks. (Abuelsamid, 2016).

One of the primary goals in adopting new technologies such as connected vehicles and autonomy is; to drive the fatality rate toward zero. However, that can only happen if those technologies work as intended and malicious

actors are prevented from tampering with the systems. Unfortunately, it is impossible to guarantee that any complex code base is free of logical errors, and according to researcher's observations; there is a significant probability that some number of those errors will lead to security vulnerabilities. With hundreds of millions of connected and automated vehicles expected to be on the road in the coming decades, the likelihood of attacks from hackers, stalkers, vandals, intruders, thieves, and those with political motivations; that may exploit those security vulnerabilities, for mass attacks increase exponentially.

The cyber security challenges in the secure communication modes in autonomous vehicles require greater level of exploration in terms of powerful decision models supporting technology adoption. In a sector such as an automobile and a subdomain of autonomous vehicles, the functionality is focused but cyber security takes a backseat. So, there is a need to focus on adoption of cyber security features which specifically in automobile sector is not done extensively. (Gekker , Hind, 2019)

Finally, data treatment must also be regulated. Security and privacy are the main goals, while ensuring the data sharing required by a cooperative driving environment. (Martínez-Díaz, Soriguera, 2018).

Based on literature review, gap analysis is being done, thereby arriving to the problem statement based on which the title of the research study has been evolved and justified. Furthermore, approaches towards designing and implementing algorithms for selecting the appropriate strategic decision model used in automobile sector are also being explored.

In a swiftly changing world, security of the vehicular network from the potential cyber attacks and the entire ecosystem of mobility is quite challenging as the stakes are very high and so is the complexity. The consumers are cautiously approaching towards the prospect of self-driving vehicles though the automakers and information technology companies are pushing themselves to keep themselves ahead of the hackers and other adversaries. In Indian context as well as in general; the investment in self-driving vehicles will be lucrative only when such vehicles will function securely. The thoughtfully developed standards can be enforced, encryption can be implemented to protect the integrity and protocols for secure development of critical vehicle systems and related networks can be implemented with caution.

Conclusion

The auto industry is among the most competitive business sectors in the world, with very little barrier to prevent customers from switching brands. Customers in the highest volume segments of the industry are also very price sensitive, and costs for manufacturers are rising continuously; as they struggle to meet ever stricter regulatory requirements while developing new technologies. It is important to focus with an exploratory approach to know the impact on both current and future products. Protecting vehicular infrastructures and human beings will require holistic approaches to design, implementation, and response when the unexpected incidences take place. The researchers attempt to check on with the awareness of the consumers with respect to autonomous vehicles, so that later, the empirical research work is proposed to be carried out.

As per the literature review carried out by researchers, fully self-driving vehicles is certainly not just a trend but, a promising aggressive automobile market in Indian context. It has been well received in the global market since a decade, consumer market in India is still under latent stage, albeit with prospective demand. Meanwhile, the time needed to overcome the technological challenges must be used, to design cooperative traffic management strategies which will guarantee success upon their introduction. Also, special attention must be paid to legal and ethical issues, which will determine when the society is ready for the future autonomous driving environment.

The research work being multidisciplinary, it was interesting to review articles, reports, published analytical reports, research papers, official websites of car making companies in global as well as Indian market. Moreover, there were thought provoking informal discussions, with the experts associated with multiple focal points coming under the purview of the area of research work. These deliberations endorsed the scope, objective and the purpose of the research undertaken and channelized it. This facilitated to emphasize the fact about criticality of cyber security implementation and threats in vehicular network. It further highlighted the need to explore various strategic decision models; that are available specifically in Indian context, to support the and come up with the proposed appropriate strategic decision model.

Autonomous Vehicles could contribute to make future mobility more efficient, safer, cleaner, and more inclusive with, the shield of optimal and innovative cyber security solutions.

References

Abuelsamid, S., (2016), A research report on Autonomous Automotive Cybersecurity

The Need to Protect Automated and Connected Vehicles, Navigant Research, Research Report Commissioned by Karamba Security Published 3Q 2016.

Aitor, C V., (2019), THESIS DOCTORAL Decision Models for Cybersecurity Risk Analysis, The Instituto de Ciencias Matemáticas (ICMAT CSIC – Institute of Mathematical Sciences, Consejo Superior de Investigaciones Científicas), https://www.researchgate.net/publication/337334597_Decision_Models_for_Cybersecurity_Risk_Analysis.

Asghar, B C., Crispo, M R. & Bruno, (2017), Security and privacy in vehicular communications: challenges and opportunities Veh. Commun., Volume: 10 Publisher: Elsevier ISSN: 2214-2096.

Bharati, S., Podder, P., Mondal, M., Md. Robiul, R., (2020); Threats and Countermeasures of Cyber Security in Direct and Remote Vehicle Communication Systems, Journal of Information Assurance and Security. ISSN 1554-1010 Volume 15 (2020) pp. 153-164 © MIR Labs, www.mirlabs.net/jias/index.html

Bimbraw, K., (2015), Autonomous Cars: Past, Present and Future: A Review of the Developments in the Last Century, the Present Scenario, and the Expected Future of Autonomous Vehicle Technology, ICINCO2015 - 12th International Conference on Informatics in Control, Automation and Robotics, January 2015.

Dibaei, M., Zheng, X., Jiang, K., Abbas, R., Liu, S., Zhang, Y., Xiang, Y., Yu, S., (2020), Attacks and defences on intelligent connected vehicles: a survey Mahdi Dibaei a, Digital Communications and Networks 6 (2020) 399–421.

El-ewini, Z., Sadatsharan, K., Selvaraj, D., Plathottam, S J. & Ranganathan, P., (2020), Cybersecurity challenges in vehicular communications, Vehicular Communications, Volume 23, June 2020, 100214.

Gekker, A., Hind, S., (2019); Infrastructural surveillance, New Media & Society 22(8):146144481987942; New Media & Society 22(8):146144481987942; SAGE Publications, October 2019.

Gupta, S., Iyer, B., (2018), The future of mobility in India's passenger-vehicle market, © 1996-2023 McKinsey & Company, July 2018.

Kim, H., Chung, J., (2021); VANET Jamming and Adversarial Attack Defense for Autonomous Vehicle Safety; Computers, Materials & Continua DOI:10.32604/cmc.2022.023073; October 2021.

Kim, K., Kim J S., Jeong S., Park, J H, Kim, H K., (2021), Cybersecurity for autonomous vehicles: Review of attacks and defense, Computers & Security Volume 103, April 2021, 102150.

Krayani, A., Barabino, G., Marcenaro, L., Regazzoni, C S., (2023), Integrated Sensing and Communication for Joint GPS Spoofing and Jamming Detection in Vehicular V2X Networks, Conference: IEEE Wireless Communications and Networking Conference (2023 IEEE WCNC), Scotland, UK.

Kugali, S., Kadadevar, S., (2020), INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) - Volume 09, Issue 06 (June 2020) ISSN (Online) : 2278-0181, DOI: 10.17577/IJERTV9IS060784, January 2020.

Li S., Shu, K., Chen, C., & Cao, D., (2021), Planning and Decision-making for Connected Autonomous Vehicles at Road Intersections: A Review, Chinese Journal of Mechanical Engineering volume 34, Article number: 133, December 2021.

Li, Y., Liu, Q., 2021, Energy Reports, Volume 7, (2021), Pages 8176-8186 - A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments, November 2021.

Masike, M., Management of enterprise cyber security: A review of ISO/IEC 27001:2022 2023 International Conference on Cyber Management and Engineering (CyMaEn); January 2023

Martínez-Díaz, M., Soriguera, F., (2018), Autonomous vehicles: theoretical and practical challenges; January 2018; www.sciencedirect.com Transportation Research Procedia 33 (2018) 275–282.

Naughton, K., (2018). Just how safe is driverless car technology, really? Bloomberg News. https://www.bloomberg.com/asia

Rajasekhar, M.V., Jaswal, A., (2015), Autonomous vehicles: The future of automobiles, IEEE International Transportation Electrification Conference (ITEC) DOI: 10.1109/ITEC-India.2015.7386874.

Tobin, J., Thorpe, C., Murphy, L., (2017), An Approach to *Mitigate Black Hole Attacks* on Vehicular Wireless Networks, ieeexplore.ieee.org/document/8108460/.

Upadhyaya, A., Shah J.S.; Attacks on VANET Security, (2018); International Journal of Computer Engineering & Technology (IJCET) Volume 9, Issue 1, Jan-Feb 2018; Print: 0976-6367 and ISSN *Online: 0976–6375.*

Yadav, S., Kumar, N., Kumar, V., Yadav, D. (2022), AUTONOMOUS VEHICLE IN INDIAN CONTEXT: A REVIEW, International Journal of Novel Research and Development; July 2022, ISSN: 2456-4184.

Wang, Y., Qin, H., Wang, Y., Ji, H., Zhang, Y., Wang, J, (2021), A Systematic Risk Assessment Framework of Automotive Cybersecurity, Automotive Innovation; March 2021.

Zwilling, M. Klien, G. Lesjak, D and Wiechetek, L., Sklodowska M., (2022), Cyber Security Awareness, Knowledge, and Behavior: A Comparative Study Journal of Computer Information Systems 62(1):82-97; January 2022.

