VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

NETWORK AND INFORMATION SECURITY (ITE4001)

DIGITAL ASSIGNMENT

JAIVIK CHAUHAN - 19BIT0039

SLOT – B1+TB1

Under The Guidance :

ASWANI KUMAR CHERUKURI

NETWORK SECURITY OF CONNECTED AND AUTONOMOUS VEHICLES

ABSTRACT :

The vehicles are increasingly connected, automated and computer-like, with the ability to synchronize mobile phones, provide passengers with the latest navigation updates, and communicate safety information to other vehicles and surrounding infrastructure. They too are able to drive on their own without human intervention. This kind of vehicles are known as - CAVs (connected and autonomous vehicles) .They are able to understand the environment, travel, navigation and behavior responsibly without the input of a person who at the same time has communication functions that make them efficient, cooperative, informative and integrated. However, with the increasing level of connectivity and automation, malicious users/hackers are easily able to use various types of attacks, which threaten the safety of CAVs.

This new generation of vehicles can have over 100 million lines of code in their modules with large number of messages being exchanged among vehicles. These vehicles have multiple connection points to the Internet. Bad code, misconfiguration and Internet exposure makes these vehicles vulnerable to different kind of malicious attacks.

So, study and risk analysis of CAV's Network and Communication Security is very important as vulnerabilities in these vehicles can be damaging to quality of life and human safety.

KEYWORD :

Auto industry; Attack; Connected and autonomous vehicles; Cyber-attacks; Cyber security; Privacy; Safety; Smart mobility; Standards; Vehicle safety;

THEME :

Security and threat analysis related to Connected and Autonomous Vehicles.

INTRODUCTION :

The automotive industry is a fast-growing and ever-emerging industry, integrating and embracing IT networks, computers and, information and communication technology (ICT) systems in general. Connected and Autonomous Vehicles (CAVs) are future of transportation but it is a technology, still in its infancy, with the potential, if used responsibly, it can transform urban landscapes and can establish the era of smart city [5].

source: https://gowlingwlg.com/

The global market for CAVs is becoming one of the largest markets in the world. It is expected to reach $7 trillion by 2050. In addition, many large car manufacturers and high-tech giants are rushing to bring active CAVs to market [3].

Specifically: from an economic point of view, CAVs can reduce energy costs , improve fuel efficiency, create more productive periods; From a social point of view, CAVs are marketed because of their increased risk and safety capabilities, which could potentially reduce traffic congestion, a beneficial impact on public health and well-being , travel behavioral improvement, increased travel equity and accessibility; From an environmental point of view, CAVs can help reduce emissions and air pollution, reduce energy consumption, and improve fuel consumption, preventing environmental degradation and reducing noise disturbance [5] .

As vehicles become more technologically advanced and connected, the threatening environment and the potential for cyber-attacks become bigger and more natural. For the widespread deployment of CAVs in future transportation systems, the potential cyber-security risks and vulnerabilities need to be addressed [3]. The attacks on self-driving cars can allow attackers to control, manipulate, or suppress the information being routed in the network. This control over the information of the users can be used for their benefit or completely disrupt the network [4].

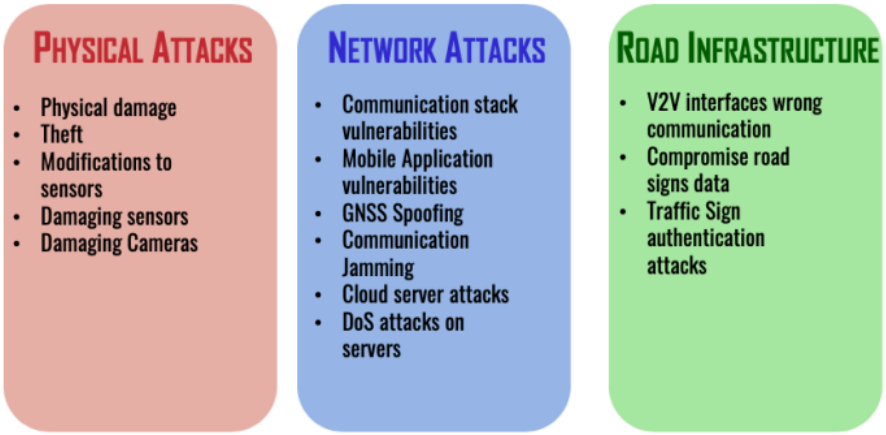
source: towardsdatascience.com

Considerable research efforts have been carried out for identifying vulnerabilities in CAVs, recommending potential mitigation techniques, and highlighting the potential impacts of cyberattacks on CAVs and related infrastructures.

The main aim of this review/survey paper is to:

- identify various attacks, vulnerabilities and cyber-risks to CAVs.
- find appropriate mitigation and defense solutions.
- conduct an analysis of the risk through risk assessment.

Also, I would present some several challenges and open problems that can be considered as future research directions.



VARIOUS ATTACK types

source: [35]

In this survey paper, I have focused more on the connected feature or the network part of CAVs (V2X - vehicle to everything attacks) as connected feature is relatively new and less research has been done on it.

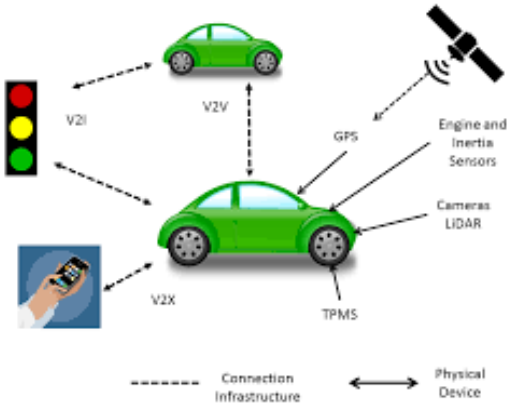
The paper is structured as follows. Section 2 introduces technical background on CAVs (what it is and basic information) and its cyber-threats and V2X (vehicle to everything communication) and then in Section 3 I have done analyzed some papers and done their literature review. In Section 4, the potential cyber-attacks are listed. Mitigation methods of cyber security attacks on CAVs are then recommended in Section 5. Section 6 has summary of different attacks and their risk assessment is done. Section 7 summarizes the paper and discusses the future challenges that could be used for CAV cyber security research.

BACKGROUND :

CVs, AVs and CAVs :

A CAV is not synonymous to a Connected Vehicle (CV) or an Autonomous Vehicle (AV); these are different.

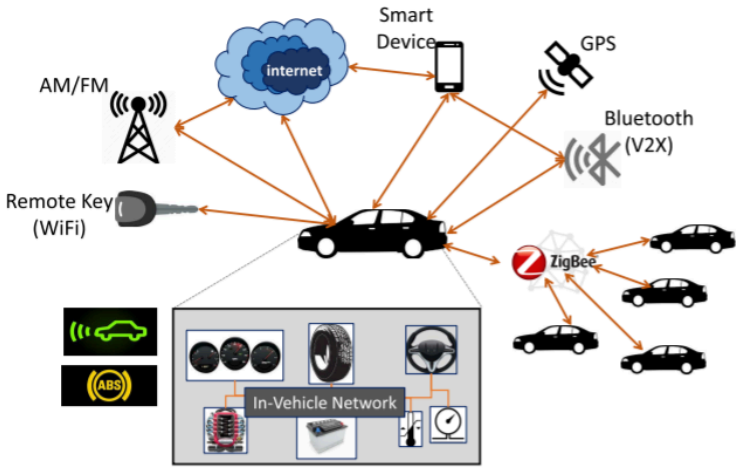
A CV is a vehicle that can communicate and exchange information wirelessly with other vehicles, external networks and infrastructure through Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), Vehicle-to-Network (V2N) and Vehicle-to -Everything (V2X) technologies [5]. While AVs are vehicles that are capable of driving themselves without human intervention.



source: http://eprints.hud.ac.uk/

If a vehicle is both connected and autonomous, then it can be classified as a CAV. Therefore, CAV is any vehicle able to understand its surroundings, move, navigate and behave responsibly without human input which at the same time has connectivity functions enabling it to be proactive, cooperative, well-informed and coordinated [34].

CAVs not only have highly connected internal components but also are highly connected to their external environments via communication networks.



source: [24]

A CAV consists of many sensing components such as laser, radar, camera, Global Positioning System (GPS), and light detection and ranging (LiDAR) (Wyglinski et al., 2013), as well as their connection mechanisms such as cellular connection, Bluetooth, Wireless Access in Vehicular Environments (WAVE) and Wi-Fi, etc. And these components open door for malicious people to exploit vulnerability and bring down the network security of CAVs.

Cyber-threats, vulnerabilities to CAVs :

source: [3]

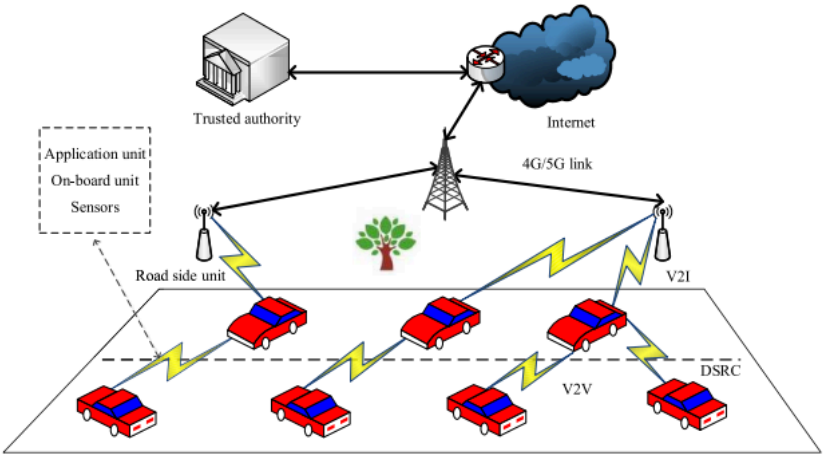
Threats can be Internal (attacking an internal vehicle systems and network communication) or External (hacking through devices, systems, applications and other technologies connected to the vehicle; for example, remote diagnostic programs, third-party applications). Attacker can take

complete or minor but important car controls such as automotive systems, motor sensor technology, and navigation systems infrastructure or unauthorized access to sensitive personal information. [22].

In the network level attacks, the attacker may target the vehicle-to-vehicle (V2V) communication network, the vehicle-to-interface (V2I) network, and interface-to-interface (I2I) network, all of which pose a significant threat to the vehicle and its ecosystem [35].

V2X :

The vehicle to everything (V2X) network enables data transfer between connected vehicles, other vehicles and CAV's infrastructure. V2X (Vehicle-to-Everything) includes V2V, V2I, and communications between vehicles and other entities such as cloud database or pedestrians. This communication is used to prevent road accidents with vulnerable pedestrians, cyclists and motorcyclists [25]. Various adversary uses this type of communication to identify network access points. Communication channels between car and external devices, for example smartphones, are established via Wi-Fi, Bluetooth, Near Field Communication (NFC) and a global mobile communication system. Once the vehicles are connected to the communication channels, they are vulnerable to network attacks. Then, the attacker may target the vehicle-to-vehicle (V2V) communication network, the vehicle-to-interface (V2I) network, all of which pose a significant threat to the vehicle as well as to its ecosystem [35].



source: [3]

LITERATURE REVIEW:

Considerable research efforts have been carried out for identifying vulnerabilities in CAVs, recommending potential mitigation techniques, and highlighting the potential impacts of cyberattacks on CAVs.

Here, is literature summary of few papers.

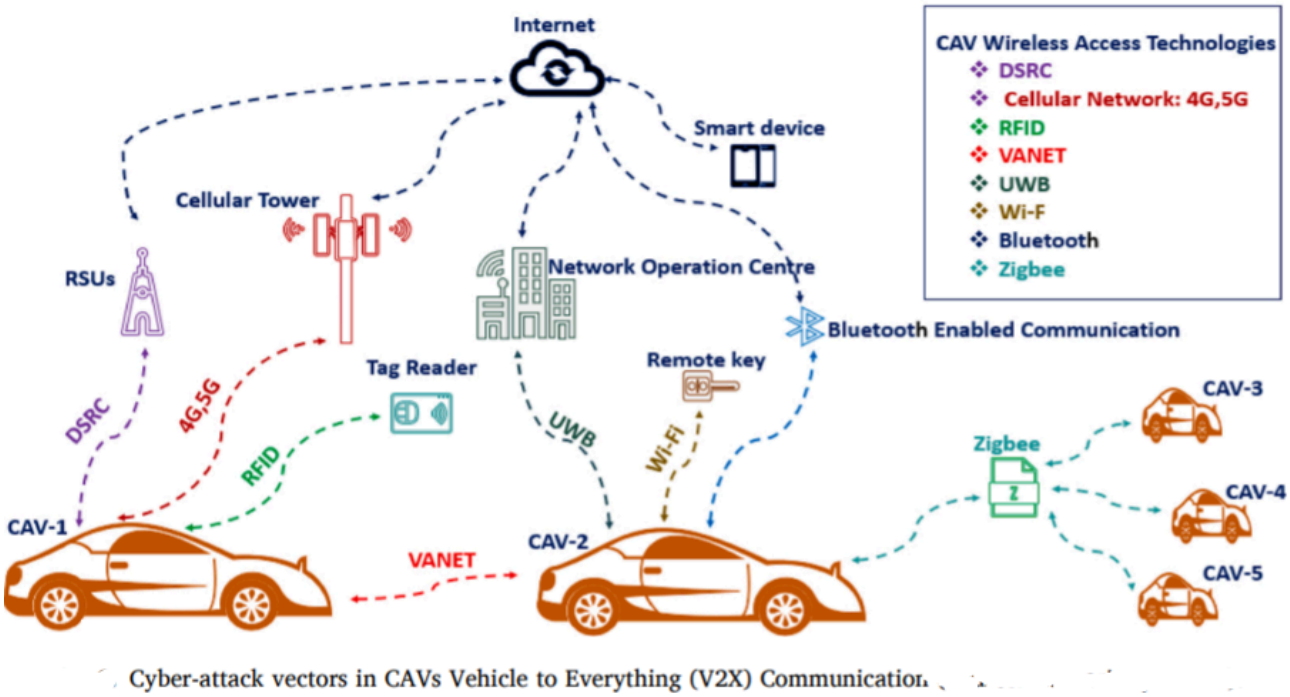
PAPERS	HIGHLIGHTED ISSUES / SUMMARY
A Survey on Cyber- Security of Connected and Autonomous Vehicles (CAVs)	In this paper, they classified the existing cyber-security risks and vulnerabilities into in-vehicle network attack Cyber-security in the environment of CAVs, introducing Existing cyber- security risks and vulnerabilities using surveys, explaining several related security and safety standards for CAVs
Cybersecurity challenges in vehicular communications	In this paper, authors have proposed 3 layer framework of autonomous and connected vehicles, threats to vehicular communication and intra-vehicle security, potential countermeasures for various threats in V2X.
Research Challenges and Security Threats to AI-Driven 5G Virtual Emotion Application s using Autonomous Vehicles, Drones and Smart Devices	This paper has Design of and AI-driven virtual emotion system in 5G environments consisting of 5G- enabled autonomous vehicles, smart UAVs, and smart devices, and It also highlights the security threats and issues caused by AI applicability.
A survey on security attacks and defense techniques for connected and autonomous vehicles	This survey paper attempts to classify attack models and defense strategies based on their characteristic without diving into technical aspects of CAVs.
Impact of cyber-attack on the wireless communication technologies used in an ITS	Presents recent and significant cybersecurity is sues affecting many areas of wireless communication networks used in VANET and ITS. The cybersecurity resilience of a futuristic VANET/ITS model is also estimated in this paper.
Safety failures and security attacks on autonomous vehicles	This paper highlights the studies that focus on the safety failures and security attacks of an autonomous vehicle and their mitigation solutions.
Review and classification of automotive security attacks	Paper categorizes security attacks on CAVs using a new classification taxonomy that can represent attacks in a better way for the concept of development and testing an automotive system.

Attacks on Self-Driving Cars and Their Countermeasures:	The paper discusses the recent attacks that have been reported/demonstrated on self-driving cars, the adopted or possible mitigation approaches, and most importantly highlights techniques proposed to ensure safe and resilient operation of CAVs even when a vehicle is currently under attack. This paper also presents government projects and initiatives for preventing vehicular networks from cyber-attacks The paper also gives future research directions to combat security vulnerabilities.

Also, I have a risk analysis of attacks on analysis part. It too has inputs from different research/survey paper.

SECURITY ATTACKS:

Since, I am focusing on network part of CAVs , I will identifying different attacks on V2X,V2I,V2V networks.



source: [10]

1) DoS attacks:

DoS attacks occur when an attacker blocks the entire communication channel with interfering signals. The attacker installs useless messages or creates certain problems in network nodes. Thus, real users do not have access to network resources. Correct messages cannot reach their destination. DoS attacks can cause delays and interfere with the recipient's response. In the case of CAVs, certain delays may affect the driving safety of the vehicle. Even one second can cause or avoid an accident. Moreover, the response time response is relatively high [3]. Also, this is attack would not cause information leakage but might cause physical damage especially in the rural area, where the V2V communication is the main data source for vehicle planning [6]. DoS attacks are dangerous and fatal to CAVs.

2) REPLAY attacks:

In a replay attack, the attacker records and retrieves the pre-valid packets over time. It usually occurs in a network or transport layer. It may confuse the authorities, confuse all roads, or damage the safety of traffic. In order to impersonate a legitimate car or RSU, playback attacks often occur in other authorizations and key agreement protocols [3].

3) Impersonation Attacks:

Every vehicle has an unique identification, which can help to recognize the vehicle and the messages. Impersonation attacks are implemented by using another identity or a fake identity. If the attackers send fake messages, the target vehicle would take wrong reactions. In addition, if the target vehicle trusts the fake message, it may respond to the attacker with private information. There are two kinds of impersonation attacks, namely node impersonation attacks and sybil attacks. In the node impersonation attacks, a single identity is spoofed at a time. Different identities are spoofed simultaneously in the sybil attacks. In addition, the sybil adversary can carry out several malicious operations, such as sending fake messages, spreading modified received messages, and dropping critical messages.

4) Eavesdropping Attacks:

The attack is done through sniffing the wireless medium. the attack is also known as a secret attack. In this attack, the adversary monitors network traffic and current victim positions and activities silently. After that, the attacker can collect the secret information of the CAVs. The difficulty in recognizing this attack is that the victim is not conscious of it. There is no direct impact on the network.

5) Data Falsification Attacks:

In attack, the adversary can send or broadcast false information and safety alerts. Message tampering, suppression, fabrication, and alteration may produce the fake message The Attack can effectively disrupt route routes, cause heavy traffic congestion, increase travel time, and resulted in unequal use of mobility resources in transport-based cyber-physical systems.

6) Routing Attacks:

Routing attacks exploit the drawback and vulnerability of routing protocols. In these attacks, the adversary can disturb the normal routing process or drop passing packets. The adversary captures packets at a location. Then, they are tunneled to another location. Routing attacks include black hole attacks , grey hole attacks , and wormhole attacks [3].

7) Infrastructure-Sign Change Attack:

This is one kind of V2I communications attack. Transport infrastructure signs help vehicles move, find, or control speed. CAVs can 'read' the symbol and perform related actions. If the attackers change the infrastructure signs such as a road sign, that will lead the vehicle in the wrong direction. In addition, if too many signs are intentionally altered, they can cause traffic congestion or traffic congestion. However, this attack will not cause information leakage. The combined severity of this attack is medium [6].

8) Attack on Cloud ID dataset and Cloud real-time traffic dataset (V2X communication):

Authority is essential for a CAV network. Each CAV will be given a Unique ID as an electronic plate. To ensure the reliability of the connection, only information from trusted CAVs from database can be accepted. All communications and information are based on authorization from the CAV cloud. If attacker infilterates the cloud and changes its configuration, then whole database would get disrupted and the CAV ecosystem will stop working. If he/she gets to know about traffic dataset, then he/she can create havoc through traffic congestion and accidents.

Similarly, If the attackers inject fake messages or modify messages, all the vehicles in the cloud database would receive wrong information. Also, the attackers could also access valuable information in the dataset.

9) Password and Key Attacks:

In this kind of attacks, attack is carried out until the system is compromised. These attacks may be categorized into three classes, namely dictionary attacks, rainbow table attacks, and brute force attacks. In the dictionary one, the adversary uses a listing of words to crack the password repeatedly. Other two forms of attacks are comparable with dictionary attacks. However, in the rainbow table attack, the adversary uses a list of precomputed hashes, which are computed from all the viable passwords and the given algorithm. The brute force one can perceive non-dictionary phrases by using operating via all of the alpha-numeric combos [3].

DEFENCE METHODS:

1) Against DoS Attacks:

DoS attacks are difficult to correct although it can be detected. Early detection will help to prevent an attack or warn the driver to take effective action. To resist DoS attacks, there are some strategies, including sliding mode and adaptive estimation, bandwidth and entropy [36], and similarity of sliding windows [37].

A real-time mechanism, which includes a set of viewers that are designed by the usage of sliding mode and adaptive estimation theory, can be used to detect DoS attacks, and estimate the effect of these attacks on the connected vehicle system. Using port-hopping mechanism, researchers have designed a simple and effective defense mechanism, which has the advantage that the detection and filtering out of malicious packets can be implemented without any change in the existing protocol. Based on the usage of bandwidth and entropy [36], authors have proposed an algorithm for the detection of DoS attacks in vehicular networks and also proposed a packet detection algorithm that can be used for preventing DoS attacks.

2) Against Replay attacks:

To combat replay attacks, famous defense strategies include noisy control signal method and cross correlator [38], reset controller [39], and techniques of timestamping and XOR encoding [40].

In noisy control signal method and cross correlator [38], author used a decentralized diagnosis algorithm to detect the replay attacks for a cooperative adaptive cruise control CAVs system. Xu et al. [39] proposed a dynamic output-feedback robust controller to improve the speed tracking ability of a connected car under a replay attack. Greene et al. [95] proposed an improved remote keyless entry system for CAVs by using timestamping and XOR encoding. It acts as a countermeasure to the replay attacks.

3) Against Impersonation Attacks:

To defend CAVs from impersonation attacks, available strategies include - secure transmission, integrity verification, authentication, and secure key agreement [38].

In integrity verification, researchers have proposed hash-based integrity verification mechanism that can be used to defend impersonation attacks effectively in vehicular cloud computing. Li et al. [41] proposed a certificate-less conditional privacy-preserving authentication protocol against impersonation attacks which also supports both privacy and security requirements in the CAV system. For secure transmission of data, researchers have proposed use of one-way hash function for transmission of valuable data to the receiver side quickly. Authentication can be achieved by using Elliptic Curve Cryptography mechanism in the CAVs.

4) Against Eavesdropping Attacks:

To prevent the eavesdropping attacks on the vehicles' queries, a fog server with the fog anonymizer [42] is used to anonymize (remove identifying particulars) the messages from the fog node. Also, resource management and scheduling mechanism can also be used as together they can provide secrecy provisioning. Prevention method includes a new trust-based recommendation mechanism [43] that ensures real-time data transmission and security in a vehicular cyber physical systems network.

5) Against Data Falsification Attacks:

For the detection of data falsification attacks, various methods include forged data filtering, reputation threshold, information sharing, location detection, dynamic time window [44].

Using the dynamic time window method, Shukla and Sengupta [44] proposed an anomaly detection strategy. In forged data filtering mechanism, the falsified traffic data is removed during data transmission in vehicular networks. In location detection mechanism, vehicles' falsified location is alleviated before it can result in a crash among an array of CAVs. In reputation threshold method, newly proposed cooperative spectrum sensing mechanism is used that helps to prevent data falsification attacks that usually happen under imperfect common control channels.

6) Against Routing Attacks:

There are various methods to prevent routing attacks and on one of them is ant colony optimization method. Here, a multi-path intelligent routing protocol is used to find an optimal path from the sender to the receiver plus it increases lifetime of the network. In order to defend attacks in CAVs, Hassan et al. [45] proposed an intelligent detection scheme. Researchers of [46] have proposed a mechanism which uses the ad hoc on-demand distance vector routing protocol and does the trust calculation. Other important strategies include swarm algorithms of artificial intelligence and variable control chart.

7) Against Password and Key Attacks:

Here we can use multifactor authentication and secure cryptographic mechanism.

In secure cryptographic mechanisms, we use keys with large sizes, secure algorithms, and secure passwords but with advanced computing power some of the cryptographic algorithms can be cracked. So, multifactor authentication can be used which puts different layers of identity security on every account. Also, it uses biometric authentication and hard tokens. Multifactor authentication can increase the security but it may not defend all password and key attacks.

8) Against Attack on CAV Cloud and dataset:

Here, all the possible attacks can happen on cloud therefore, a combination of all these mentioned techniques could be used to mitigate the cloud attack.

Also, For CAV system, the authority of each CAV's identity should be assigned by the government or relevant legitimate organizations. All the CAVs information and its security should be handled safely by trusted third-parties , vehicle manufacturers/suppliers and the government.

ANALYSIS:

In this section, I would be providing summary and doing risk assessment/analysis of some of the attacks that I mentioned in the paper. I would be using the formula:

Risk is calculated as combination of all the factors to do the assessment .

Risk Range –> (0-5)

Likelihood -> (0-10)

So, here I have made a table having columns for the analysis : attack type, access requirements, assets affected, Importance, Detection possibilities, severity level, likelihood, CIA affected, Risk.

ATTACK TYPE	CONSEQUENCE	ASSETS AFFECTED	IMPORTANCE	DETECTION	SEVERITY LEVEL	LIKELIHOOD	CIA AFFECTED	RISK
Eavesdropping attack	Leakage of personal information	In-vehicle system security and V2X communication.	High	Low	Medium	5-9	Confidentiality	3
Dos Attack	Block vehicle communication channel	With other vehicles, Infrastructure communication	Medium	High	Medium	3-5	Availability and Integrity	2
Replay attack	Confuse authorities, mislead the entire traffic and damage the CAV safety	Damages different sensors, keyless system of CAVs	Low	Medium	Low	5-7	Availability and Integrity	2
Infrastructure change attack	Infrastructure changing	Confuses the CAV system (Wrong reaction)	Low - Medium	Medium	Medium	2-4	Integrity	1.5
Cloud/dataset attack	Wrong info from Cloud database	CAV's Cloud database	Medium	Medium	Medium	1-3	All three are affected	3
Routing attack	Disturb normal routing process and also causes	V2X Communication	High	Low	Medium	3-8	Availability	3

	dropping of passing packets							
Password and Key attack	Password or key gets cracked. Personal info can also leak.	Keyless features, Telematic modules of system, also communication system gets compromised.	High	Medium	High	5-9	Authenticity	3.5
Data Falsification attack	Mislead receiver's reaction and result in fatalities	IoT , CPS system of CAV gets confused.	High	Low	High	4-6	Integrity	3.5

With the development of CAVs, the vulnerabilities as well as their counter-measures are going to increase. These attacks mentioned and many more can be prevented or defended with appropriate defense/mitigation strategies. The balance between low overhead and secure communication is an on-going challenge for CAVs, as the algorithm must maintain a highly reactive system response rate while ensuring communication is protected from sniffing or spoofing. Proper use of authentication plus encryption can be the key for mitigation techniques and safe-secure CAV ecosystem.

CAVs must be able to mitigate against the vulnerabilities of an unsecured communication channel. As CAVs have their own unique requirements and limitations that restrict their ability to implement the existing authentication and encryption mechanisms used in other industries, manufacturing companies and government should work together to create an ecosystem/environment where CAVs can be produced safely as well as the research on-going and new researches get boost and funding.

FUTURE RESEARCH TRENDS:

Are CAVs safe and secure? Not yet.

CAV development is an emerging environment, and much information about CAVs is confidential. In addition, no international standards for AV development, safety, and security are available. This makes CAV safety and security research extremely difficult [17].

Main future research is going to be focused on connection, security, data processing and efficiency of CAVs. Also, companies and governments have to create 'TRUST' among people around CAVs so that people can feel safe and but these futuristic, self-driving, autonomous vehicles. Therefore, governments have started making rules, standards for CAVs. Many research is still going-on on defining the standards that can be implemented by manufacturers and still the cars are safe for transportation.

Also, research is going on adding more connection features to CAVs to make it Truly Connected Vehicle (with 5G/6G) such as integrating RFID tags, adding online payments to cars i.e. vehicular paymentss, 24*7 connected to internet, cloud and nearby vehicles.

Future trends would also include functioning of CAVs in real-time traffic environment, how CAVs going to work in smart cities and that to securely.

CONCLUSION:

CAVs are future of transportation. They help reduce road accidents, improve quality of life, and promote efficient accident-free transportation systems. However, there are various security and privacy challenges in the CAV area. But they place great concern on safety and are vulnerable victims of invaders. Therefore, interest in the safety of CAVs has been growing rapidly. Over the past decade, many attack models and CAV defense strategies have been discussed and evaluated.

In this paper, I have focused on network/connected part of CAVs . I have highlighted major attacks possible on CAVs as well as suggested mitigation techniques to neutralize them and also done risk assessment of the attacks I highlighted.

REFERENCES :

1. Some, Evariste; Gondwe, Gregory; Rowe, Evan W. (2019). *[IEEE 2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS) - Granada, Spain (2019.10.22-2019.10.25)] 2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS) - Cybersecurity and Driverless Cars: In Search for a Normative Way of Safety. , (), 352–357.* doi:10.1109/IOTSMS48152.2019.8939168

2. K. Ren, Q. Wang, C. Wang, Z. Qin and X. Lin, "The Security of Autonomous Driving: Threats, Defenses, and Future Directions," in Proceedings of the IEEE, vol. 108, no. 2, pp. 357-372, Feb. 2020, doi: 10.1109/JPROC.2019.2948775.

3. X. Sun, F. R. Yu and P. Zhang, "A Survey on Cyber-Security of Connected and Autonomous Vehicles (CAVs)," in IEEE Transactions on Intelligent Transportation Systems, doi: 10.1109/TITS.2021.3085297.

4. A. Chowdhury, G. Karmakar, J. Kamruzzaman, A. Jolfaei and R. Das, "Attacks on Self-Driving Cars and Their Countermeasures: A Survey," in IEEE Access, vol. 8, pp. 207308-207342, 2020, doi: 10.1109/ACCESS.2020.3037705.

5. Liu, Na; Nikitas, Alexandros; Parkinson, Simon (2020). Exploring expert perceptions about the cyber security and privacy of Connected and Autonomous Vehicles: A thematic analysis approach. Transportation Research Part F: Traffic Psychology and Behaviour, 75(), 66–86. doi:10.1016/j.trf.2020.09.019

6. Qiyi He, Xiaolin Meng, Rong Qu, "Towards a Severity Assessment Method for Potential Cyber Attacks to Connected and Autonomous Vehicles", Journal of Advanced Transportation, vol. 2020, Article ID 6873273, 15 pages, 2020.

7. E. Some, G. Gondwe and E. W. Rowe, "Cybersecurity and Driverless Cars: In Search for a Normative Way of Safety," 2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS), 2019, pp. 352-357, doi: 10.1109/IOTSMS48152.2019.8939168.

8. El-Rewini, Zeinab; Sadatsharan, Karthikeyan; Selvaraj, Daisy Flora; Plathottam, Siby Jose; Ranganathan, Prakash (2020). Cybersecurity challenges in vehicular communications. Vehicular Communications, 23(), 100214–. doi:10.1016/j.vehcom.2019.100214

9. Kim, Hyunbum; Ben-Othman, Jalel; Mokdad, Lynda; Son, Junggab; Li, Chunguo (2020). Research Challenges and Security Threats to AI-Driven 5G Virtual Emotion Applications using Autonomous Vehicles, Drones and Smart Devices. IEEE Network, (), 1–7. doi:10.1109/MNET.011.2000245

10. Khan, Shah Khalid; Shiwakoti, Nirajan; Stasinopoulos, Peter; Chen, Yilun (2020). *Cyber-attacks in the next-generation cars, mitigation techniques, anticipated readiness and future directions. Accident Analysis & Prevention, 148(), 105837–.* doi:10.1016/j.aap.2020.105837

11. X. Wang, C. Xu, Z. Zhou, S. Yang and L. Sun, "A Survey of Blockchain-based Cybersecurity for Vehicular Networks," *2020 International Wireless Communications and Mobile Computing (IWCMC)*, 2020, pp. 740-745, doi: 10.1109/IWCMC48107.2020.9148566.

12. S. Malik and W. Sun, "Analysis and Simulation of Cyber Attacks Against Connected and Autonomous Vehicles," 2020 International Conference on Connected and Autonomous Driving (MetroCAD), 2020, pp. 62-70, doi: 10.1109/MetroCAD48866.2020.00018.

13. Y. Wang, Q. Liu, E. Mihankhah, C. Lv and D. Wang, "Detection and Isolation of Sensor Attacks for Autonomous Vehicles: Framework, Algorithms, and Validation," in IEEE Transactions on Intelligent Transportation Systems, doi: 10.1109/TITS.2021.3077015.

14. A. O. A. Zaabi, C. Y. Yeun and E. Damiani, "Autonomous Vehicle Security: Conceptual Model," 2019 IEEE Transportation Electrification Conference and Expo, Asia-Pacific (ITEC Asia-Pacific), 2019, pp. 1-5, doi: 10.1109/ITEC-AP.2019.8903691.

15. Linkov, Vaclav & Zamecnik, Petr & Havlíčková, Darina & Pai, Chih-Wei. (2019). Human Factors in the Cybersecurity of Autonomous Vehicles: Trends in Current Research. Frontiers in Psychology. 10. 10.3389/fpsyg.2019.00995.

16. Khan, Firoz & Ramasamy, Lakshmana & Kadry, Seifedine & Meqdad, Maytham N. & Nam, Yunyoung. (2021). Autonomous vehicles: A study of implementation and security. International Journal of Electrical and Computer Engineering. 11. 3013-3021. 10.11591/ijece.v11i4.pp3013-3021.

17. Cui, Jin; Liew, Lin Shen; Sabaliauskaite, Giedre; Zhou, Fengjun (2018). A Review on Safety Failures, Security Attacks, and Available Countermeasures for Autonomous Vehicles. Ad Hoc Networks, (), S1570870518309260–. doi:10.1016/j.adhoc.2018.12.006

18. Nanda, Ashish; Puthal, Deepak; Rodrigues, Joel J. P. C.; Kozlov, Sergei A. (2019). Internet of Autonomous Vehicles Communications Security: Overview, Issues, and Directions. IEEE Wireless Communications, 26(4), 60–65. doi:10.1109/MWC.2019.1800503

19. Pham, M., & Xiong, K. (2021). *A survey on security attacks and defense techniques for connected and autonomous vehicles. Computers & Security, 109, 102269.* doi:10.1016/j.cose.2021.102269

20. Rathee G, Sharma A, Iqbal R, Aloqaily M, Jaglan N, Kumar R. A Blockchain Framework for Securing Connected and Autonomous Vehicles. *Sensors*. 2019; 19(14):3165. https://doi.org/10.3390/s19143165

21. Chow, Man Chun & Ma, Maode & Pan, Zhijin. (2021). Attack Models and Countermeasures for Autonomous Vehicles. 10.1007/978-3-030-76493-7_12.

22. Seetharaman, A., Patwa, N., Jadhav, V., Saravanan, A. S., & Sangeeth, D. (2020). Impact of Factors Influencing Cyber Threats on Autonomous Vehicles. Applied Artificial Intelligence, 35(2), 105–132. doi:10.1080/08839514.2020.1799149

23. McCall, S., Yucel, C., & Katos, V. (2021). Education in Cyber Physical Systems Security: The Case of Connected Autonomous Vehicles. 2021 IEEE Global Engineering Education Conference (EDUCON). doi:10.1109/educon46332.2021.9454

24. Chattopadhyay, Anupam; Lam, Kwok-Yan; Tavva, Yaswanth (2020). Autonomous Vehicle: Security by Design. IEEE Transactions on Intelligent Transportation Systems, (), 1–15. doi:10.1109/TITS.2020.3000797

25. Ahangar, M. N., Ahmed, Q. Z., Khan, F. A., & Hafeez, M. (2021). A Survey of Autonomous Vehicles: Enabling Communication Technologies and Challenges. Sensors, 21(3), 706. doi:10.3390/s21030706

26. Mancini, Federico; Bruvoll, Solveig; Melrose, John; Leve, Frederick; Mailloux, Logan; Ernst, Raphael; Rein, Kellyn; Fioravanti, Stefano; Merani, Diego; Been, Robert (2020). [IEEE 2020 IEEE Conference on Communications and Network Security (CNS) - Avignon, France (2020.6.29-2020.7.1)] 2020 IEEE Conference on Communications and Network Security (CNS) - A Security Reference Model for Autonomous Vehicles in Military Operations. , (), 1–8. doi:10.1109/CNS48642.2020.9162227

27. Gulde, André and Engel, Tobias, "Future mobility technologies and their relevance for IS research: Autonomous driving and security" (2021). MWAIS 2021 Proceedings. 14. https://aisel.aisnet.org/mwais2021/14

28. D. Minovski, C. Åhlund and K. Mitra, "Modeling Quality of IoT Experience in Autonomous Vehicles," in IEEE Internet of Things Journal, vol. 7, no. 5, pp. 3833-3849, May 2020, doi: 10.1109/JIOT.2020.2975418.

29. X. Peng, H. Zhou, B. Qian, K. Yu, F. Lyu and W. Xu, "Enabling Security-Aware D2D Spectrum Resource Sharing for Connected Autonomous Vehicles," in IEEE Internet of Things Journal, vol. 7, no. 5, pp. 3799-3811, May 2020, doi: 10.1109/JIOT.2020.2975754.

30. C. Schmittner, J. Dobaj, G. Macher and E. Brenner, "A Preliminary View on Automotive Cyber Security Management Systems," 2020 Design, Automation & Test in Europe Conference & Exhibition (DATE), 2020, pp. 1634-1639, doi: 10.23919/DATE48585.2020.9116406.

31. Y. Fu, F. R. Yu, C. Li, T. H. Luan and Y. Zhang, "Vehicular Blockchain-Based Collective Learning for Connected and Autonomous Vehicles," in IEEE Wireless Communications, vol. 27, no. 2, pp. 197-203, April 2020, doi: 10.1109/MNET.001.1900310.

32. Maeng, K., Kim, W., & Cho, Y. (2021). Consumers' attitudes toward information security threats against connected and autonomous vehicles. Telematics and Informatics, 63, 101646. doi:10.1016/j.tele.2021.101646

33. H. Kim, J. Ben-Othman, L. Mokdad, J. Son and C. Li, "Research Challenges and Security Threats to AI-Driven 5G Virtual Emotion Applications Using Autonomous Vehicles, Drones, and Smart Devices," in IEEE Network, vol. 34, no. 6, pp. 288-294, November/December 2020, doi: 10.1109/MNET.011.2000245.

34. Nikitas, Alexandros; Michalakopoulou, Kalliopi; Njoya, Eric Tchouamou; Karampatzakis, Dimitris (2020). Artificial Intelligence, Transport and the Smart City: Definitions and Dimensions of a New Mobility Era. Sustainability, 12(7), 2789–. doi:10.3390/su12072789

35. Khan, Muhammad Khurram; Quadri, Amanullah (2020). Augmenting cybersecurity in autonomous vehicles: Innovative recommendations for aspiring entrepreneurs. IEEE Consumer Electronics Magazine, (), 1–1. doi:10.1109/MCE.2020.3024513

36. Z. A. Biron, S. Dey, and P. Pisu, "Real-time detection and estimation of denial of service attack in connected vehicle systems," IEEE Trans. Intell. Transp. Syst., vol. 19, no. 12, pp. 3893–3902

37. S. Kumar and K. S. Mann, "Detection of multiple malicious nodes using entropy for mitigating the effect of denial of service attack in VANETs," in Proc. 4th Int. Conf. Computer Sci. (ICCS), pp. 72–79.

38. R. Merco, Z. A. Biron, and P. Pisu, "Replay attack detection in a platoon of connected vehicles with cooperative adaptive cruise control," in Proc. Annu. Amer. Control Conf. (ACC), Jun. 2018, pp. 5582–5587.

39. X. Xu, X. Li, P. Dong, Y. Liu, and H. Zhang, "Robust reset speed synchronization control for an integrated motor-transmission powertrain system of a connected vehicle under a replay attack," IEEE Trans. Veh. Technol., early access, Sep. 1, 2020.

40. K. Greene, D. Rodgers, H. Dykhuizen, Q. Niyaz, K. Al Shamaileh, and V. Devabhaktuni, "A defense mechanism against replay attack in remote keyless entry systems using timestamping and XOR logic," IEEE Consum. Electron. Mag., vol. 10, no. 1, pp. 101–108, Jan. 2021.

41. J. Li, Y. Ji, K.-K.-R. Choo, and D. Hogrefe, "CL-CPPA: Certificate-less conditional privacy-preserving authentication protocol for the Internet of vehicles," IEEE Internet Things J., vol. 6, no. 6, pp. 10332–10343, Dec. 2019.

42. M. Arif, G. Wang, and V. E. Balas, "Secure VANETs: Trusted communication scheme between vehicles and infrastructure based on fog computing," Stud. Informat. Control, vol. 27, no. 2, pp. 235–246, Jan. 2019.

43. W. Liang, J. Long, T.-H. Weng, X. Chen, K.-C. Li, and A. Y. Zomaya, “TBRS: A trust based recommendation scheme for vehicular CPS network,” Future Gener. Comput. Syst., vol. 92, pp. 383–398, Mar. 2019

44. R. M. Shukla and S. Sengupta, “Analysis and detection of outliers due to data falsification attacks in vehicular traffic prediction application,” in Proc. 9th IEEE Annu. Ubiquitous Comput., Electron. Mobile Commun. Conf. (UEMCON), pp. 688–694.

45. Z. Hassan, A. Mehmood, C. Maple, M. A. Khan, and A. Aldegheishem, “Intelligent detection of black hole attacks for secure communication in autonomous and connected vehicles,” IEEE Access, vol. 8, pp. 199618–199628, 2020.

46. A. Bhawsar, Y. Pandey, and U. Singh, “Detection and prevention of wormhole attack using the trust-based routing system,” in Proc. Int. Conf. Electron. Sustain. Commun. Syst. (ICESC), Jul. 2020, pp. 809–814.

47. N. B. Khankari and G. V. Kale, “One time password generation for multifactor authentication using graphical password,” Int. J. Eng. Res. Gen. Sci., vol. 3, no. 5, pp. 489–494, 2020.

48. Cao Y, Xiao C, Cyr B, Zhou Y, Park W, Rampazzi S, Chen QA, Fu K, Mao ZM. Adversarial sensor attack on LiDAR-based perception in autonomous driving In: ACM SIGSAC Conference on Computer and Communications Security. ACM; 2019. p. 2267-81.

49. Sommer F, Dürrwang J, Kriesten R. Survey and Classification of Automotive Security Attacks. Information. 2019; 10(4):148. https://doi.org/10.3390/info10040148

50. A. Bazzi, B. M. Masini, A. Zanella, and I. Thibault, ‘‘On the performance of IEEE 802.11p and LTE-V2 V for the cooperative awareness of connected vehicles,’’ IEEE Trans. Veh. Technol., vol. 66, no. 11, pp. 10419–10432, Nov. 2017

51. R. Gupta, S. Tanwar, N. Kumar, and S. Tyagi, ‘‘Blockchain-based security attack resilience schemes for autonomous vehicles in industry 4.0: A systematic review,’’ Comput. Electr. Eng., vol. 86, Sep. 2020, Art. no. 106717

****