International Journal of Basic and Applied Sciences, 14 (4) (2025) 515-521

International Journal of Basic and Applied Sciences

Website: www.sciencepubco.com/index.php/IJBAS
https://doi.org/10.14419/x1ejje10
Research paper

Designing of New Reliable Control Architecture for Connected Autonomous Vehicles Against Cyber Attacks

Shwetansh Priyadarshi [1]*, Dr. Deepak Bharadwaj [2]

[1] Research Scholar GD Goenka University, Gurugram
[2] Associate Professor DBS Global University, Dehradun
**Corresponding author E-mail: shwetansh08@gmail.com*

Received: July 8, 2025, Accepted: August 10, 2025, Published: August 19, 2025

Abstract

Autonomous vehicles were introduced with the idea that they would make jobs easy, it will help in reducing accident rates, reduce pollutants, lower harmful gas emissions, and lighter traffic congestion, etc. Connected vehicles use a variety of devices, sensors, cameras, and modules like LiDAR, GPS, RADAR, onboard computers, ultrasonic sensors, etc., to make proper driving decisions and to be competent to work on the road. In recent articles on cyber-attacks/cyber-crimes/accidents, data states that hackers and other ill-motive organisations can do remote hacking, tamper with the sensor data, and they may crash a vehicle or access the primary control by attack, which may result in significant losses. We have observed in the past few years that Autonomous vehicle makers and the administration are refraining from investing in completely Automated vehicles. The interest rate of people in connected AVs has gradually fallen with each passing year, and many surveys clearly mentioned that the main reason for this is the lack of a strong security framework. This paper provides a brief about cyber-attacks on AVs and different approaches to deal with them.

Keywords: *Autonomous Vehicles; Connected Vehicles; Cyber-Attacks; Cyber-Crimes.*

1. Introduction

Before the 2000s, and especially in the 1990s, the thought of fully autonomous vehicles was hardly considered realistic; not too many people had imagined a car capable of driving itself using its sensors, methods, and intelligence. At that time, most of the countries showed very little interest in the concept of autonomous driving, as there was no significant need for such technology. However, in recent times, the study of autonomous driving has become a major focus in both the automotive and research industries [18] [19] [20]. This shift began due to concern about increasing accident rates caused by reckless driving and human error, the physical and mental demands required for driving, the rise in traffic congestion, and environmental issues such as the emission of harmful gases like CO2. To handle these problems, researchers thought of a more efficient vehicle capable of addressing all these challenges. As shown in Figure 1a, market studies indicate a notable transformation for CAVs with projections suggesting that the market share for Connected and Autonomous Vehicles (CAVs) could grow tenfold within the next decade.

According to recent articles and data from the Automobile industry, many car manufacturers have come up with autonomous vehicles that are road-ready and are asserted to be completely safe. However, data from agencies which track and report road accidents indicate that the rate of accidents involving Connected and Autonomous Vehicles (CAVs) has risen over the years. CAVs are vehicles that operate solely using a combination of sensors, radars, Lidars, Actuators, high vision cameras, Global Positioning System (GPS), and complex algorithms (refer to Figure 1). These sensors, cameras are mounted on autonomous vehicles and generate vast amounts of data every hour. This data is very crucial for training the systems of CAVs and improving vehicle performance. However, the massive volume of data also introduces a huge number of risks, particularly in terms of cybersecurity. There are chances of various types of cyber-attacks/cyber-crimes possible on Autonomous vehicles [2]. There are several research studies and media reports that highlight that CAVs are still not entirely secure. Continual hacking incidents have resulted in loss of life, cybercrimes/cyber-attacks, and significant property damage. Moreover, there are potential consequences of hacking CAVs that we cannot even think of, leading to a general sense of insecurity among users. Surveys show that public interest and trust in CAVs have been gradually declining each passing year.

When discussing about cyber-attacks on Connected and Autonomous Vehicles (CAVs), it is important to consider that such attacks are not limited to a single vehicle. CAVs are connected vehicles, and they work on the rule of vehicle-to-vehicle communication (V2V) and vehicle-to-infrastructure (V2I) communication [3]. Unlike regular vehicles, CAVs continuously share data with other vehicles and infrastructure components to make them part of a broader connected network. As a result, cyber-attacks on CAVs lead to triggering widespread cyber-crimes with consequences far beyond our imagination. An example occurred in 2015, when two researchers in the United States successfully hacked a Jeep Cherokee, disrupted its multimedia system, and affected its accelerator [4]. This incident highlights the severity and

importance of the real-world implications of cybersecurity in autonomous vehicles. This paper explains the operational mechanisms of CAVs, examines the various types of cyber-attacks, and aims to provide potential solutions to enhance their security.

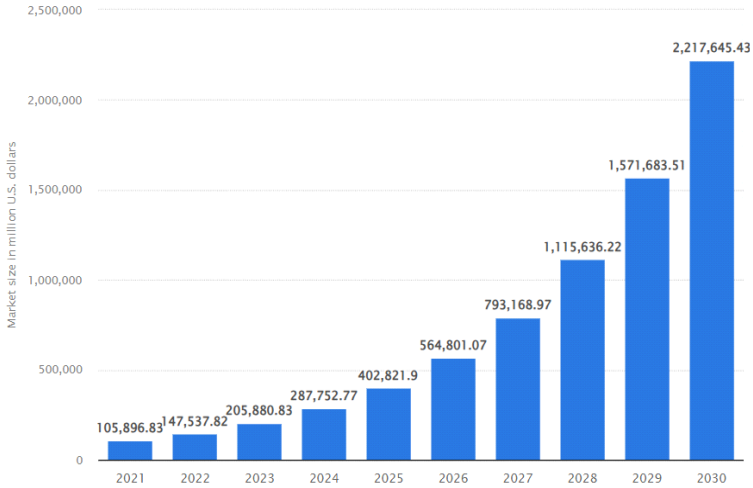

Fig. 1: Connected Autonomous Cars Global Market Size 2021-2030 [1] The CAV Market Is Estimated to Reach 4,206.4B U.S. Dollars by 2032.

2. Ethical and policy implications of cybersecurity in AVs

Whenever the topic of Autonomous cars comes into the picture, there are a few things that get discussed in parallel since the very beginning. The Vulnerabilities in Autonomous cars always pose a challenge for policy formations, implementations, and governance. The Autonomous cars, being an independent unit, rely on Sensors, radars, cameras, deep learning models, Artificial intelligence, etc. This independent behaviour also leads to cybersecurity vulnerabilities, which not only create security issues and technical failures but also policy challenges. A small technical issue can lead to loss of life, major accidents, damage to infrastructures, privacy violations, and can be misused by attackers. These things drag the immediate attention and raise serious questions about trust, governance, and policy formations.

For people in Administration and car companies, there is an ethical obligation to minimize risk for car owners, footpath users, and people around. When an Autonomous vehicle gets attacked, attackers first try to take control of the car and disable the safety systems inside the car. Here, making a car's system secure becomes the moral responsibility of car companies. Moreover, if the car is getting attacked, then multiple questions come into the picture for the administration and policy makers, i.e., the manufacturer should be held responsible, the programmer, the owner, or the car company. But, with the growing AV market, the car makers have invested much in security software systems, and it has been promised that the market will see more secure cars shortly. Again, there arises concern for normal people who wish to own an AV, highly advanced software system, a robust infrastructure will lead to price surge potentially limiting the normal people to afford a AV.

Since Autonomous vehicle is a very growing field, as there numerous technical factor, latest technologies are getting involved, and with every passing day, these cars will be getting advanced, and there is very great scope for future research and multiple latest applications to be implemented on it. This raises another concern for policymakers, as this is a growing topic; the laws and the policies cannot remain the same, because the laws framed today will not sustain tomorrow. Moreover, these policies need to be flexible for cross-border implementations and need frequent updates and approvals with growing technology. The same needs to be implemented with the insurance companies and the laws need to be framed for them as well, establishing a central database on a global level, which works across borders, is a challenge. And also doing documentation, necessary certification, and making it globally valid will be a challenge.

3. Literature review

Unlike previous surveys on Connected and Autonomous Vehicles (CAVs), this study specifically focuses on the safety mechanisms of autonomous cars, the extent of potential cyber-crimes and cyber-attacks, and how these attacks can manipulate the vehicle's target destination. A holistic approach has been followed to examine all possible attacks, their effect on route manipulation scenarios, and the development of potential solutions to them. These solutions are anticipated as significant value to car engineers who are working on autonomous vehicles, as well as to the broader research and development industry.

To support this study, a comprehensive search was conducted using keywords such as "Autonomous Cars," "CAVs," "Security," and "Denial of Service" to identify relevant industry white papers and academic publications from leading journals. Out of an initial pool of 170 publications, 70 were selected for detailed review, as the existing body of work focusing specifically on cyber-attacks and route manipulation in CAVs remains relatively limited.

To secure the Autonomous cars and the complete infrastructure, there are models in place, and deep learning models are integrated to safeguard Autonomous vehicles from cyber-attacks and any such activities. These deep learning models enhance the security feature of Connected Autonomous vehicles and many such models with good Accuracy have been developed and discussed in previous work by many researchers. Multiple models of deep learning came into the limelight after they were able to attain higher accuracy in terms of defeating cyber-attacks and were discussed in multiple research publications, are Deep autoencoders, long short-term memory networks, Convolution Neural Networks, CNN-LSTM Hybrids, Deep Reinforcement Learning, RNN, and Hybrid Models.

In the process of this Research and Development work, more than 250 articles were referred and till now only 51 very suitable articles were considered because the study done till now gets outdated with every passing day as Autonomous car industry is growing with emerging technologies. And this opens doors for researchers of not just the technology field but also the law researchers, humanitarian sciences, and other departments as well. The policies made for Autonomous cars in 2021 cannot be the same because there is a complete change in vehicle infrastructure and working. The safety systems are not the same, the level of Automation has increased, and so are to be the laws. It's not just the deep learning models that need revision, the components, the policies, and many more things need to be studied and changes

are required on a regular basis. We are using the Dwarf mongoose algorithm, but the new researchers need to find better models and algorithms than this. There can be a better optimal solution, but it cannot be the best in terms of an Autonomous vehicle.

4. Related work

There are many similar research works which highlight the role of Deep learning models in safeguarding the Connected Autonomous Vehicles. We have used some very similar works as Base Papers to develop our algorithm. These works are totally based on "Intrusion Detection System" and aimed to work against the attacks on the Internal networks that links the various components of the Vehicles and are considered as veins of the Autonomous vehicle system. In these discussions, a protocol that is very crucial to understand Controller Area Network (CAN), used inside the in-vehicle network, has been developed for robust security in self-driven vehicles [33] [34] [35]. With CAN, there has been a parallel discussion about- on-board diagnostic port, also called OBD-2, which is the access point of these vehicles. So, to understand how an autonomous vehicle gets attacked and what components need to be accessed, the researchers have segregated the study into bits, i.e., apart from sensors, cameras, and lidars, what are the major things that get attacked.
Electronic Control Units (ECUs): - These are the tiny computers controlling systems like: - Engine, Brake, Steering, gear, functionalities, infotainment systems, Advanced Driver Navigation system (ADAS), and Navigation.
Communication Interfaces: - This Contains 5G, WIFI, Bluetooth, Ethernet, CAN Bus, V2V, V2I, V2P, V2X.
Software: - Path Planning and Path Securing algorithms, decision making, object detection, and all these are done by deep learning models.
Cloud Service: -This consists of real-time data analysis, broadcasting over the air updates, remote diagnostics, etc.

5. Attack taxonomy

If an attacker wants to attack Autonomous cars, then from this perspective, there are a few crucial things. The Electronic Control Unit (ECU), CAN Bus, and OBD-2 Port/Security Gateways, these systems make the architecture of Autonomous Vehicles robust against Cyber-attacks. Multiple deep learning models block attackers from getting access to the system, and all the models have a certain level of accuracy; moreover, they are yet to attain 98% plus accuracy.

1) Convolutional Neural Networks (CNNs): - CNN model is one among the most frequently used models under deep learning. It is used for its feature of processing the visual data, i.e., images and videos. Moreover, the CNN model is specialised in detecting shapes, patterns, edges, etc., which makes it super fit for highly advanced autonomous cars. For Example: - Traffic light displays stop, there is a turn symbol board, or a Men at Work board, etc. In such cases, CNN models are very efficient. Convolution is normally considered as a kernel/filter that is passed through the images to detect or to extract all features like edges, signs, colours, etc.

Working of CNN Model: - Let's consider a real-time scenario where a car's front Camera detects an image, and post that this is how things will process: -

a) Layer 1: - Image is inserted as Input (200*200) RGB Image and in 3D matrix it will work as (Length*width*channels) i.e. (200*200*3).
b) Layer 2: - It is called as Convolution Layer, it is more like a filter or kernel, and images are moved out of it, and it will extract all the features, such as colours, edges, corners, etc.
c) Layer 3: - Post Layer 2, Rectified Linear Unit (ReLU) is applied. ReLU(x)=max (0, x). Its only purpose is to have non-linearity, and this helps in Research on Complex features.
d) Layer 4: - It is called as Pooling Layer. Its job is to speed speedup computing, increasing efficiency, make the network faster, and save from overfitting. It also cuts off the spatial size, e.g., (200*200 - 100*100).
e) Layer 5: - Here we include more above layers, i.e., more pooling and convolution layers, and the whole process is repeated. This is done to increase learning and get more abstract features.
f) Layer 6: - This is called the Flattening Layer, here the system is prepared for deciding things, i.e., it converts the last set of feature maps to a D vector.
g) Layer 7: - This is known as a fully connected layer, where the learned features are taken by the neural network, and then the classification of the object is done.
h) Layer 8: - This is called the output layer. Output will be: (e.g., stop symbol = 85%, speed limit symbol = 9%, etc.)

2) Recurrent Neural Network (RNN): - RNN is a deep learning model that is introduced to deal with a sequential series of data, i.e., past and present occurrences. RNNs work on a concept which is slightly different from other neural networks; it memorizes the past memory and uses that for generating the present output. If it is related to Autonomous cars, speed over time changes, drivers' behaviour in different scenarios, or in last 30 minutes are tracked, CAN inputs over time are tracked, tracking the movements of pedestrians based on previous data, etc.

Working of RNN: - Let's assume that our sensor is getting data every second, and this is about speed. And it's like T0 – 0km/h, T1= 20km/h, T2= 85km/h, etc. Now, in the case of RNN, a hidden state is maintained, and this gets updated after every input.
Suppose Input series is A0, A1, A2, A3, Hidden state is S0, S1, S2, S3 then output is Y0, Y1, Y2, Y3. So, the output depends on the input At and the hidden state St-1(Refer to Fig. 2).

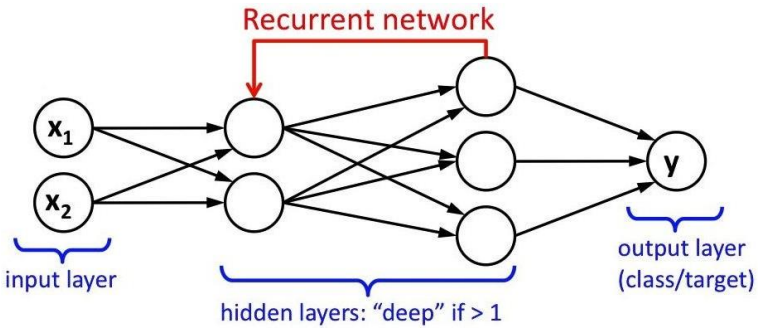

Fig. 2: Pictorial Representation of Recurrent Neural Network (RNN) Working [8].

Why RNN Works in Autonomous Vehicles?
The CAN Bus sends data on a regular basis among ECUs. Now the problem is that hackers try to send fake data which looks normal at first impression, but they are not in sequence. And when there is a mismatch in sequence, then RNN comes into the picture. So, the RNN is trained on the normal pattern sequences from CAN Bus. And post-training, it is aware of patterns expected, i.e., it is easily able to distinguish between the normal and abnormal patterns and sequences, and flags out the abnormal sequences during run time.
Why RNN Fails in Autonomous Vehicles and How it Can be Improved?
As Autonomous cars and this complete technology are still emerging, there are loopholes as well. In RNN, remembering the long sequences is a struggle, and due to the short memory problem, this becomes a major consequence of RNN. So, an Alternative to it, or we can say enhancement, was done to RNN, and then Long Short-Term Memory (LSTM) and Gated Recurrent Unit (GRU) have been introduced.

6. Control architecture

Here in the control Architecture of the Autonomous car, we will present how cars are attacked and how our model is different and advanced in preventing these attacks. In a scenario, when an autonomous car is moving on the road, multiple things work in the background to make things work. The cameras embedded will check for all signs, lanes, and pedestrians. Similarly, Lidar, Radar, GPS, Ultrasonic sensors, etc. do their jobs, and after this sensor fusion happens, to get a reliable picture and to have the proper understanding of the real-world scenario. Post sensor fusion deep learning models come into the picture, these models classify the signs, images, symbols, people, etc (Refer to Fig. 3).

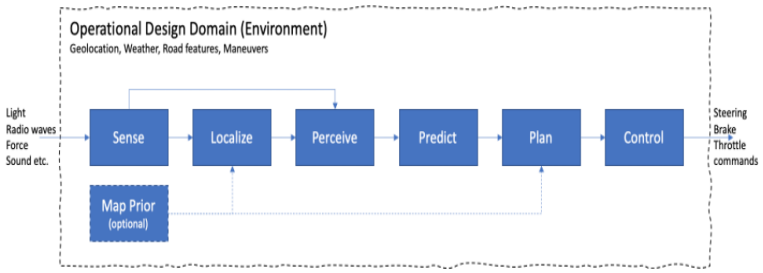

Fig. 3: Control Architecture of Connected Autonomous Vehicle.

Now the vehicle's system needs to predict the upcoming scenarios i.e., will the person cross the road, will the car moving in front turn, etc. And all this is done with the help of RNN and LSTM, which take the help of past data to predict what is going to happen next. Post this stage, the car knows the exact scenarios i.e., path planning, motion planning, what is going to happen next, and how it should act. All the analysis and decisions made by deep learning models are considered commands and are processed to Electronic Control Units (ECUs) via CAN Bus.
Since we found loop holes, accuracy, and efficiency issues in existing models, so we started with Artificial Neural Network(ANN) model which turned out with an Test accuracy of 85.47%, post that we proceeded for Convolution Neural Network(CNN) model and it resulted with an Test accuracy of 86% and then we Came up with our Hybrid model which uses CNN, Long short term memory(LSTM) and Gated Recurrent Unit(GRU). Our purpose of using this hybrid model is that with CNN, feature extraction can be done, and loopholes of RNN can be fixed by using LSTM and GRU, which are used for sequential Learning and Long memories. By using our hybrid model, we achieved a Test Accuracy of 85.47%, and on top of it, we are performing hyperparameter tuning.
Steps Performed: -

1) Hyperparameters (neurons in each layer) are optimized using the Dwarf Mongoose Optimization Algorithm (DMOA).
2) A dictionary and CSV log are used to track previously evaluated architectures, preventing redundant computations.
3) Each candidate model is trained for 5 epochs using early stopping to prevent overfitting.
4) Accuracy is measured on the test set to guide the optimization process.

6.1. Model evaluation

- Best Model Selection: After optimization, the best-performing model is reloaded for evaluation.
- Performance Metrics: The model's performance is assessed using the following metrics:
- Accuracy: Overall correctness of the model.
- Precision: Proportion of true positives among predicted positives.
- Recall: Proportion of true positives among actual positives.
- F1-Score: Harmonic mean of precision and recall.

6.2. Discussion: How is the route of CAVs safeguarded?

We are using a hybrid model, which uses CNN+LSTM+GRU. This combination helps in overcoming all the challenges faced in existing deep learning models. By using LSTM, we have a huge memory stack to remember the sequential Learning, which was a consequence of RNN. Moreover, the traditional RNNs have a slow learning rate, and in return the performance we have is very poor, and overall result it has been proven as inefficient. In this model, LSTM+ GRU is used purposefully for memory as they have control over memory flow with Gates. GRUs are equipped with the Update Gate and Reset Gate concept, where the Update Gate keeps the tag on information, i.e. how much information to be stored, and the Reset Gate decides on the concept of deleting the old information, i.e., how much old information to be wiped off. Basically, in GRU, the hidden state memory keeps updating itself at every time step, and this makes this hybrid model more efficient than RNN. And as we are optimizing the hyperparameters using the Dwarf Mongoose Optimization Algorithm (DMOA) makes this architecture becomes more robust.

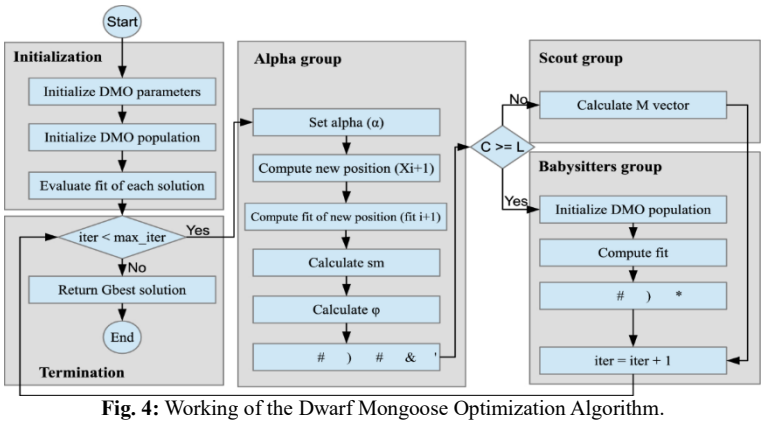

Fig. 4: Working of the Dwarf Mongoose Optimization Algorithm.

DMOA, introduced very recently, has proven its capability being a metaheuristic algorithm. DMOA works on the patterns to attain the best possible solution, and it keeps on refining the solution. This is a lightweight, very adaptive and easy to implement algorithm which makes it a best fit for complex system like Autonomous Vehicles where cyber threat is very much expected problem. The challenges are well known that CAVs need to travel in various environments, and consist of multi-point data sources and huge security threats, then in this case DMOA is the best optimal solution (Refer to Fig. 5).

7. Experimental results

In this overall process of research and development, we have studied various existing deep learning models, their loopholes, constraints, and real-time data processing challenges. In Autonomous Vehicles, the decision making happens in milliseconds, which is far less than a human to act, but with speed comes challenges. If there are slight delays due to sensor errors, it can cause misjudging a person or a vehicle on the road, and that can also lead to severe consequences. Another challenge can be, the data inflow rate from various sources is at various speeds, and processing all at once is also a big challenge. With growing time, we have growing technology, and old computing stacks won't be the same and need to be upgraded regularly. A single Autonomous vehicle generates 1-5 TB of data per day, and processing it without proper bandwidth is also a challenge. The other scenario can be bad weather, failure of equipment, bad lighting effects, etc. This can also lead or cause trouble in data processing. Moreover, on-board systems in Autonomous vehicles have power limitations and heating constraints, and cloud processing is slow as compared to local processing. This also poses a critical challenge for car companies.
We have evaluated multiple deep learning models in this, such as CNN, ANN, RNN, and multiple hybrid models. And we also come across loopholes and multiple challenges in these models, efficiency issues, and cost issues. CNNs used for object detection, lane detection are expensive compared to other models. If there are delays in Frames per Second (FPS) can lead to accidents, and they have also failed in new weather conditions. And consuming processed data of new weather conditions may fail the CNN system, and is also expensive as well as highly time-consuming. As is commonly known, on-board systems in vehicles have energy and thermal limitations, which a constraints for the CNN model size. If there are pixel changes, the CNN may misjudge obstacles, and this could lead to misreading or misjudging a symbol or a sign. If we talk about the ANN model, it's the extension of CNN shortcomings. The ANN models were meant for handling huge amounts of data in milliseconds; this is impacted by latency in high inference. If there are mismatches in sensor time leads to wrong predictions, and the ANN training needs to be updated regularly. We have also found a performance drop when there is a drop in the quality of the signal, and apart from this, almost all the loopholes of CNN exist in ANN too.

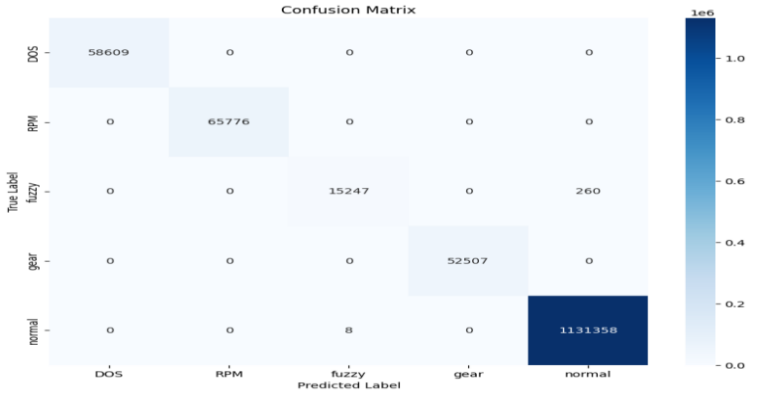

Fig. 5: A Confusion Matrix Visualized Using Seaborn Heatmap to Analyse Prediction Errors Across.

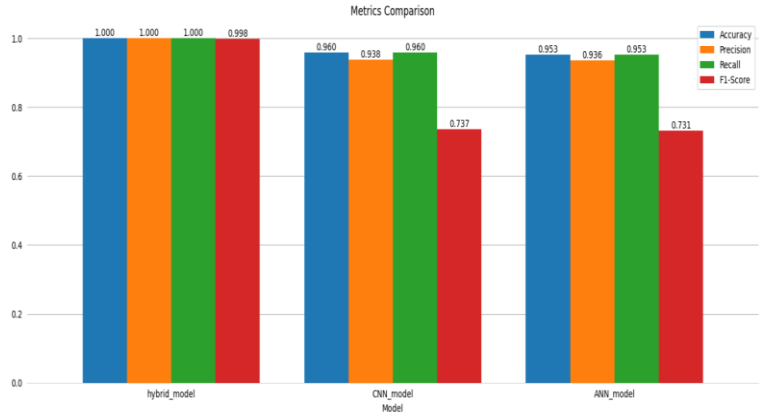

Fig. 6: Comparison of Different Metrics, Precision, Recall, and F1 Score for the Models.

It can be clearly understood that the errors faced during the processing of data in different models and the clear comparison between all the models shows the Novelty of our model over all the preexisting models Fig. 5. This can also be seen that the performance, accuracy and robustness towards cyber attacks are also very high in our proposed model Fig. 6.

8. Conclusion

This article has taken a detailed approach to study all the previous existing deep learning models, the working of Autonomous vehicles, possible cyber threats in Connected Autonomous Vehicles, and then summing up all the existing loopholes. We have presented a Robust Deep Learning model, which can counter all the existing models, a very efficient, simple in execution, fast in process, and easy to implement. We have discussed all the major possible cyber-attacks on Connected Autonomous vehicles and how these were easily possible in previous models. We have discussed how we are overcoming all these cyber threats with our model and using the Dwarf Mongoose optimization Algorithm, which is also the most recently introduced algorithm.
We have discussed all possible solutions to overcome previous cyber threat cases in the mentioned articles. Our process of data collection is from a very authentic repository, we have taken care of every data processing step, and a detailed evaluation of all existing deep learning models. We have also discussed the potential areas where the research work can still be done, and with the passing time, challenges can be expected. Our research can provide a very detailed insight to CAV industry experts, Research and development engineers, researchers of this industry, and all upcoming car makers who are planning to launch Autonomous vehicles in the coming days. We expect our research can help in a safe Autonomous vehicle with a robust software architecture, which will safeguard the interests of car makers, car owners, administration, and nearby infrastructure.

References

[1] Anastasios, G., Aristeidis, K. (2023). Autonomous Vehicles: Sophisticated Attacks, Safety Issues, Challenges, Open Topics, Blockchain, and Future Directions
[2] Shaoshan, L., Liyun, L., Jie, Tang. Creating Autonomous Vehicles Systems
[3] Miller, C., & Valasek, C. (2015). Remote exploitation of an unaltered passenger vehicle. Black Hat USA, 2015, 91
[4] CAV, Cav mounted devices, " https://ecotrons.com/news/introduction-to-autonomous-driving-sensors-blog/", online web source
[5] Z. Ju, H. Zhang, X. Li, X. Chen, J. Han, and M. Yang, "A survey on attack detection and resilience for connected and automated vehicles: From vehicle dynamics and control perspective," IEEE Transactions on Intelligent Vehicles, 2022 https://doi.org/10.1109/TIV.2022.3186897.
[6] T. Limbasiya, K. Z. Teng, S. Chattopadhyay, and J. Zhou, "A systematic survey of attack detection and prevention in connected and autonomous vehicles," Vehicular Communications, p. 100515, 2022. https://doi.org/10.1016/j.vehcom.2022.100515.
[7] M.Dibaei, X. Zheng, K. Jiang, R. Abbas, S. Liu, Y. Zhang, Y. Xiang, and S. Yu, "Attacks and defences on intelligent connected vehicles: a survey," Digital Communications and Networks, vol. 6, no. 4, pp. 399–421, 2020. https://doi.org/10.1016/j.dcan.2020.04.007.
[8] E. Aliwa, O. Rana, C. Perera, and P. Burnap, "Cyberattacks and counter measures for in-vehicle networks," ACM Computing Surveys (CSUR), vol. 54, no. 1, pp. 1–37, 2021. https://doi.org/10.1145/3431233.
[9] L. Liu, C. Chen, Q. Pei, S. Maharjan, and Y. Zhang, "Vehicular edge computing and networking: A survey," Mobile Networks and Applications, vol. 26, no. 3, pp. 1145–1168, 2021. https://doi.org/10.1007/s11036-020-01624-1.
[10] X. Sun, F. R. Yu, and P. Zhang, "A survey on cyber-security of connected and autonomous vehicles (cavs)," IEEE Transactions on Intelli gent Transportation Systems, 2021. https://doi.org/10.1109/TITS.2021.3085297.
[11] Statista, "System architecture for Autonomous Vehicles." https://encyclopedia.pub/entry/8473, online web source.
[12] M. Pham and K. Xiong, "A survey on security attacks and defense tech niques for connected and autonomous vehicles," Computers & Security, p. 102269, 2021. https://doi.org/10.1016/j.cose.2021.102269.
[13] Statista, "Components which can be attacked in CAVs." https://www.researchgate.net/figure/Cybersecurity-attack-vectors-in-CAVs_fig3_374030057, online web source.
[14] Y. Li, Q. Luo, J. Liu, H. Guo, and N. Kato, "Tsp security in intelligent and connected vehicles: Challenges and solutions," IEEE Wireless Communications, vol. 26, no. 3, pp. 125–131, 2019. https://doi.org/10.1109/MWC.2019.1800289.
[15] C. Maple, M. Bradbury, A. T. Le, and K. Ghirardello, "A connected and autonomous vehicle reference architecture for attack surface analysis," Applied Sciences, vol. 9, no. 23, p. 5101, 2019. https://doi.org/10.3390/app9235101.
[16] I. Butun, P. Österberg, and H. Song, "Security of the internet of things: Vulnerabilities, attacks, and countermeasures," IEEE Communications Surveys & Tutorials, vol. 22, no. 1, pp. 616–644, 2019. https://doi.org/10.1109/COMST.2019.2953364.
[17] Z. Ju, H. Zhang, X. Li, X. Chen, J. Han, and M. Yang, "A survey on attack detection and resilience for connected and automated vehicles: From vehicle dynamics and control perspective," IEEE Transactions on Intelligent Vehicles, 2022. https://doi.org/10.1109/TIV.2022.3186897.
[18] T. Limbasiya, K. Z. Teng, S. Chattopadhyay, and J. Zhou, "A systematic survey of attack detection and prevention in connected and autonomous vehicles," Vehicular Communications, p. 100515, 2022. https://doi.org/10.1016/j.vehcom.2022.100515.
[19] E. Aliwa, O. Rana, C. Perera, and P. Burnap, "Cyberattacks and counter measures for in-vehicle networks," ACM Computing Surveys (CSUR), vol. 54, no. 1, pp. 1–37, 2021. https://doi.org/10.1145/3431233.

[20] K. Kim, J. S. Kim, S. Jeong, J.-H. Park, and H. K. Kim, "Cybersecurity for autonomous vehicles: Review of attacks and defense," Computers & Security, p. 102150, 2021. https://doi.org/10.1016/j.cose.2020.102150.

[21] D. K. Hong, J. Kloosterman, Y. Jin, Y. Cao, Q. A. Chen, S. Mahlke, and Z. M. Mao, "Avguardian: Detecting and mitigating publish-subscribe overprivilege for autonomous vehicle systems," in Proceedings of the European Symposium on Security and Privacy (Euro S&P), pp. 445–459, IEEE, 2020. https://doi.org/10.1109/EuroSP48549.2020.00035.

[22] P. Xiong, S. Buffett, S. Iqbal, P. Lamontagne, M. Mamun, and H. Molyneaux, "Towards a robust and trustworthy machine learning system development: An engineering perspective," Journal of Information Security and Applications, vol. 65, p. 103121, 2022. https://doi.org/10.1016/j.jisa.2022.103121.

[23] T. Lauser, D. Zelle, and C. Krauß, "Security analysis of automotive protocols," in Proceedings of the Computer Science in Cars Symposium, pp. 1–12, 2020. https://doi.org/10.1145/3385958.3430482.

[24] A. S. Thangarajan, M. Ammar, B. Crispo, and D. Hughes, "Towards bridging the gap between modern and legacy automotive ecus: A software-based security framework for legacy ecus," in Proceedings of the 2nd Connected and Automated Vehicles Symposium (CAVS), pp. 1 5, IEEE, 2019. https://doi.org/10.1109/CAVS.2019.8887788.

[25] A. K. Malhi, S. Batra, and H. S. Pannu, "Security of vehicular ad-hoc networks: A comprehensive survey," Computers & Security, vol. 89, p. 101664, 2020. https://doi.org/10.1016/j.cose.2019.101664.

[26] V. Desnitsky, N. Rudavin, and I. Kotenko, "Modeling and evaluation of battery depletion attacks on unmanned aerial vehicles in crisis man agement systems," in Proceedings of the International Symposium on Intelligent and Distributed Computing, pp. 323–332, Springer, 2019. https://doi.org/10.1007/978-3-030-32258-8_38.

[27] V. L. Thing and J. Wu, "Autonomous vehicle security: A taxonomy of attacks and defences," in Proceedings of the international conference on internet of things (ithings) and ieee green computing and communications (greencom) and ieee cyber, physical and social computing (cpscom) and ieee smart data (smartdata), pp. 164–170, IEEE, 2016. https://doi.org/10.1109/iThings-GreenCom-CPSCom-SmartData.2016.52.

[28] F. Van Wyk, Y. Wang, A. Khojandi, and N. Masoud, "Real-time sensor anomaly detection and identification in automated vehicles," IEEE Trans actions on Intelligent Transportation Systems, vol. 21, no. 3, pp. 1264 1276, 2019. https://doi.org/10.1109/TITS.2019.2906038.

[29] D. Wei and X. Qiu, "Status-based detection of malicious code in internet of things (iot) devices," in Proceedings of the IEEE Conference on Communications and Network Security (CNS), pp. 1–7, IEEE, 2018. https://doi.org/10.1109/CNS.2018.8433183.

[30] S. Jeong, B. Jeon, B. Chung, and H. K. Kim, "Convolutional neural network-based intrusion detection system for avtp streams in auto motive ethernet-based networks," Vehicular Communications, vol. 29, p. 100338, 2021. https://doi.org/10.1016/j.vehcom.2021.100338.

[31] T. Shu and M. Krunz, "Privacy-preserving and truthful detection of packet dropping attacks in wireless ad hoc networks," IEEE Transactions on mobile computing, vol. 14, no. 4, pp. 813–828, 2014. https://doi.org/10.1109/TMC.2014.2330818.

[32] Statista "how attack on one CAV can impact other CAVs and complete Infrastructure." https://www.researchgate.net/figure/Cyber-attack-vectors-in-CAVs-Vehicle-to-Everything-V2X-Communication-Various-wireless_fig8_344947562, online web source.

[33] Miller, C.; Valasek, C. Remote Exploitation of an Unaltered Passenger Vehicle. Black Hat USA 2015, 2015, 1–91.

[34] Nie, S.; Liu, L.; Du, Y. Free-Fall: Hacking Tesla from Wireless to CAN Bus. Keen Security Lab in Black Hat USA. 2017. Available online: free-fall-hacking-tesla-from-wireless-to-can-bus (accessed on 20 March 2024).

[35] Cai, Z.; Wang, A.; Zhang, W.; Gruffke, M.; Schweppe, H. Roadways to Exploit and Secure Connected BMW Cars. Keen Security Lab in Black Hat USA. 2019. Available online: Microsoft Word - 0-Days&Mitigations-Roadways-to-Exploit-and-Secure-Connected-BMW-Cars.docx (accessed on 20 March 2024).

[36] R. Passerone, D. Cancila, M. Albano, S. Mouelhi, S. Plosz, E. Jantunen, A. Ryabokon, E. Laarouchi, C. Heged˝ us, and P. Varga, "A methodol ogy for the design of safety-compliant and secure communication of autonomous vehicles," IEEE Access, vol. 7, pp. 125022–125037, 2019. https://doi.org/10.1109/ACCESS.2019.2937453.

[37] S. Peter and T. Givargis, "Towards a timing attack aware high-level synthesis of integrated circuits," in Proceedings of the 34th International Conference on Computer Design (ICCD), pp. 452–455, IEEE, 2016. https://doi.org/10.1109/ICCD.2016.7753326.

[38] L. Li, J. Sun, Y. Liu, M. Sun, and J.-S. Dong, "A formal specification and verification framework for timed security protocols," IEEE Transactions on Software Engineering, vol. 44, no. 8, pp. 725–746, 2017. https://doi.org/10.1109/TSE.2017.2712621.

[39] Y. Sasaki, T. Emaru, and A. A. Ravankar, "SVM based pedestrian detection system for sidewalk snow removing machines," in Proc. IEEE/SICE Int. Symp. Syst. Integration, 2021, pp. 700–701. https://doi.org/10.1109/IEEECONF49454.2021.9382618.

[40] Y.Bian,J.Ding,M.Hu,Q.Xu,J.Wang,andK.Li,"Anadvancedlane keeping assistance system with switchable assistance modes," IEEE Trans. Intell. Transp. Syst., vol. 21, no. 1, pp. 385–396, Jan. 2020. https://doi.org/10.1109/TITS.2019.2892533.

[41] Chowdhury, Muktadir, Ashlesh Gawande, and Lan Wang. "Secure information sharing among autonomous vehicles in NDN." 2017 IEEE/ACM Second International Conference on Internet-of Things Design and Implementation (IoTDI). 2017 https://doi.org/10.1145/3054977.3054994.

[42] Shin, H., Kim, D., Kwon, Y., & Kim, Y. (2017, September). Illusion and dazzle: Adversarial optical channel exploits against lidars for automotive applications. In International Conference on Cryptographic Hardware and Embedded Systems (pp. 445-467). Springer, Cham. https://doi.org/10.1007/978-3-319-66787-4_22.

[43] Litman, Todd. Autonomous vehicle implementation predictions. Victoria, Canada: Victoria Transport Policy Institute, 2017.

[44] B. Sheehan, F. Murphy, M. Mullins, and C. Ryan, "Connected and autonomous vehicles: A cyber-risk classification framework," Transp. Res. Part A Policy Pract., vol. 124, no. November 2018, pp. 523–536, 2019, https://doi.org/10.1016/j.tra.2018.06.033.

[45] M. F. Zolkipli and A. Jantan, "Malware behavior analysis: Learning and understanding current malware threats," Proc. - 2nd Int. Conf. Netw. Appl. Protoc. Serv. NETAPPS 2010, no. September, pp. 218–221, https://doi.org/10.1109/NETAPPS.2010.46.

[46] Lee, H.; Jeong, S.H.; Kim, H.K. OTIDS: A Novel Intrusion Detection System for In-vehicle Network by Using Remote Frame. In Proceedings of the 2017 15th Annual Conference on Privacy, Security and Trust (PST), Calgary, AB, Canada, 28–30 August 2017; pp. 57–5709. https://doi.org/10.1109/PST.2017.00017.

[47] Lo,W.; Alqahtani, H.; Thakur, K.; Almadhor, A.; Chander, S.; Kumar, G. A hybrid deep learning based intrusion detection system using spatial-temporal representation of in-vehicle network traffic. Veh. Commun. 2022, 35, 100471. https://doi.org/10.1016/j.vehcom.2022.100471.

[48] GuardKnox. Zonal Architecture: The Foundation for Next Generation Vehicles. Available online: https://learn.guardknox.com/ zonal-architecturethe-foundation-for-next-generation-vehicles-1 (accessed on 5 August 2023).

[49] Lo,W.; Alqahtani, H.; Thakur, K.; Almadhor, A.; Chander, S.; Kumar, G. A hybrid deep learning based intrusion detection system using spatial-temporal representation of in-vehicle network traffic. Veh. Commun. 2022, 35, 100471. https://doi.org/10.1016/j.vehcom.2022.100471.

[50] Eckermann,E.WorldHistoryoftheAutomobile;SAEPress:Warrendale,PA,USA,2001.

[51] Zhang,T.;Antunes,H.;Aggarwal,S.DefendingConnectedVehiclesAgainstMalware:ChallengesandaSolutionFramework. IEEEInternetThingsJ.2014,1,10–21. https://doi.org/10.1109/JIOT.2014.2302386.