

Developing a machine learning-based algorithm for secure routing in autonomous vehicles

Shwetansh Priyadarshi, Alok Srivastava

Department of Electronics and Communication, School of Engineering Sciences, GD Goenka University, Gurugram, Haryana, India

Article Info

Article history:

Received Oct 12, 2025

Revised May 23, 2026

Accepted Jul 5, 2026

Keywords:

Autonomous cars
Connected vehicles
Cyber-crimes
Malicious-attacks
Route diversion

ABSTRACT

Over the last several years, we have noticed that the administration and car companies have been refraining from investing capital in connected autonomous cars. A chain of interconnected sensors, actuators, and devices—combining lidar, GPS, radar, in-system machines, cameras, and more—allows autonomous cars to learn how to operate in real-time scenarios. However, data from recent cyberattacks and mishaps suggests that malicious attackers can access this sensor data or even the main control system through hacking, leading to a variety of losses. As time passes by, people will be less interested in connected autonomous vehicles (CAVs), and various surveys say that it will be mainly because of the absence of a proper security infrastructure. A study of cyberattacks on CAVs and strategies to eliminate them is discussed in this study. In this study, we have proposed a hybrid model solution that uses convolutional neural network (CNN), long short-term memory (LSTM), and gated recurrent unit (GRU), and we are optimizing the Hyperparameters using the dwarf mongoose optimization algorithm (DMOA). The proposed model is also tested in Comparison with other existing models, and we are able to detect DoS, fuzzy, spoofing the driving gear, and spoofing the RPM gauge attacks with an accuracy of more than 98%.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Shwetansh Priyadarshi
Department of Electronics and Communication, School of Engineering Sciences
GD Goenka University
Gurugram, Haryana, India
Email: shwetansh08@gmail.com

1. INTRODUCTION

As security vulnerabilities in connected autonomous vehicles (CAVs) are a major concern for human life and infrastructure security, it is always suggested to have a robust architecture in terms of cybersecurity for CAVs. Many Autonomous car manufacturers have impactful ideas that focus on the security area, and they have made huge strides. However, the proposed solution methods are not able to meet the requirements, and there are still several security vulnerabilities that persist across the industry. In this research, Level 5 of CAVs are evaluated. With this recommended solution, it is expected to provide a safe and secure environment for Autonomous cars and car users. This solution should be able to help in processing the operation of dataset segregation to be used for emergency (SOS), mapping, and manoeuvre scenarios by linking to the databases connected in the CAV architecture. The solution available over the globe uses convolutional neural networks (CNN), recurrent neural networks (RNN), or artificial neural network (ANN) model for training their CAV systems, which are hardly able to achieve an accuracy of 85% [1]-[6]. But, the model which we are proposing is a hybrid model of RNN and CNN with hyperparameter

tuning and is expected to have 99% accuracy. The solution expected in this paper is based on machine Learning, which provides a real-time interconnection layer [7].

2. LITERATURE REVIEW

For this Article, we have used 150+ manuscripts for our reference study, and after careful, in-depth study, we found around 50 manuscripts aligning closely to our research area. The cybersecurity issue, data security challenges, and also the cyberattacks in Autonomous cars are a very vast area, and our research is very much restricted to securing the route of connected autonomous cars. Our research area also draws a thin line between previous research and our research as securing the route of fully autonomous cars encompasses all the major issues in Autonomous cars. If there is any malfunction in the data coming from the cloud, if the ADAS of AV is attacked, or if the sensors, radars, GPS or any car mounted equipment's which collects data from external sources are being compromised, then it is very likely that the route of Autonomous cars can be compromised. There are certain points of access that cyber criminals exploit to get access to CAVs' systems and that need robust security in order to avoid these attacks, which we found missing in the previous research papers.

In our research, we have tried to cover those areas and also provide a latest and very robust mechanism which not only safeguards the route of Autonomous cars but also provides a safe driving environment for cars and car owners, in which car drivers' safety is also not compromised. The Previous deep learning models i.e. CNN, ANN, or traditional RNN failed in one way or another, and in this research, we have tried to address all the existing loopholes in these models. In solution to the gaps and loopholes in these models, we have proposed a hybrid model that comprises of CNN+long short-term memory (LSTM)+ gated recurrent unit (GRU). This helps in adjusting and fixing even the smallest failures of any individual model. This model is followed with an aim to achieve higher accuracy and provide a robust and secure model; after that we have tried optimization with dwarf mongoose optimization algorithm (DMOA) i.e., hyperparameters (neurons in each layer) are optimized using the DMOA.

3. RESEARCH METHOD

3.1. Working of autonomous vehicles

CAVs, also known as independent cars i.e. it depends upon the level of Automation these cars have as shown Table 1, perform actions using a combination of super-advanced features that allow them to understand their surroundings, make decisions, and control the vehicle without human assistance [8]-[10]. So, in order to understand complete functioning of Autonomous vehicles, it can be segregated on a role basis:

- a) **Sensors:** These sensors help Autonomous vehicles with vision and give them the ability to perform actions. CAVs are well equipped with smart sensors to detect the surroundings. Autonomous Vehicles are equipped with Lidar, Radar, Cameras, and Ultrasonic sensors.
- b) **Localization:** In order to navigate properly, CAVs need exact locations on a regular basis. Autonomous vehicles are equipped with GPS, High-definition maps, and sensor fusion, which combines data from sensors and maps.
- c) **Perception:** This is about what is happening in and around the vehicle. In order to keep track of cars, objects, street walkers, cyclists, road signs, and traffic signals. It uses AI and machine vision to understand the raw data from sensors.
- d) **Planning:** This is all about how autonomous cars plan their work, what algorithm is being used to navigate from one place to another, making real-life decisions, planning complete route, and approaching the destination.
- e) **Control:** This segment is all about the major control of how AVs deal with steering, brakes, and acceleration. The complete system manages and adjusts itself to keep the vehicle on course safely.
- f) **Artificial intelligence:** It works as the brain of CAVs. The car's system is well trained with huge datasets i.e. various case scenarios and how to handle them. It can predict behaviour, recognize patterns, and act according to various situations.

3.2. Types of autonomous vehicles

When the vehicles started coming to market at that time not even 0.1% automation was there and with time the automation level increased; this can be seen in Table 1.

3.3. Working of deep learning models

Connected Autonomous cars use various algorithms to function based on AI and machine learning, such as cryptographic algorithms and set of protocols as a combination to safeguard the cars from cyber

threats [11]. These algorithms are the backbone on which the complete AVs system work such as securing the connections and communications, controlling the access, and safeguarding the data, as shown in Figure 1.

- a) Encryption algorithm: Encryption is mainly divided into two types, i.e. symmetric and Asymmetric algorithm. Symmetric algorithms are used for large amounts of data and in that cars use advanced encryption standard (AES) for storing data and safeguarding communication [12]-[15]. Moreover, Asymmetric algorithm encrypted key exchange, authentication, secure login. It used RSA for digital signs and interchanging the keys and elliptic curve cryptography (ECC) is used for efficient embedded system in vehicles.
- b) Hashing algorithm: It is used for data integration by using SHA-256 / SHA-3 to verify software's and securing blockchain logs.
- c) Secure communication protocols: Its uses transport layer security (TLS) for data encryption between V2X, datagram TLS (DTLS) used for UDP based Communication, IPsec used for protecting data packets.
- d) Message authentication codes (MACs): is used in order to verify and protect messages with the help of hash-based message authentication code (HMAC).
- e) Intrusion detection algorithms: It is used to detect suspicious behaviour and any invasion attempts on car. There are two types of IDS used normally machine learning-based and rule-based IDS.
- f) Digital signatures: is a supplementary way of protection used for verifying the message and data coming from various sources. It uses elliptic curve digital signature algorithm (ECDSA) and RSA Digital Signatures.
- g) Blockchain: This is not mandatorily used but it is used for securing the logging of data to avoid tampering.

Table 1. Level of automation

Category	Human assistance	Level of automation
Traditional	Yes	0 – Manual Control
Smart	Yes/No	1 – Driver Required
Smart	Yes/No	2 – Partial Support Required
Autonomous	Yes/No	3 – Conditional Assistance
Autonomous	Yes/No	4 – Highly Automated
Autonomous	No	5 – Fully Automated

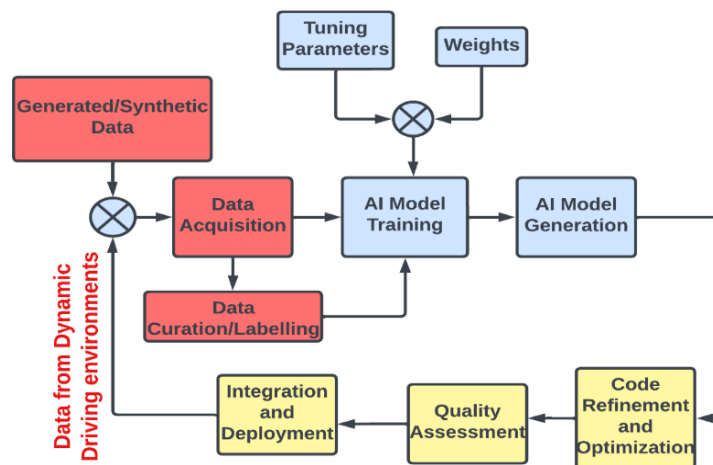


Figure 1. Working of ML algorithms [13]

3.4. Existing models

There are models on which Autonomous cars work i.e. how these algorithms function. So, overall, this is performed by machine learning which comes under the AI segment of CAVs [16]-[25]. Here instead of doing programming, system is made to learn and enhance itself with the help of huge datasets. These trainings involve algorithms that can evaluate data, recognize patterns, and predict coming situations based on available patterns. Deep learning plays a very vital role in working of autonomous vehicles such as seeing, analysing, and reacting. These models are eyes, brain, hands for autonomous vehicles Figure 2.

- a) CNNs: It is used for anticipation, detecting objects, recognizing traffic signals and signs, detecting the marking of lanes. It uses semantic segmentation to distinguish between walkable area and driving area, lane recognition, etc. It also uses single shot detector (SSD) for faster tracking of object and acting as per the requirement.
- b) RNNs and LSTMs: These models are used for detecting the behaviour of cars, and pedestrians. Here LSTM is used for predicting the behaviours of other cars, and pedestrians.
- c) Transformer models: This model is introduced for self-attention, and evaluation of scenes and deciding the appropriate action. This model is also responsible for Sensor fusion (e.g., combining LiDAR + cameras).

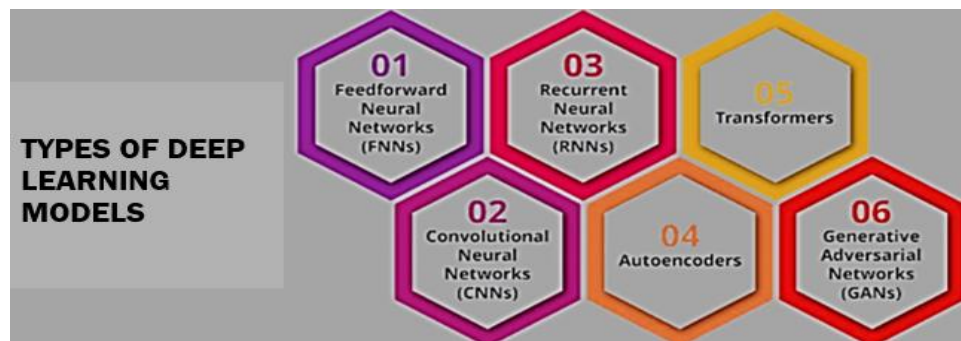


Figure 2. Models of deep learning used in CAV [20]

3.5. Types of attacks addressed in our model

In the proposed model we are focusing on 4 major cyber-attacks, which have devastating consequences on autonomous vehicles such as loss of vehicle, loss of life, loss of Infrastructure, large scale traffic Incidents which lead to loss of life for other road users too [25]-[35]. Attacks included in our model are:

- a) DoS attack: DoS stands for denial-of-Service attack by flooding the autonomous vehicles communication system, so that the cars network resources are unavailable to provide the service. These malicious traffic makes the actual data inflow troublesome and this leads to failing of sensors and safety devices in autonomous vehicles.
- b) Fuzzy attacks: Fuzzy attacks are ways to expose the vulnerabilities of autonomous cars by inserting the random data packets into the vehicle's controller area network which makes the behaviour of vehicle outside the expectations of car owner or can be called as very unpredictable for car users.
- c) Spoofing the driving gear: This is one of the dangerous attacks in autonomous vehicle where attackers send false status of vehicles current gear status to the controller area network bus. For example: - park, reversal, neutral, and drive. this leads to unsafe actions by vehicle which will be contradictable to vehicle and environment's current demand.
- d) Spoofing the RPM gauge: Spoofing the revolution per minute (RPM) gauge in an autonomous vehicle is a cyber-attack practice by attackers to inject a false or malicious message about the RPM or the engine's speed to the controller area network-bus. This act is done with an aim to trick the action of control system of vehicle which leads to misunderstanding at electronic unit control (ECU) Level. Here, when ECU believes that the vehicle or engine is running at different speed than the actual speed which leads to actions like changing the gear or some unpredictable action that can be hazardous.

3.6. Proposed model

Even after using deep learning techniques and introducing models like CNN, RNN, and ANN. we are unable to achieve accuracy in terms of cyber-attacks. This is a potential threat that is causing loss of data, loss of lives, and loss of infrastructure. To overcome this, we are introducing a model that will be having higher accuracy than the existing models [35]-[40]. If we try to understand the accuracy by data CNN- 85% accuracy, RNN- 85.6% accuracy, ANN- 80% accuracy, which have been highlighted in previous studies as well [41]. We are introducing a model that will be a combination of an advanced RNN and CNN model and this will increase the accuracy percentage Figure 3. Moreover, in this hybrid model we will be introducing concept of hyperparameter tuning on dataset of CNN and advanced RNN. So, this will give us a higher accuracy, which is expected to be 95% and above.

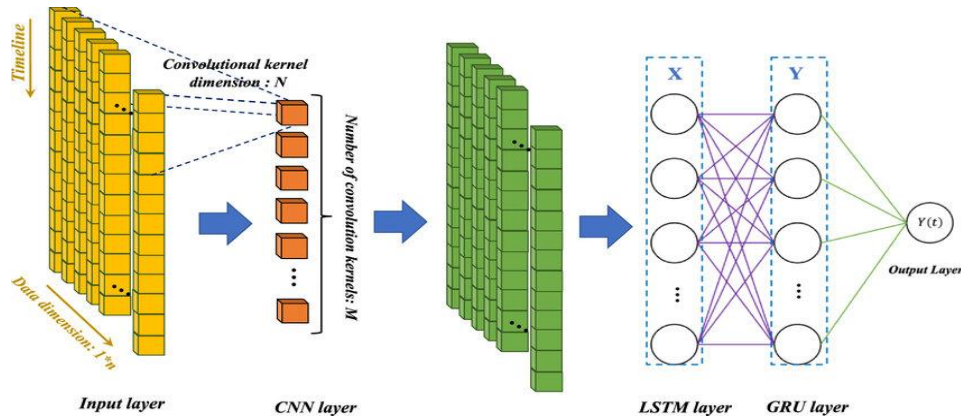


Figure 3. Representation of hybrid model

3.7. Flow-chart of proposed model

This section consists of a flowchart that explains the entire workflow of our model and how the results are achieved Figure 4. Starting from data loading till classification of attacks is explained in this flowchart.

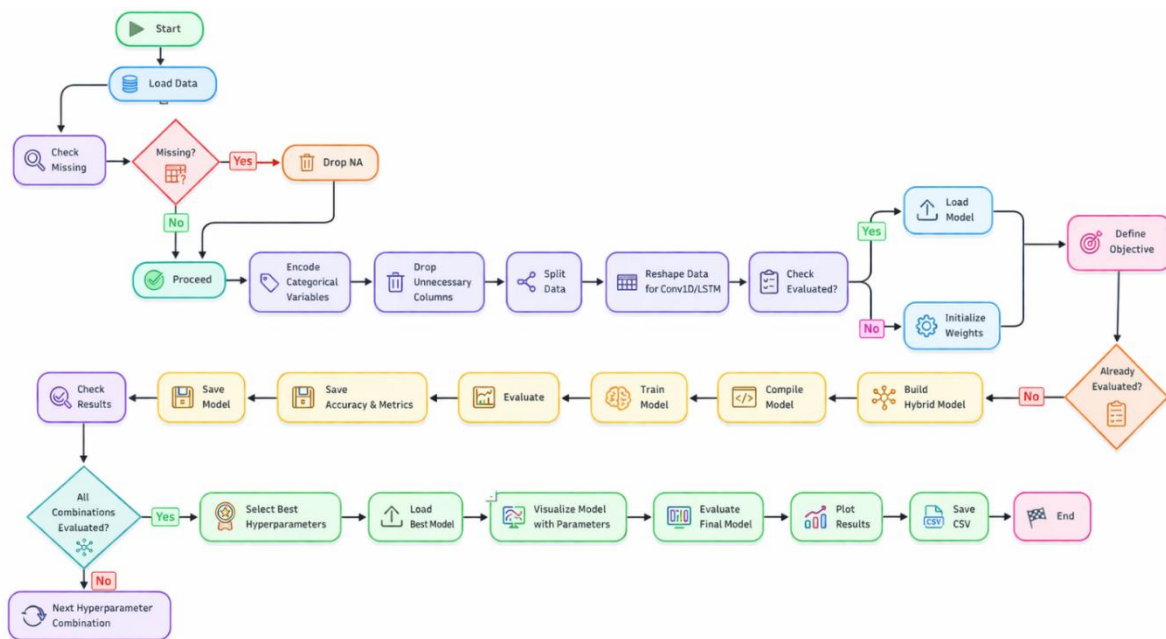


Figure 4. Workflow of proposed model

3.8. Model architecture

In the year of 2025, still Autonomous car is an emerging topic and when we say or term it as Emerging it means that lot can be changed and lot can be improved. The mounted equipment's i.e. the cameras, the sensors they struggle in heavy fog and in hilly areas. This equipment fails or struggle in detected traffic incidents, pedestrian activities [42]-[45]. If we talk about the highly equipped and advanced deep learning models i.e. CNN, ANN, RNN struggles or fail when the scenario differs from the training data. These Autonomous cars completely rely on internet which also creates threat of Cyber-attacks [46]. This leads to fear among people who are scared of giving full control to machines.

We are proposing a model by addressing all the research gaps in the previous research papers. Our model Comprises of CNN+LSTM+GRU model as shown in Figure 5, in this LSTM and GRU are the types of latest RNN models which helps in overcoming all the challenges faced by traditional RNN. We have used

these models to overcome the challenges faced by the other model i.e. CNN for feature extraction with LSTM and GRU for sequence learning. The Result attained by this model was 85.47% which was near to accuracy attained by CNN model. Then, in order to achieve better accuracy, we have done optimization using DMOA. The Neurons in each layer are optimized by using the DMOA. A dictionary and CSV logs are used to track the previously evaluated architectures, which prevents from redundant computations. Then we are performing model training by training Each candidate model for 5 epochs and using early stopping which prevents overfitting. Post that performance evaluation is done by measuring the Accuracy on the test set to guide the optimization process. After optimization, the best-performing model is reloaded for evaluation.

3.9. Experimental procedure

In our Research, we have performed multiple steps starting from data collection, data evaluation, removal of null values, performing over fitting and underfitting, correlation analysis. And post this we evaluate all the existing models and check for the accuracy. Once we are aware of the loopholes in the existing models then we have performed the process on our model and then applied hyper parameter tuning using DMOA.

If we start from the very basic requirements, then it will be the software requirements. We used python and Anaconda. This is a prerequisite for performing this procedure, post which we moved to data pre-processing part. Data pre-processing is all about preparing the raw data and making it suitable for machine learning model. This is the very first step in developing a Machine Learning Model. And to make it happen we need to import all the necessary libraries which performs the operations under Data Pre-processing. In next steps, processing of CAN log files happens i.e. output directory gets created if it doesn't exist and then iterates through CSV files in input directory. Each file is read in while handling parsing errors, and it is also ensured that all the expected columns exist and then cleaned dataset is saved. In Further steps, class labels are assigned i.e. all the processed CSV files are read and it is ensured that column structure is consistent. It reads Processed CSV files, adds a new class Column. Here Default is normal, sets a specific class labels based on the file name and the flag value (T for Attacks). Then Combines all dataset into one and saves it. Once this is done, then dataset is combined and saved which are in Hexadecimal form. Now, the Hexadecimal values are converted to Decimal Values and then we get the updated dataset. Now, we perform a sanity on dataset to check if the structure is proper or not. In next steps, we perform class distribution visualization Figure 6.

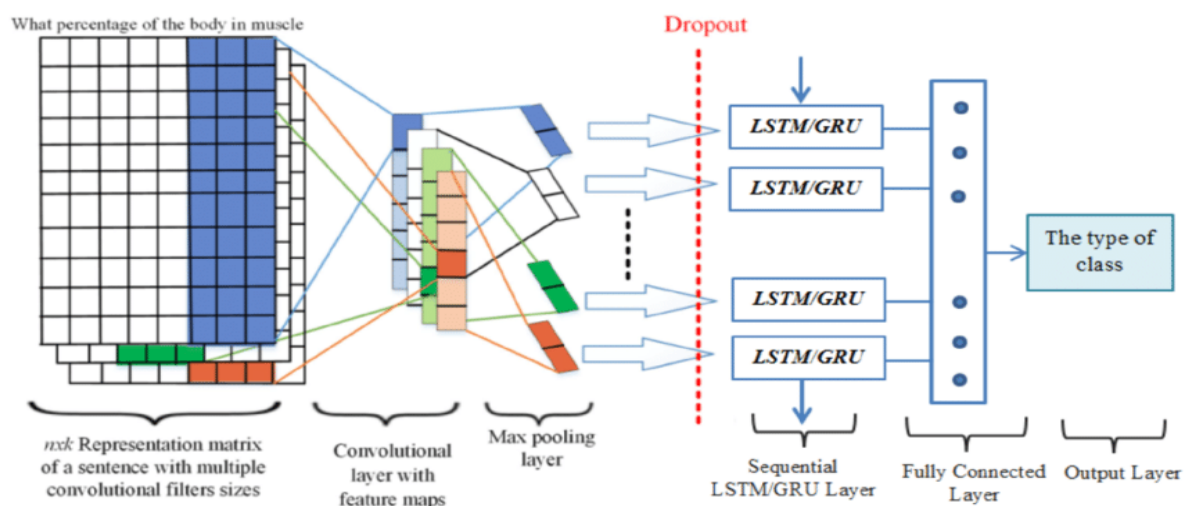


Figure 5. Architecture of a hybrid model- CNN+LSTM+GRU

In next steps, we encode categorical variables (Flag, class) into numerical values and then we perform Feature correlation analysis i.e. computes and visualizes feature correlations as shown in Figure 7. Moving next, we perform Activity of Dropping unnecessary features in which we remove all the low relevance features. At this stage we have our final dataset ready for use, now we separate the dataset into test set and train set i.e. we are separating features (x) from labels (y). Here, we are separating the dataset in a proportion of 80% for training and 20% for testing. Once this is completed, we will evaluate all the existing models and its accuracy before we moved to our model.

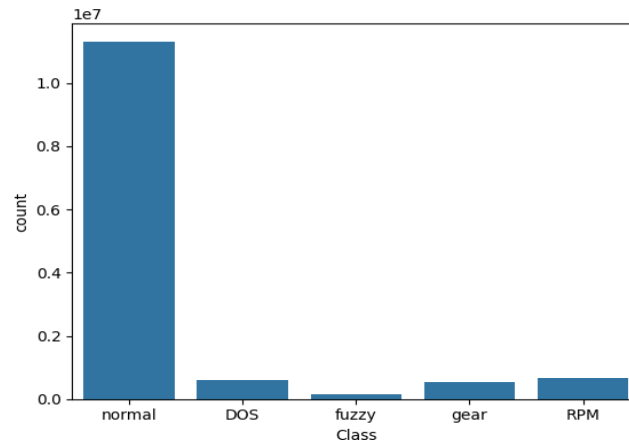


Figure 6. Class distribution visualization

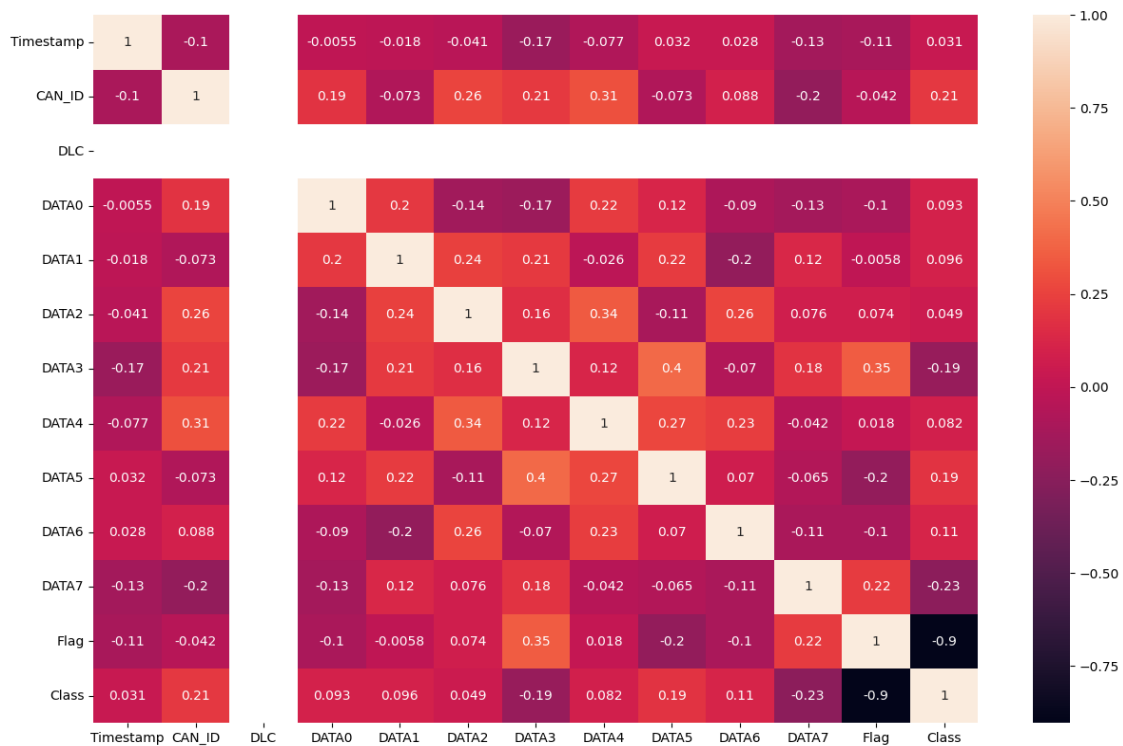


Figure 7. Feature correlation analysis

Post this we test all the existing models i.e., ANN, CNN, RNN and other Hybrid Models to test their Accuracy. And on the basis of that we decided that what are the neural networks that can give our model a better face. So, once we Completed the Validation we formed a Hybrid Model of CNN, LSTM and GRU. CNN fulfils our need of feature Extraction with LSTM and GRU meets the requirement of Sequential Learning. Below is the Result Attained from our Model Table 2.

Table 2. Results achieved from hybrid model				
	Precision	Recall	F1-score	Support
Accuracy			0.85	1323765
Macro Average	0.17	0.20	0.18	1323765
Weighted Average	0.73	0.85	0.79	1323765

Since the Attained Accuracy was not meeting our requirement, we Performed Hyper-parameter Tuning. The Process of Optimization with DMOA was performed. Here hyper-parameters (neurons in each Layer) are optimized using DMOA. Then all the Evaluation Combinations are tracked i.e., a dictionary and CSV log are used to track previously evaluated architectures, preventing redundant computations. And once this is done, we perform Model training, where Each candidate model is trained for 5 epochs using early stopping to prevent overfitting. At last, Accuracy is measured on the test set to guide the optimization process Table 3.

Table 3. Results post hyper-parameter tuning

Accuracy	Precision	Recall	F1-Score
0.999797	0.999797	0.999797	0.998233

3.10. Mathematical expressions and symbols

Post that performance evaluation is done by measuring the Accuracy on the test set to guide the optimization process. After optimization, the best-performing model is reloaded for evaluation as shown in Figure 8.

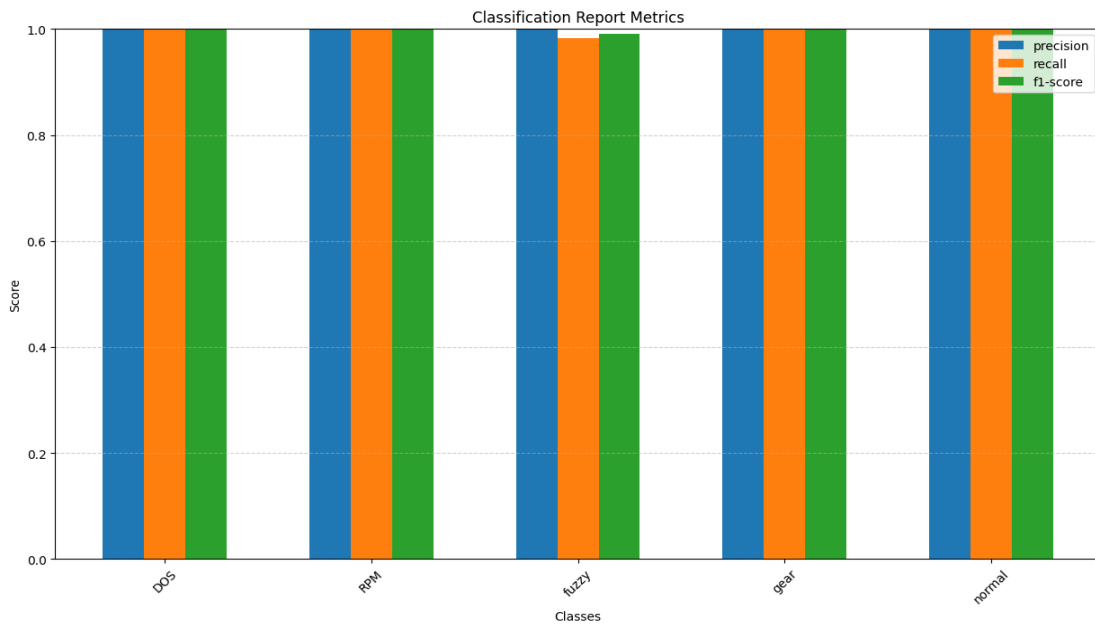


Figure 8. Classification plot for our hybrid model

Explanation:

- z_j : Raw output (logits) from your model for class j
(computed as $z = W_o h^{(d)} + b_o$)
- e^{z_j} : Exponential of that value (makes everything positive)
- Denominator: Sum of exponentials of all class scores

$$y_j = \frac{e^{z_j}}{\sum_{k=1}^5 e^{z_k}}, \text{ where } z = w_o h^{(d)} + b_o$$

the final prediction vector is

$$\hat{y} = [y_1, y_2, y_3, y_4, y_5], \sum y_j = 1$$

$$z = W_o h^{(d)} + b_o$$

Process of linear transformation:

$h^{(d)}$: Final hidden layer output (from CNN + LSTM + GRU)

W_o : Weight matrix

b_o : Bias

This produces the logits (z values) before SoftMax. Final prediction vector

$$\hat{y} = [y_1, y_2, y_3, y_4, y_5]$$

This is the final output.

Each y_j = probability of class j

4. RESULTS AND DISCUSSION

4.1. Why DMOA?

The DMOA is a very latest metaheuristic optimization algorithm which is totally inspired by the foraging behavior of dwarf mongoose. Similarly, we have other algorithms like grey wolf whale optimization, particle swarm optimization algorithm, genetic algorithm, and ant colony [47]. We cannot say that DMOA is the most superior optimization Algorithm of all the existing ones for deep learning but as per our requirement and use it is quite powerful for continuous optimization, tuning of hyper parameters and this algorithm have shown best results in engineering optimization tasks. The dwarf mongoose is specialized in exploring, searching wide regions of the solution spaces and it focuses on the best candidate solution.

4.2. Comparison table (Key Findings)

In this research we have not only developed a Hybrid model but also worked on all the existing loopholes found in previous models. In order to develop a Hybrid model which is the combination of CNN+LSTM+GRU i.e. CNNs for feature extraction, with LSTM and GRUs to process temporal dependencies and sequential Learning, we have also studied individually the CNN, ANN, RNN, LSTM. The individual study of models helped us in knowing the positive part and also the loopholes which makes these models outdated with time. As Autonomous cars are growing topic and there are lot more things to come, lot more technologies are about to come and many more to get outdated. So, this field can never have optimal solutions for its problems, at least in near future we cannot imagine it.

4.3. Limitations and scope for future research

As it is already known that Autonomous cars are emerging topic and with every passing day things, technologies, infrastructure, models, level of Automation, etc. is changing and parallelly the types of cyber-Attacks are also changing. So, Our Proposed model can be suitable for the Current day Scenario but it cannot be guaranteed that this will be able to meet all the future Cyber Attacks and Upcoming challenges. Our Model cannot be an optimal solution to all the Attacks in terms of Autonomous Vehicles and with new technologies arriving in market this needs to be upgraded. If we take example of DMOA which was launched in 2022 and as per the current scenario and requirement, we found it to be a perfect metaheuristic Algorithm. But in coming days this will be definitely changing and this model will be termed as outdated.

4.4. Achieved results

We have not just fixed the current Problems but also applied that latest algorithm i.e., we have applied optimization with Dwarf Mongoose Algorithm on Hybrid model as shown in Table 4. This helped us in attaining much higher accuracy than the previous existing models as shown in Figure 9.

The hyper parameter tuning performed over the hybrid model will tweak the performance of model which leads to optimal results as shown in Figure 10. Basically, what happens inside hyper parameter is really interesting, it is a kind of experimental method till the best values are achieved. So, we can call a good hyper parameter tuning when the overall performance from the Deep learning model is high as per the allotted metrics as shown in Figure 11.

Table 4. Comparison between 3 models

Model name	Accuracy	Precision
CNN Model	0.96	0.96
ANN Model	0.85	0.85
Hybrid Model	0.99	0.99

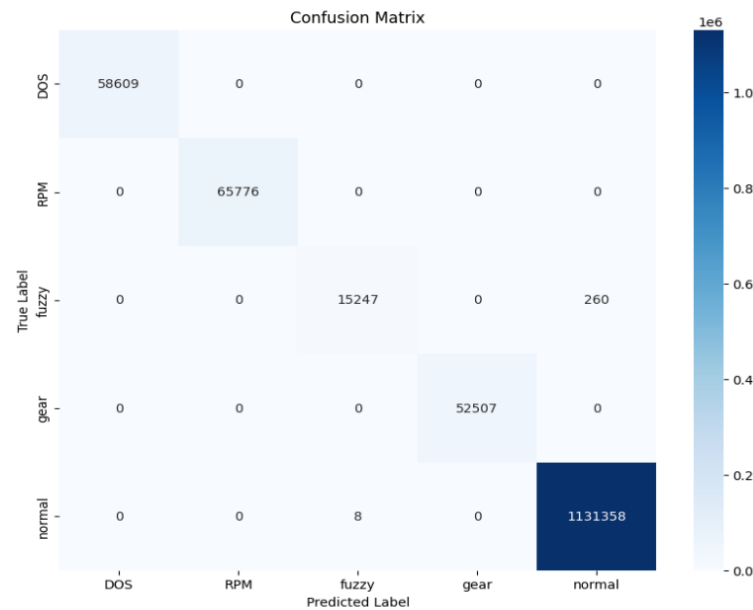


Figure 9. Confusion matrix is visualized using seaborn heatmap to analyse prediction errors across classes

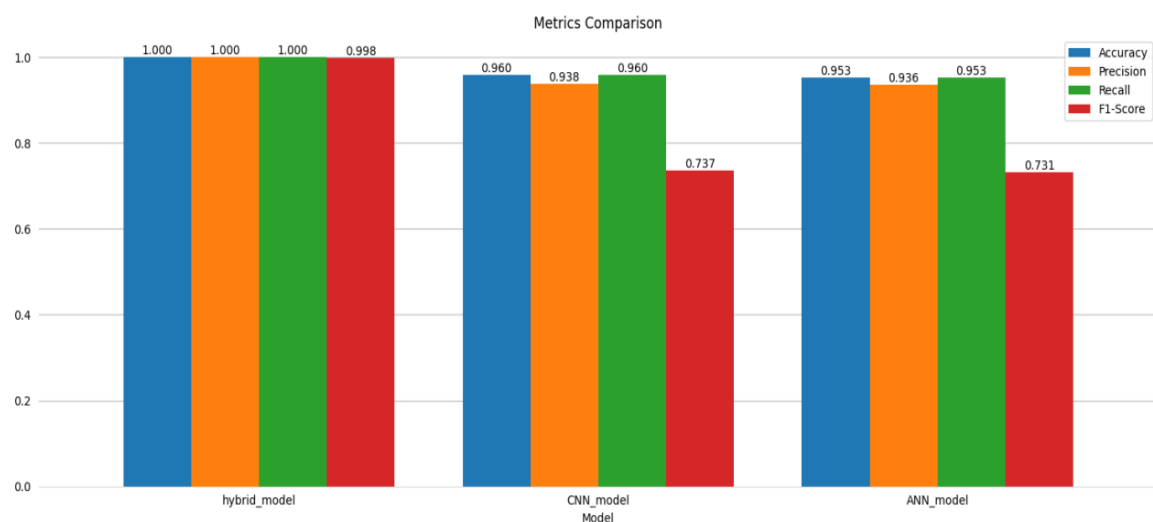


Figure 10. Comparison of different metrics, precision, recall and f1 score for the models

```

Accuracy: 0.9997975471477188
Precision: 0.9997974910546847
Recall: 0.9997975471477188
F1: 0.9982339049929143

```

Figure 11. End result for proposed model

5. CONCLUSION

Deep learning plays an important role in detecting complex datasets and distinguishing between attacked data and genuine data, making them more reliable, accurate, and faster for investigating issues. In this study, we address the challenge of cyber-attacks which diverts the route of AVs or leads to loss of life and infrastructure due to data tampering. The hybrid model which we are suggesting here for Autonomous vehicles meets the ISO standard.

ACKNOWLEDGMENTS

This study presented in this paper is with support of GD Goenka University, India. This research is part of my doctoral degree in school of engineering sciences under supervision of multiple professors and staffs. This research is performed with an aim of achieving sustainable model to provide safe environment for Autonomous car users. The Authors are thankful to the University and entire department for regular feedbacks and support.

FUNDING INFORMATION

There was no funding involved in this research.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Shwetansh Priyadarsh	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓		✓	
Alok Srivastava	✓			✓						✓		✓		

C : **C**onceptualization

M : **M**ethodology

So : **S**oftware

Va : **V**alidation

Fo : **F**ormal analysis

I : **I**nterpretation

R : **R**esources

D : **D**ata Curation

O : Writing - **O**riginal Draft

E : Writing - Review & **E**dit

Vi : **V**isualization

Su : **S**upervision

P : **P**roject administration

Fu : **F**unding acquisition

CONFLICT OF INTEREST STATEMENT

This research manuscript which is all about thoughts of giving a safer Autonomous Vehicle is not having any conflict of interest, i.e., in personal, professional, and financial way. We have tried performing all the activities in this research with an aim to give a transparent and genuine research.

DATA AVAILABILITY

- We have used dataset for performing this research and from which we segregated into test, train and validation dataset. The complete dataset can be found on: - <https://ocslab.hksecurity.net/Datasets/car-hacking-dataset>
- We have tried giving a model that is more robust and secure than the existing models and for that we have chosen DMOA which we found more superior than the other optimization Algorithms. Base paper for my research can be found here: - <https://doi.org/10.3390/s24123848>
- There is one more base paper which was closely relevant to our research and to which we referred in our journey: <https://doi.org/10.1016/j.vehcom.2024.100837>

Other relevant data of research and detailed result analysis can be made available on genuine request by mailing to the corresponding author on the contact details provided.

REFERENCES

- [1] S. K. Khan, N. Shiwakoti, P. Stasinopoulos, and Y. Chen, "Cyber-attacks in the next-generation cars, mitigation techniques, anticipated readiness and future directions," *Accident Analysis & Prevention*, vol. 148, p. 105837, Dec. 2020, doi: 10.1016/j.aap.2020.105837.
- [2] Q. He, X. Meng, R. Qu, and R. Xi, "Machine learning-based detection for cyber security attacks on connected and autonomous vehicles," *Mathematics*, vol. 8, no. 8, p. 1311, Aug. 2020, doi: 10.3390/math8081311.
- [3] S. K. Khan, N. Shiwakoti, P. Stasinopoulos, and M. Warren, "Security assessment in Vehicle-to-Everything communications with the integration of 5G and 6G networks," in *2021 International Symposium on Computer Science and Intelligent Controls (ISCSIC)*, Nov. 2021, pp. 154–158, doi: 10.1109/iscsic54682.2021.00037.
- [4] S. Khalid Khan, N. Shiwakoti, and P. Stasinopoulos, "A conceptual system dynamics model for cybersecurity assessment of connected and autonomous vehicles," *Accident Analysis & Prevention*, vol. 165, p. 106515, Feb. 2022, doi: 10.1016/j.aap.2021.106515.
- [5] S. Khalid Khan, N. Shiwakoti, P. Stasinopoulos, and M. Warren, "Modelling cybersecurity regulations for automated vehicles," *Accident Analysis & Prevention*, vol. 186, p. 107054, 2023, doi: 10.1016/j.aap.2023.107054.
- [6] J. Raiyn, "Data and cyber security in autonomous vehicle networks," *Transport and Telecommunication Journal*, vol. 19, no. 4, pp. 325–334, Nov. 2018, doi: 10.2478/tjt-2018-0027.

- [7] J. Takahashi, "An overview of cyber security for connected vehicles," *IEICE Transactions on Information and Systems*, vol. E101.D, no. 11, pp. 2561–2575, Nov. 2018, doi: 10.1587/transinf.2017ici0001.
- [8] A. Ganesan, J. Rao, and K. Shin, "Exploiting consistency among heterogeneous sensors for vehicle anomaly detection," in *SAE Technical Paper Series*, Mar. 2017, vol. 1, doi: 10.4271/2017-01-1654.
- [9] H. Lee, S. H. Jeong, and H. K. Kim, "OTIDS: a novel intrusion detection system for in-vehicle network by using remote frame," in *2017 15th Annual Conference on Privacy, Security and Trust (PST)*, Aug. 2017, pp. 57–5709, doi: 10.1109/pst.2017.00017.
- [10] M. Abdalla and Y. Arshad, "Information security: cybersecurity standards adoption among Malaysian public listed companies," *International Journal of Engineering Research and Technology (IJERT)*, vol. 9, pp. 929–933, 2020.
- [11] C. Natoli and V. Gramoli, "The balance attack or why forkable blockchains are ill-suited for consortium," in *2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, 2017, pp. 579–590, doi: 10.1109/dsn.2017.44.
- [12] M. Patel et al., "Autonomous vehicles: Ethical dilemmas," *International Journal of Advanced Research and Publications*, vol. 3, no. 8, 2019.
- [13] X. Jin, W. M. Haddad, Z. Jiang, A. Kanellopoulos, and K. G. Vamvoudakis, "An adaptive learning and control architecture for mitigating sensor and actuator attacks in connected autonomous vehicle platoons," *International Journal of Adaptive Control and Signal Processing*, vol. 33, no. 12, pp. 1788–1802, 2019, doi: 10.1002/acs.3032.
- [14] B. S. Lim, S. L. Keoh, and V. L. L. Thing, "Autonomous vehicle ultrasonic sensor vulnerability and impact assessment," in *2018 IEEE 4th World Forum on Internet of Things (WF-IoT)*, Feb. 2018, pp. 231–236, doi: 10.1109/wf-iot.2018.8355132.
- [15] Y. Qian, M. Chen, J. Chen, M. S. Hossain, and A. Alamri, "Secure enforcement in cognitive internet of vehicles," *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 1242–1250, Apr. 2018, doi: 10.1109/jiot.2018.2800035.
- [16] M. Amoozadeh et al., "Security vulnerabilities of connected vehicle streams and their impact on cooperative driving," *IEEE Communications Magazine*, vol. 53, no. 6, pp. 126–132, 2015, doi: 10.1109/mcom.2015.7120028.
- [17] S. Plosz and P. Varga, "Security and safety risk analysis of vision guided autonomous vehicles," in *2018 IEEE Industrial Cyber-Physical Systems (ICPS)*, May 2018, pp. 193–198, doi: 10.1109/icphys.2018.8387658.
- [18] H. Shin, D. Kim, Y. Kwon, and Y. Kim, "Illusion and dazzle: adversarial optical channel exploits against lidars for automotive applications," in *Cryptographic Hardware and Embedded Systems – CHES 2017*, Springer International Publishing, 2017, pp. 445–467.
- [19] S. Jeong, B. Jeon, B. Chung, and H. K. Kim, "Convolutional neural network-based intrusion detection system for AVTP streams in automotive Ethernet-based networks," *Vehicular Communications*, vol. 29, p. 100338, 2021, doi: 10.1016/j.vehcom.2021.100338.
- [20] B. D. Silva, "Exploring the relationship between cybersecurity culture and cyber-crime prevention: a systematic review," *International Journal of Information Security and Cybercrime*, vol. 12, no. 1, pp. 23–29, 2023, doi: 10.19107/ijisc.2023.01.03.
- [21] B. Geluvaraj et al., "The future of cybersecurity: Role of AI, ML, and DL," *Proceedings of the International Conference on Communication, Computing and Networking Technologies (CCNCT)*, 2018.
- [22] J. Raijn, "Road traffic congestion management based on a search-allocation approach," *Transport and Telecommunication Journal*, vol. 18, no. 1, pp. 25–33, Feb. 2017, doi: 10.1515/ttj-2017-0003.
- [23] M. Uma and G. Padmavathi, "A survey on various cyber attacks and their classification," *International Journal of Network Security*, vol. 15, no. 6, pp. 391–397, 2013.
- [24] C. Schmittner, T. Gruber, P. Puschner, and E. Schoitsch, "Security application of failure mode and effect analysis (FMEA)," in *Computer Safety, Reliability, and Security*, Springer International Publishing, 2014, pp. 310–325.
- [25] P. A. Zandbergen, "Accuracy of iPhone locations: a comparison of assisted GPS, WiFi and cellular positioning," *Transactions in GIS*, vol. 13, no. s1, pp. 5–25, 2009, doi: 10.1111/j.1467-9671.2009.01152.x.
- [26] R. Kastner, T. Michalke, T. Burbach, J. Fritsch, and C. Goerick, "Attention-based traffic sign recognition with an array of weak classifiers," in *2010 IEEE Intelligent Vehicles Symposium*, 2010, pp. 333–339, doi: 10.1109/ivs.2010.5548143.
- [27] J. Petit, M. Feiri, and F. Kargl, "Revisiting attacker model for smart vehicles," in *2014 IEEE 6th International Symposium on Wireless Vehicular Communications (WiVeC 2014)*, 2014, pp. 1–5, doi: 10.1109/wivec.2014.6953258.
- [28] W. Luo, B. Yang, and R. Urtasun, "Fast and furious: real time end-to-end 3D detection, tracking and motion forecasting with a single convolutional net," in *2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 2018, pp. 3569–3577, doi: 10.1109/cvpr.2018.00376.
- [29] Y. He, N. Zhao, and H. Yin, "Integrated networking, caching, and computing for connected vehicles: a deep reinforcement learning approach," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 1, pp. 44–55, Jan. 2018, doi: 10.1109/tvt.2017.2760281.
- [30] R. Oucheikh, M. Fri, F. Fedouaki, and M. Hain, "Deep real-time anomaly detection for connected autonomous vehicles," *Procedia Computer Science*, vol. 177, pp. 456–461, 2020, doi: 10.1016/j.procs.2020.10.062.
- [31] R. Eustice, "University of Michigan's work toward autonomous cars," *Ann Arbor, MI, USA*, 20115.
- [32] H. Qassim, A. Verma, and D. Feinzimer, "Compressed residual-VGG16 CNN model for big data places image recognition," in *2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC)*, Jan. 2018, pp. 169–175, doi: 10.1109/ccwc.2018.8301729.
- [33] O. Avatefipour et al., "An intelligent secured framework for cyberattack detection in electric vehicles' CAN bus using machine learning," *IEEE Access*, vol. 7, pp. 127580–127592, 2019, doi: 10.1109/access.2019.2937576.
- [34] B. Martínez-Rodríguez, S. Bilbao-Arechabala, and F. Jorge-Hernandez, "Security architecture for swarms of autonomous vehicles in smart farming," *Applied Sciences*, vol. 11, no. 10, p. 4341, May 2021, doi: 10.3390/app11104341.
- [35] ISO, "Road vehicles—terms and definitions," *ISO/DIS 34501*, 2021.
- [36] G. Thandavarayan, M. Sepulcre, and J. Gozalvez, "Cooperative perception for connected and automated vehicles: evaluation and impact of congestion control," *IEEE Access*, vol. 8, pp. 197665–197683, 2020, doi: 10.1109/access.2020.3035119.
- [37] H. Alghodhaifi and S. Lakshmanan, "Autonomous vehicle evaluation: a comprehensive survey on modeling and simulation approaches," *IEEE Access*, vol. 9, pp. 151531–151566, 2021, doi: 10.1109/access.2021.3125620.
- [38] ASAM, "Autonomous vehicle safety standard," 2022.
- [39] C. Techblog, "Operational design domain," 2021.
- [40] F. Zhu, Y. Lv, Y. Chen, X. Wang, G. Xiong, and F.-Y. Wang, "Parallel transportation systems: toward IoT-enabled smart urban traffic control and management," *IEEE Transactions on Intelligent Transportation Systems*, vol. 21, no. 10, pp. 4063–4071, Oct. 2020, doi: 10.1109/tits.2019.2934991.
- [41] R. Shrestha, S. Y. Nam, R. Bajracharya, and S. Kim, "Evolution of V2X communication and integration of blockchain for security enhancements," *Electronics*, vol. 9, no. 9, p. 1338, Aug. 2020, doi: 10.3390/electronics9091338.
- [42] J. Mason, R. M. Brach, and M. Brach, *Vehicle accident analysis and reconstruction methods*. SAE International, 2022.
- [43] J. Chung et al., "Empirical evaluation of GRU networks," *arXiv:1412.3555*, 2014.

- [44] K. Koscher *et al.*, “Experimental security analysis of a modern automobile,” in *2010 IEEE Symposium on Security and Privacy*, 2010, pp. 447–462, doi: 10.1109/sp.2010.34.
- [45] A. Ahmed, W. Song, Y. Zhang, M. A. Haque, and X. Liu, “Hybrid BO-XGBoost and BO-RF models for the strength prediction of self-compacting mortars with parametric analysis,” *Materials*, vol. 16, no. 12, p. 4366, 2023, doi: 10.3390/ma16124366.
- [46] B. Il Kwak, J. Woo, and H. K. Kim, “Know your master: Driver profiling-based anti-theft method,” in *2016 14th Annual Conference on Privacy, Security and Trust (PST)*, Dec. 2016, pp. 211–218, doi: 10.1109/pst.2016.7906929.

BIOGRAPHIES OF AUTHORS



Shwetansh Priyadarshi     was Born on 12 July 1994 to Mr. Durgesh Narayan Srivastava and Mrs. Poonam Srivastava, now married to Harshita Shrivastava. He hails from State of Uttar Pradesh which belongs to a Culture Rich beautiful Country known as India. He Completed his B. tech from Dr. MGR University, Chennai and his M.tech from Abdul Kalam Technical University, Lucknow and is currently Pursuing his Ph.D. from GD Goenka University, Gurugram. He has published multiple research articles on autonomous vehicles, machine learning and artificial intelligence. Now, he is working on a very innovative topic of cyber attacks on autonomous vehicles which is expected to be a milestone in the coming years. He can be contacted at email: shwetansh08@gmail.com.



Dr. Alok Srivastava     is an Associate professor and Head of Department in Electronics and Communication Department of GD Goenka University, Gurugram. He is having good knowledge of Electronics and have expertise in networks, embedded system, cyber-attacks. He has mentored many Ph.D. scholar and has given valuable support during their research Journey. He is Currently Supervising and Mentoring Shwetansh in his research work. He can be contacted at email: alok.srivastava@gdgu.org.