A Minor Project Report

on

An Intelligent Anomaly Detection for DDoS Attacks in Autonomous Vehicle Networks

by

Stuti Shukla – 21BIT207

Kaavya Vyas – 21BIT225

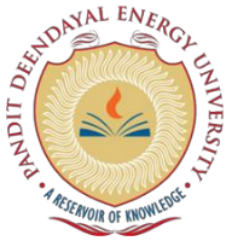
Vishw Patel – 21BIT231

Under the Guidance of

Dr Manish Mandloi

Assistant Professor

Submitted to



Department of Information and Communication Technology,

School of Technology,

Pandit Deendayal Energy University, Gandhinagar

AY 2024-2025

CERTIFICATE

This is to certify that the seminar report entitled "**An Intelligent Anomaly Detection for DDoS Attacks in Autonomous Vehicle Networks**" submitted by **Stuti Shukla – 21BIT207, Kaavya Vyas – 21BIT225 and Vishw Patel – 21BIT231** has been conducted under the supervision of **Dr Manish Mandloi, Assistant Professor, Department of ICT**, and is hereby approved for the partial fulfilment of the requirements for the award of the degree of Bachelor of Engineering in the Department of **Information and Communication Technology** at Pandit Deendayal Energy University, Gandhinagar. This work is original and has not been submitted to any other institution for the award of any degree.

Sign:

Name of Guide:

Designation:

Department:

School of Technology,

Pandit Deendayal Energy University, Gandhinagar

Sign:

Name of Examiner:

Designation:

Department:

School of Technology,

Pandit Deendayal Energy University, Gandhinagar

DECLARATION

We hereby declare that the minor project report entitled "**An Intelligent Anomaly Detection for DDoS Attacks in Autonomous Vehicle Networks**" is the result of our own work and has been written by us. This report has not utilized any language model or natural language processing artificial intelligence tools for the creation or generation of content, including the literature survey.

The use of any such artificial intelligence-based tools was strictly confined to the polishing of content, spell checking, and grammar correction after the initial draft of the report was completed. No part of this report has been directly sourced from the output of such tools for the final submission.

This declaration is to affirm that the work presented in this report is genuinely conducted by us and to the best of our knowledge, it is original.

Stuti Shukla – 21BIT207

Kaavya Vyas – 21BIT225

Vishw Patel – 21BIT231

Information and Communication Technology Department,

School of Technology,

Pandit Deendayal Energy University,

Gandhinagar

Date: December 10, 2024

Place: Gandhinagar

ACKNOWLEDGEMENT

We would like to express our sincere gratitude to everyone who contributed to the successful completion of this project.

First and foremost, we would like to thank our project supervisor Dr Manish Mandloi, Assistant Professor, Department of ICT for their constant guidance, invaluable feedback, and support throughout the course of this project. His expertise and encouragement have been instrumental in shaping the direction of this work.

We would also like to extend our gratitude to all the faculty and staff of Pandit Deendayal Energy University for their insightful suggestions and assistance. Their perspectives have significantly enriched the project. We are deeply thankful to our peers and colleagues for their support, encouragement, and collaborative spirit, which have been a source of motivation and strength throughout this journey.

Our special thanks to our college for providing the resources, infrastructure, and conducive environment necessary for the successful execution of this project. The facilities and support extended have been integral to achieving the goals of this research. We also owe a debt of gratitude to the authors of the literature and research papers we referred to, as their work provided a strong foundation for this project. Finally, we would like to thank our family and friends for their unwavering support, patience, and understanding during this project. Their encouragement has helped us maintain the focus and determination needed to complete this work.

Thank you all for your contributions and support. To all who have contributed, directly or indirectly, to this project, we offer our heartfelt appreciation and gratitude.

LIST OF FIGURES

LIST OF TABLES

TABLE OF CONTENTS

CHAPTER 1: INTRODUCTION AND OBJECTIVES

1.1 Introduction:

Intelligent transportation systems of self-driving cars or onboard control systems are now recognized as one of the cornerstones of current and future transport systems that have great potential in improving efficiency and safety of passenger transportation. Such systems heavily depend on tested networks to enable car to communicate with other facilities and cloud services as they make real time decisions. Nevertheless, the security of these systems has become one of the most important issues today. One of the greatest vulnerabilities is in the systems of self-driving vehicles that greatly depend on the communication between cars, and on the vehicles and the infrastructure surrounding them. Of these, Distributed Denial-of-Service (DDoS) attacks form a large threat category. DDoS is an attack that jams a system's operation by saturating legitimate and illegitimate traffic from multiple sources typified by a botnet. Whereas conventional DoS attacks are launched from one source system, DDoS attacks are more complex to address form their origin because they are scattered.

The consequences of DDoS attack on autonomous vehicle networks are extremely severe and devastating for their performance. Such attacks can shut down Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication, leading causing downtime, operational delays, monetarily losses and even human loss since the key safety features can be incapacitated. Compared to conventional IT networks, deterministic and extremely dependable communication is expected in AV networks in order to perform tasks such as recognizing obstacles, building a map, and steering in time. Disruptions to such systems are often catastrophic; therefore, there is a need to come up with a security model that is more advanced in protecting the AV networks for DDoS attacks.

For AV networks, a DDoS attack can have grave repercussions if pulled through to its completion. These are issues of vehicle-to-vehicle and vehicle-to-everything communication, disconnections in operation that affect control, and vulnerability of lives as the self-driving systems lose their real-time decision-making capacity. Prior anomaly detection techniques are not well-positioned to neutralize such complex and emerging threats. These systems are unable to distinguish normal traffic spikes and actual attack patterns let alone in high-speed and large data sets as are seen in autonomous transportation systems. Solving these issues necessitates a new approach to the use of cybersecurity. Specifically, this research aims at proposing a multi-layered anomaly detection system based on both the sensitivity of superior machine learning algorithms and the feasibility for real application. This study intents to develop a reliable system of detecting and handling DDoS attacks in real-time using modern methodologies including reinforcement learning, and classification models to contribute to the construction of a safer and more secure environment promoting autonomous mobility.

This research integrates and evaluates the methodologies proposed in three seminal works: real time DDoS attack detection in ITS, a tree-based detection model using Gini index for the selection of features and a deep learning-based IDS for IoT networks. Through such deployment, the study seeks to evaluate the impact and combinational effectiveness of the mentioned approaches towards improving the detection of the DDoS attack, specifically in environments that are dynamic and have limited resources

1.2 Objectives:

The research plan of the project is as follows:

1. It is proposed to carry out the implementation of three different approaches to DDoS attacks' detection, regarding to which the selected research papers can be referred to. In this way, the research replicates such models and assesses the suitability of the underlying theory or the effectiveness of the analyzed situations. It is important for knowing how such methods work and in which situations they provide the best results.
2. The implemented models are verified in real life like situation which includes Intelligent Transportation System (ITS) and IoT. This is done by evaluating their ability to detect intrusions, the time taken for such detections, and their ability to make detections and responses when operating in dynamic and resource scarce scenarios. The evaluation also shows how effectively these models can handle false positive and false negatives when launched in DoS attack detection.

3. Some have aimed at explaining the whole process in detail in order to show the advantages and disadvantages of one approach compared to another. For instance, deep learning- based solutions may promise a high accuracy but at the cost of high computational resources while the tree bases model may be faster and using fewer resources. Knowledge of the trade-offs allows specification of the circumstances that may be optimal for each of the models.

4. From the implementation and the performance results, possibilities for the improvement of these methodologies are discussed. Details would include integration of complementary facets of the models; enhancement of the algorithmic parts for application in ITS and IoT environments for better resource utilization; or alteration for improved scalability.

5. The findings from the current study are therefore expected to be useful for designing higher security models for both ITS and IoT environments. The paper helps enrich cybersecurity scholarship by presenting practical recommendations for novel threats and develops new ideas in addressing the DDoS attack issue.

CHAPTER 2: LITERATURE REVIEW

Table 1- Literature Review

Title	Year	Authors	Database Used	Techniques Applied	Outputs	Challenges
A novel deep learning-based intrusion detection system for IoT DDoS security	2024	Selman Hizal, Unal Cavusoglu, Devrim Akgun	Simulation based data	DNN (Deep Neural Networks), CNN (Convolutional Neural Networks), LSTM (Long Short-Term Memory), RNN (Recurrent Neural Network).	Developed a two-stage classification model, where the first stage performs binary classification (attack vs. no attack), second stage performs multiclass classification (DDoS subtype identification).	Developing deep learning models that can run efficiently on resource-constrained edge devices while maintaining high performance.
An intelligent DDoS attack detection tree-based model using Gini index feature selection method	2023	Mohamed Aly Bouke, Azizol Abdullah	UNSW-NB15 dataset	Python and the ITMO FS (Information Technologies, Mechanics and Optics University FS) library [59] to calculate the Gini index (GI), IDS	Accuracy -98%, Gini index feature selection of 13 out of 45 security features, misclassifying only 2% of the testing instances.	Processing large DAS datasets, mitigating privacy concerns, computational cost, environmental impacts.
Towards a machine learning-based framework for DDOS attack detection in software-defined IoT (SD-IoT) networks	2023	Jalal Bhayo, Syed Attique Shah, Sufian Hameed, Awais Ahmed, Jamal Nasir, Dirk Draheim	Traffic is captured by a logging mechanism to SDN-WISE controller, which writes into a log file that converted into dataset.	Naive Bayes (NB), Decision Tree (DT), and Support Vector Machine (SVM) algorithms	NB - 97.4% SVM - 96.1%, DT - 98.1% Average throughput of 48 packets per second, Accuracy - 97.2%.	Only focuses on the flooding DDoS attacks; can be extended to other types of DDoS attacks and with different types of IoT networks.

Real-time DDoS flooding attack detection in intelligent transportation systems	2022	H Karthikeyan, G Usha	Real-time traffic data from urban areas and highways	Reinforcement learning, Q-learning, to optimize the detection threshold and decision-making process.	Accuracy of 90%, Vehicle to Vehicle and Vehicle to Infrastructure, Distributed Denial of Service (DDoS) in impairing Road Side Units (RSU) of IITS, evading classical data filtering methods.	Flooding attacks should be mitigated in the future to ensure a completely secure connection.
Anomaly Detection Using Ensemble Learning for Intrusion Detection in IoT based Smart cities	2022	Chaimae Hazman, Said Benkiran e, Azidine Guezzaz, Mourade Azrour and Mohamed Abdedai me	IoT-23, BoT-IoT, Edge-IIoT	Ensemble Learning, Boruta, Mutual Information, Correlation	ACC: 99.9%, Recall: 99.9%, Precision: 99.9%, Training: 33.68s, Detection: 0.02156s	Low computatio nal overhead, accurate detection in diverse IoT environmen ts, handling large-scale data
Enhanced Anomaly Detection System for IoT Based on Improved Dynamic SBPSO	2022	Asima Sarwar, Abdullah M. Alnajim, Safdar Nawaz Khan Marwat, Salman Ahmed, Saleh Alyahya, Waseem Ullah Khan	IoTID20, UNSW-NB15	Improved Dynamic Sticky Binary Particle Swarm Optimization (IDSBPSO), Particle Swarm Optimization (PSO)	Higher or similar accuracy with fewer features, reduced computational cost and prediction time	Increased data dimensional ity, outdated datasets, incomplete/ noisy datasets, low processing ability of IoT devices, and memory capacity limitations
A lightweight Anomaly based DDoS flood attack detection for Internet of vehicles	2021	Kuthada Mohan	SUMO, OMNET++, INET, and VEINS	J48 and SVM machine learning models on a Raspberry Pi 3b+	29 features with 90350 instances which make it a heavy anomaly model, reducing the number of features from 29 to 4.	Can extend the instances in the dataset for various cyber-attacks which can

						be used to model an intrusion detection system for the Internet of vehicles.
A Taxonomy of DDoS Attack Mitigation Approaches Featured by SDN Technologies in IoT Scenarios	2020	Felipe S. Dantas Silva, Esau Silva, Emidio P. Neto, Marcilio Lemos, Augusto J. Venancio Neto, Flavio Esposito	Science Direct, MDPI Sensors	Taxonomy, SDN-based mitigation, Distributed control, Flow filtering, Honeypots, Rate-limiting, Moving Target Defense (MTD)	Comprehensive taxonomy for DDoS mitigation in IoT using SDN, highlights effectiveness of SDN in containing threats	Scalability of SDN solutions, difficulty in detecting low-rate attacks, centralized vs. distributed architectures
A Survey of DDoS Attacking Techniques and Defence Mechanisms in the IoT Network	2019	Ruchi Vishwakarma, Ankit Kumar Jain	Telecommunication-Systems – Volume73	Analysis of DDoS Attacks, Malware and Botnets, Defence Mechanisms Comparison	Comprehensive comparison of existing DDoS defense techniques, Identification of security gaps	Limited resources in IoT devices, Evolving attack patterns, High complexity in real-time mitigation
An Approach to Secure Internet of Things Against DDoS	2016	Krushang Sonar, Hardik Upadhyay, H Upadhyay Gperi	Contiki OS and Cooja Cn. simulation environment	Performed in C language with Contiki OS and Cooja Simulation, Intrusion Prevention System	Each node calculates Residual Energy, then it is compared with predefine Residual Energy, applied to either Network Side or Distributed on Agent at Border Router	Work can be extended to make it Intrusion Prevention System which can identify and secure IoT network.

CHAPTER 3: RESEARCH GAPS AND PROBLEM STATEMENT

The research gaps of the papers considered are given below:

1. The requirement for obtaining new datasets, which should cover the traffic of IoT devices currently in existence and incorporate various sorts of threats. It is crucial and well-accepted that performance of IDS depends on the datasets used in training and testing processes. However, most of the current datasets are either old or do not capture the current IoT traffic characteristics. This results in an absence of methods to effectively identify the threats that apply to the current environments of IoT. These datasets should also incorporate a broader variety of malicious activities to improve IDS system robustness and reliability.

2. The requirement to design IDS systems capable of operating in low-power environments of IoT devices in real-time. IoT devices are normally constrained in terms of computational capability, storage capacity and energy resources. Many existing IDS solutions do not work as expected within these constraints as most are built for traditional IT systems which are endowed with immense resources. This results in the creation of a very important void that cannot be easily filled in an ability to detect threats in real-time without overwhelming the devices or hindering their basic functions. The IDS of the future, therefore, has to be designed with efficiency in mind, to minimize false positives and negatives while at the same time, integrate lightweight algorithms and efficient energy usage.

3. The requirement to expand on incorporating machine learning techniques to enhance IDS systems and to counter different and continually evolving threats of IoT settings. Regardless, traditional machine learning (ML) techniques have demonstrated a capability to enhance IDS in the past, but many current solutions are constrained and rigid. Due to the fact that IoT environments are inevitably dynamic and diverse, there is a need to counteract polymorphic malware and adversarial attack within IDS solutions. However, current systems solely implemented rudimentary or stagnant ML models that cannot learn new threats or fluctuations of network activity. To achieve more powerful and flexible IDSs, there should be the focus on further development of more sophisticated ML models, like deep learning, reinforcement learning etc.

Problem Statement:

The rapid evolution of IoT and ITS has introduced a new set of challenges in defending against Distributed Denial of Service (DDoS) attacks. One significant issue that the existing literature seems to overlook is the finite comparative performance of these models within the volatile and resource-limited environment for IoT & ITS applications. In addition, the effectiveness of these methodologies employing large data sets and realistic attack scenarios must be analyzed in order to examine the feasibility and capability for implementation of these technologies into real-time detection systems. This research seeks to address these problems by deploying and comparing three well-known approaches to DDoS detection. The performance of these systems will be assessed in terms of some critical indicators with an aim of comparing, integrate and recommend on the future development of detection systems for improved IoT and ITS.

CHAPTER 4: METHODOLOGY ADOPTED

In order to identifying and prevent DDoS attacks on autonomous vehicle networks, we used a series of steps like: data acquisition, feature extraction, model training, and model assessment. Our work started with the UNSW-NB15 dataset, which is one of the most popular datasets with labelled normal and attack traffic data, including different DDoS attacks. They were used in the training and evaluating of our binary and multi-class classifiers as detailed below.

The preprocessing step was a necessary undertaking in view of making the data more qualitatively better and more usable. To this end, a correlation-based feature selection was performed to narrow down the amount of features used originally to a limited set of features bearing the most relation to accurate detection and to minimize computational cost. Some of the other preprocessing steps that was carried out include de-duplicating the data set, containing the data and make it consistent.

The first model created and used was based upon Q-learning to ascertain network traffic patterns in order to dynamically self-optimize continual use. This reinforcement learning model was particularly effective for real-time learning of the changes in environment in cases where the attack behaviors dynamically change. Since states have been defined/actions and rewards incorporated, the model was able to train itself to distinguish between normal patterns and detect thresholds.

Binary and multi class classification deep-learning models were used during the study. These models were trained using the UNSW-NB15 dataset; specifically, the binary classifier aimed at binary classification of normal traffic and attack traffic; and the other classifier was for multi-class classification of attack types. For each model, the training process was carried out over more than 40 epochs with the purpose of hyperparameter tuning in order to improve accuracy and reduce computational time. These models demonstrated near-perfect accuracy within the tasks, and affirmed how they could be beneficial when greater precision and efficiency of categorization is required.

Moreover, we created the model related to the decision tree base on the splitting criterion of the Gini index. This model was a rule-based model for anomaly detection with focus on model simplicity and comprehensibility. The tree-based model was tuned by using parameters where criterion was entropy, depth limit of 20 and minimum samples was set for split and leaf nodes. However, its recall rate was marginally lower than the deep-learning models and although it might not have been as powerful, its ability to run more efficiently and being designed in an open topology allowed it to find great value especially in resource-limited scenarios like those found in Onboard systems in Self-Driving cars. In this paper, accuracy was employed to evaluate all the mentioned models for better and comprehensive analysis of the performance. Computational task was also examined regarding the tree-based method to its enforceability in real life problems.

The Q-learning model demonstrated fair adaptability, the deep-learning models were extolled for precision or a snappy exactness, and the tree-based model reeled out fair execution with reasonable lucidity. This approach offered a comprehensive research approach to identify techniques to build defenses against DDoS attacks in auto-driving vehicle networks for the improvement of the same networks. Other preprocessing steps involved included; removing dups, normalizing the data and standardizing across dataset.

CHAPTER 5: DETAILS OF WORK EXECUTION

The process of completion of this work included first, data preprocessing, second, model implementation and third the model's validation as well as comparisons. At each step of the implementation, it was made sure that the provided must be reliable and realistic solutions.

To train and assess the models, the UNSW-NB15 dataset became the primary dataset used in the study. In this study, the dataset of network traffic behaviors and various types of DDoS attacks was preprocessed for better quality and applicability. By performing subsequent feature selection technique known as the correlation-based feature selection (CFS) algorithm, computational efficiency was achievable; while crucial features were retained in the analysis. Other preprocessing steps involved were the extraction of duplicate records eliminated, data values Standardization and Checking for Inter-instance Similarity.

In the implementation phase, Q-learning model was developed to implement an adaptive system using the principles of reinforcement learning for real-time anomaly detection. This model was applied using the preprocessed data set and reward-based system for detection of abnormal patterns and adaptive change of thresholds. As such, the algorithm was especially suitable for the highly dynamic topologies of self-driving car systems due to its capability of learning from shift in attack behaviors.

Binary as well as multi-class classifiers were performed subsequently utilizing the deep-learning procedure. These models were trained on the UNSW-NB15 dataset, where the binary classifier is built to distinguish between normal and attack traffic and the multi-class classifier for identification of specific types of attacks. The training phase comprised 40 cycles, and during the learning phase, hyperparameters had to be adjusted depending on the best accuracy and the shortest amount of time. Concerning the first research question, the superior accuracy obtained by all these models showed their reliability and applicability in accurate anomaly detection.

Another model created was the classification tree using the Gini index as a split measure. This model was the simplest and most easily interpretable, which comes handy for developing systems for resource-limited devices such as onboard units in self-driving cars. The tree-based model was selected with the best hyperparameters and consisted of entropy as the criterion, a maximum depth of 20, and optimized values for minimum samples per split and leave nodes. This configuration made it possible so as to balance accuracy together with the number of iterations computed to achieve the same level of accuracy.

In the evaluation phase all models invoking accuracy were tested to determine their efficiency. Computational efficiency was also assessed which was mainly focused on tree-based model for foreseeable implementation. By comparing the results from the two approaches, clear signals of the advantages and limitations of the approaches emerged and this allowed for the identification of their utility in complex layered sociotechnical systems such as the probabilistic application of connected autonomous vehicles networks.
By following these outlined stages, we were able to show that it is possible to use more advanced ML and RL techniques for recognizing DDoS attacks on AV networks. The detailed execution process makes sure that the models developed are quite sound, optimal for implementation and relevant to the real world.

CHAPTER 6: RESULTS AND DISCUSSIONS

In this paper, we compared three different strategies for identification of DDoS attacks in the context of autonomous vehicle networks. The performances of the models were evaluated, the ease with which they could be deployed as well as their applicability in the real-world setting were also evaluated. Below is a detailed discussion of the results:

1. Q-Learning Model:

The Q-learning model was used on a set of data containing attack and normal traffic data generated from simulation. This model gave indication to the capacity of the model adjusting in a dynamic manner to traffic characteristics and limits. It is such flexibility that qualifies the model for real-time anomaly detection in contexts where the traffic pattern may be constantly shifting.

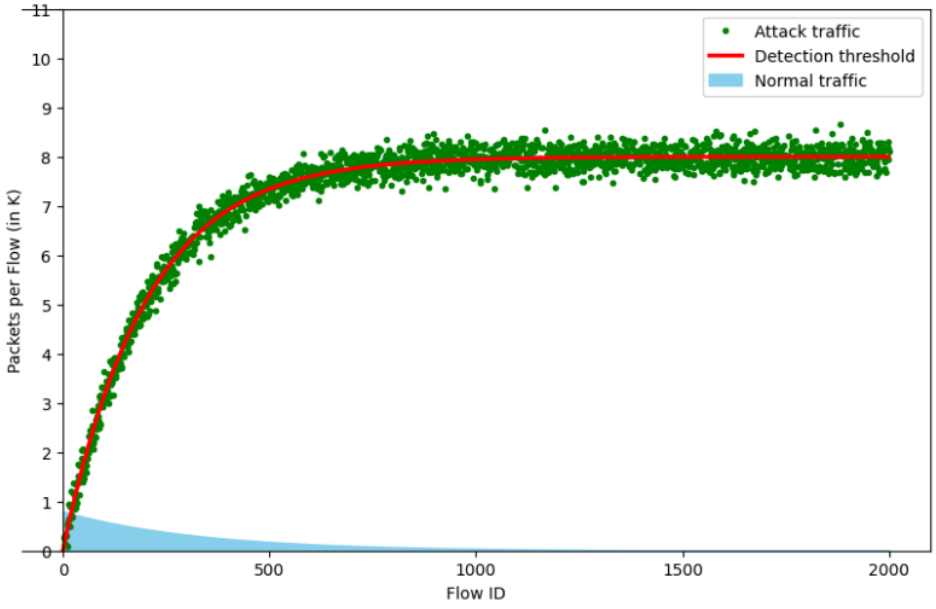


Figure 1-Result of DDoS attack detection using Q-Learning Model

One major advantage of this approach is its ability to distinguish between cases with changing attackers' behavior and respond adequately to traffic increase. This feature makes Q-learning model especially suitable for the autonomous vehicle networks where quick and wise modifications are needed to safeguard the network.

2. Binary and Multi-Class Classifier Models:

The binary and multi-class classifier models were used in training and testing of the UNSW-NB15 dataset. These models provided high performance, a 100% accuracy of binary classification and 99.53% multi-class classification after 40 epochs.

```
Epoch 40/40
1082/1082 ━━━━━━━━━━━━━━━━━━━━ 3s 2ms/step - accuracy: 1.0000 - loss: 1.5717e-10 - val_accuracy: 1.0000 - val_loss: 3.9876e-18
580/580 ━━━━━━━━━━━━━━━━━━━━ 1s 1ms/step
Level 1 (Binary) Accuracy: 100.00%
```

Figure 2-Result achieved using the Binary Classifier

```
Epoch 40/40
1082/1082 ━━━━━━━━━━━━━━━━━━━━ 4s 2ms/step - accuracy: 0.9906 - loss: 0.0282 - val_accuracy: 0.9943 - val_loss: 0.0165
580/580 ━━━━━━━━━━━━━━━━━━━━ 1s 1ms/step
Level 2 (Multiclass) Accuracy: 99.55%
```

Figure 3-Result achieved using the Multiclass Classifier

The close to one hundred percent precision demonstrably illustrates the resilience of these models to correctly identify and categorise network traffic abnormalities. The binary classifier proved efficient in differentiating normal traffic from attack traffic and the multiple class classifier proved efficient in classifying multiple classes of attack. These outcomes provide evidence that deep-learning classifiers are as accurate as they are proficient in situations that require high levels of specificity and swift decision making.
The possibility achieved by such accuracy demonstrates the efficiency of these models in improving the security of the network of AVs when accurate classifying of various kinds of attacks is required.

3. Tree-Based Model Using Gini Index

The decision tree-based model, leveraging the Gini index, achieved an accuracy of 93.09% with the following optimal parameters:
Criterion: entropy, Max depth: 20, Min samples leaf: 1, Min samples split: 10

```
Best parameters: {'criterion': 'entropy', 'max_depth': 20, 'min_samples_leaf': 1, 'min_samples_split': 10}
Accuracy: 93.09%
```

Figure 4-Results achieved using the Tree-Based Model with the Gini Index

Despite having a slightly lower overall performance in comparison with the deep-learning classifiers, this model has such advantages as high interpretability and a much lower computational cost. The model has the properties of transparency of decision making which can be useful when the choice influences security activities and the rationale of choosing one option has to be explained.

Moreover, the high efficiency and the ability to work with limited computing resources make it suitable for using in scarce-resource environments like automobiles' onboard systems in

autonomous vehicles. The sacrifice of precision for comprehensibility establishes this model as a possible solution for certain restricted uses, where the model's explicit structure makes sense.

Comparative Analysis:
The results of the three approaches reveal their respective strengths and trade-offs:

1. The primary strength of the Q-learning model includes flexibility and situation awareness, serving well the dynamic conditions of the environment.

2. The binary as well as multi-class classifiers are highly accurate, and favoured for applications where accurate novel class detection and fast classification of attack types is essential.

3. The tree-based model considers the second aspect's requirements of low computational power and clearly understandable results while being rather fast.

Such a comparative analysis only goes to show the flexibility of these approaches to meet the security concerns of autonomous vehicle networks given the various types of security concerns identified in this study, and the possibility of improving network immunity against DDoS attacks.

CHAPTER 7: CONCLUSION AND FUTURE SCOPES

7.1 Conclusion:

The subject of interest in this study is the protection of the autonomy vehicle network against DDoS attacks using an anomaly detection system. Applying adaptive models and employing machine learning techniques, we have suggested solutions to the significant challenges of enhancing cybersecurity in evolving, less-resourced centers.

We first analyzed the problem from a theoretical perspective with a Q-learning model that allowed us to model the traffic and observe how the attack traffic grew exponentially compared to the normal traffic that decreased with time. This laid the ground work towards grasping real time adaptive detection thresholds. Based on this, we trained binary and multi-class classification models on UNSW-NB15 dataset and the results of 100% and 99.53% for differentiation of the types of attack prove the efficiency of the models. As for the computation and understanding improvements we also adopted tree-based model, using the Gini index which was precisely in the middle with 93.09% accuracy.

This multiple-layered analysis appears to be a systematic approach in studying anomaly detection based on theoretical flexibility mixed with usage of adaptations. The combination of simulation, classification, and interpretability forms the basis for subsequent systems capable to detect efficiently and effectively DDoS attacks in autonomous vehicle networks in real-time.

7.2 Future Scopes

The proposed work also opens several paths for future research. One direction in the future work of the presented models is to incorporate them into the practical AV systems to test and enhance them further under dynamic actual conditions. There is always a chance for these expansions, or more advanced reinforcement learning models like the Deep Q-Networks (DQNs) or Actor-Critic could be implemented for better scalability as well as detection probability in large-scale networks. To increase the defenses to cover as many types of attacks as possible and support anomaly detection in large-scale vehicular networks, faster acquisition of larger datasets containing more types of attacks and network traffic densities should be employed, as well as FL. There is also need to enhance robustness to adversarial example and to design models that are energy efficient in order to deploy deep learning models onboard in limited resource setting. Finally, the implementation of the XAI methods would help to address the question of trust in the models for security professionals would understand how the models arrive to their conclusions. Exploring these directions will produce better secured, scaled, and intelligent methods for anomaly detection for enhancing the security of next generation transport systems.

REFERENCES

Bhayo, J., Shah, S. A., Hameed, S., Ahmed, A., Nasir, J., & Draheim, D. (n.d.). Towards a machine learning-based framework for DDoS attack detection in software-defined IoT (SD-IoT) networks. *Department of Computer Science, National University of Computer and Emerging Sciences (NUCES-FAST)*

Bouke, M. A., & Abdullah, A. (2023). An intelligent DDoS attack detection tree-based model using *Gini index feature selection method*. Microprocessors and Microsystems, 98, 104823.

Dantas Silva, F. S., Silva, E., Neto, E. P., Lemos, M., Neto, A. J. V., & Esposito, F. (2020). A taxonomy of DDoS attack mitigation approaches featured by SDN technologies in IoT scenarios. *ScienceDirect, MDPI Sensors*.

Hazman, C., Benkirane, S., Guezzaz, A., Azrour, M., & Abdedaime, M. (2022). Anomaly detection using ensemble learning for intrusion detection in IoT-based smart cities. *Cluster Computing, 26*(6), 4069–4083.

Hizal, S., Cavusoglu, U., & Akgun, D. (2024). A novel deep learning-based intrusion detection system for IoT DDoS security. *Internet of Things, 28*, 101336.

Karthikeyan, H., & Usha, G. (2022). Real-time DDoS flooding attack detection in intelligent transportation systems. *Computers and Electrical Engineering, 101,* Article 107995.

Mohan, K. (2021). A lightweight anomaly-based DDoS flood attack detection for Internet of Vehicles. *SUMO, OMNET++, INET, and VEINS*.

Sarwar, A., Alnajim, A. M., Marwat, S. N. K., Ahmed, S., Alyahya, S., & Khan, W. U. (2022). Enhanced anomaly detection system for IoT based on improved dynamic SBPSO. *Sensors, 22*(13), 4926.

Sonar, K., & Upadhyay, H. (2016). An approach to secure the Internet of Things against DDoS. *Contiki OS and Cooja Simulation Environment*.

Vishwakarma, R., & Jain, A. K. (2019). A survey of DDoS attacking techniques and defence mechanisms in the IoT network. *Telecommunication Systems, 73*.

final_report.pdf

ORIGINALITY REPORT

19%	11%	12%	9%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Pandit Deendayal Petroleum University Student Paper	5%
2	www.mdpi.com Internet Source	2%
3	pureportal.bcu.ac.uk Internet Source	1%
4	"Proceedings of International Conference on ICT for Sustainable Development", Springer Nature, 2016 Publication	1%
5	ceur-ws.org Internet Source	1%
6	digital.lib.usu.edu Internet Source	1%
7	H. Karthikeyan, G. Usha. "Real-time DDoS flooding attack detection in intelligent transportation systems", Computers and Electrical Engineering, 2022 Publication	1%

8	www.researchgate.net Internet Source	1 %
9	Mohamed Aly Bouke, Azizol Abdullah, Sameer Hamoud ALshatebi, Mohd Taufik Abdullah, Hayate El Atigh. "An intelligent DDoS attack detection tree-based model using Gini index feature selection method", Microprocessors and Microsystems, 2023 Publication	1 %
10	Jalal Bhayo, Syed Attique Shah, Sufian Hameed, Awais Ahmed, Jamal Nasir, Dirk Draheim. "Towards a machine learning-based framework for DDOS attack detection in software-defined IoT (SD-IoT) networks", Engineering Applications of Artificial Intelligence, 2023 Publication	<1 %
11	umpir.ump.edu.my Internet Source	<1 %
12	ouci.dntb.gov.ua Internet Source	<1 %
13	Asima Sarwar, Abdullah M. Alnajim, Safdar Nawaz Khan Marwat, Salman Ahmed, Saleh Alyahya, Waseem Ullah Khan. "Enhanced Anomaly Detection System for IoT Based on Improved Dynamic SBPSO", Sensors, 2022 Publication	<1 %

14	Submitted to University of Sydney Student Paper	<1%
15	www.springerprofessional.de Internet Source	<1%
16	Submitted to Cerritos College Student Paper	<1%
17	Santos, Fabio. "Supporting the Task-Driven Skill Identification in Open Source Project Issue Tracking Systems", Northern Arizona University, 2023 Publication	<1%
18	"Advanced Technology for Smart Environment and Energy", Springer Science and Business Media LLC, 2023 Publication	<1%
19	C. Rajathi, P. Rukmani. "Hybrid Learning Model for intrusion detection system: A combination of parametric and non-parametric classifiers", Alexandria Engineering Journal, 2025 Publication	<1%
20	Chandrapal Singh, Ankit Kumar Jain. "A Comprehensive Survey on DDoS Attacks Detection & Mitigation in SDN-IoT Network", e-Prime - Advances in Electrical Engineering, Electronics and Energy, 2024 Publication	<1%

21	Submitted to Chester College of Higher Education Student Paper	<1%
22	Submitted to Georgia State University Student Paper	<1%
23	Philogene Kyle Dimpas, Royce Vincent Po, Mary Jane Sabellano. "Filipino and english clickbait detection using a long short term memory recurrent neural network", 2017 International Conference on Asian Language Processing (IALP), 2017 Publication	<1%
24	Siraj Uddin Qureshi, Jingsha He, Saima Tunio, Nafei Zhu, Ahsan Nazir, Ahsan Wajahat, Faheem Ullah, Abdul Wadud. "Systematic review of deep learning solutions for malware detection and forensic analysis in IoT", Journal of King Saud University - Computer and Information Sciences, 2024 Publication	<1%
25	wiredspace.wits.ac.za Internet Source	<1%
26	www.marketresearch.com Internet Source	<1%
27	jdc.jefferson.edu Internet Source	<1%

28	Kothakonda Chandhar, Devesh Pratap Singh, Joel Alanya-Beltran, Shaik Vaseem Akram, Kothandaraman D, Mohit Tiwari. "Enhanced Anomaly Detection System for IOT Based on Improved Dynamic SBPSO", 2023 International Conference on Artificial Intelligence and Smart Communication (AISC), 2023 Publication	<1 %
29	Praveen Jesudhas, T. Raghuveera. "A Novel Computationally Efficient Approach to Identify Visually Interpretable Medical Conditions from 2D Skeletal Data", Computer Systems Science and Engineering, 2023 Publication	<1 %
30	Submitted to The Robert Gordon University Student Paper	<1 %
31	clok.uclan.ac.uk Internet Source	<1 %
32	Avtar Singh, Harpreet Kaur, Navjot Kaur. "A novel DDoS detection and mitigation technique using hybrid machine learning model and redirect illegitimate traffic in SDN network", Cluster Computing, 2023 Publication	<1 %
33	Chaimae Hazman, Azidine Guezzaz, Said Benkirane, Mourade Azrour. "A smart model	<1 %

integrating LSTM and XGBoost for improving IoT-enabled smart cities security", Cluster Computing, 2024
Publication

34	Jinpeng Han, Zhiyang Ju, Xiaoguang Chen, Manzhi Yang, Hui Zhang, Rouxing Huai. "Secure Operations of Connected and Autonomous Vehicles", IEEE Transactions on Intelligent Vehicles, 2023 Publication	<1 %
35	doczz.net Internet Source	<1 %
36	dspace.daffodilvarsity.edu.bd:8080 Internet Source	<1 %
37	link.springer.com Internet Source	<1 %
38	mofald.gov.np Internet Source	<1 %

Exclude quotes	On	Exclude matches	< 8 words
Exclude bibliography	On		

final_report.pdf

PAGE 1

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Article Error You may need to use an article before this word.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Article Error You may need to use an article before this word. Consider using the article **the**.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

PAGE 2

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word. Consider using the article **the**.

Article Error You may need to use an article before this word.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Article Error You may need to use an article before this word. Consider using the article **the**.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

PAGE 3

P/V You have used the passive voice in this sentence. You may want to revise it using the active voice.

Run-on This sentence may be a run-on sentence.

P/V You have used the passive voice in this sentence. You may want to revise it using the active voice.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Article Error You may need to use an article before this word. Consider using the article **the**.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

PAGE 4

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Article Error You may need to remove this article.

PAGE 5

Article Error You may need to use an article before this word. Consider using the article **the**.

Article Error You may need to use an article before this word.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

PAGE 6

PAGE 7

PAGE 8

Article Error You may need to use an article before this word.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Confused You have used either an imprecise word or an incorrect word.

Article Error You may need to use an article before this word.

Missing "," Review the rules for using punctuation marks.

Article Error You may need to remove this article.

Proofread This part of the sentence contains an error or misspelling that makes your meaning unclear.

Article Error You may need to remove this article.

Confused You have used either an imprecise word or an incorrect word.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Wrong Article You may have used the wrong article or pronoun. Proofread the sentence to make sure that the article or pronoun agrees with the word it describes.

Prep. You may be using the wrong preposition.

Missing "," Review the rules for using punctuation marks.

PAGE 9

Article Error You may need to remove this article.

Article Error You may need to remove this article.

Article Error You may need to use an article before this word. Consider using the article **a**.

Confused You have used either an imprecise word or an incorrect word.

Wrong Form You may have used the wrong form of this word.

Wrong Form You may have used the wrong form of this word.

P/V You have used the passive voice in this sentence. You may want to revise it using the active voice.

Missing "," Review the rules for using punctuation marks.

Proofread This part of the sentence contains an error or misspelling that makes your meaning unclear.

Confused You have used either an imprecise word or an incorrect word.

Article Error You may need to use an article before this word.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

PAGE 10

Missing "," Review the rules for using punctuation marks.

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word. Consider using the article **the**.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Missing "," Review the rules for using punctuation marks.

Missing "," Review the rules for using punctuation marks.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Prep. You may be using the wrong preposition.

Article Error You may need to use an article before this word.

P/V You have used the passive voice in this sentence. You may want to revise it using the active voice.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Article Error You may need to remove this article.

Article Error You may need to use an article before this word. Consider using the article **the**.

Article Error You may need to use an article before this word.

PAGE 12

Article Error You may need to use an article before this word. Consider using the article **the**.

Article Error You may need to use an article before this word. Consider using the article **the**.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Missing "," Review the rules for using punctuation marks.

Run-on This sentence may be a run-on sentence.

PAGE 13

Prep. You may be using the wrong preposition.

Article Error You may need to use an article before this word.

PAGE 14

S/V This subject and verb may not agree. Proofread the sentence to make sure the subject agrees with the verb.

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word.

S/V This subject and verb may not agree. Proofread the sentence to make sure the subject agrees with the verb.

Garbled This sentence contains several grammatical or spelling errors that make your meaning unclear. Proofread the sentence to identify and fix the mistakes.

P/V You have used the passive voice in this sentence. You may want to revise it using the active voice.

Prep. You may be using the wrong preposition.

Run-on This sentence may be a run-on sentence.

Article Error You may need to use an article before this word. Consider using the article **a**.

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Prep. You may be using the wrong preposition.

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word.

Proofread This part of the sentence contains an error or misspelling that makes your meaning unclear.

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word.

PAGE 17

Wrong Article You may have used the wrong article or pronoun. Proofread the sentence to make sure that the article or pronoun agrees with the word it describes.

Article Error You may need to remove this article.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Hyph. Review the rules for using punctuation marks.

Article Error You may need to use an article before this word.

PAGE 18

Article Error You may need to use an article before this word.

Article Error You may need to remove this article.

PAGE 19

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Compound These two words should be a compound word.

Article Error You may need to use an article before this word.

Wrong Form You may have used the wrong form of this word.

Proofread This part of the sentence contains an error or misspelling that makes your meaning unclear.

Article Error You may need to use an article before this word. Consider using the article **a**.

Prep. You may be using the wrong preposition.