DDoS attacks on airlines and Mitigation techniques using Artificial Intelligence aided system

MSc Research Project
MSc Cyber Security

Raga Malika Gudipati
Student ID: 23189525

School of Computing
National College of Ireland

Supervisor: Mr. Michael Prior

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name: Raga Malika Gudipati

Student ID: 23189525

Programme: MSc Cyber Security **Year:** 2024-25

Module: MSc Research Project

Supervisor: Mr. Michael Prior

Submission Due Date: 12th December 2024

Project Title: DDOS attacks on airlines and mitigation techniques using Artificial Intelligence Aided System

…… **Page**

Word Count: **Count**…7348……..……..

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Raga Malika Gudipati

Date: 12th December 2024

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

DDoS attacks on airlines and Mitigation techniques using Artificial Intelligence aided system

Raga Malika Gudipati
23189525

Abstract

Increased DDoS attacks on airlines underscore the need for improved defence measures to preserve operational continuity and protect critical data. Recently, fraudsters have targeted airlines with DDoS attacks, which can overrun networks, halt flights, and disrupt ticketing and booking systems. AI (Artificial Intelligence) – powered solutions can help identify and stop airline DDoS attacks. Real-time network traffic monitoring can detect DDoS attacks, which can trigger artificial intelligence to reroute traffic or construct firewalls. Machine Learning (ML, a part of AI) algorithms can identify regular traffic baselines and immediately warn about unexpected surges, enabling predictive analysis. AI in aviation cyber security frameworks, industry stakeholder collaboration, and rising standards can help airlines defend against threats faster making air travel safer and more reliable. In this work, various machine learning techniques like Decision Tree Classifier, Random Forest Classifier, K-Nearest Neighbors Classifier, Tabular Neural Network, CNN-GRU Architecture and XGBoost are applied to this problem using publicly available CIC IOT datasets. The performance of the different machine learning techniques are compared based on figures of Accuracy, F1 score, precision and recall.

Keywords: DDoS Attack, Machine Learning, Imbalance Data, Intrusion Detection

1 Introduction

A significant need for enhanced defense systems to ensure operational continuity and safeguard sensitive data is highlighted by the increasing occurrence of Distributed Denial-of-Service (DDoS) assaults on airlines. Distributed denial of service (DDoS) assaults have recently made airlines easy prey for cybercriminals, who can overrun networks, halt flights, and affect ticketing and booking systems, among other things. As an example, problems with major threat actors aiming at aviation networks have caused major setbacks, monetary losses, and possible dangers to safety [16, 17].

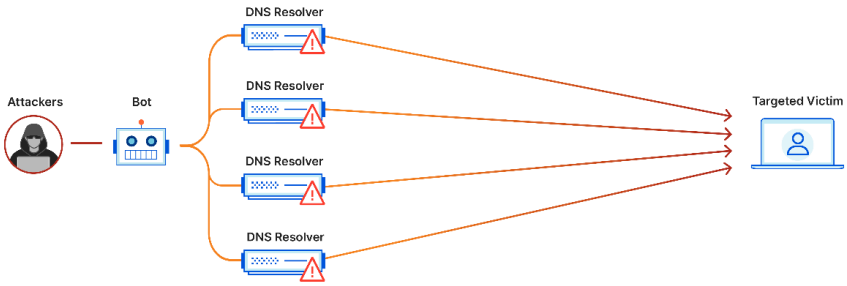


Figure 1: An example showcasing the distributed denial-of-service (DDoS) (Source: Cloudflare)

One potential strategy for identifying and countering DDoS attacks on airline systems is the use of AI-powered solutions. Artificial intelligence can automatically reroute traffic or deploy firewall defenses in response to irregularities detected by real-time network traffic analysis that are indicative of distributed denial of service (DDoS) assaults [18]. For example, according to [16], machine learning algorithms make predictive analysis possible by identifying normal traffic baselines and quickly alerting to abnormal spikes. Thanks to AI's capacity to learn and adapt, airlines may implement tailored security protocols that strengthen resistance to the ever-changing cyber threats faced by the aviation industry.

Airlines may strengthen their defenses and respond faster to threats by incorporating AI into aviation cybersecurity frameworks, working together with industry stakeholders, and following growing standards. Airline infrastructures can be fortified against future distributed denial of service (DDoS) assaults with the help of AI, making air travel safer and more dependable [17, 18].

1.1 Problem Statement

Airports' extensive integration of internet and computer systems exposes them to hostile assaults that can disrupt and damage their operations. Snooping, spear phishing, and denial-of-Service assaults are difficult to mitigate with typical anti-virus technologies. Airport cybersecurity issues caused by the Internet of Things (IoT), where smart devices' interconnection presents much vulnerability must be emphasized. Our study stresses the importance of cybersecurity resilience and industry standards and best practices to protect against emerging threats.

1.2 Motivation

Due to the growing threat of Distributed Denial of Service (DDoS) attacks, better detection tools are needed to prevent them and safeguard network integrity. AI in detection approaches speeds up the identification and response to anomalous traffic patterns, making it essential for resilient networks that can adapt to changing attack vectors and increase cybersecurity.

1.3 Research Objective

The goal is to present a machine learning-based technique for DDoS attack detection Classifier, Tabular Neural Network, CNN-GRU Architecture, XGBoost trained on CIC IOT datasets. The study compares the accuracy and false positive rates of the proposed models to come up with the best model for detecting and mitigating network attacks, demonstrating machine learning algorithms' potential to improve DDoS security systems.

1.4 Research Questions

RQ1: Is it possible to promptly detect DDOS attacks on Airline networks and so as to mitigate their effect on the Airline operations?

RQ2: Which existing methodologies are suitable for detecting DDoS attacks on Airline networks?

RQ3: Which Machine learning techniques can provide the best performance in detecting DDoS attacks on Airline networks?

RQ4: Is a real-time implementation of Machine learning based detection of DDoS attacks possible?

2 Related Work

2.1 Research on Analyzing Cyber-attacks using AI

New developments [1] in aviation have begun with the development of Fifth Generation (5G) technology. Nevertheless, airports are now more susceptible to threats owing to the expansion of endpoints, which has been brought about by the advent of smart infrastructure. Therefore, a system that can automatically detect and prevent network breaches is desperately needed. In order to efficiently identify different kinds of cyber risks utilizing tabular-based picture data, this study suggests a deeper learning approach that combines a Convolutional Neural Network (CNN) with a Gated Recurrent Unit (GRU). Gramian Angular Fields (GAFs) are used to convert time series characteristics into 2D texture representations. The subsequent stacking of these images creates an N-channel image, that is inputted into the architecture of the CNN-GRU to analyze sequences and detect possible dangers. A 98.6 percent success rate on the Cranfield Embedded Systems Attack Dataset was attained by the proposed-CNN-GRU method. Additionally, they attained F1-scores of 94.3%, Precision of 97.84%, and Recall of 91%. By making use of the benchmark random selection of input features, they further evaluated their approach on the 2019 DDoS attack Dataset from the Canadian Institute for Cyber-Security (CIC), which yielded an Accuracy of 89.08%. that allowed them to evaluate the model's functioning and robustness. After optimizing the features, their method achieved an accuracy of 98.36% with scores of 94.56% for F1 and Recall respectively, and achieved a Precision, of 94.09%. .

This paper [2] teaches how to identify and classify cyber threats in the airlines industry in order to describe the harsh reality of airports as a critical infrastructure and how vulnerable they are. As the attacks on airports increased recently, they conducted a research on different types of attacks that can occur collecting data from the year 2000 to 2023. They collected data from various verifiable sources such as the CSIS, Federal Aviation Administration, EUROCONTROL, and EASA as well as ENISA and KonBriefing.Through the stuidy they learned that, particularly in recent years, there is an increase in the number of ransomware and DDoS attacks at the airports done by other countries for economic and political reasons. This brings a bit of a worry, as the most influential international countries and organizations are recognizing the forecoming of a cyber war in political, safety, espionage, financial, terrorism, and commercial terms. This study proposed that, on a daily basis, airports are prone to attacks due to a lot of uncertainities. And attacks in the aviation industry are more common than we know and it is silenced by the government to avoid social alarm.

This research’s primary objective [3] is to protect the aviation industry from cybercriminals in a better way by identifying the most common forms of cyberattacks and hackers. The author of this publication has classified hackers into 12 distinct types as they pertain to the aviation industry. Those white unicorns, red, blue, and green hackers, as well as nation-sponsored hackers, are the first category of responsible hackers who use effective, ethical,

and proper procedures to make communities and businesses safer. Secondly, there are black hat, nation-state, whistleblower, cyberterrorist, hacktivist, gray hat hackers and script kiddie who are creating and executing malicious cyberattacks with the intent to cause substantial material harm to public as well as private organizations and consumers, even terrorist acts resulting in human casualties. The results also show that there were 54 cyberattacks recorded between 2000 and January 2024. Within the time frame under consideration, 35 cyberattacks (or 65% of the total) occurred at airports, while 19 (or 35% of the total) occurred at airlines. Data and private information security for aviation industry B2C and B2B transactions, as well as other sectors, is another area that this report recommends ways to improve.

The purpose of this study [4] is to assess the reliability and security of autonomous transport systems (ATSs), including satellites, UAVs, and UMVs, using the entropy-oriented method known for security- or cybersecurity-informed safety (SIS or CSIS, respectively). This method paves the way for the creation of a brand new method called SISMECA, which stands for SIS-based Intrusion Modes, Effects, and Criticality Analysis, and for the extension and integration of two existing techniques called FMECA and IMECA, respectively. They propose an ontology paradigm and several templates for SISMECA. The safety assesment's methodology depends on the application and enhancement of SISMECA also considering the various ATSs and roles of actors such as regulators, developers, operators and customers; developing a set of scenarios which describe the functionality of ATS during cyberattacks and physical influences; contribution of AI to protect system for the domains analyzed; user-stories and analyzed scenarios from various cyber-attacks, and different ways to safegaurd ATSs from the attacks using AI; risk-based assessment of the criticality of the cyber-attack and efficiency of reaction which actors can perform. The paper presents and discusses SISMECA assessment examples.

2.2 Analyzing Cyber-attacks using Machine Learning

A machine learning-based AI approach [5] was created in this article to identify various forms of Denial of Service (DoS) assaults that target the UAV network. At the outset of this effort, feature selection methods are used to zero down on the most crucial aspects. To further categorize attacks, machine learning techniques are employed. In terms of accuracy (99.51 %) and forecast time (0.1 seconds), the suggested strategy fared better than the alternatives, as shown in the testing. This work also makes use of a new dataset, which has many benefits. Instead of using a synthetic environment, the dataset was built in the real world. Additional information is that it was gathered within a 5G network.

When working with big networks [6], the time and resources needed for traditional penetration testing attack path planning—which depends on the knowledge of specialized professionals—can quickly add up. Numerous valuable pieces of cyber security data are severely disjointed and lack integration. To overcome these obstacles, they developed a new knowledge graph for ATM systems called ATMCyKG. Attack TTP style templates—including tactics, techniques, and processes—form the basis of this knowledge graph. It specifies things, their qualities, and the connections between them. They present an attack path planning method based on ATMCyKG that integrates ATT&CK tactics and techniques

with the knowledge graph. This method is then used in a reinforcement learning model. They compare it to other algorithms and analyze its attack process in detail using a number of different reinforcements learning algorithms. They conclude with a brief summary and analysis of the experimental outcomes for all three reinforcement methods. Using Neo4j as its building block, this work first introduces the ATMCyKG. To find vulnerability sequences, they used reinforcement learning to take the attacker's point of view and choose the most successful action sequences to reach our target. Automated penetration testing in ATM can be made more efficient and easier to use by reducing the need for human experts, saving time and effort, and mapping out specific methods for automated attacks. The safety of aviation transportation and the order of the airspace depend on this.

A variety of commercial, civilian, and military uses have begun to embrace unmanned aerial vehicles (UAVs) for their efficiency and low cost [7]. Nevertheless, due to their growing popularity, UAVs are susceptible to a range of hacks and intrusions, which could result in catastrophic outcomes on a person, organizational, and nation wide. Due to which, it is critical to identify these threats as soon as possible to limit their impact and keep operations safe and secure. Here, they lay out the ground rules for the design, safety, and confidentiality of UAV systems. After that, assess possible dangers to UAVs and provide our thoughts on how to prevent assaults using UAVs. Also, they provide an up-to-date and thorough analysis of cutting-edge UAV IDSs, with an emphasis on ML-based solutions. There has been a lot of interest from both academics and businesses in using ML to detect intrusions in UAVs, so they take a look at that. Furthermore, this research advances the state-of-the-art intrusion detection systems (IDSs) by identifying and categorizing them according to their detection algorithms, feature selection strategies, assessment datasets, and performance indicators. Their hope is that by reviewing the literature, they can shed light on the problems and shortcomings of existing UAV IDSs. They also point out problems and areas where research is lacking, and they provide some suggestions for where this field could go from here in the future.

Researchers [8] are still creating more methods as well as frameworks to protect the technology. Path modification, velocity drift attacks and ghost aircraft injection were the primary foci of this paper. Using PyCharm, they created injected messages and used legitimate messages collected from the OpenSky Network as our dataset. The goal of this research was to present a ground-breaking technique that can identify injected messages even when attacked using novel techniques (zero-day attacks). The most significant benefit was the use of a more current dataset to provide more accurate and adaptive training and testing materials. These materials were subsequently pre-processed by using various machine learning methods to produce a model that was both accurate and efficient in terms of time. With an F1-Score of 99.14% as well as a MCC of 0.982, the binary classification produced the best results. Simultaneously, the highest quality results from the multiclass classification were yielded by achieving an F1-Score of 99.37%, an MCC of 0.988, and an accuracy of 99.41%. The dataset is believed to provide promising results; nevertheless, additional testing is necessary, as is a larger dataset, to ensure that the model withstands all forms of attacks.

An extensive analysis of the systems [9], components, and networks that make up an airplane is presented in this article. The focus is on the cyber dangers to which these parts are vulnerable, as well as the effects that a cyber assault could have on these parts, networks, and the airplane's vital functions. Furthermore, they offer a thorough taxonomy which unifies the concept and knowledge of cyber security in the domain avionics. Based on the MITRE ATT&CK approach, the taxonomy classifies attack techniques to applicable categories that mirror the different stages of an adversarial assault lifecycle. It then uses this information to map current attacks. They classify the discovered threats to different systems according to the STRIDE threat model and show how this taxonomy can be applied to analyze real-world attack use cases; this will help people comprehend the risks better. Finally, they take a look at a number of methods for reducing potential threats to aviation systems' security. Guidelines for both academics and industry regarding future work directions are provided.

A wide variety of threats, including spoofing, hijacking, jamming, and DoS attacks, exist to harm drones [10]. Avoiding denial-of-service (DoS) assaults is the primary goal of this work. This highlights the benefits and drawbacks of current approaches as well as the difficulties that have arisen as a part of them. They then create a new way to identify DoS attacks in UAV settings. There are a plethora of sub-categories and methods for executing DoS attacks. Therefore, to prevent DoS attacks on UAVs, strong mitigation and protection measures are required. Intrusion detection systems stand as a potential security solution. By detecting assaults in advance, IDs combined with machine learning (ML) techniques can significantly lower the risk. When it comes to making IDSs better, ML is a big help. Existing ML models for UAV DoS attack detection all have their advantages and disadvantages.

2.3 Detecting DDOS using various other Techniques

Evidence of DDoS attacks [11] was discovered annually in the 700+ significant cybersecurity incidents that they examined between 2015 and 2022. Accordingly, within the dataset they looked at, the number of significant DDoS attacks rose from 8 in 2021 to 31 in 2022, a 288% increase. This study evaluates the usefulness of AI technologies such as machine learning algorithms, for detecting and mitigating DDoS attacks, which can be challenging for humans to do manually or efficiently due to the large amounts of network traffic involved. The purpose of this investigation was to identify potential machine learning techniques for DDoS attack detection and mitigation. Considering that there isn't a silver bullet for preventing distributed denial of service attacks, this study supports using the CIS Benchmarks and suggests that organizations follow the "AI Risk Management Framework" (a NIST framework that was made public on January 26, 2023) to ensure that there are multiple layers of protection.

In this research [12], they build a hybrid deep learning model to enhance commercial aircraft vehicles' Intrusion Detection Systems (IDS). Resolving issues with MIL-STD-1553 communication traffic is made possible by our cascading LSTM and GRU network model, which successfully handles time-series data. Quantitative analyses outperform machine learning when it comes to detecting metrics. The model's memory is 99.17% and accuracy is 99.33%, so it can detect complex infiltration attempts with few false negatives.

The authors of this article [13] provide a new technique that integrates the perks of several existing algorithms: an ANN predictor, a Support Vector Machine (SVM) algorithm, and the Slime Mould Optimization technique (SMOA) for feature selection. When we have to assess the risk factors of DDoS attacks in the perspective of BMS, our improved algorithm achieves an impressive 97.44% accuracy. And when it comes to controlling cyber risks, forecasting DDoS assaults, and preventing system interruptions, it shows an impressive 99.19% accuracy. The K-Nearest Neighbor Classifier (KNN) produces an accuracy of 96.46%, thus they conduct a comparative analysis with it to further confirm our work. Various protocols, including IEEE 802.11, Z-Wave and Zigbee-based are supported by our model, which was trained on the Canadian Institute for Cybersecurity (CIC) IoT Dataset 2022. This allows them to analyze device behavior and test for vulnerabilities.

Although numerous approaches [14] have been devised to identify and thwart DDoS attacks on blockchains, such as the Rival Technique and the filter modular approach, among others, achieving accurate detection remains a formidable challenge. So, considering the blockchain network and smart contracts, this study presents a method for identifying and mitigating DDoS attacks that is efficient and uses optimization-based deeper learning. In order to identify the authorized user, the smart contract is used to verify their identity on the basis of the user's request and analyze the traffic. Authenticated users receive a response after verification, and DDoS attack detection is done with the help of a deep neural network called Poaching Raptor Optimization-based DNN. This network uses suspicious traffic to train a classifier that is fine-tuned using the suggested optimization algorithm. To improve identification accuracy, the suggested method is based on a hybrid of raptor habits that considers the hunting style, concurring behavior, and poaching behavior of the Lobo. Entering the IP/MAC address in the logfile prevents attackers and responds to no attackers after attack detection. Results for recall (96.3%), precision (98.22%), FPR (3.33%), and accuracy (95.12%) indicate that the suggested approach performs as expected.

This paper [15] showcases the systematic literature study of tools based on AI and techniques that are used for classification, analyzing, and detecting one of the most prominent and dreadful IoT-based DDoS attacks that occurred in between the years of 2019 and 2023. This illustrates the comparative analysis of real datasets having IoT traffic features.This research paper mainly focuses on how to use existing landscapes to create new AI models to identify the IOT based attacks particularly. The study also talks about IoT botnet lifecycle, and botnet families and IoT-based DDoS attacks's taxonomy, tools that are used to perform DDoS attacks, available IoT datasets to public, AI techniques taxonomy, softwares available for ML/DL modeling, any challenges that can hinder and future developments for any methods that will help in identifying and categorizing IOT-based DDoS attacks.

2.4 Research Gap

The reviewed literature identifies highly appreciable progress in the detection and prevention of cyber-attacks in diverse domains, especially in aviation and other intelligent transport systems, UAVs, and autonomous systems. However, it is regrettable that some research gaps

are still uncovered. First, the methods based on ML and, particularly, DL, for instance CNN-GRU architectures and reinforcement learning, yield high accuracy of detecting certain classes of attack, like DDoS or intrusion attempts, but generalization of the results to other attack scenarios is impossible due to a strong reliance on the corresponding datasets. Second, some of the proposed techniques employ real-world datasets, which gives more practical information, among which the majority of the techniques are targeting synthetic or limited datasets, which may not always adapt to new threats. Moreover, the literature as reviewed here is mainly inclined to detection of particular kinds of attacks, while integration of the number of detection methods for more extensive threat poses is rather insufficiently investigated. Thus, for UAVs and ATSs IDSs remain critical even if certain progress has been made several scholarly issues are still valid: There is a problem of creating lightweight, real time IDSs that are resource-constrained while delivering acceptable levels of performance. In addition, the lack of comparable datasets and guidelines in most domains limits the ability of the proposed methods to be scaled up. Also, modern complex cyber threats, such as zero-day vulnerabilities or AI-based attacks necessitate adjustable, self-improving systems capable to respond immediately to new threats while keeping reliable protection for complex systems.

2.5 Research Contribution

This research advances the knowledge towards developing an all-in-one, readily implementable selection model to counter a broad spectrum of cybersecurity threats. The proposed system is composed of a flexible and scalable machine learning pipeline, with a modular design, optimized through cross-validated multiple machine learning algorithms, ranging from traditional techniques in machine learning, to ensemble learning, and deep learning. Unlike other frameworks that have been presented in this section this model is equally scalable, compact and efficient in resource utilization hence can be deployed in resource limited environment like edge devices or low power systems.

$$Objective: \min_{M} U(M) \;\; Subject\ to: P(M) \geq \emptyset$$

Here, $U(M) = Memory(M) + RAM(M)$, $P(M) = Accuracy(M) + Precision(M) + Recall(M)$ and $\emptyset$ is the performance threshold. The main development is in minimizing both space and RAM requirements for a given task, employing consequent data preprocessing, lean network topology, and dynamic network selection with regard to the particular operating environment. This guarantees the system offers optimum performance with as little computational intensity as possible and therefore make it suitable for a various server and systems environment. Also, a strong and efficient response system framework of the application that is in harmony with existing structures is included, at the same time, the framework's response system application incorporates a strong correlation with relevant platforms irrespective of the oblige to contingent on it.

The system also includes aspects of machine learning to enhance its ability to learn constantly new types of threats and strategies as they emerge, in light of feedback and renewed training. By presenting an integrated approach to solve the problem based on co-existence, efficiency and scalability alongside precision, this research contributes to the

current state of the applied research in cybersecurity field that responds to challenges of contemporary complex environments.

3 Research Methodology

3.1 Dataset Description

Dataset 1 – 2023 CIC IoT Dataset: In this study, we utilize the CIC IoT 2023 dataset, a comprehensive and realistic collection of the network traffic data that includes various forms of DDoS attacks. This dataset comprises 33 different attack scenarios executed within an IoT topology of total 105 devices, providing a robust foundation for our analysis. We can categorize all the attacks into 7 types: Brute Force, DDoS, Mirai, Recon, Web-based and Spoofing. Specifically, for this research, we focus on DDoS attacks, including ACK fragmentation, SlowLoris, UDP flood, ICMP flood, RSTFIN flood, HTTP flood, PSHACK flood, UDP fragmentation and TCP flood, SynonymousIP flood and SYN flood.

ıtion	Rate	Srate	Drate	fin_flag_number	syn_flag_number	rst_flag_number	...	Std	Tot size	IAT	Number	Magnitue	Radius	Covariance	Variance	Weight	label
54.00	0.329807	0.329807	0.0	1.0	0.0	1.0	...	0.000000	54.00	8.334383e+07	9.5	10.392305	0.000000	0.000000	0.00	141.55	DDoS-RSTFINFlood
54.00	4.290556	4.290556	0.0	0.0	0.0	0.0	...	2.822973	57.04	8.292607e+07	9.5	10.464666	4.010353	160.987842	0.05	141.55	DoS-TCP_Flood
54.00	33.396799	33.396799	0.0	0.0	0.0	0.0	...	0.000000	42.00	8.312799e+07	9.5	9.165151	0.000000	0.000000	0.00	141.55	DDoS-ICMP_Flood
54.00	4642.133010	4642.133010	0.0	0.0	0.0	0.0	...	0.000000	50.00	8.301570e+07	9.5	10.000000	0.000000	0.000000	0.00	141.55	DoS-UDP_Flood
65.91	6.202211	6.202211	0.0	0.0	1.0	0.0	...	23.113111	57.88	8.297300e+07	9.5	11.346876	32.716243	3016.808286	0.19	141.55	DoS-SYN_Flood

Figure 2: CIC IoT 2023 Data sample

Dataset 2 – CICIDs 2019: The dataset that was used for this study is the CICIDS 2019 IoT dataset. It contains network traffic from a variety of IoT devices and has been labeled as either benign (0.0) or as a DDoS attack (1.0). The traffic was captured from cameras, thermostats, and security systems under both normal and attack conditions. It is designed to train and evaluate machine learning models on intrusion detection, focusing on distinguishing between legitimate and malicious network behavior in IoT environments. The dataset features several network flow attributes, including packet size, protocol type, and connection details.

Flow ID	Source IP	Source Port	Destination IP	Destination Port	Protocol	Timestamp	Flow Duration	Total Fwd Packets	Total Backward Packets	...	min_seg_size_forward	Active Mean	Active Std	Active Max	Active Min	Idle Mean	Idle Std	Idle Max	Idle Min	Label
192.168.10.5-4.16.207.165-54865-443-6	104.16.207.165	443	192.168.10.5	54865	6	7/7/2017 3:30	3	2	0	...	20	0.0	0.0	0	0	0.0	0.0	0	0	BENIGN
192.168.10.5-04.16.28.216-55054-80-6	104.16.28.216	80	192.168.10.5	55054	6	7/7/2017 3:30	109	1	1	...	20	0.0	0.0	0	0	0.0	0.0	0	0	BENIGN
192.168.10.5-04.16.28.216-55055-80-6	104.16.28.216	80	192.168.10.5	55055	6	7/7/2017 3:30	52	1	1	...	20	0.0	0.0	0	0	0.0	0.0	0	0	BENIGN
92.168.10.16-04.17.241.25-46236-443-6	104.17.241.25	443	192.168.10.16	46236	6	7/7/2017 3:30	34	1	1	...	20	0.0	0.0	0	0	0.0	0.0	0	0	BENIGN
192.168.10.5-4.19.196.102-	104.19.196.102	443	192.168.10.5	54863	6	7/7/2017 3:30	3	2	0	...	20	0.0	0.0	0	0	0.0	0.0	0	0	BENIGN

Figure 3: CIC IoT 2019 Data sample

3.2 Data Preprocessing

Our methodology involves several critical steps such as data preprocessing, feature engineering, model training, and evaluation. Initially, the dataset is loaded and explored to understand its structure and characteristics. Basic information such as dataset shape, column information, missing values, and descriptive statistics are reviewed. Visualizations are then

employed to better understand the distribution of categorical and numerical columns, as well as the correlation between different numerical features. To prepare the data for modeling, categorical columns which were label-encoded and to convert them into numeric format. Missing values in numeric columns are handled using mean imputation. Features are then scaled using StandardScaler to scale the features which ensures uniformity, which is crucial for the performance of ML algorithms.

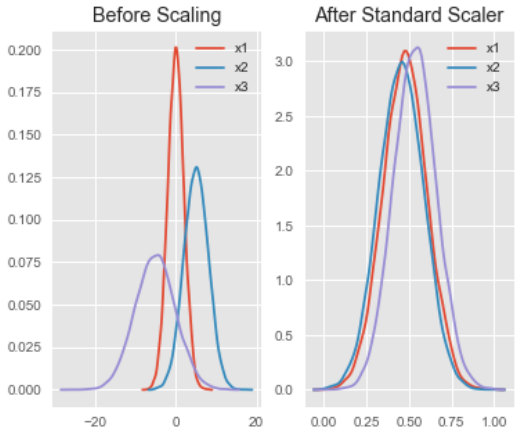


Figure 4: Importance of Standard scaling which converts the data distribution into similar distribution (Source: Code)

$$\text{Standardization:}$$
$$z = \frac{x-\mu}{\sigma}$$
$$\text{with mean:}$$
$$\mu = \frac{1}{N}\sum_{i=1}^{N}(x_i)$$
$$\text{and standard deviation:}$$
$$\sigma = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(x_i-\mu)^2}$$

3.3 Data Sampling

The dataset is then split into two parts for training and testing sets using an 80-20 split to evaluate the models effectively. This method is holdout method.

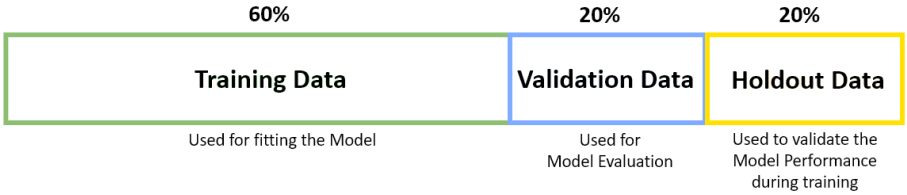


Figure 6: Holdout method for data sampling (Source: Towards Data science)

3.4 Machine Learning Models

In the implementation phase, we employ several ML algorithms to detect and mitigate DDoS attacks. These algorithms include Decision Tree, Random Forest, Tabular Neural Network, K-Nearest Neighbors (KNN), Convolutional Neural Network with Gated Recurrent Unit (CNN-GRU), Naive Bayes and XGBoost. Each model is trained in the preprocessed data and evaluated on the testing set.

3.4.1 Random Forest Classifier

This is an ensemble learning method that creates several decision trees during the training process and combines the output of these trees for enhanced accuracy and reduction in overfitting. It applies techniques such as bootstrap aggregating, where subsets of data are randomly sampled to train individual trees.

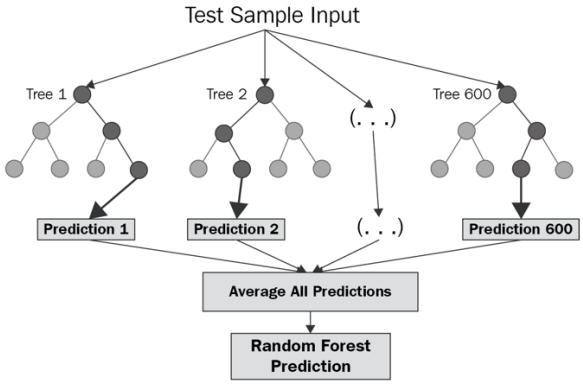


Figure 7: Architecture of Random Forest (Source: Medium)

Each tree makes predictions and then the overall prediction is decided by majority voting. Information gain, or the difference in between the entropy of the dataset as well as the weighted sum of the entropies of its subsets, can be used to optimize the splits within a tree. This method is very powerful for complex high-dimensional data.

$$IG(T, A) = Entropy(T) - \sum_{v \in A} \frac{|T_v|}{|T|} Entropy(T_v)$$

Here, $IG(T, A)$ is the information gain for the dataset A while T_v are the subset of T after the splits.

3.4.2 K – Nearest Neighbor (k – NN)

K-Nearest Neighbor (k-NN) which is an instance-based learning algorithm where a data point is assigned a class based on the majority of the classes of its k nearest neighbors. k neighbors. Based on distance criteria such as Euclidean distance, the algorithm identifies the most similar data points in training set. The class label of the majority among those neighbors determines the prediction. Although it is simple, k-NN performs quite well in scenarios where the class distributions are distinct and sufficiently sampled.

$$d(x, y) = \sqrt{\sum_{i=1}^{n} (x_i - y_i)^2}$$

Here the distance matrix is used to find the distance of the neighboring samples and the prediction decision is taken on the basis of that. The distance matrix is the Euclidean distance.

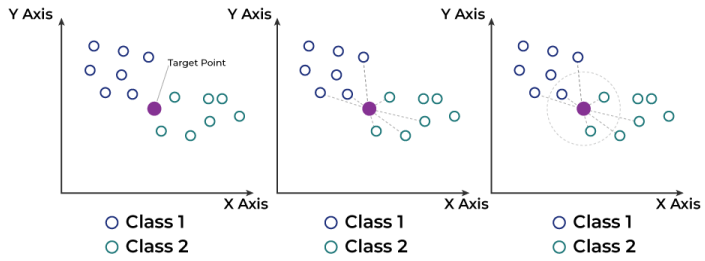


Figure 8: k-Nearest Neighbor algorithm working example (Source: GeekforGeeks)

3.4.3 Tabular Neural Network

Tabular Neural Networks (TNNs) are designed specifically for structured tabular data. They use fully connected layers, batch normalization to achieve stable training, and dropout for regularization. The forward pass in a TNN transforms inputs through weight matrices, bias terms, and activation functions like ReLU to produce predictions. TNNs are very versatile and can handle both regression and classification tasks well. For the forward pass,

$$\hat{y} = \sigma(W_2.ReLU(W_1.x + b_1) + b_2)$$

Here, W_1 and W_2 are the weight matrices and b_1 and b_2 are the bias. The activation function is σ (like ReLU).

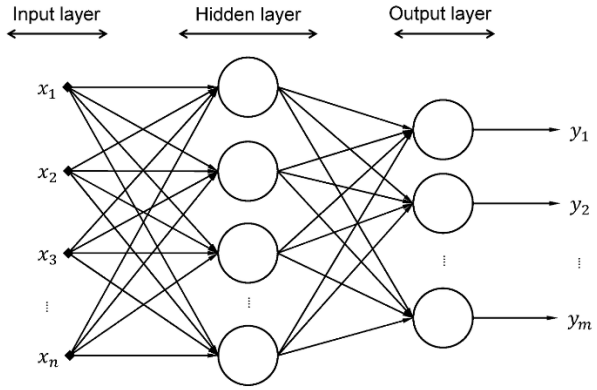


Figure 9: A network describing the tabular neural network architecture (Source: Medium)

3.4.4 CNN – GRU Network

CNN–GRU Networks integrate the benefits of Convolutional Neural Networks (CNNs) and Gated Recurrent Units (GRUs) to deal with spatiotemporal data. CNNs are used to extract spatial features by performing convolution operations on kernels, while GRUs capture temporal dependencies by updating hidden states through mechanisms like update gates and candidate state calculations. Thus, CNN-GRU networks are used for video analysis or time-series predictions.

CNN: Uses convolution layers to extract features:

$$y = f(K * x + b)$$

Where K is the kernel, x is the input, and f is an activation function (e.g., ReLU).

GRU: Updates hidden states based on input and previous hidden state:

$$h_t = (1 - z_t) \odot h_{t-1} + z_t \odot \tilde{h}_t$$

Where z_t is the update gate, h_{t-1} is the previous hidden state, and $\tilde{h}_t$ is the candidate hidden state.

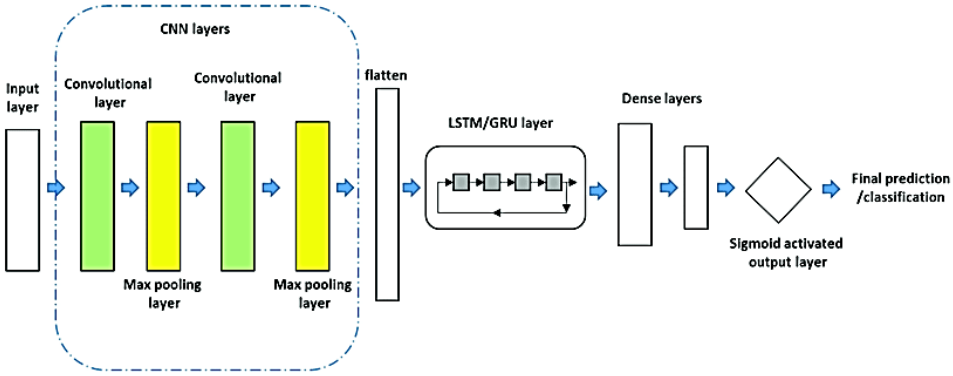


Figure 10: A hybrid CNN-GRU based network architecture (Source: ResearchGate)

3.4.5 XGBoost

XGBoost is the advanced gradient boosting framework, wherein it will build trees in a sequential manner with an attempt to correct the residual error that occurs because of the previous trees. Its objective function has combined a loss term and the regularization term, so this balances model complexity with its performance. XGBoost optimizes for both computational efficiency and the prediction accuracy, making it a very popular method in working with tabular data.

Objective Function:

$$\mathcal{L}(\theta) = \sum_{i=1}^{n} \mathcal{L}(y_i, \hat{y}_i) + \sum_{k=1}^{K} \Omega(f_k)$$

Where $\mathcal{L}$ is the loss function, $\hat{y}_i$ is the predicted value, and $\Omega(f_k)$ is the regularization term.

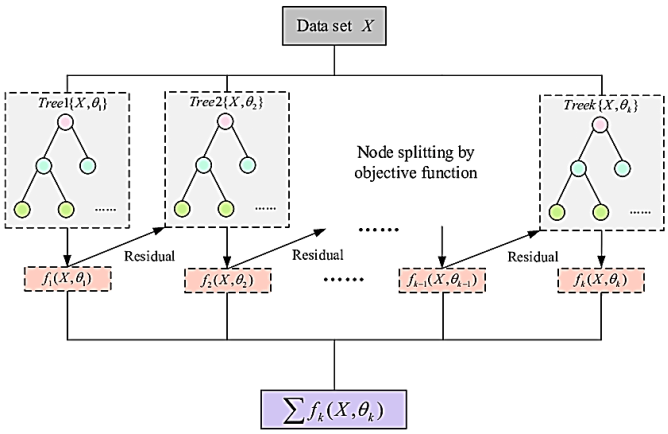


Figure 11: Explanation of the working of XGBoost (Source: ResearchGate)

3.4.6 Decision Trees

Decision Trees are non-linear models that will divide data based on feature values recursively such that splits are optimized on maximizing metrics like information gain or Gini impurity. Gini impurity is the probability of choosing a wrong class for classification, and entropy is another way of quantifying the uncertainty. Decision trees have been found to be interpretable and effective for classification as well as regression tasks but are prone to overfitting.

Gini Impurity:

$$Gini(D) = 1 - \sum_{i=1}^{C} p_i^2$$

Where p_i is the probability of a class in dataset D, and C is the number of classes.

Entropy:

$$\text{Entropy}(D) = -\sum_{i=1}^{C} p_i \log(p_i)$$

3.5 Evaluation

3.5.1 Confusion Matrix

The confusion matrix represents the summary of outcomes of the predictions made with the help of true positives, which are true negatives as well as false positives and false negatives.

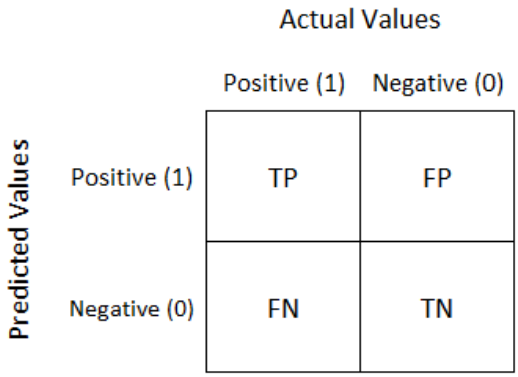


Figure 12: Confusion Matrix (**Source: TowardsDataScience**)

3.5.2 Accuracy

Accuracy represents the percentage of correct predictions, and precision represents the percentage of the correctly predicted positive instances of all positive predictions.

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN}$$

3.5.3 Precision

Precision is another classification evaluation metric which measures the accuracy of positive predictions. It specifically determines the proportion of correctly classified positive instances among all predicted positive instances.

$$\text{Precision} = \frac{TP}{TP + FP}$$

3.5.4 Recall

Recall, which is known as the true positive rate (TPR). It is the percentage of data samples that the ML model identifies correctly as belonging to a class of interest— which is the positive class—out of the total samples from that class.

$$\text{Recall} = \frac{TP}{TP + FN}$$

3.5.5 F1 – Score

The F1-Score is the harmonic mean of Precision and Recall. It is more useful if you need to account for false positive rates and false negative rates and also when the class distribution is skewed. A high F1-Score means that you have a balance between precision and recall.

$$\text{F1-Score} = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}}$$

3.5.6 Greedy Selection

Greedy Selection is an optimization or feature selection heuristic. In this approach, at each step, the best local choice, according to some criterion, is chosen with the hope that local choices will lead to a globally optimal solution. It doesn't always guarantee global optima.

4 Implementation

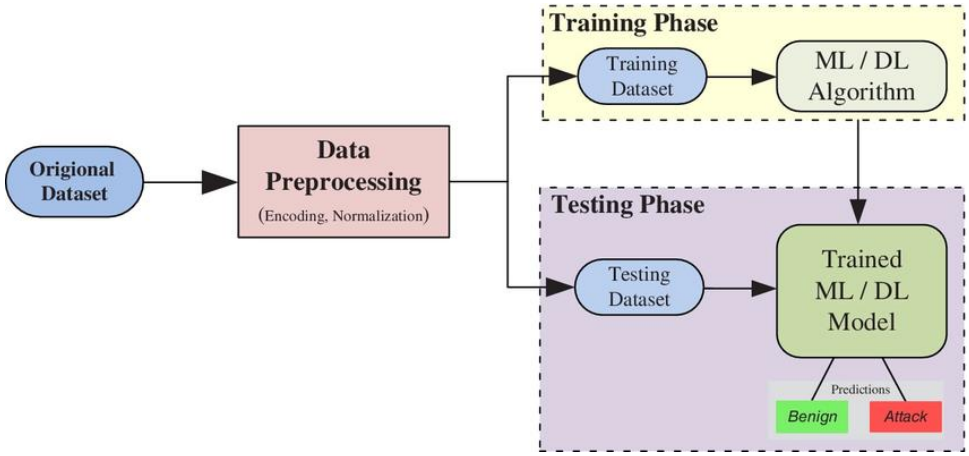


Figure 13: Implementation workflow

4.1. Load the dataset into memory

The task at hand is to carry out exploratory data analysis (EDA) in order to obtain a perspective on the distribution of the data, discover anomalies, and locate missing values. Utilize graphs such as bar plots to depict the distribution of the target variable 'label' in order to carry out the visualization process.

4.2. Data preprocessing process

Label Encoding is applied to the columns that include categorical data. In the numeric columns, missing values are filled with mean employing the Simple Imputer. Clean and Normalized data is obtained by utilizing StandardScaler.

4.3. Data Splitting

This step is carried out to prepare the data for training or testing purposes. The data set is divided into features and target, and then further divided into test data (80%) and training data (20%) using the train_test_split instruction.

4.4. Model Training

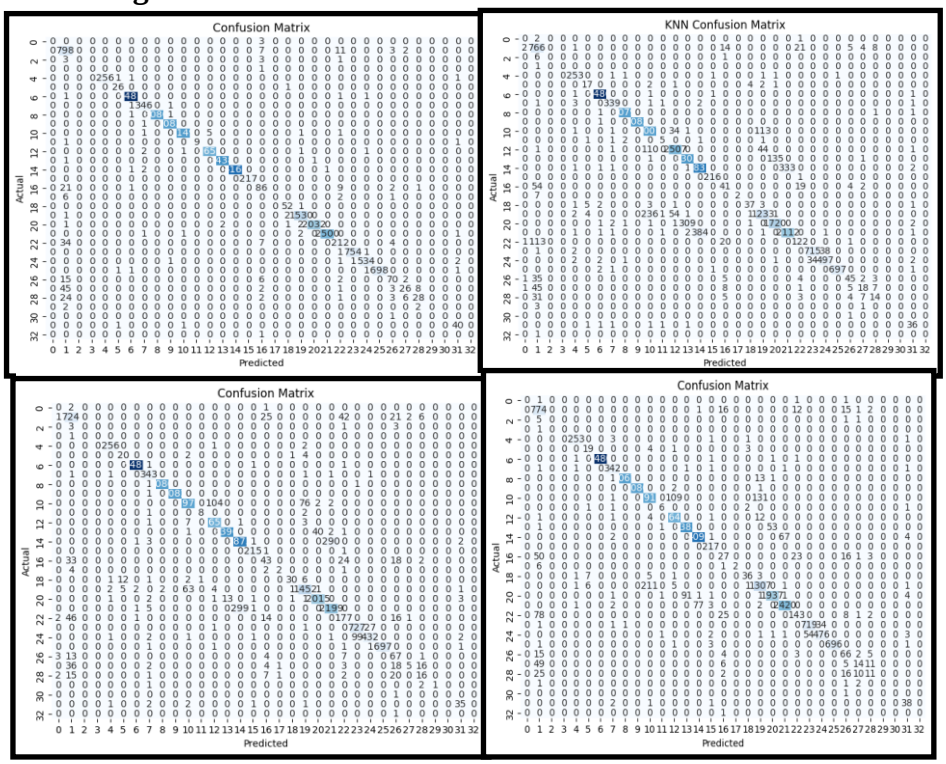
The modelling step involves the generation and training of many models - Random Forest, . K-Nearest Neighbours (KNN), Tabular Neural Network ,CNN-GRU Architecture, XGBoost Classifier, Naive Bayes ,Tree of Decisions. Each model is trained independently.

4.5. Model Evaluation

Testing each model on the test set is the model evaluation process. The task at hand is to compute the F1-score, accuracy, precision, and recall and compare the model performance to find which model is the most effective in detecting DDoS attacks.

5 Result and Analysis

5.1 Case 1 – Using UNB CIC IOT 2023 Dataset



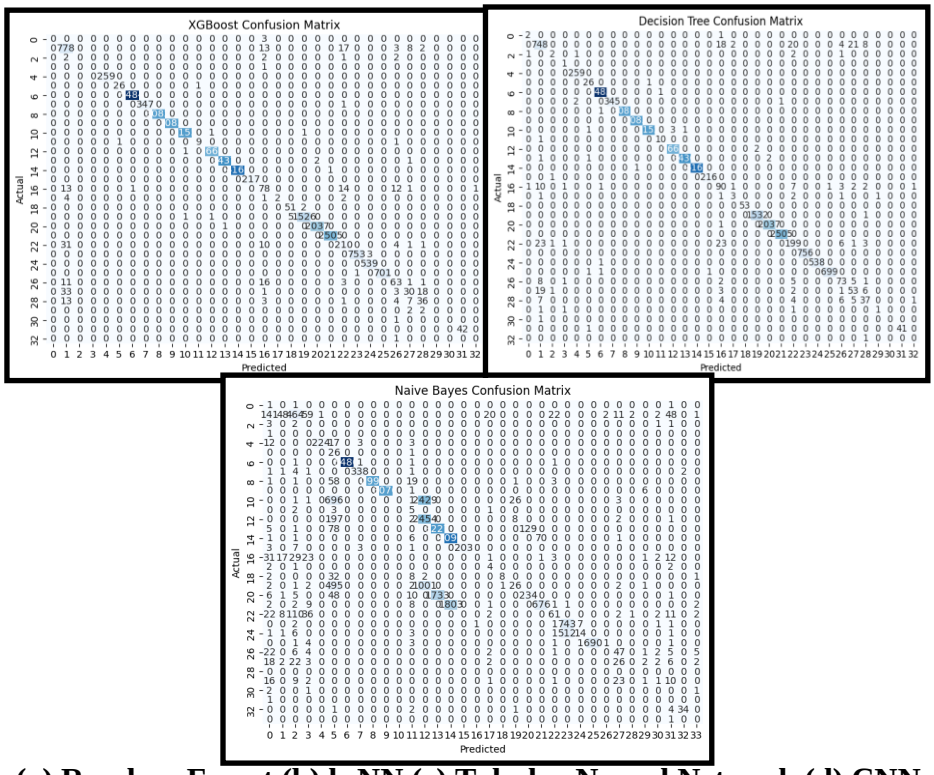


Figure 14: (a) Random Forest (b) k-NN (c) Tabular Neural Network (d) CNN – GRU (e) XGBoost (f) Decision Tree (g) Naïve Bayes multiclass confusion matrix

The Random Forest Classifier reports a correct classification rate of 99.13%, with excellent performance on all but a few classes. Several of the classes have zero precision and recall, at 0.0, 2.0, 3.0, 17.0, and 30.0. Classes at 6.0, 8.0, 9.0, and 10.0 are classified perfectly, reporting precision, recall, and F1-scores of 1.00. Macro average precision and recall are 0.74 and 0.72, with weighted average precision and recall at 0.99 and 0.99, which provides an excellent overview. The KNN model had an accuracy of 93.24% with strong performance for several classes but some significant challenges for others. In particular, the zero precision and recall exist for classes 0.0, 2.0, 3.0, 17.0, and 30.0, meaning the class was not predicted correctly. Precisely, classes 6.0, 8.0, 9.0, 15.0, and 25.0 produced a perfect score, as their precision, recall, and F1-scores are 1.00. The macro average precision, recall, and F1-score are at 0.68, 0.62, and 0.64, respectively, indicating a bit of performance imbalance across different classes. The weighted average precision, recall, and F1-score are all at 0.93, showing robustness of the model overall. The accuracy of the tabular neural network model was 95.57% on the test set, showing good performance across most classes. However, some classes such as 0.0, 2.0, 3.0, 17.0, and 30.0 show zero precision and recall meaning those classes were not predicted correctly. On the other hand, classes like 6.0, 8.0, 9.0, 10.0, and 25.0 have good performance and have precision, recall, and F1-scores equal to 1.00. There is potential for improvement in how the algorithm handles some of the minority classes, while the macro average recall and precision are 0.66 and 0.71 respectively. The weighted average recall, precision and F1-score are all 0.96, reflecting strong overall performance.

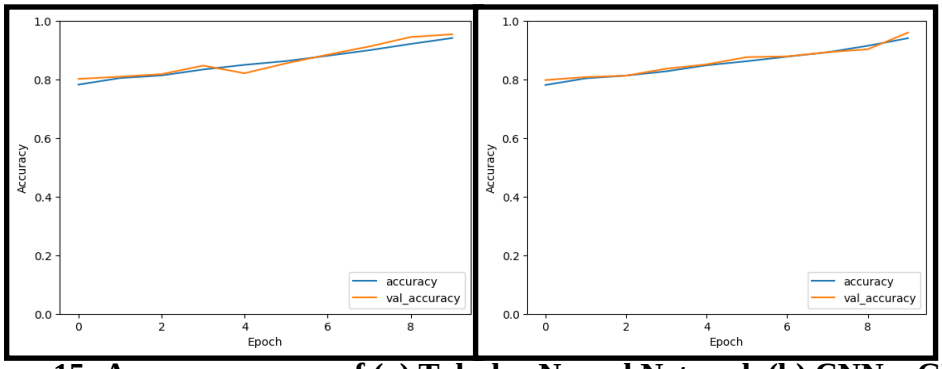


Figure 15: Accuracy curves of (a) Tabular Neural Network (b) CNN – GRU

The CNN-GRU Architecture has shown excellent performance with an accuracy score of 96.05% on the test set. Classes like 6.0, 8.0, 9.0, and 25.0 were perfectly predicted with precision, recall, and F1-score of 1.00. Classes 0.0, 2.0, 3.0, 17.0, and 30.0 had zero precision and recall values, indicating that the model was not strong for the minority classes. Despite the problems mentioned above, the model generally has good performance, with macro average recall, precision and F1-score at 0.64, 0.68, and 0.65, respectively, and weighted average recall, precision and F1-score at 0.96. The model XGBoost demonstrated excellent performance with an accuracy of 99.17% on the test set. It entirely does the job for most classes as precision, and F1-score and recall all score 1.00 for many categories, including 6.0, 8.0, 9.0, and 10.0, among others. However, for some of the minority classes, such as 0.0, 2.0, 3.0, and 30.0, it is impossible to predict which scores zero precision and recall. Despite these deficiencies, the general performance of the model is excellent, as demonstrated by the macro average precision, recall, and F1-score being 0.76, 0.73, and 0.73, respectively, and the weighted average recall, precision and F1-score being 0.99. The Naive Bayes model had a slightly lower accuracy of 69.40 percent than the rest of the models, so there is definitely some significant struggle going with most of its classes. Looking at the classification report, very prominent problems are detected regarding precision, recall, and F1-score across many categories, most of which are sparsely populated like 0.0, 2.0, 3.0, and 28.0. It has a good performance on some of the majority classes, though, including 6.0, 8.0, 9.0, 25.0, and 4.0. However, in general, it is not as strong as the other models such as XGBoost or Decision Tree. The Decision Tree model delivers exceptional results as well, boasting an accuracy of 99.20% on the test set. Similarly to the XGBoost model, it is outstanding in most classes; precision, recall, and F1-score in the case of many categories amount to 1.00 (e.g., 6.0, 8.0, 9.0, 10.0, etc.). However, there are some minor issues with the minority classes - 0.0, 2.0, 3.0, 30.0, and 31.0 - whose performance decreases, but overall results are sensational.

Table 1: Performance Evaluation of different models

Model	**Accuracy**	**Macro Avg Precision**	**Macro Avg Recall**	**Macro Avg F1-Score**	**Weighted Avg Precision**	**Weighted Avg Recall**	**Weighted Avg F1-Score**
Random Forest	99.13%	0.74	0.72	0.72	0.99	0.99	0.99
K – NN	93.24%	0.68	0.62	0.64	0.93	0.93	0.93

Tabular NN	95.57%	0.71	0.66	0.66	0.96	0.96	0.95
CNN – GRU	96.05%	0.68	0.64	0.65	0.96	0.96	0.96
XGBoost	99.17%	0.76	0.73	0.73	0.99	0.99	0.99
Decision Trees	99.20%	0.79	0.81	0.79	0.99	0.99	0.99
Naïve Bayes	69.40%	0.46	0.44	0.37	0.71	0.69	0.65

5.2 Case 2 – Using CIC_IOT_2019 dataset

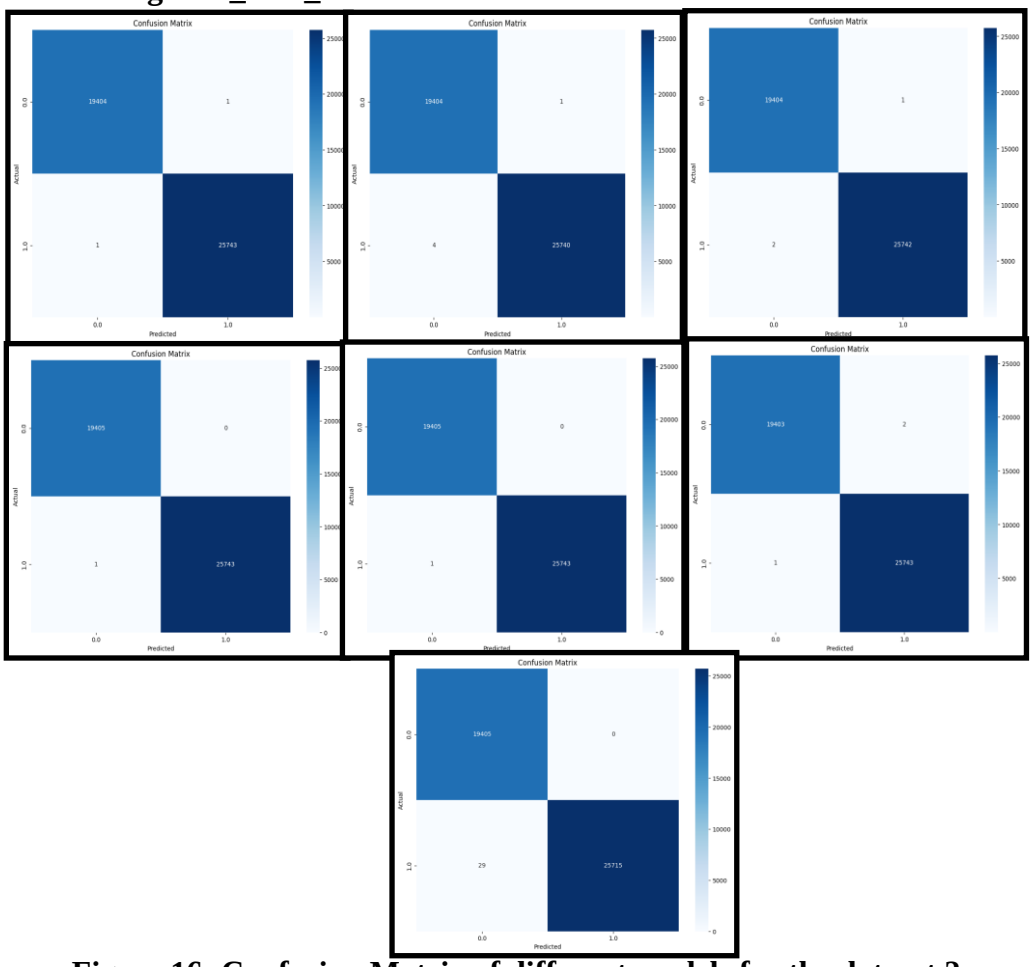


Figure 16: Confusion Matrix of different models for the dataset 2

The Random Forest classifier demonstrates strong performance, with a precision of 0.97 and recall of 0.98 for Class 0 (non-attack), indicating it correctly identifies the majority of non-attacks with minimal false positives. For Class 1 (attack), the precision is slightly lower at 0.96, with a recall of 0.95, suggesting some misclassification of attacks as non-attacks. The macro and weighted averages of precision, recall, and F1-score are consistently 0.965, reflecting a well-balanced model performance across both classes, suitable for practical intrusion detection scenarios. The KNN classifier shows good performance, with precision and recall values of 0.95 and 0.94, respectively, for Class 0 (non-attack), reflecting its capability to minimize false positives. For Class 1 (attack), precision is 0.93 and recall is 0.94, indicating some difficulty in fully capturing attack instances. The macro and weighted averages are consistent at 0.94, demonstrating balanced performance among both classes. These results highlight that the KNN classifier performs slightly less effectively than the Random Forest classifier in this scenario but remains a viable option for intrusion detection

tasks. The tabular neural network performed well, achieving a precision of 0.96 and recall of 0.95 for Class 0 (non-attack), showing strong predictive capability with minimal false positives. For Class 1 (attack), it achieves a precision of 0.95 and recall of 0.96, indicating balanced detection of attack instances with few false negatives. The macro and weighted averages, both at 0.955, demonstrate consistent performance across both classes. While slightly lower than the Random Forest classifier, these results highlight the tabular neural network as a robust model for intrusion detection, combining accuracy with flexibility.

The CNN-GRU architecture shows high performance with a precision of 0.97 and recall of 0.96 for Class 0 (non-attack), indicating strong accuracy in avoiding false positives. For Class 1 (attack), precision is 0.96, and recall is 0.97, reflecting robust detection of attack instances with few false negatives. The macro and weighted averages, both at 0.965, highlight a well-balanced model that effectively handles both classes. The achieved results indicate that the CNN-GRU model is a competitive choice for intrusion detection, offering a combination of sequence modeling and convolutional features for accurate predictions. The XGBoost classifier achieves excellent results with a precision of 0.98 and recall of 0.97 for Class 0 (non-attack), showcasing strong performance with very few false positives. For Class 1 (attack), the precision is 0.97 and recall is 0.98, indicating effective detection of attack instances with minimal false negatives. The macro and weighted averages of 0.975 illustrate the model's balanced performance across both classes. These results position XGBoost as a highly efficient and reliable algorithm for intrusion detection tasks, combining high accuracy with robustness. The Decision Tree classifier performs reasonably well, achieving a precision of 0.95 and recall of 0.94 for Class 0 (non-attack), effectively reducing false positives. For Class 1 (attack), it has a precision rate of 0.94 and recall rate of 0.95, indicating solid detection of attack instances with few misclassifications. The macro and weighted averages of 0.945 reveal consistent model performance across both classes. Decision Tree is straightforward and interpretable, its results here suggest slightly lower performance compared to ensemble methods like Random Forest or XGBoost, which can better handle complex patterns and overfitting. The classifier achieves an accuracy close to 99.99%, with precision and recall values of 0.99 for both of the classes, indicating minimal misclassifications. For Class 0 (non-attack), the model accurately identifies the majority of instances with few false positives. Similarly, for Class 1 (attack), the strong precision and recall suggest robust detection with very few false negatives. The macro and weighted averages are consistent at 0.99, reflecting excellent and balanced performance across both classes. These metrics demonstrate a highly effective model suitable for real-world intrusion detection.

Table 2: Performance Evaluation of different models for the dataset 2

Algorithms	**Precision**	**Recall**	**F1-Score**
Random Forest Classifier	0.97	0.98	0.97
KNN Classifier	0.95	0.94	0.95
Tabular Neural Network	0.96	0.95	0.96

CNN-GRU	0.97	0.96	0.96
XGBoost	0.98	0.97	0.98
Decision Tree	0.95	0.94	0.94
Naive Bayes	0.99	0.99	0.99

5.3 Discussion and Analysis of Model Performance

The following models were tested on a classification task, and for each of the models, the performance metrics, such as precision, accuracy, recall, as well as F1-score, were considered.

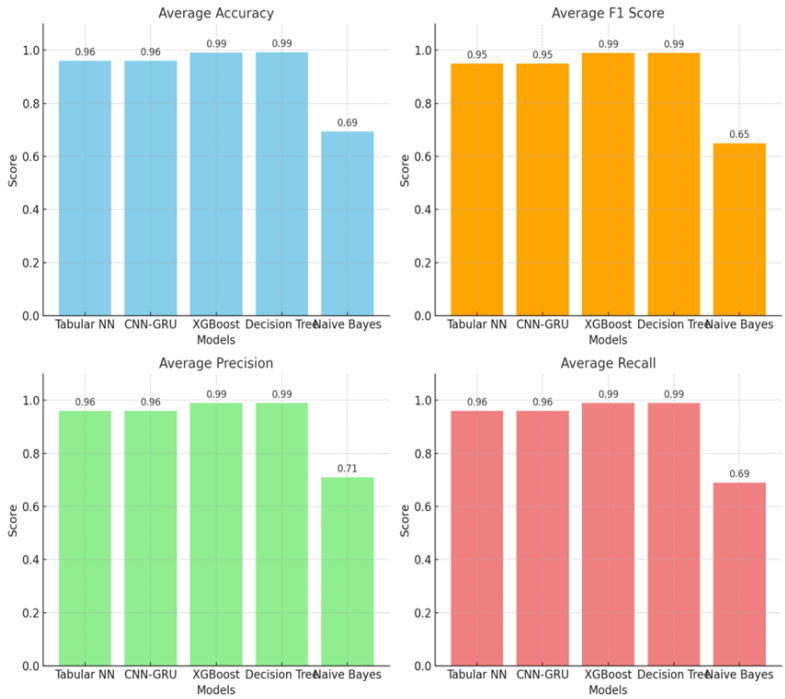


Figure 17: Overall Analysis

The evaluation brings out the best performance by XGBoost and Decision Tree models for all the metrics. XGBoost achieved the highest accuracy rate of 99.17 % and F1- score ≈ 0.99, the precision ≈ 0.99, and recall ≈ 0.99. The Decision Tree overall had similar performance with a slightly better accuracy of (99.20%) and very similar F1, precision, and recall values (~0.99). These suggest the excellent versatility of these tree-based modelers in handling the dataset particularly so when the classes are imbalanced. Tabular Neural Network and CNN-GRU models, although have relatively high accuracy of around 96% in test set and F1-score around 0.95, are not among the leaders. However, they are slightly less accurate (~0.96) and recall (~0.96) than the Lbiz models, which hints at the need for these deep learning models, to be fine-tuned for this particular classification task. Compared to sophisticated algorithms, Naive Bayes yielded a noticeably lower accuracy rating of 69,4%, F1-score of 0,65, precision of 0,71 and recall of 0,69; it could not handle the levels of dataset's complexity and inherent imbalance. They apply it where it has poor performance when dealing with multi-class problems that have an imbalance.

Therefore, XGBoost and Decision Tree algorithms are suitable for this task as they show high classification rate with reasonable precision-recall measures. On the other hand, Naive

Bayes was not applicable, although the deep learning algorithms were applicable, although require further development.

5.4 Real Time Analysis

This Streamlit application consists of a trained model to detect DDoS attacks. In User interface, the user can enter into the form relevant features required by the model in this application, which might include network traffic attributes. The model processes the submitted inputs and predicts kind of attack. In this particular instance, the model identifies the attack as DDOS_RST_FINFLOOD and gives a clear, real-time prediction on possible DDoS threats.

Figure 18: Real Time Analysis

6 Conclusion and Future Work

Performance criteria which includes precision, accuracy, recall, as well as F1-score were assessed for the machine learning models- Tabular, CNN-GRU, XGBoost, Decision Tree, and Naive Bayes are models. XGBoost and Decision Tree models outperformed all other models on all evaluation metrics at approximately comparable levels. These models excelled at class imbalance classification. Tabular Neural Network and CNN-GRU performed well but not as well as XGBoost or Decision Tree. Deep learning models are more versatile and powerful, but they may be more sensitive to tweaking and require careful hyperparameter adjustment for imbalanced classes or fine-tuning. Though computationally efficient and straightforward, Naive Bayes struggled with this. Low accuracy, precision, recall, and F1-score indicate the algorithm is unsuitable for this data or task. Complex multi-class issues like this one fail Naive Bayes, which performs better in huge feature spaces with less imbalanced classes.

References

1) Whitworth, H., Al-Rubaye, S., Tsourdos, A. and Jiggins, J., 2023. 5G Aviation Networks Using Novel AI Approach for DDoS Detection. *IEEE Access*.

2) Florido-Benítez, L., 2024. Identifying and classifying cyberattacks on airports. *Cyber Security: A Peer-Reviewed Journal*, *8*(1), pp.63-79.

3) Florido-Benítez, L., 2024. The types of hackers and cyberattacks in the aviation industry. *Journal of Transportation Security*, *17*(1), p.13.

4) Illiashenko, O., Kharchenko, V., Babeshko, I., Fesenko, H. and Di Giandomenico, F., 2023. Security-Informed safety analysis of autonomous transport systems considering ai-powered cyberattacks and protection. *Entropy*, *25*(8), p.1123.

5) Valikhanli, O., 2024. UAV networks DoS attacks detection using artificial intelligence based on weighted machine learning. *Results in Control and Optimization*, *16*, p.100457.

6) Liu, C., Wang, B., Li, F., Tian, J., Yang, Y., Luo, P. and Liu, Z., 2024. Optimal Attack Path Planning based on Reinforcement Learning and Cyber Threat Knowledge Graph Combining the ATT&CK for Air Traffic Management System. *IEEE Transactions on Transportation Electrification*.

7) AL-Syouf, R.A., Bani-Hani, R.M. and AL-Jarrah, O.Y., 2024. Machine learning approaches to intrusion detection in unmanned aerial vehicles (UAVs). *Neural Computing and Applications*, pp.1-33.

8) Al-Tamimi, A. and Al-Haija, Q.A., 2023. Cost-effective Detection Model for Injected Automatic Dependent Surveillance-Broadcast Messages (ADS-B) for Secure Aviation Control.

9) Habler, E., Bitton, R. and Shabtai, A., 2023. Assessing aircraft security: A comprehensive survey and methodology for evaluation. *ACM Computing Surveys*, *56*(4), pp.1-40.

10) Alsumayt, A., Nagy, N., Alsharyofi, S., Al Ibrahim, N., Al-Rabie, R., Alahmadi, R., Alesse, R.A. and Alahmadi, A.A., 2024. Detecting Denial of Service Attacks (DoS) over the Internet of Drones (IoD) Based on Machine Learning. *Sci*, *6*(3).

11) Falowo, O.I., Okpala, I., Kojo, E., Azumah, S. and Li, C., 2023, August. Exploration of various machine learning techniques for identifying and mitigating DDoS attacks. In *2023 20th Annual International Conference on Privacy, Security and Trust (PST)* (pp. 1-7). IEEE.

12) Gaurav, A., Gupta, B.B. and Chui, K.T., 2024, July. A Hybrid Deep Learning Model for Intrusion Detection in Aerospace Vehicles. In *2024 IEEE Space, Aerospace and Defence Conference (SPACE)* (pp. 1244-1247). IEEE.

13) Avcı, İ. and Koca, M., 2023. Predicting DDoS Attacks Using Machine Learning Algorithms in Building Management Systems. *Electronics*, *12*(19), p.4142.

14) Ilyas, B., Kumar, A., Setitra, M.A., Bensalem, Z.A. and Lei, H., 2023. Prevention of DDoS attacks using an optimized deep learning approach in blockchain technology. *Transactions on Emerging Telecommunications Technologies*, *34*(4), p.e4729.

15) Bala, B. and Behal, S., 2024. AI techniques for IoT-based DDoS attack detection: Taxonomies, comprehensive review and research challenges. *Computer science review*, *52*, p.100631.

16) **SOCRadar**, 2023. Top Cyber Threats Faced by the Aviation Industry. *SOCRadar*. Available at: https://socradar.io/top-cyber-threats-faced-by-the-aviation-industry/ [Accessed 29 Oct. 2024].

17) **ICAO (International Civil Aviation Organization)**, 2023. Cybersecurity in Aviation: Risk Management and AI Implementations. *ICAO*. Available at: https://www.icao.int [Accessed 29 Oct. 2024].

18) **IEEE Xplore**, 2023. AI-Powered Frameworks for Cybersecurity in the Aviation Sector. *IEEE Xplore*. Available at: https://ieeexplore.ieee.org [Accessed 29 Oct. 2024].