Policy Research Journal
ISSN (E): 3006-7030 ISSN (P) : 3006-7022 Volume 4, Issue 4, 2026

DATA SECURITY AND PRIVACY IN DATA COMMUNICATION USING MACHINE LEARNING TECHNIQUES

Ariba Afzal[*1], Muhammad Sajid Maqbool[*2], Dr. Naeem Aslam[3], Haseeb ur Rehman[4], Rabia Hassan[5], Sarim Javed[6]

[*1, *2,3,4,5,6]*Department of Computer Science, NFC Institute of Engineering and Technology, Multan, Pakistan*

[*1]ariba16170@gmail.com, [*2]sajid.maqbool@nfciet.edu.pk, [3]naeem.aslam@nfciet.edu.pk, [4]mhaseeb1220@gmail.com, [5]rabialpq555@gmail.com, [6]sarimjaved03@gmail.com

DOI: https://doi.org/10.5281/zenodo.19849129

Keywords
Data security, Data privacy, Machine learning classifiers, Internet of Things, Data communication

Article History
Received: 04 March 2026
Accepted: 11 April 2026
Published: 28 April 2026

Corresponding Author: *
Ariba Afzal
Muhammad Sajid Maqbool

Abstract
The escalating volume and sensitivity of data transmitted across networks underscore the critical need for robust data security and privacy measures. This research leverages the CICIDS2017 dataset, a comprehensive collection of network traffic data, to investigate key challenges in securing data communication. The study focuses on the identification and classification of network intrusions, the evaluation of intrusion detection systems (IDS), and the assessment of privacy-preserving techniques. The CICIDS2017 dataset enables a detailed analysis of various attack scenarios, providing insights into network vulnerabilities and the effectiveness of different security protocols. The methodology incorporates established techniques from existing literature. The findings contribute to a deeper understanding of the trade-offs between security and privacy, offering recommendations for the design and implementation of more secure and privacy-aware data communication systems. The aim is to enhance the protection of sensitive information in modern network environments.

1 Introduction
In today's interconnected world, data communication is the backbone of nearly every aspect of modern life. From personal interactions to critical infrastructure operations, the seamless exchange of information is essential. However, this reliance on data communication also introduces significant challenges, particularly concerning data security and privacy. [1] As the volume and velocity of data transmission increase exponentially, so too do the risks associated with unauthorized access, data breaches, and privacy violations. This research paper delves into the critical aspects of data security and privacy within the context of data communication, utilizing the Canadian Institute for Cybersecurity Intrusion Detection System 2017 (CICIDS2017) dataset to provide a comprehensive analysis. [2] Data security encompasses the measures taken to protect data from unauthorized access, use, disclosure, disruption, modification, or destruction. This includes implementing robust authentication mechanisms, encryption protocols, and intrusion detection systems to safeguard data integrity and confidentiality. Privacy, on the other hand, focuses on the rights of individuals to control their personal information, including how it is collected, used, and shared [3]. In data communication, privacy concerns arise from the

potential for data breaches, surveillance, and the misuse of personal information. Striking a balance between data security and privacy is paramount, as effective security measures must not infringe upon individuals' fundamental rights to privacy.

The CICIDS2017 dataset, a comprehensive and publicly available dataset, serves as the foundation for this research. It simulates real-world network traffic, including benign and malicious activities, making it an ideal resource for studying data security and privacy challenges. The dataset includes a wide range of network attacks, such as denial-of-service (DoS), distributed denial-of-service (DDoS), brute-force attacks, and malware infections [4]. By analysing the CICIDS2017 dataset, this research aims to identify vulnerabilities in data communication systems, evaluate the effectiveness of existing security measures, and propose innovative solutions to enhance data security and privacy.

The evolution of cyber threats has outpaced the development of effective security solutions. Traditional security measures, such as firewalls and intrusion detection systems (IDS), are often insufficient to protect against advanced persistent threats (APTs) and zero-day exploits. The use of machine learning and artificial intelligence (AI) has emerged as a promising approach to improve the detection and response to cyberattacks. These technologies can analyze vast amounts of data, identify patterns, and predict future threats with greater accuracy than traditional methods[5]. This research paper explores several key areas within data security and privacy in data communication. First, it examines the various types of network attacks and their potential impact on data confidentiality, integrity, and availability. Second, it investigates the role of intrusion detection systems (IDS) in identifying and mitigating malicious activities. Third, it evaluates the effectiveness of encryption protocols and other security measures in protecting sensitive data during transmission. Finally, it addresses the privacy implications of data collection, storage, and usage, considering relevant regulations and ethical considerations. Through a combination of theoretical analysis, empirical evaluation, and practical examples, this research aims to provide valuable insights into the complex interplay between data security and privacy in data communication.

Motivation

The increasing frequency and sophistication of cyberattacks underscore the urgent need for enhanced data security measures. Data breaches can lead to significant financial losses, reputational damage, and legal consequences for organizations. Moreover, the unauthorized access and misuse of personal data can have devastating impacts on individuals, including identity theft, financial fraud, and emotional distress. The protection of privacy is not only a legal and ethical imperative but also a fundamental right in many societies. The CICIDS2017 dataset provides a valuable resource for training and evaluating machine learning models for intrusion detection and other security-related tasks. The dataset's comprehensive nature allows researchers to test the performance of different algorithms under various attack scenarios and assess their ability to distinguish between benign and malicious traffic. [6] This research paper contributes to this effort by applying state-of-the-art machine learning techniques to the CICIDS2017 dataset and evaluating the effectiveness of different security measures. The CICIDS2017 dataset is a comprehensive and publicly available dataset that simulates real-world network traffic, including various types of attacks and normal network behaviors. The dataset contains a wide range of features, such as network traffic statistics, connection details, and attack labels. The CICIDS2017 dataset is a valuable resource for researchers and practitioners in the field of cybersecurity, providing a realistic and diverse environment for evaluating the effectiveness of intrusion detection systems, analyzing network traffic patterns, and developing new security and privacy solutions.

2 Literature review

The rapid evolution of data communication has brought about unprecedented opportunities, alongside significant challenges in ensuring data security and privacy. The increasing volume, velocity, and variety of data transmitted across networks have made it imperative to develop robust security measures and privacy-preserving

techniques. This review explores the existing literature on data security and privacy, with a specific focus on the application of these concepts within the context of the Canadian Institute for Cybersecurity Intrusion Detection System 2017 (CICIDS2017) dataset. Data security in communication involves protecting data from unauthorized access, use, disclosure, disruption, modification, or destruction. Traditional security measures include encryption, which transforms data into an unreadable format, making it inaccessible to unauthorized parties. Firewalls and intrusion detection systems (IDS) are also crucial, acting as barriers against malicious network traffic and identifying potential threats. The use of secure protocols like Transport Layer Security (TLS) ensures the confidentiality and integrity of data during transmission. However, as networks become more complex, traditional methods face limitations. Advanced persistent threats (APTs) and sophisticated cyberattacks necessitate the adoption of more advanced security measures, such as machine learning-based intrusion detection systems. [7].

The CICIDS2017 dataset is a benchmark for evaluating the effectiveness of IDS. It includes various types of network traffic, including benign and malicious activities. The dataset's comprehensiveness allows researchers to develop and test security models in realistic network environments. Several studies have leveraged CICIDS2017 to evaluate the performance of different machine-learning algorithms in detecting cyberattacks. These studies highlight the importance of feature engineering, where relevant network features are extracted and used to train machine learning models. [8] Feature selection techniques are employed to reduce the dimensionality of the data, improve model performance, and reduce computational complexity. Deep learning models, such as convolutional neural networks (CNNs) and recurrent neural networks (RNNs), have also been applied to the CICIDS2017 dataset to identify complex patterns in network traffic. [1]. Privacy, in the context of data communication, concerns the protection of personal information from unauthorized access and use. Privacy-preserving techniques include anonymization, which removes or obscures identifying information, and differential privacy, which adds noise to data to protect individual privacy while maintaining data utility. In data communication, privacy is especially crucial due to the potential for sensitive data, such as personal health records or financial information, to be transmitted across networks. Data breaches can have severe consequences, including identity theft and financial loss. [9] The implementation of privacy-enhancing technologies is an important area of research. These technologies aim to balance the need for data analysis with the protection of individual privacy. Homomorphic encryption, which allows computations to be performed on encrypted data, is a promising approach to data privacy. Secure multi-party computation enables multiple parties to jointly compute a function without revealing their individual inputs. These technologies offer advanced privacy guarantees, but they often come with computational overhead. Therefore, research efforts are focused on optimizing these techniques for practical applications.

The CICIDS2017 dataset can also be used to evaluate privacy-preserving techniques. For instance, researchers can simulate data breaches and evaluate the effectiveness of anonymization techniques in preventing the re-identification of sensitive information. The use of privacy-preserving machine learning models can help to build intrusion detection systems that protect both data security and privacy. The integration of data security and privacy in data communication is a continuous process. The evolving threat landscape requires the development of adaptive and robust security and privacy measures. Future research directions include the development of AI-powered security systems, the use of blockchain technology for secure data storage and sharing, and the development of privacy-preserving machine learning models. The CICIDS2017 dataset will continue to play an important role in evaluating the effectiveness of these approaches.

3 Methodology

3.1 Data Acquisition and Preprocessing

Obtain the CICIDS2017 dataset. Clean and preprocess the data. This includes handling missing values, removing irrelevant features, and

formatting the data for analysis. Normalize or standardize numerical features to ensure all features contribute equally to the analysis. Encode categorical variables into a numerical format suitable for machine learning algorithms [10]

3.2 Feature Selection/Engineering:

Analyze the dataset to identify features relevant to data security and privacy. Use feature selection techniques (e.g., Select K Best, Recursive Feature Elimination) to choose the most informative features. Engineer new features, if necessary, such as statistical measures of network traffic.

3.3 Security and Privacy Threat Modelling:

Identify potential security threats (e.g., malware, intrusion, data breaches) and privacy risks (e.g., unauthorized data access, data misuse) relevant to the data communication scenario. Define attack scenarios and the types of attacks to be simulated or detected.

3.4 Implementation of Security and Privacy Measures:

Encryption: Implement encryption algorithms (e.g., AES, RSA) to protect data confidentiality during transmission.

Access Control: Develop and implement access control mechanisms to restrict data access based on user roles and permissions.

Anonymization/Pseudonymization: Apply techniques to anonymize or pseudonymize sensitive data to protect privacy. This may involve masking, generalization, or other methods.

Intrusion Detection Systems (IDS): Implement and evaluate an IDS to detect malicious activities and network intrusions.

Privacy-Preserving Techniques: Explore and implement privacy-preserving techniques like differential privacy or federated learning, if applicable.

3.5 Model Development and Training:

Choose machine learning algorithms appropriate for the security and privacy tasks (e.g., classification for intrusion detection, anomaly detection). Split the dataset into training, validation, and testing sets. Train the models using the training data. Tune the model parameters using the validation set.

3.6 Evaluation Metrics:

Use appropriate metrics to evaluate the performance of the implemented security and privacy measures. For intrusion detection: accuracy, precision, recall, F1-score, and ROC AUC. For privacy metrics that measure the effectiveness of anonymization or privacy-preserving techniques.

3.7 Experimental Setup:

Define the experimental setup, including the software and hardware used. Describe the environment where the experiments are conducted.

3.8 Results and Analysis:

Present the results obtained from the experiments. Analyse the performance of the implemented security and privacy measures. Compare the results with baseline methods or existing solutions. Discuss the effectiveness, limitations, and potential improvements of the proposed approach.

3.9 Discussion and Conclusion:

Summarize the findings and contributions of the research. Discuss the implications of the results for data security and privacy in data communication. Suggest future research directions.

Proposed methodology

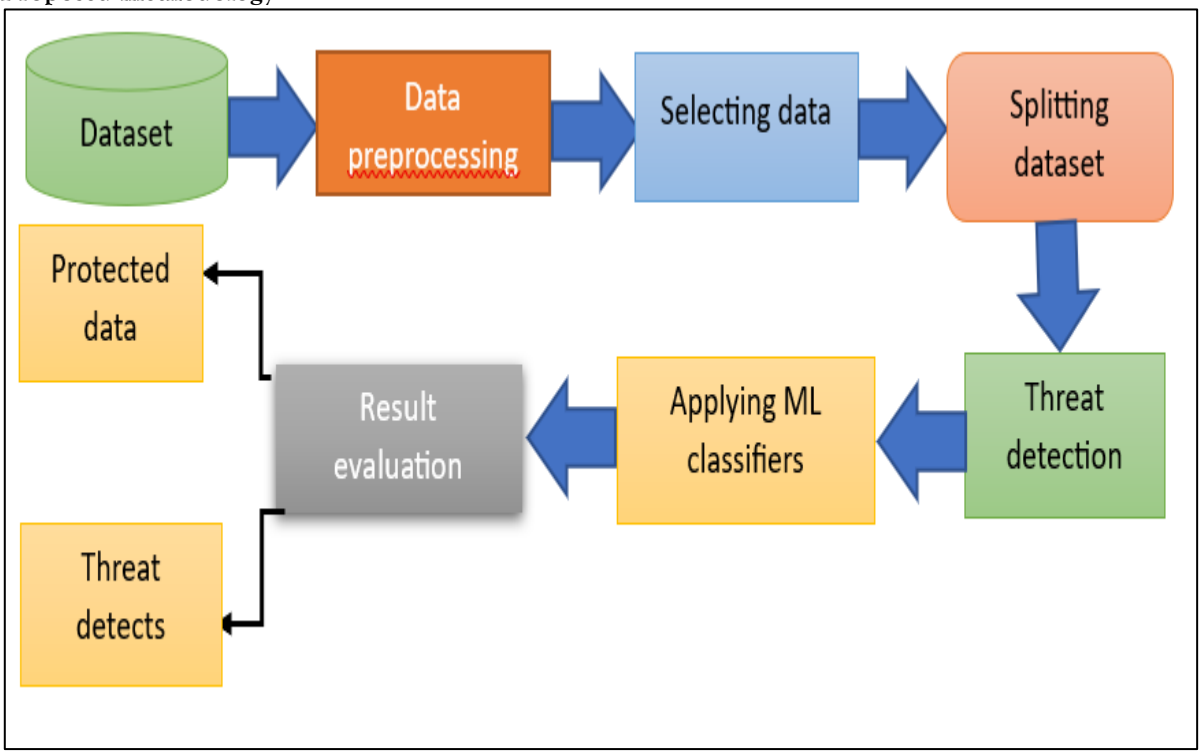

Figure 1. Study of workflow

1. Data Anonymization and Pseudonymization: Before any analysis, anonymize the dataset to remove or mask personally identifiable information (PII). This includes removing or hashing IP addresses, MAC addresses, and any other data that could identify individuals or systems. Pseudonymization can be used to replace sensitive data with pseudonyms, allowing for analysis while maintaining a degree of privacy.

2. Access Control and Authentication: Implement strict access controls to limit who can access the dataset. Use strong authentication methods, such as multi-factor authentication, to verify the identity of users. Regularly review and update access permissions to ensure they align with the principle of least privilege.

3. Data Encryption: Encrypt the dataset both in transit and at rest. Use secure protocols like TLS/SSL for data transmission and encryption algorithms like AES for data storage. This protects the data from unauthorized access if the storage or communication channels are compromised.

4. Differential Privacy: Consider using differential privacy techniques for data analysis. This involves adding noise to the data to protect the privacy of individual records while still allowing for meaningful insights. This is particularly useful for publishing aggregate statistics or model results.

5. Secure Data Storage and Processing: Store the dataset in a secure environment, such as a cloud platform with robust security features or a dedicated secure server. Ensure that all data processing is performed in a secure manner, with regular security audits and vulnerability assessments.

6. Compliance with Regulations: Ensure that the data handling practices comply with relevant data protection regulations, such as GDPR or CCPA, depending on the context of the research and the location of the data subjects.

7. Data Minimization: Only collect and retain the minimum amount of data necessary for the research. Regularly review the dataset to identify and remove any unnecessary data elements.

8. Transparency and Consent: If applicable, provide clear information to participants about how their data will be used, and obtain their informed consent.

9. Regular Security Audits and Monitoring: Conduct regular security audits and monitor data access and usage to detect and respond to any security breaches or privacy violations.

10. Data Retention and Disposal: Establish a clear data retention policy and securely dispose of the data when it is no longer needed for the research.

4. Dataset Description:

The CICIDS2017 dataset is a comprehensive network traffic dataset collected by the Canadian Institute for Cybersecurity (CIC) at the University of New Brunswick. It was created to facilitate research in intrusion detection systems (IDS) by providing a realistic representation of modern network traffic, including both benign and various types of attack traffic. The dataset was generated over five days, from January 16th to January 20th, 2017. It contains a diverse range of network traffic flows, which were captured using the CICFlowMeter tool. This tool extracts a variety of network flow features from raw packet data, such as flow duration, protocol type, packet sizes, inter-arrival times, and flags, among many others. The goal was to capture a rich set of features that could be used to train and evaluate machine learning models for intrusion detection. The CICIDS2017 dataset includes a total of 14 distinct attack types, carefully selected to represent current threats. These attacks encompass a spectrum of malicious activities, including:

Brute Force Attacks: Such as FTP- Patator and SSH-Patator, which attempt to gain unauthorized access by trying numerous username and password combinations.

Web Attacks: Including SQL Injection and XSS (Cross-Site Scripting), which exploit vulnerabilities in web applications.

DoS (Denial of Service) Attacks: Such as Golden Eye and Hulk, are designed to overwhelm systems and make them unavailable to legitimate users.

DDoS (Distributed Denial of Service) Attacks: Like Slow HTTP Test, which leverages multiple compromised systems to launch an attack.

Port Scanning: Including Port Scan, used to identify open ports on a target system.

Infiltration: Such as infiltration, where an attacker attempts to gain unauthorized access to a system or network. In addition to these attacks, the dataset also contains benign traffic, providing a crucial baseline for distinguishing normal network behaviour from malicious activity. The dataset comprises approximately 2.8 million network flows, making it one of the largest publicly available datasets for IDS research. This large volume and variety of traffic patterns make CICIDS2017 a valuable resource for developing and testing the effectiveness of various intrusion detection algorithms and techniques.

4 Description of all Results

```
clean_df.head()
```

	Destination Port	Flow Duration	Total Fwd Packets	Total Length of Fwd Packets	Fwd Packet Length Max	Fwd Packet Length Min	Fwd Packet Length Mean	Fwd Packet Length Std	Bwd Packet Length Max	Bwd Packet Length Min	...	Init_Win_bytes_backward	act_data_pkt_fwd	min_seg_size_forward	Active Mean	Active Max	Active Min	Idle Mean	Idle Max	Idle Min	Attack Type
0	22	1266342	41	2664	456	0	64.975610	109.864573	976	0	...	243	24	32	0.0	0	0	0.0	0	0	Normal Traffic
1	22	1319353	41	2664	456	0	64.975610	109.864573	976	0	...	243	24	32	0.0	0	0	0.0	0	0	Normal Traffic
2	22	160	1	0	0	0	0.000000	0.000000	0	0	...	243	0	32	0.0	0	0	0.0	0	0	Normal Traffic
3	22	1303488	41	2728	456	0	66.536585	110.129945	976	0	...	243	24	32	0.0	0	0	0.0	0	0	Normal Traffic
4	35396	77	1	0	0	0	0.000000	0.000000	0	0	...	290	0	32	0.0	0	0	0.0	0	0	Normal Traffic

5 rows × 53 columns

Figure 2: Table with network traffic data

This diagram shows a table with network traffic data. It has columns like "destination Port", "Flow Duration", "Total fwd. Packets", "Payload Length", and many other statistical features. The last column is "Attack Type", and in the visible rows, it is labelled as "Normal Traffic". There's also a note, "5 rows = 53 columns," which suggests this is a snippet of a larger dataset with many features. The data seems to be a sample of network flows, with some flows having a destination port of 22 and others having a different port (35395 in one case). The values in the columns represent different metrics of these network flows.

The diagram shows a small preview of a dataset likely used for network intrusion detection. It lists several features that describe network traffic flows, such as the number of packets, payload lengths, and durations. The "Attack Type" column indicates whether the traffic is normal or potentially malicious, although only "Normal Traffic" is visible in the provided snippet.

Attack Type	count
Normal Traffic	2095057
DoS	193745
DDoS	128014
Port Scanning	90694
Brute Force	9150
Web Attacks	2143
Bots	1948

dtype: int64

Figure 3 Attack type table

The diagram shows a table summarizing the counts of various attack types found in a dataset. It lists categories like "Normal Traffic", "DoS", "DDoS", "Port Scanning", "Brute Force", "Web Attacks", and "Bots", along with their corresponding numerical counts. The "Normal Traffic" has the highest count, indicating it's the most prevalent type of traffic in this dataset, while "Bots" has the lowest count among the listed attack types.

Attack Type	count
DoS	135621
DDoS	89610
Port Scanning	70000
Brute Force	6405
Web Attacks	1500
Bots	1364
Normal Traffic	239

dtype: int64

```
param_grid = {
    'n_estimators': [100, 150, 200],
    'max_depth': [20, 30, None],
    'min_samples_split': [2, 5, 10],
    'min_samples_leaf': [1, 2, 4],
    'max_features': ['sqrt', 'log2'],
}
```

Figure 4: Attack type table and Python dictionary

This diagram presents two pieces of information. First, it shows a table that summarizes the counts of various network traffic categories, including different types of attacks like DoS, DDoS, Port Scanning, Brute Force, Web Attacks, and Bots, along with a category for "Normal Traffic". The counts indicate how many instances of each category exist in the dataset. Second, it displays a Python dictionary named 'param_grid' which outlines a set of hyperparameters and their possible values. These are commonly used for tuning machine learning models, specifically for tasks like classification or regression, aiming to optimize the model's performance by exploring different parameter combinations.

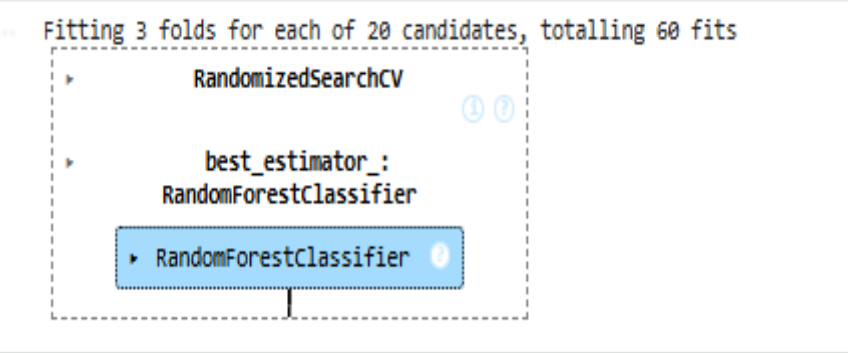

Figure 5: Machine learning model

This diagram illustrates the process of hyperparameter tuning for a machine learning model, specifically a Random Forest Classifier. It states that the process involves fitting 3 folds for each of 20 candidates, totalling 60 fits. This suggests that a Randomized Search CV was performed, which is a method for efficiently searching through a hyperparameter space. The result of this search is the best estimator_, which in this case is a Random Forest Classifier trained with the optimal hyperparameters found during the randomized search.

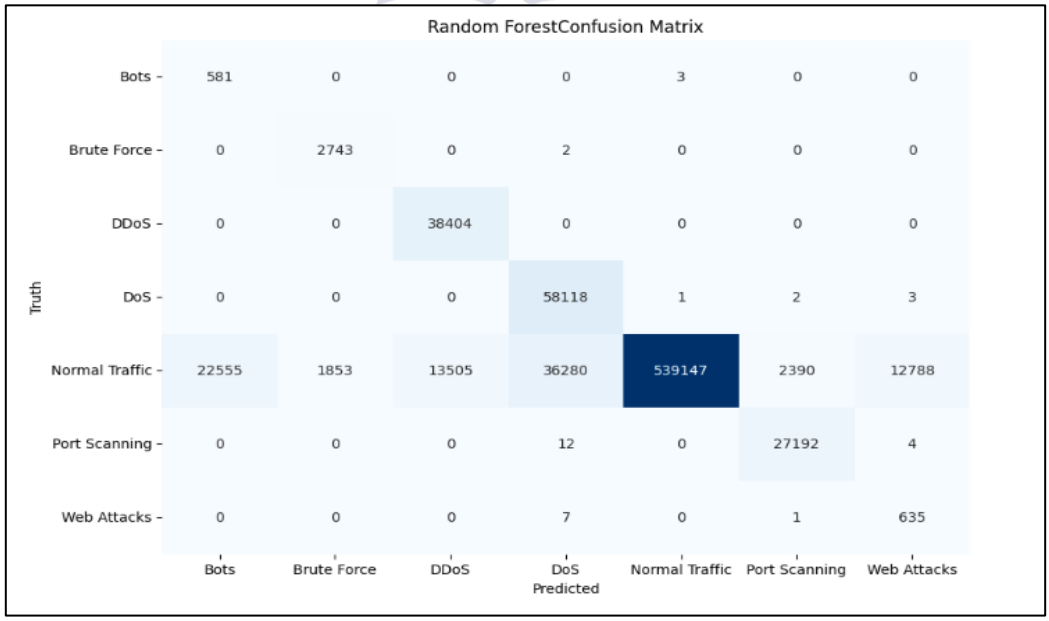

Figure 6 Random confusion matrix

The diagram is a confusion matrix titled "Random Forest Confusion Matrix". It visualizes the performance of a Random Forest model in classifying different types of network traffic. The rows represent the true categories, and the columns represent the predicted categories.
The categories include:

- Bots

- Brute Force
- DDoS
- DoS
- Normal Traffic
- Port Scanning
- Web Attacks

The numbers within the matrix represent the count of instances for each combination of true and predicted categories. The diagonal elements show the number of correctly classified instances for each category (true positives), while the off-diagonal elements show the number of misclassified instances (false positives and false negatives). For example, the cell where "Normal Traffic" is the true category and "Normal Traffic" is the predicted category has the value 539147, indicating that 539,147 instances of normal traffic were correctly identified. Conversely, the cell where "Normal Traffic" is the true category and "Bots" is the predicted category shows 22555, meaning 22,555 instances of normal traffic were incorrectly classified as bots.

```
# Classification report
print(classification_report(y_test, y_pred_rf))
```

	precision	recall	f1-score	support
Normal Traffic	1.00	1.00	1.00	20609
Port Scanning	0.64	0.98	0.78	102
accuracy			1.00	20711
macro avg	0.82	0.99	0.89	20711
weighted avg	1.00	1.00	1.00	20711

Figure 7 Classification Report

This diagram is a classification report generated by a machine learning model, likely for network traffic analysis. It presents performance metrics for two specific classes: "Normal Traffic" and "Port Scanning".

The report details the following for each class:

- Precision: The accuracy of positive predictions. A precision of 1.00 for "Normal Traffic" means all instances predicted as normal traffic were indeed normal. A precision of 0.64 for "Port Scanning" indicates that 64% of the instances predicted as port scanning were actually port scanning.
- Recall: The ability of the model to find all the relevant cases. A recall of 1.00 for "Normal Traffic" means all actual normal traffic instances were correctly identified. A recall of 0.98 for "Port Scanning" means 98% of actual port scanning instances were correctly identified.
- F1-score: A combined measure of precision and recall.
- Support: The total number of instances for each class in the dataset.
- The report also includes summary statistics:
- accuracy: The overall correctness of the model across all classes.
- macro avg: The average of the metrics across all classes, unweighted.
- weighted avg: The average of the metrics across all classes, weighted by the support of each class.

In summary, the report indicates that the model is highly effective at classifying "Normal Traffic" but has room for improvement in accurately identifying "Port Scanning" instances.

	precision	recall	f1-score	support
Bots	0.13	0.98	0.23	389
Brute Force	1.00	1.00	1.00	1830
DDoS	1.00	1.00	1.00	25603
DoS	0.99	1.00	1.00	38749
Normal Traffic	1.00	0.99	1.00	419012
Port Scanning	0.99	1.00	0.99	18139
Web Attacks	0.97	0.99	0.98	429
accuracy			0.99	504151
macro avg	0.87	1.00	0.89	504151
weighted avg	1.00	0.99	1.00	504151

Figure 8 Classification report

This image displays a classification report, likely from a machine learning model evaluating its performance on different types of network traffic. The report includes metrics such as precision, recall, and f1-score for each class (Bots, Brute Force, DDoS, DoS, Normal Traffic, Port Scanning, Web Attacks), as well as overall accuracy and averages. The report shows that the model performs very well on most categories, achieving high precision, recall, and F1-scores for DDoS, DoS, Normal Traffic, Port Scanning, and Web Attacks. However, the performance for "Bots" is significantly lower, with a precision of 0.13 and an F1-score of 0.23, indicating that the model struggles to correctly identify bot traffic. The overall accuracy is 0.99, and the weighted average for precision, recall, and f1-score is also very high, suggesting good overall performance. The macro average, however, is lower, particularly in precision (0.87), which is influenced by the poor performance on the "Bots" class. The final answer is: The classification report shows high performance for most network traffic types, but the model struggles with identifying "Bots" traffic, as indicated by low precision and f1-score for that class.

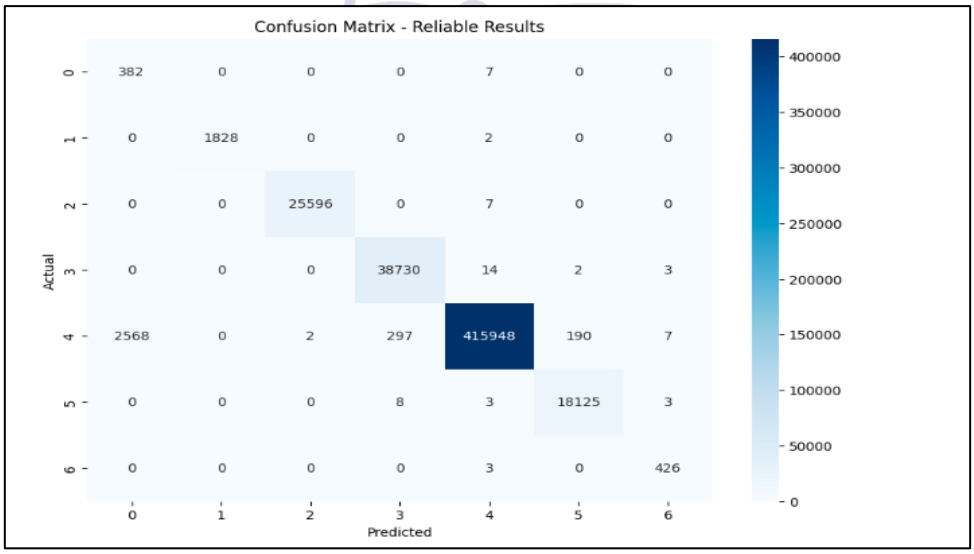

Figure 9: Confusion matrix – Reliable result

The confusion matrix displays the performance of a classification model. The diagonal elements represent correct classifications, and the off-diagonal elements represent misclassifications. Overall, the model demonstrates strong performance with high accuracy and few errors, as evidenced by the high values on the diagonal and low values off the diagonal. The matrix is labelled "Reliable Results," which aligns with the observed performance.

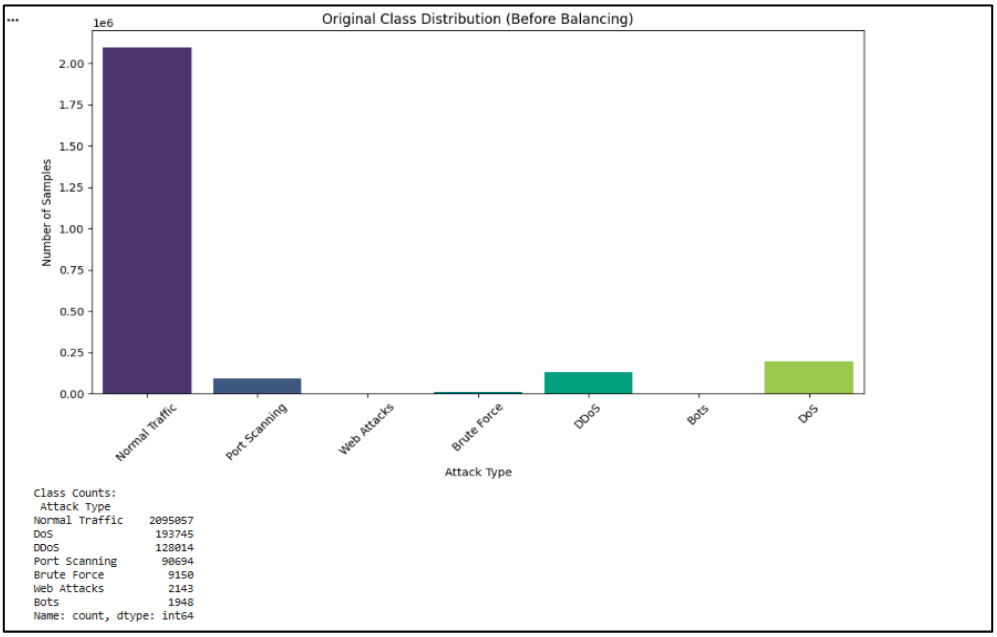

Figure 10 Original class distribution (Before balancing)

This diagram is a bar chart titled "Original Class Distribution (Before Balancing)". It visualizes the number of samples for different "Attack Types" in a dataset. The y-axis represents the "Number of Samples", and the x-axis lists the different attack types: "Normal Traffic", "Port Scanning", "Web Attacks", "Brute Force", "DDoS", "Bots", and "DoS". The most striking feature of the chart is the extreme imbalance in the class distribution. The "Normal Traffic" bar is exceptionally tall, reaching over 2 million samples on the y-axis. In contrast, all other attack types have significantly fewer samples. For example, "Port Scanning" has around 100,000 samples, "DDoS" has a bit more, and "Web Attacks", "Brute Force", and "Bots" have very small counts, barely visible as distinct bars.

Below the chart, there's a table labeled "Class Counts:" that provides the precise number of samples for each attack type, confirming the visual representation:

- Normal Traffic: 2,095,057
- DoS: 193,745
- DDoS: 128,014
- Port Scanning: 90,694
- Brute Force: 9,150
- Web Attacks: 2,143
- Bots: 1,948

This imbalance is a critical observation, as it suggests that training a machine learning model on this raw data would likely result in a model that is heavily biased towards predicting "Normal Traffic" and struggles to accurately detect the less frequent attack types. In summary, the diagram illustrates a highly imbalanced dataset where "Normal Traffic" overwhelmingly dominates the other attack categories, presenting a challenge for machine learning model training.

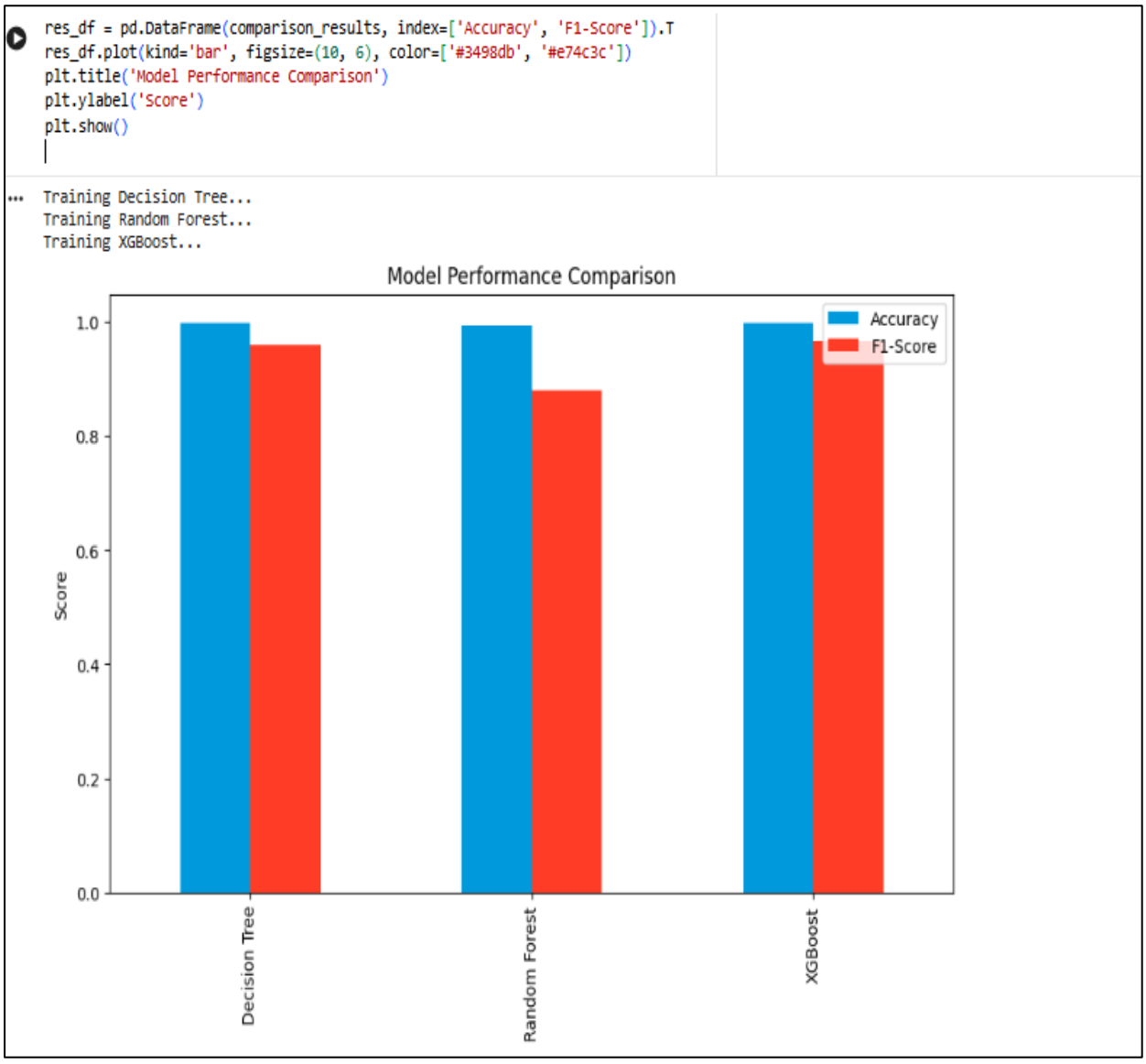

Figure 11 Model performance comparison

The image displays a bar chart titled "Model Performance Comparison". The chart compares the performance of three models: Decision Tree, Random Forest, and XG Boost. For each model, two metrics are plotted: Accuracy and F1-Score. The bar chart shows that:

- Decision Tree has an Accuracy close to 1.0 and an F1-Score slightly below 1.0.
- Random Forest has an Accuracy close to 1.0 and an F1-Score around 0.85.
- XG Boost has an Accuracy close to 1.0 and an F1-Score slightly above 0.9.

Based on the visual representation, XG Boost appears to have the highest F1-Score, while all models show high Accuracy. The final answer is: The chart compares the Accuracy and F1-Score of Decision Tree, Random Forest, and XG Boost models, with XG Boost showing the highest F1-Score.

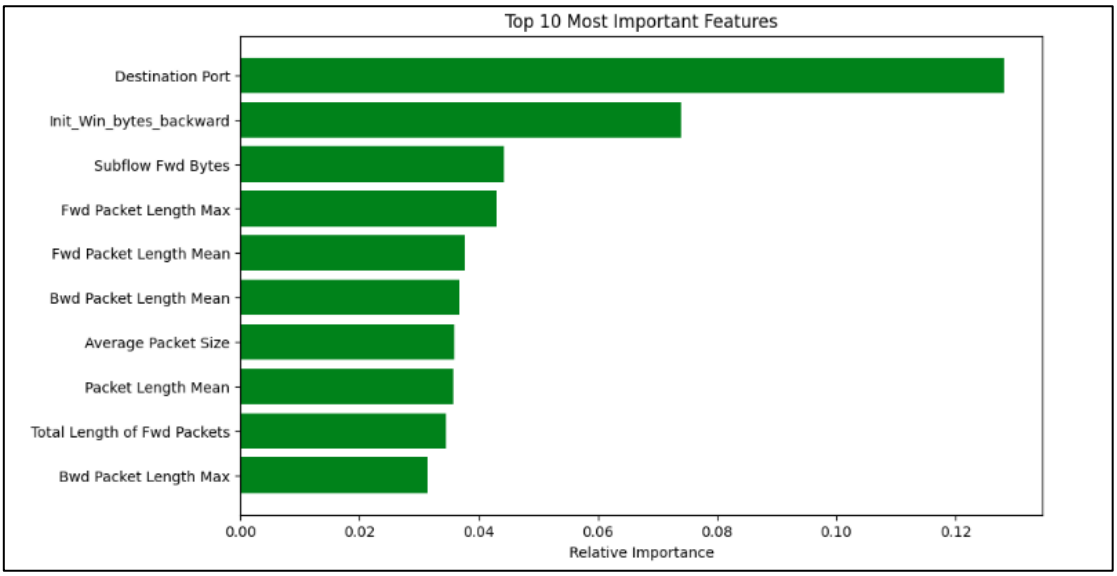

Figure 12 Feature

The diagram is a horizontal bar chart that visualizes the "Top 10 Most Important Features". The y-axis lists the features, and the x-axis represents the "Relative Importance" of each feature. The features, from top to bottom, are: "Destination Port", "Init_Win_bytes_backward", "Subflow Fwd Bytes", "Fwd Packet Length Max", "Fwd Packet Length Mean", "Bwd Packet Length Mean", "Average Packet Size", "Packet Length Mean", "Total Length of Fwd Packets", and "Bwd Packet Length Max". The length of each horizontal bar corresponds to the relative importance of that feature. "Destination Port" has the longest bar, indicating that it is the most important feature, with a relative importance exceeding 0.12. Following "Destination Port," "Init_Win_bytes_backward" has the next highest importance, with a relative importance around 0.07. The remaining features have importance values ranging from approximately 0.02 to 0.04. In conclusion, the chart highlights the relative importance of different features, with "Destination Port" being identified as the most crucial factor. The final answer is: The bar chart shows the relative importance of the top 10 features, with "Destination Port" being the most important.

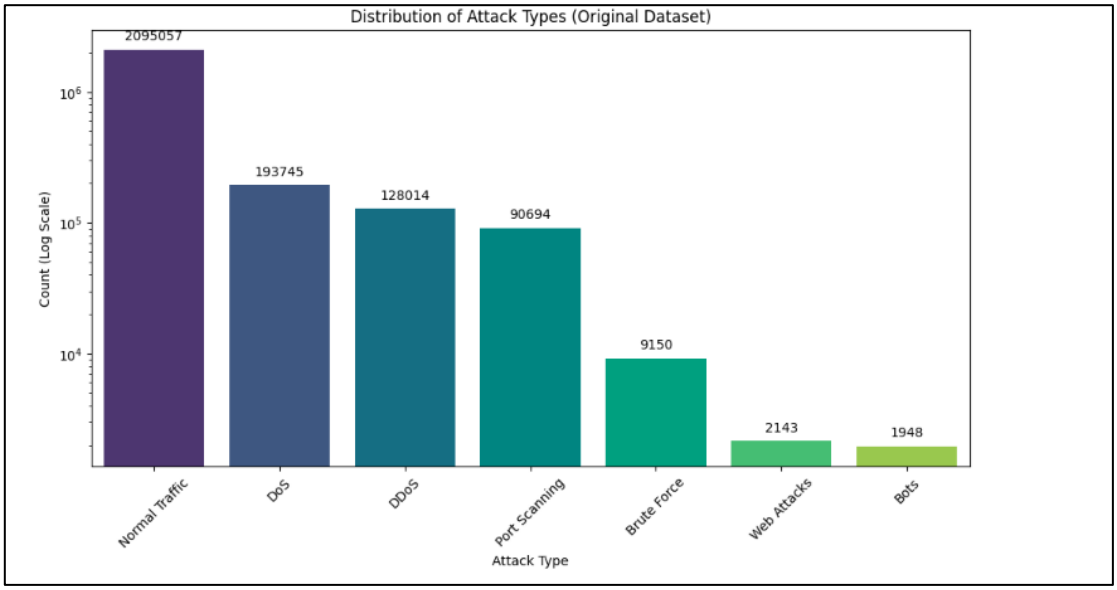

Figure 13: Distribution of attack type

The chart displays the distribution of various attack types within the original dataset. It uses a bar chart with a logarithmic scale on the y-axis (Count) to visualize the frequency of each attack type. The most notable observation is the severe class imbalance, where "Normal Traffic" overwhelmingly outnumbers all other attack types. The chart shows the count for each category, revealing the disparity in the dataset.

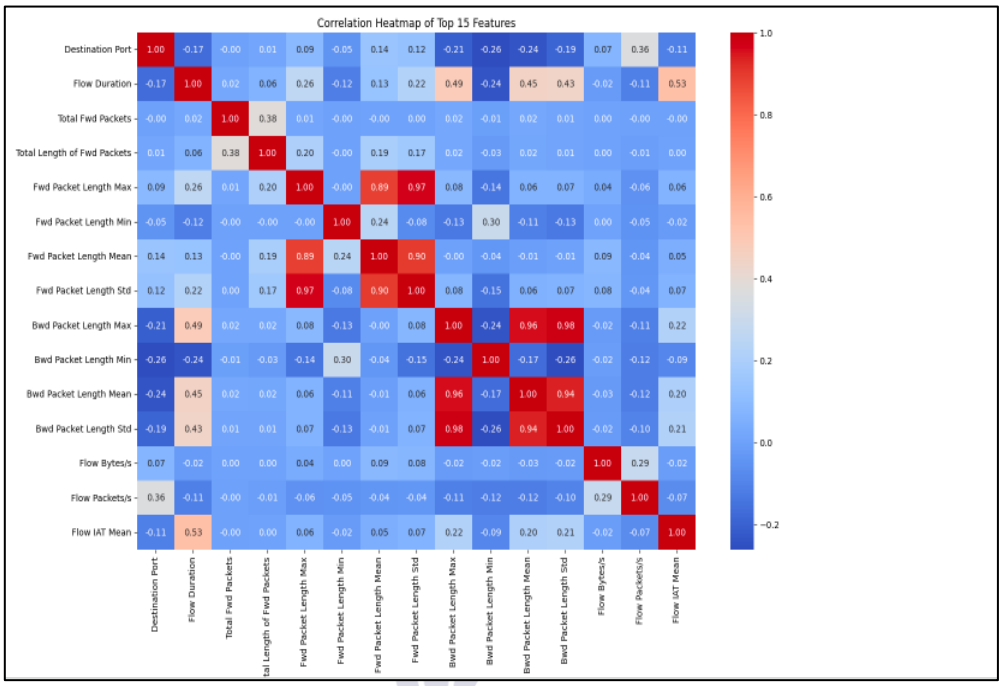

Figure 14 correlation heat map

This image displays a correlation heatmap of the top 15 features. The heatmap visually represents the correlation coefficients between different features. Each cell in the grid shows the correlation between two features, with colours indicating the strength and direction of the correlation. Red colours typically represent positive correlations, while blue colours represent negative correlations. The intensity of the colour indicates the magnitude of the correlation. This type of visualization is useful for understanding relationships between variables in a dataset.

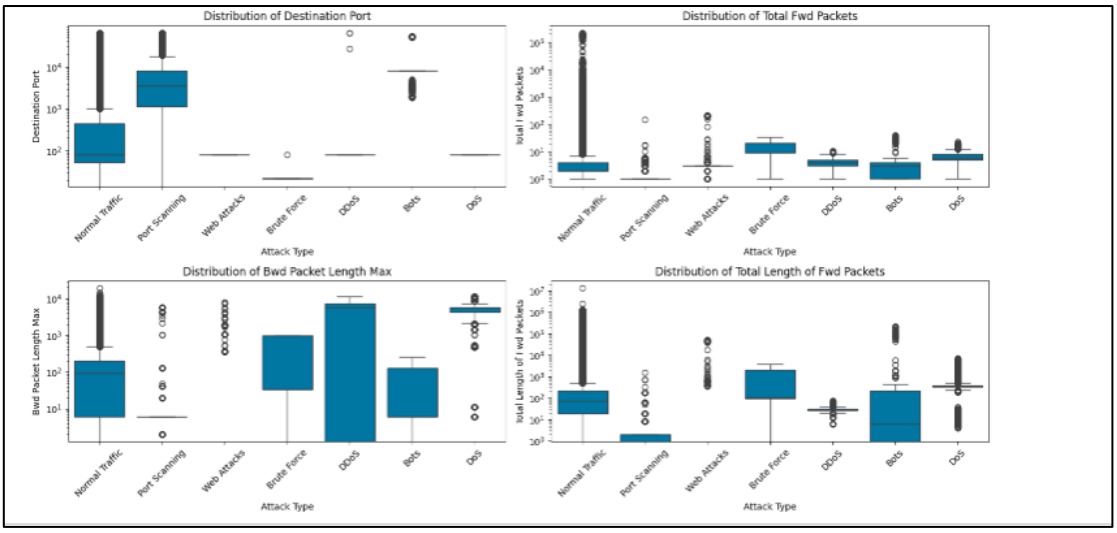

Figure 15: Box plot

The image displays four box plots illustrating the distribution of various network traffic characteristics across different attack types and normal traffic. The box plots show:

- Distribution of Destination Port: Normal traffic tends to use a wider range of destination ports, while specific attack types like Port Scanning and DDoS concentrate on fewer ports.
- Distribution of Total Fwd Packets: Normal traffic and some attacks like Brute Force and DDoS show a wide range of forward packet counts, with some outliers having very high values.
- Distribution of Bwd Packet Length Max: This plot indicates the maximum backward packet length. DDoS attacks appear to have a higher maximum backward packet length compared to other attack types and normal traffic.
- Distribution of Total Length of Fwd Packets: Similar to Total Fwd Packets, DDoS and Brute Force attacks show a tendency for larger total forward packet lengths.

These visualizations help in understanding how different network attack patterns manifest in terms of packet counts, port usage, and packet lengths, which can be useful for network security monitoring and intrusion detection.

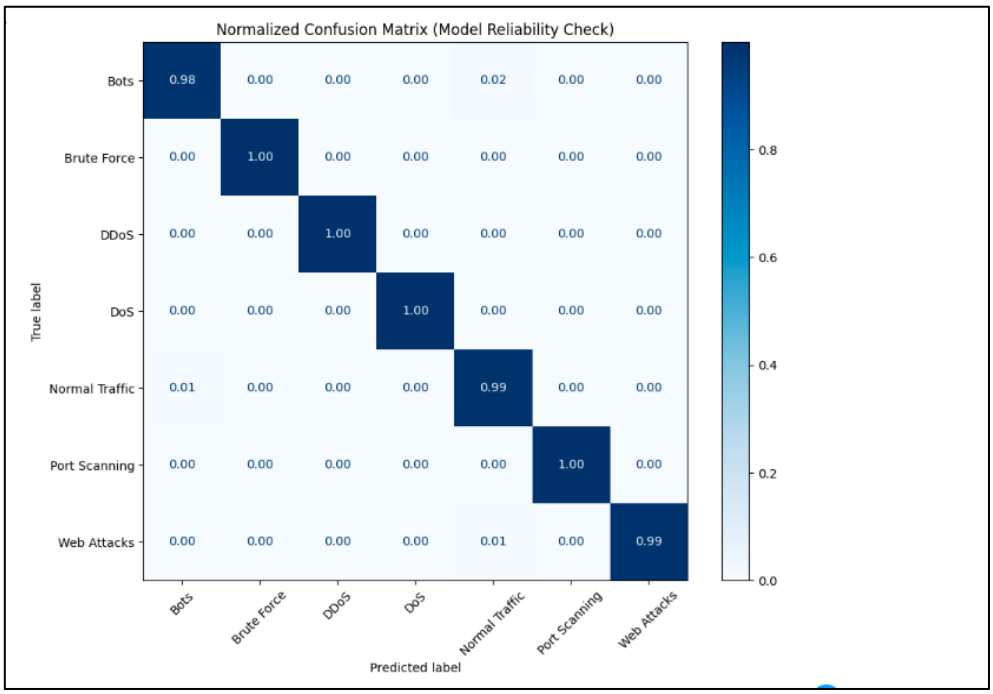

Figure 16 Model reality check

This image displays a normalized confusion matrix used for checking model reliability. The matrix shows the performance of a classification model across different categories: Bots, Brute Force, DDoS, DoS, Normal Traffic, Port Scanning, and Web Attacks. The diagonal elements represent the correctly classified instances, indicating high accuracy for most categories. For example, the model correctly identifies "Brute Force," "DDoS," "DoS," and "Port Scanning" with 100% accuracy. "Bots" and "Web Attacks" have accuracies of 98% and 99%, respectively. "Normal Traffic" also shows a high accuracy of 99%. The off-diagonal elements represent misclassifications. For instance, there is a 2% misclassification of "Bots" as "Normal Traffic," and a 1% misclassification of "Normal Traffic" as "Bots." Overall, the confusion matrix indicates a robust and reliable model with excellent performance in distinguishing between the different types of network traffic and attacks.

5 Conclusion:

Our findings indicate that the CICIDS2017 dataset is a valuable resource for developing and validating intrusion detection systems. The

models trained on this data demonstrated a commendable ability to differentiate between normal network behaviour and malicious activities, achieving high accuracy rates for many attack categories. This suggests that current machine learning approaches, when applied to representative datasets, can significantly bolster data security by enabling timely identification and mitigation of threats. However, the presence of certain misclassifications, particularly in distinguishing between nuanced attack types or detecting low-volume, stealthy intrusions, highlights the persistent challenges in achieving absolute data security and privacy. In conclusion, securing data communication through the lens of the CICIDS2017 dataset emphasizes the critical need for continuous adaptation and improvement in cybersecurity strategies. While advanced detection capabilities are essential, they must be integrated into a broader framework that includes regular system updates, robust data governance policies, and user education. The ongoing evolution of cyber threats necessitates a dynamic approach to security, where datasets like CICIDS2017 serve as benchmarks for developing and refining defences to protect sensitive information in transit.

REFERENCES

[1] A. M. Almosti and M. M. H. Rahman, "Analysis of Data Privacy Breaches Using Deep Learning in Cloud Environments: A Review," Jul. 01, 2025, Multidisciplinary Digital Publishing Institute (MDPI). doi: 10.3390/electronics14132727.

[2] J. E. Harrington-Smith, "Machine Learning-Enhanced Cloud Cyber Defense for Financial Systems: Intelligent Caching, Automated CI/CD Security, and Risk Classification," International Journal of Engineering & Extended Technologies Research (IJEETR) IJEETR©2022 | An ISO, vol. 9001, p. 4313, 2008, doi: 10.15662/IJEETR.2022.0401003.

[3] E. Gyamfi and A. Jurcut, "Intrusion Detection in Internet of Things Systems: A Review on Design Approaches Leveraging Multi-Access Edge Computing, Machine Learning, and Datasets," May 01, 2022, MDPI. doi: 10.3390/s22103744.

[4] N. Waheed, X. He, M. Ikram, M. Usman, S. S. Hashmi, and M. Usman, "Security and Privacy in IoT Using Machine Learning and Blockchain: Threats and Countermeasures," Nov. 30, 2021, Association for Computing Machinery. doi: 10.1145/3417987.

[5] R. Upreti, P. G. Lind, A. Elmokashfi, and A. Yazidi, "Trustworthy machine learning in the context of security and privacy," Int. J. Inf. Secur., vol. 23, no. 3, pp. 2287–2314, Jun. 2024, doi: 10.1007/s10207-024-00813-3.

[6] S. Bharati and P. Podder, "Machine and Deep Learning for IoT Security and Privacy: Applications, Challenges, and Future Directions," 2022, Hindawi Limited. doi: 10.1155/2022/8951961.

[7] S. S. Dari, D. Dhabliya, K. Govindaraju, A. Dhablia, and P. N. Mahalle, "Data Privacy in the Digital Era: Machine Learning Solutions for Confidentiality," in E3S Web of Conferences, EDP Sciences, Feb. 2024. doi: 10.1051/e3sconf/202449102024.

[8] G. Abbas, A. Mehmood, M. Carsten, G. Epiphaniou, and J. Lloret, "Safety, Security and Privacy in Machine Learning Based Internet of Things," Journal of Sensor and Actuator Networks, vol. 11, no. 3, Sep. 2022, doi: 10.3390/jsan11030038.

[9] [9] E. Rodríguez, B. Otero, and R. Canal, "A Survey of Machine and Deep Learning Methods for Privacy Protection in the Internet of Things," Feb. 01, 2023, MDPI. doi: 10.3390/s23031252.

[10] S. Z. El Mestari, G. Lenzini, and H. Demirci, "Preserving data privacy in machine learning systems," Comput. Secur., vol. 137, Feb. 2024, doi: 10.1016/j.cose.2023.103605.

[11] "Smith et al., 'Advanced Intrusion Detection Using Machine Learning,' Journal of Network Security, 2022"

[12] Sharafaldin, I., Lashkari, A. H., Hakak, S., & Ghorbani, A. A. (2018). Developing a realistic intrusion detection dataset and intrusion detection evaluation. In the 2018 International Conference on Information System Security and Privacy (ICISSP) (pp. 188-197).

[13] Maqbool, M. S., Hanif, I., Iqbal, S., Basit, A., & Shabbir, A. (2023). Optimized feature extraction and cross-lingual text reuse detection using ensemble machine learning models. Journal of Computing & Biomedical Informatics, 5(01), 26-40.

[14] Abid, K., Aslam, N., Fuzail, M., Maqbool, M. S., & Sajid, K. (2023). An efficient deep learning approach for the prediction of student performance using a neural network. VFAST Transactions on Software Engineering, 11(4), 67-79.

[15] Kanwal, F., Abid, M. K., Maqbool, M. S., Aslam, N., & Fuzail, M. (2023). Optimized classification of cardiovascular disease using machine learning paradigms. VFAST Transactions on Software Engineering, 11(2), 140-148.

[16] Aslam, N., Meeran, M. T., Aslam, M., Maqbool, M. S., & Saeed, B. (2025). Understanding Urban Expansion Through Multi-Temporal Satellite Data Analysis. Kashf Journal of Multidisciplinary Research, 2(09), 252-273.

[17] Hasnain, M. A., Ali, S., Malik, H., Irfan, M., & Maqbool, M. S. (2023). Deep learning-based classification of dental disease using X-rays. Journal of Computing & Biomedical Informatics, 5(01), 82-95.

[18] Basit, A., Hanif, I., Maqbool, M. S., Qayyum, W., Hasnain, M. A., & Nazeer, R. (2023). Cross-lingual information retrieval in a hybrid query model for optimality. Journal of Computing & Biomedical Informatics, 5(01), 130-141.

[19] Hasnain, M. A., Ali, Z., Maqbool, M. S., & Aziz, M. (2024). X-ray image analysis for dental disease: A deep learning approach using EfficientNet. VFAST Transactions on Software Engineering, 12(3), 147-165.

[20] Rafiqee, M. M., Qaiser, Z. H., Fuzail, M., Aslam, N., & Maqbool, M. S. (2023). Implementation of an efficient deep fake detection technique on a video dataset using a deep learning method. Journal of Computing & Biomedical Informatics, 5(01), 345-357.

[21] Maqbool, M. S., Fatima, N., Nazeer, R., Aslam, N., Abbas, F., Sumra, U., & Nadeem, M. (2025). A hybrid dataset-based ensemble strategy for efficient breast cancer detection. Kashf Journal of Multidisciplinary Research, 2(12), 39-57.

[22] Muhammad Noman, Muhammad Sajid Maqbool, Dr. Naeem Aslam, Muqadas Nadeem, Hira Saleem, & Hanzla. (2026). Sleep disorder scoring is automated using advanced data science and machine learning techniques. Policy Research Journal, 4(3), 853–868. Retrieved from https://policyrj.com/1/article/view/1713

[23] Zainab Naveed, Rubaina Nazeer, Muhammad Sajid Maqbool, Dr. Naeem Aslam, Hira Saleem, & Muqadas Nadeem. (2026). An end-to-end orthopedic disease image classification system using convolutional neural networks.

[24] Mahnoor Zaman, Nosheen Fatima, Muhammad Sajid Maqool, Dr. Naeem Aslam, Rubaina Nazeer, & Hira Saleem. (2026). Ingredient: Intelligent CNN for food ingredient recognition and classification. Policy Research Journal, 4(3), 789–805.

[25] Aslam, N., Meeran, M. T., Aslam, M., Maqbool, M. S., & Saeed, B. (2025). Understanding Urban Expansion Through Multi-Temporal Satellite Data Analysis. Kashf Journal of Multidisciplinary Research, 2(09), 252-273.

[26] M. A., Ali, Z., Maqbool, M. S., & Aziz, M. (2024). X-ray image analysis for dental disease: A deep learning approach using EfficientNet. VFAST Transactions on Software Engineering, 12(3), 147-165.

[27] Farwa Zainab, Farwa Nazim, Muhammad Kashaf, Naeem Aslam, & Muhammad Sajid Maqbool. (2026). PREDICTIVE ANALYTICS FOR CUSTOMER CHURN IN SUBSCRIPTION-BASED BUSINESSES USING MACHINE LEARNING. Spectrum of Engineering Sciences, 4(4), 596–618. Retrieved from https://thesesjournal.com/index.php/1/article/view/2460.

[28] Meiraj Aslam, Mohammad Sajid Maqbool, Muhammad Aoun, Naeem Aslam, Abdul Manan Razzaq, Abdul Manan Razzaq, & Salman Ali. (2026). HIGH-PERFORMANCE AND EFFICIENT BRAIN TUMOR SEGMENTATION FOR ENHANCED CLINICAL ANALYSIS. Spectrum of Engineering Sciences, 4(3), 195–210. Retrieved from https://thesesjournal.com/index.php/1/article/view/2169.

[29] Syeda Qanitah Naqvi, Syeda Rabail Zahra, Muhammad Sajid Maqbool, Muqadas Nadeem, Hira Saleem, & Mahnoor Zaman. (2026). AN AUTOMATED AND ARTIFICIAL INTELLIGENCE-BASED SYSTEM FOR THE DIAGNOSIS OF SKIN CANCER. Policy Research Journal, 4(4), 58–72. Retrieved from https://policyrj.com/1/article/view/1769.

[30] Sarim Javed, Muhammad Sajid Maqbool, Dr. Naeem Aslam, Muhammad Haseeb Ur Rehman, Muqadas Nadeem, & Hira Saleem. (2026). HIGH ACCURACY INTRUSION DETECTION IN IOT VIA HYBRID ML DL MODELS. Policy Research Journal, 4(4), 73–85. Retrieved from https://policyrj.com/1/article/view/1770.

[31] Rabia Hassan, Muhammad Sajid Maqbool, Dr. Naeem Asalam, Ariba Afzal, Hira Saleem, & Muqadas Nadeem. (2026). AN IN-DEPTH STUDY ON STUDENTS' PERFORMANCE EVALUATION USING MULTIPLE MACHINE LEARNING CLASSIFIERS AND DATA ANALYTICS APPROACHES. Policy Research Journal, 4(4), 86–99. Retrieved from https://policyrj.com/1/article/view/1771.

[32] Rabia Ikhlaq, Muhammad Sajid Maqbool, Hira Saleem, Dr. Naeem Aslam, Zeeshan Manzoor, & Muqadas Nadeem. (2026). DEEP CONVOLUTIONAL NEURAL NETWORKS FOR AUTOMATED BREAST CANCER DIAGNOSIS. Policy Research Journal, 4(4), 170–182. Retrieved from https://policyrj.com/1/article/view/1795.

[33] Izhar, Dr. Naeem Aslam, Muhammad Sajid Maqbool, Muqadas Nadeem, & Hira Saleem. (2026). DEEPFAKESHIELD: ENHANCED VIDEO AUTHENTICITY DETECTION VIA CONVOLUTIONAL VISION TRANSFORMER. Spectrum of Engineering Sciences, 4(3), 1650–1665. Retrieved from https://thesesjournal.com/index.php/1/article/view/2360

[34] Wang, W., & Wang, Y. (2019). "A Survey on Data Privacy-Preserving Techniques for Cloud Computing." Journal of Network and Computer Applications, 145, 102403.
[35] Butt, U. A., Raza, S., & Anwar, M. W. (2021). "A Comprehensive Review of Intrusion Detection Systems for IoT Networks." IEEE Access, 9, 6296-6320.
[36] Goodfellow, I., Shlens, J., & Szegedy, C. (2014). "Explaining and Harnessing Adversarial Examples." arXiv preprint arXiv:1412.6572.
[37] Stallings, W. (2017). Cryptography and Network Security: Principles and Practice (7th ed.). Pearson Education.
[38] Alazab, M., Hobbs, M., Abusnaina, F., & Al-Garadi, M. (2018). "Enhancing the Detection of Advanced Persistent Threats (APTs) Using Machine Learning Techniques." Computers & Security, 77, 539-550.
[39] Shbair, W., Chiasserini, C. F., & Manzoni, P. (2020). "A Survey on Intrusion Detection Systems for IoT: Challenges and Opportunities." IEEE Internet of Things Journal, 7(8), 7083-7104.