Securing the Internet of Medical Things: A Machine Learning Approach for Cyber Threat Detection

M. Agus Syamsul Arifin*, *Member, IAENG,* and A. Taqwa Martadinata, *Member, IAENG*

***Abstract*— The Internet of Things (IoT) has transformed various fields, including healthcare, through its branch known as the Internet of Medical Things (IoMT). IoMT enables remote healthcare systems and applications, providing critical and emergency healthcare services in urban areas and connecting isolated rural communities to healthcare. However, the interconnection of these critical devices is still needed to reduce costs effectively. To address this challenge, we propose an intelligent Intrusion Detection System (IDS) for IoMT networks, leveraging machine learning technology. We utilize and compare four classification algorithms to determine the best IDS model: Random Forest, Decision Tree, Gradient Boosting, and K-Nearest Neighbors. The performance of the IDS model is evaluated based on accuracy, precision, F1-Score, TPR, FPR, TNR, and FNR and validated using 10-fold cross-validation. Test results show that the IDS model using the Random Forest algorithm achieves the highest performance, with an accuracy of 99% on the test data.**

***Index Terms*—Internet of Medical Things (IoMT), Machine Learning, Intrusion Detection System (IDS), Cyber Threat**

I. INTRODUCTION

The Internet of Things (IoT) has revolutionized many fields, including healthcare, by introducing one of its branches, known as the Internet of Medical Things (IoMT). IoMT devices are projected to account for 40% of the IoT market [1]. Remote healthcare systems and applications are enabled through the Internet of Medical Things (IoMT), an automated system facilitating critical and emergency healthcare services in urban areas. Additionally, it connects isolated rural communities to various healthcare services [2], [3]. IoMT has emerged as a strategic priority for future e-healthcare due to its capability to enhance patient care and its potential to deliver more reliable clinical data [4]. IoMT systems allow the remote monitoring of patients with chronic diseases, thereby enabling timely diagnostics that can potentially save lives in emergencies [1], [5], [6], In addition to facilitating rapid medical responses, IoMT also reduces the cost of healthcare treatment [7], [8], [9]. However, the interconnectivity of critical devices within healthcare systems introduces new vulnerabilities [10], [11]. Apart from critical devices, IoMT also connects software applications within the healthcare systems [12], thus exposing various protocols to accommodate every service in the healthcare system.

Threats that can occur in the IoMT system include DoS (Denial of Service), DDoS (Distributed Denial of Service), spoofing [13], and data theft attacks. In cybersecurity, attackers aim to steal data and launch attacks that can disrupt data traffic and devices used in IoMT networks. This is because IoT/IoMT devices generally have limited computational resources [14], [15] presenting a security gap susceptible to disabling communication among devices in IoT/IoMT networks.

The Intrusion Detection System (IDS), a significant achievement in information security research, can identify an intrusion, whether it is presently occurring or has already taken place [16]. This research aims to propose solutions for addressing cyber threats within the IoMT system through a machine-learning approach. The dataset chosen for this study is the CICIoMT2024 [13] dataset, as it includes communication data from real devices within the IoMT network. This selection ensures that the developed Intrus will be more relevant and reliable in detecting threats to the IoMT network. The algorithms to be utilized and compared in this study include Decision Tree (DT), Random Forest (RF), Gradient Boosting (GB), and K-Nearest Neighbors (KNN). This research contributes in several ways:

- We are developing an optimal IDS model for threat detection in IoMT networks using a machine-learning approach.
- We provide a comparative analysis of the performance of various classification algorithms in machine learning to identify the most effective algorithms for integration into IDS models in IoMT networks. This includes an in-depth evaluation and comparison of algorithms such as Random Forest, Decision Tree, Gradient Boosting, and K-Nearest Neighbors to determine the most effective IDS model.

This paper is structured as follows: Section 2 presents the related work. Section 3 describes the design and methodology of this research. Sections 4 discuss the experimental results and provide an analysis. Finally, Section 5 concludes this research.

II. Related Work

A commonly utilized IoT protocol within the IoMT system is Message Queueing Telemetry Transport (MQTT) [17]. In this research, the dataset used also uses the MQTT

Manuscript received April 27, 2024; revised January 11, 2025. This research was supported by the Ministry of Education, Culture, Research, and Technology of the Republic of Indonesia through the National Competitive Research Program,

M. Agus Syamsul Arifin is a Senior Lecturer at the Universitas Bina Insan, Lubuklinggau, Indonesia (corresponding author to provide e-mail: mas.arifin@univbinsainsan.ac.id; mas.agus1988@gmail.com).

A. Taqwa Martadinata is Lecturer at the Universitas Bina Insan, Lubuklinggau, Indonesia. (e-mail: taqwa@univbinainsan.ac.id).

protocol. This protocol is widely adopted due to its subscriber/publisher model, which ensures lightweight messaging [10], [18], [19]. The MQTT protocol lacks integrated security, where messages are transmitted as plain text within data packets [20] making them vulnerable to potential cyber-attacks [21]. The integration of critical healthcare devices with IoT protocols has led to a progressively open communication system resulting in new and dangerous vulnerabilities. To address this challenge, a reliable Intrusion Detection System (IDS) is crucial. An effective approach to developing such a system is by leveraging machine learning techniques.

Machine learning is a potent technique for constructing an IDS model by utilizing datasets to train a model capable of detecting attacks on computer networks. Some research on the application of machine learning for IDS models in detecting cyber threats is conducted by Mas Arifin et al. [22], this research applies machine learning methods to detect malicious activities on SCADA networks using the IEC 60870-5-104 protocol. Research conducted by M. Hilda et al. [23] uses dual IDS which is built using gradient boosting and decision tree algorithms to detect threats in computer networks. In the IoT system, research conducted by K. Alissa et al. [24] utilized various machine learning algorithms to construct IDS models, including decision trees, an XGBoost model, and logistic regression, for detecting botnet malware attacks within devices on IoT networks.

TABLE I
COMPARISON WITH OTHER WORK

Ref & (year)	Method	Pros. And cons.
A. Binbusayyis et al. [12] (2022)	NB, DT, KNN, MLP, SVM	The IDS model created has good performance. However, this research does not utilize a dedicated dataset for IoMT networks, raising doubts about the reliability of the resulting IDS model.
P. Kulshrestha et al. [27] (2023)	MNB, LR, LRSGD, LSVC, DT, EVC, BG, RF, GBC, XGB, and ADB	This research compares many machine learning algorithms to find the best IDS model. The best IDS model is generated using the Adaptive Boosting algorithm. This research does not use the IoMT dataset in training the IDS model.
U. Zukaib et al. [28] (2024)	Meta-Learning	This paper presents the results of research using the meta-learning method to build IDS models with good results in detecting interference, the datasets used in this study are WUSTL-IIOT-2021, IoTID20 and WUSTL-EHMS-2020 these datasets are generated from general IoT devices and IoMT. However, the devices used in the IoMT dataset in this research paper have less diverse types and types of devices when compared to the dataset used by the author so that the diversity of data in the dataset in the author's research is more varied so that it will produce a more reliable IDS model because the media for training the IDS model has more varied data.
Z. Sun et al. [29] (2024)	PSO-AdaBoost	The IDS model created has good performance, However, this research uses the NSL KDD dataset to create an IDS model where this dataset contains general computer network data, not IoT or even IoMT networks.
Our Work (2024)	**RF, GB, DT, and KNN**	**The IDS model created has good performance, uses relevant datasets IoMT networks and provides multiclass classification.**

Several methods are employed to secure data and devices within the IoT system from cyber threats. Research conducted by A. Almogren et al. [25] uses Fuzzy to prevent Sybil attacks in IoMT networks. The research of R. Punithavathi et al. [26] used Crypto Hash to guarantee IoMT device data from ransomware attacks. Research conducted by A. Binbusayyis et al. [12] developed an IDS model using machine learning algorithms to detect threats in the IoMT network. They utilized the 2018 BoT-IoT dataset as training material for the IDS model. Research conducted by P. Kulshrestha et al. [27], U. Zukaib et al. [28], and Z. Sun et al. [29] utilize various machine learning algorithms to develop an IDS model for cyber threat detection, but these studies do not utilize IoMT datasets in constructing IDS models.

The IDSs do not perform well when the dataset used is not relevant, as the traffic characteristics between common computer networks and IoMT differ. Therefore, in this research, we will utilize relevant datasets to ensure that the IDS model constructed is reliable in detecting cyber threats in the IoMT network. In this study, we use a dataset that encompasses a broader variety of device types and data sources. This diversity contributes to the robustness of our IDS models, enabling them to generalize better across different IoMT scenarios and detect a wider range of intrusion activities. Table 1 presents previous research related to the application of machine learning for IDS and compares it with our study.

Unlike previous studies such as those by Binbusayis et al. (2022) and Kulshrestha et al. (2023), our research employs dedicated IoMT datasets. This ensures that our IDS models are trained and tested on data that accurately reflects the unique characteristics and challenges of IoMT environments, enhancing the reliability and applicability of our results. Our approach supports multiclass classification, which is a crucial feature for comprehensive intrusion detection. This capability allows for more granular and detailed identification of various intrusion types, as opposed to the binary classification often employed in other studies. Our IDS model's performance is validated empirically, demonstrating superior results in terms of detection accuracy and false alarm rates. This empirical validation underscores the practical viability of our proposed approach in real-world IoMT networks.

III. DESIGN AND METHOD

A. Proposed Method

In this research, we utilize the CICIoMT2024 dataset [13], which is designed to realistically represent IoMT devices. This dataset includes 18 attack scenarios involving 40 IoMT devices, comprising 25 physical devices and 15 simulated devices. Figure 1 shows the proposed method to find the best algorithm for the IDS model.

After preprocessing, this dataset consists of 19 classes, namely: *benign, arp_spoofing, ddos_mqtt_connect, ddos_mqtt_publish, dos_mqtt_connect, dos_mqtt_publish, malformed_mqtt, os_scan, ping_sweep, port_scan, vul_scan, ddos_icmp, ddos_syn, ddos_tcp, ddos_udp, dos_icmp, dos_syn, dos_tcp, and dos_udp*. With a more extensive range of classes, the IDS model will be more precise in detecting cyber threats on IoMT networks.

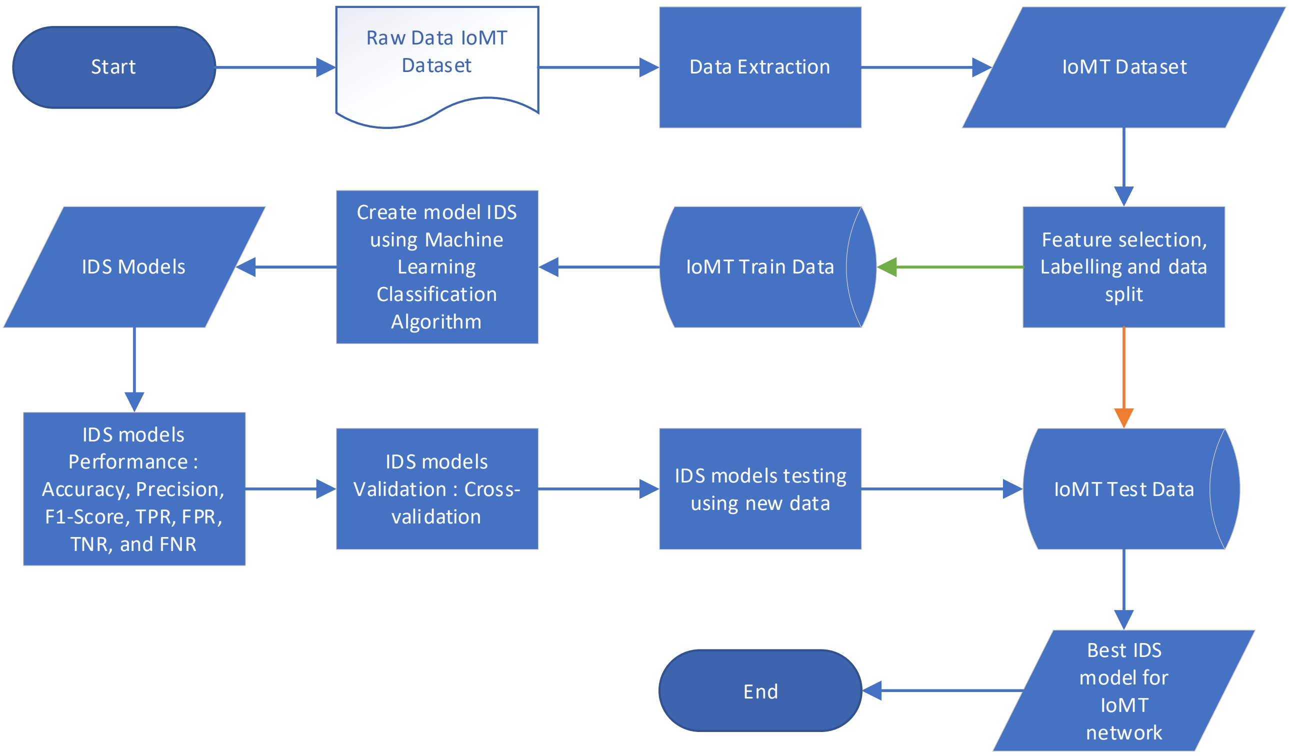

Fig. 1. Proposed method to find the best algorithm for the IDS model in this study

Then we divided the dataset into training data and test data, with the training data amounting to 7,160,831 (85%) samples and the test data amounting to 1,254,521 (15%) samples. The training data was used to train the IDS model with various predefined algorithms, measure performance, and perform validation. This split ensures a sufficient amount of data for training and validation, supporting the robustness of the evaluation process. The trained IDS model was then tested to assess its capability to detect cyber threats using the test data.

B. Classifier Algorithm

This research employs 4 classification algorithms and compares them to determine the best algorithm for creating an IDS model. The algorithms used are Decision tree (DT), Random forest (RF), Gradient boosting (GB), and K-nearest neighbors (KNN). The classification algorithms used in this research are commonly employed to model IDS for detecting cyber threats in the network.

The research conducted by N. Oliveira et al. [30] used a Random forest algorithm to detect anomalies with an intelligent IDS model on computer networks. A study conducted by D. Upadhyay et al. [31] utilized a gradient-boosting algorithm for feature selection to be used in constructed an IDS model for a smart grid network. L. Ahakonye et al. [32] in their research used decision trees combined with chi-square to build an IDS model to detect cyber threats in Industrial Internet of Things (IIoT) networks. G. Liu et al. [33] in their research used the KNN algorithm to improve the ability of the IDS model to detect attacks on wireless sensor networks (WSN).

C. IDS model Performance and Validation

To measure the performance of the IDS model, we use the accuracy, precision, and F-measure (F1-Score) values. The confusion matrix is represented as true positive (TP), true negative (TN), false positive (FP), and false negative (FN). We also measured the True Positive Rate (TPR), False Positive Rate (FPR), False Negative Rate (FNR), and True Negative Rate TNR) values. These metrics provide a detailed understanding of the IDS model's strengths and weaknesses, allowing for targeted improvements and optimizations. By thoroughly evaluating these performance indicators, we ensure that our IDS model not only detects intrusions effectively but also minimizes false alarms, thereby enhancing its practical applicability in real-world IoMT environments. The performance metrics are determined by Equations (1)–(8).

$$\text{Accuracy} = \frac{(TN+TP)}{(TN+TP+FN+FP)} \tag{1}$$

$$\text{Precision} = \frac{TP}{(TP+FP)} \tag{2}$$

$$\text{F1 Measure} = 2\frac{(\text{Precision x Recall})}{(Precision + Recall)} \tag{3}$$

$$\text{TPR} = \frac{TP}{(TP+FN)} \tag{4}$$

$$\text{FPR} = \frac{FP}{(FP+TN)} \tag{5}$$

$$\text{FNR} = \frac{FN}{(FN+TP)} \tag{6}$$

$$\text{TNR} = \frac{TN}{(TN+FP)} \tag{7}$$

This rigorous performance evaluation underscores the robustness and reliability of our proposed IDS model, setting a benchmark for future research in securing IoMT networks. Our comprehensive approach, detailed metric analysis, and advanced machine learning techniques collectively contribute to the development of a highly effective intrusion detection system tailored to the unique challenges of IoMT cybersecurity.

We use cross-validation to validate the created IDS model and detect overfitting. Cross-validation is commonly employed in IDS research using machine learning, as seen in the research by [34] and [35]. In this study, we used 10-fold to validate that the IDS model is not overfitting [36]. Cross-validation will randomize the samples for each repetition with the same relative to the number of subsets [37].

IV. Result and Analysis

In this section, we will discuss the performance and validation results of the IDS model and then test the IDS model using test data that is different from the training data and compare each algorithm used to create the IDS model.

A. Performance of the IDS Model

We measured the performance of each algorithm used to model the IDS. As mentioned in the previous section, during the preprocessing process, we split the dataset into training data and testing data. Figure 2 and Figure 3 below show the number of classes in the dataset used in this study. These figures provide a visual representation of the distribution of normal data and various types of attacks within the dataset. Understanding the class distribution is crucial for assessing the effectiveness of the IDS model, as it highlights the potential challenges in detecting minority class instances, which often correspond to more sophisticated or less frequent attack types.

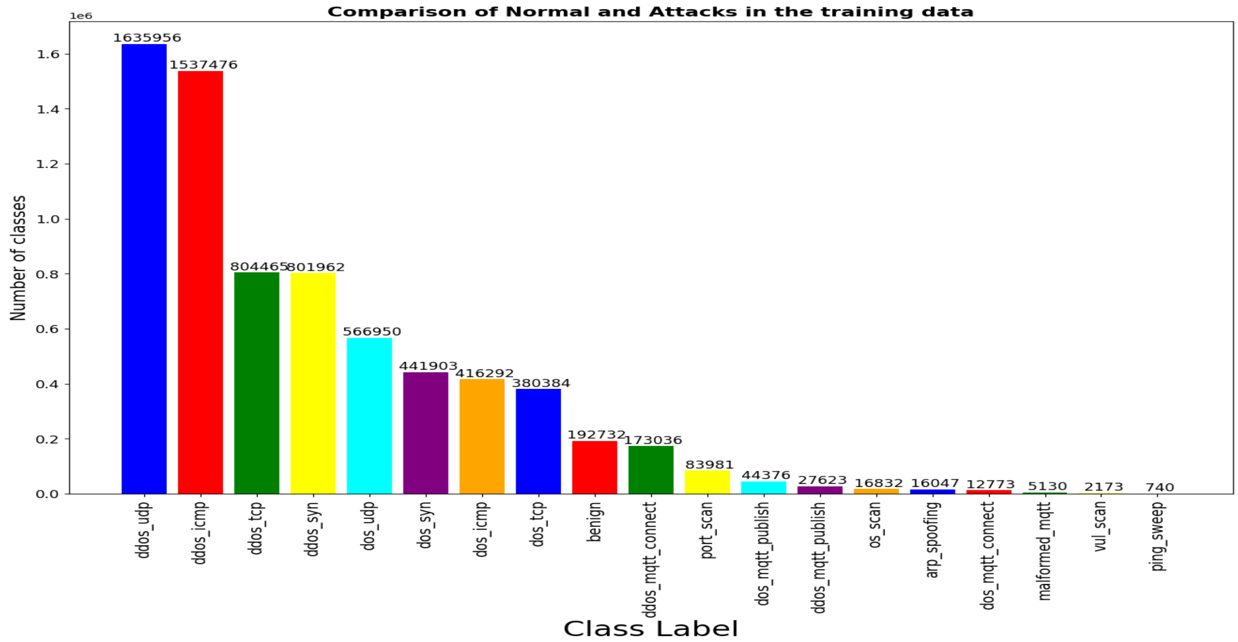

Fig. 2. Comparison of normal data and attacks in the training data

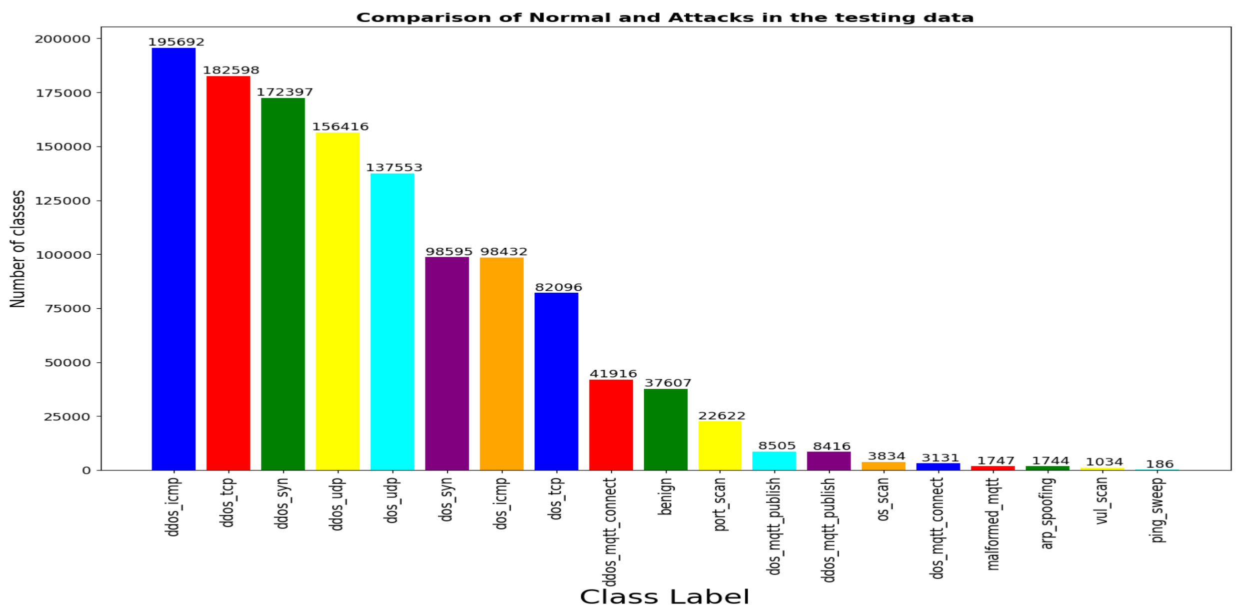

Fig. 3. Comparison of normal data and attacks in the test data

IDS model performance measurement is carried out to see the model's ability to detect cyber threats in the IoMT network. In the results obtained, the accuracy of each IDS model created with each algorithm used in this study shows good performance. Table 2 shows the IDS model accuracy comparison for each algorithm for training data. This comparison highlights the effectiveness of different machine learning techniques in identifying potential intrusions within the network.

TABLE II
IDS MODEL ACCURACY COMPARISON FOR EACH ALGORITHM ON TRAINING DATA

Classifier	Accuracy
Random Forest (RF)	99,8%
Decision Tree (DT)	100%
Gradient Boosting (GB)	99,3%
K Nearest Neighbors (KNN)	99,1%

The high accuracy rates across various algorithms indicate that the models are well-tuned and capable of discerning between normal and malicious activities with a high degree of precision. This is critical for the practical deployment of IDS in IoMT environments, where the timely and accurate detection of threats is paramount.

Table 3 shows the IDS model performance using the Random Forest algorithm, while Table 4 shows the IDS model performance using the Decision tree for training data. Table 5 shows the IDS model performance using the Gradient Boosting algorithm, while Table 6 shows the IDS model performance using K-Nearest neighbors for training data. These tables provide a detailed comparative analysis of how each algorithm performs in terms of detecting intrusions within the IoMT network.

TABLE III
IDS MODEL PERFORMACE USING RANDOM FOREST ALGORITHM ON TRAINING DATA

Class	Precision	F1-Score	TPR	FPR	FNR	TNR
benign	1.00	1.00	1.00	0.00	0.00	1.00
arp_spoofing	1.00	1.00	1.00	0.00	0.00	1.00
ddos_mqtt_connect	1.00	1.00	1.00	0.00	0.00	1.00
ddos_mqtt_publish	1.00	1.00	1.00	0.00	0.00	1.00
dos_mqtt_connect	1.00	1.00	1.00	0.00	0.00	1.00
dos_mqtt_publish	1.00	1.00	1.00	0.00	0.00	1.00
malformed_mqtt	1.00	1.00	1.00	0.00	0.00	1.00
os_scan	1.00	1.00	1.00	0.00	0.00	1.00
ping_sweep	1.00	1.00	1.00	0.00	0.00	1.00
port_scan	1.00	1.00	1.00	0.00	0.00	1.00
vul_scan	1.00	1.00	1.00	0.00	0.00	1.00
ddos_icmp	1.00	1.00	1.00	0.00	0.00	1.00
ddos_syn	1.00	1.00	1.00	0.00	0.00	1.00
ddos_tcp	1.00	1.00	1.00	0.00	0.00	1.00
ddos_udp	1.00	1.00	1.00	0.00	0.00	1.00
dos_icmp	1.00	1.00	1.00	0.00	0.00	1.00
dos_syn	1.00	1.00	1.00	0.00	0.00	1.00
dos_tcp	1.00	1.00	1.00	0.00	0.00	1.00
dos_udp	1.00	1.00	1.00	0.00	0.00	1.00

TABLE IV
IDS MODEL PERFORMACE USING DECISION TREE ALGORITHM ON TRAINING DATA

Class	Precision	F1-Score	TPR	FPR	FNR	TNR
benign	1.00	1.00	1.00	0.00	0.00	1.00
arp_spoofing	1.00	1.00	1.00	0.00	0.00	1.00
ddos_mqtt_connect	1.00	1.00	1.00	0.00	0.00	1.00
ddos_mqtt_publish	1.00	1.00	1.00	0.00	0.00	1.00
dos_mqtt_connect	1.00	1.00	1.00	0.00	0.00	1.00
dos_mqtt_publish	1.00	1.00	1.00	0.00	0.00	1.00
malformed_mqtt	1.00	1.00	1.00	0.00	0.00	1.00
os_scan	1.00	1.00	1.00	0.00	0.00	1.00
ping_sweep	1.00	1.00	1.00	0.00	0.00	1.00
port_scan	1.00	1.00	1.00	0.00	0.00	1.00
vul_scan	1.00	1.00	1.00	0.00	0.00	1.00
ddos_icmp	1.00	1.00	1.00	0.00	0.00	1.00
ddos_syn	1.00	1.00	1.00	0.00	0.00	1.00
ddos_tcp	1.00	1.00	1.00	0.00	0.00	1.00
ddos_udp	1.00	1.00	1.00	0.00	0.00	1.00
dos_icmp	1.00	1.00	1.00	0.00	0.00	1.00
dos_syn	1.00	1.00	1.00	0.00	0.00	1.00
dos_tcp	1.00	1.00	1.00	0.00	0.00	1.00
dos_udp	1.00	1.00	1.00	0.00	0.00	1.00

TABLE V
IDS MODEL PERFORMACE USING GRADIENT BOOSTING ALGORITHM ON TRAINING DATA

Class	Precision	F1-Score	TPR	FPR	FNR	TNR
benign	0.97	0.98	0.98	0.00	0.02	0.99
arp_spoofing	0.80	0.79	0.78	0.00	0.22	0.99
ddos_mqtt_connect	1.00	1.00	1.00	0.00	0.00	1.00
ddos_mqtt_publish	1.00	1.00	1.00	0.00	0.00	1.00
dos_mqtt_connect	1.00	1.00	1.00	0.00	0.00	1.00
dos_mqtt_publish	0.99	1.00	1.00	0.00	0.00	1.00
malformed_mqtt	0.85	0.80	0.76	0.00	0.24	0.99
os_scan	0.87	0.68	0.55	0.00	0.45	0.99
ping_sweep	0.68	0.47	0.35	0.00	0.65	0.99
port_scan	0.91	0.94	0.94	0.00	0.04	0.99
vul_scan	0.67	0.56	0.48	0.00	0.52	0.99
ddos_icmp	1.00	1.00	1.00	0.00	0.00	1.00
ddos_syn	1.00	1.00	1.00	0.00	0.00	1.00
ddos_tcp	1.00	1.00	1.00	0.00	0.00	1.00
ddos_udp	1.00	1.00	1.00	0.00	0.00	1.00
dos_icmp	1.00	1.00	1.00	0.00	0.00	1.00
dos_syn	1.00	1.00	1.00	0.00	0.00	1.00
dos_tcp	1.00	1.00	1.00	0.00	0.00	1.00
dos_udp	1.00	1.00	1.00	0.00	0.00	1.00

TABLE VI
IDS MODEL PERFORMACE USING K-NEAREST NEIGHBORS ALGORITHM ON TRAINING DATA

Class	Precision	F1-Score	TPR	FPR	FNR	TNR
benign	1.00	1.00	1.00	0.00	0.00	1.00
arp_spoofing	1.00	1.00	1.00	0.00	0.00	1.00
ddos_mqtt_connect	1.00	1.00	1.00	0.00	0.00	1.00
ddos_mqtt_publish	1.00	1.00	1.00	0.00	0.00	1.00
dos_mqtt_connect	1.00	1.00	1.00	0.00	0.00	1.00
dos_mqtt_publish	1.00	1.00	1.00	0.00	0.00	1.00
malformed_mqtt	1.00	1.00	1.00	0.00	0.00	1.00
os_scan	1.00	1.00	1.00	0.00	0.00	1.00
ping_sweep	1.00	1.00	1.00	0.00	0.00	1.00
port_scan	1.00	1.00	1.00	0.00	0.00	1.00
vul_scan	1.00	1.00	1.00	0.00	0.00	1.00
ddos_icmp	1.00	1.00	1.00	0.00	0.00	1.00
ddos_syn	1.00	1.00	1.00	0.00	0.00	1.00
ddos_tcp	1.00	1.00	1.00	0.00	0.00	1.00
ddos_udp	1.00	1.00	1.00	0.00	0.00	1.00
dos_icmp	1.00	1.00	1.00	0.00	0.00	1.00
dos_syn	1.00	1.00	1.00	0.00	0.00	1.00
dos_tcp	1.00	1.00	1.00	0.00	0.00	1.00
dos_udp	1.00	1.00	1.00	0.00	0.00	1.00

Based on the performance results of the IDS (Intrusion Detection System) model evaluated on the training data using various algorithms the Random Forest algorithm demonstrates perfect performance across all classes with Precision, F1-Score, TPR (True Positive Rate), FPR (False Positive Rate), FNR (False Negative Rate), and TNR (True Negative Rate) all achieving values of 1.00 or 100%. This indicates that the model accurately detects all types of attacks and benign data without any errors. Similar to Random Forest, the Decision Tree algorithm also exhibits perfect performance across all classes with Precision, F1-Score, TPR, FPR, FNR, and TNR all scoring 1.00. This demonstrates that the model is highly effective in identifying all types of attacks and benign data.

For the Gradient Boosting algorithm, the model performance varies slightly among the classes. Several classes such as benign, ddos_mqtt_connect, ddos_mqtt_publish, dos_mqtt_connect, dos_mqtt_publish, ddos_icmp, ddos_syn, ddos_tcp, ddos_udp, dos_icmp, dos_syn, dos_tcp, and dos_udp maintain perfect performance. However, some classes like arp_spoofing, malformed_mqtt, os_scan, ping_sweep, and vul_scan show variations with lower Precision, and F1-Score values, indicating some detection errors. The K-Nearest Neighbors algorithm demonstrates perfect performance across all classes with Precision, F1-Score, TPR, FPR, FNR, and TNR all achieving values of 1.00. This indicates that the model is also highly effective in detecting all types of attacks and benign data. Overall, the IDS model exhibits excellent performance on the training data with minor variations observed in the Gradient Boosting algorithm. The Random Forest, Decision Tree, and K-Nearest Neighbors algorithms show perfect performance across all classes.

The performance of each model trained using the training data in this study is shown in the confusion matrix. Figure 4 presents the confusion matrix for the Random Forest algorithm, illustrating its ability to correctly classify normal and attack data points. Figures 5 and 6 display the confusion matrices for the Decision Tree and Gradient Boosting algorithms, respectively, highlighting their classification performance and the distribution of true positives, true negatives, false positives, and false negatives. Figure 7 shows the confusion matrix results for the K-Nearest Neighbors algorithm, further detailing its effectiveness in distinguishing between normal and attack data.

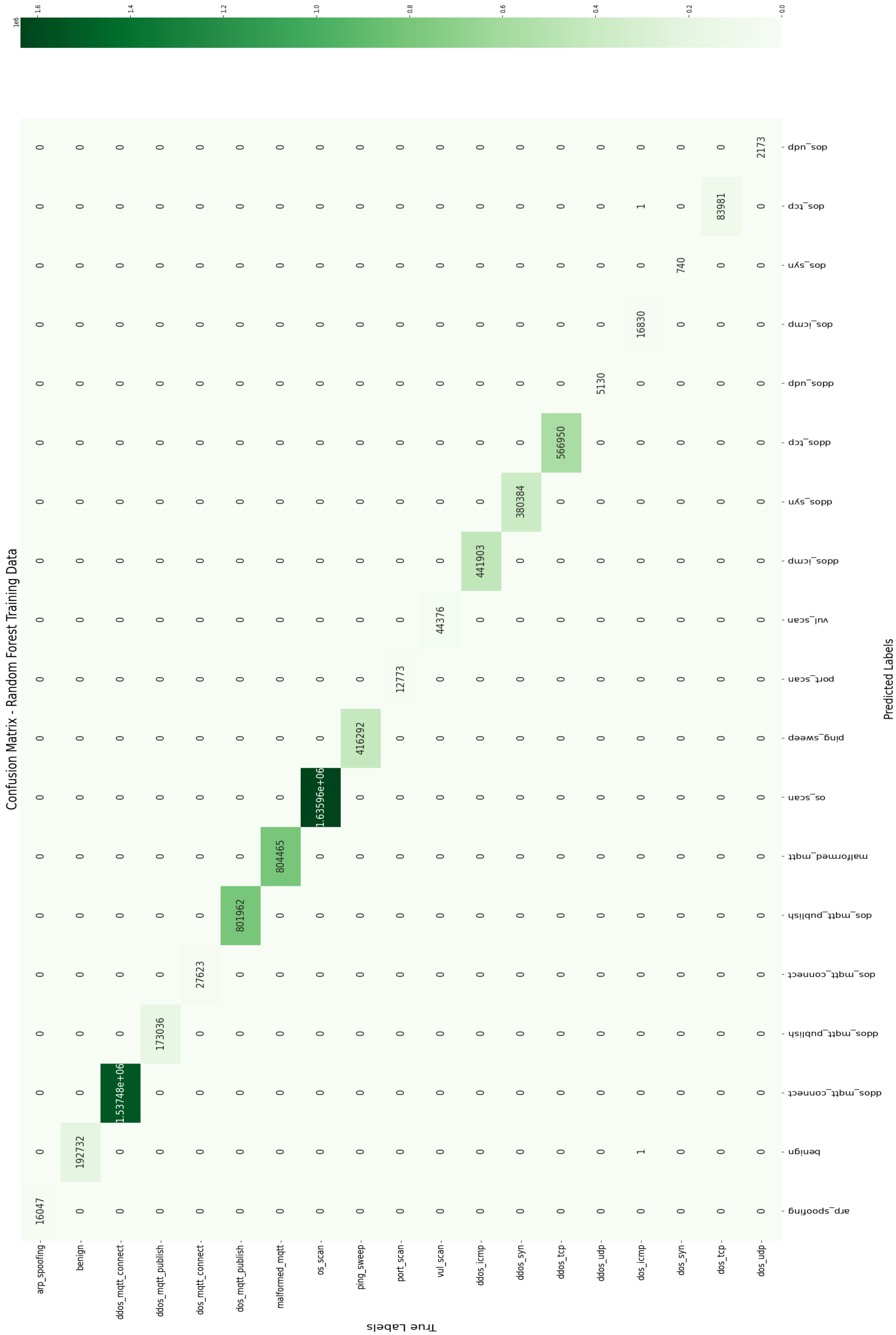

Fig. 4. Confusion Matrix for Random Forest Algorithm on Training Data

Fig. 5. Confusion Matrix for Decision Tree Algorithm on Training Data

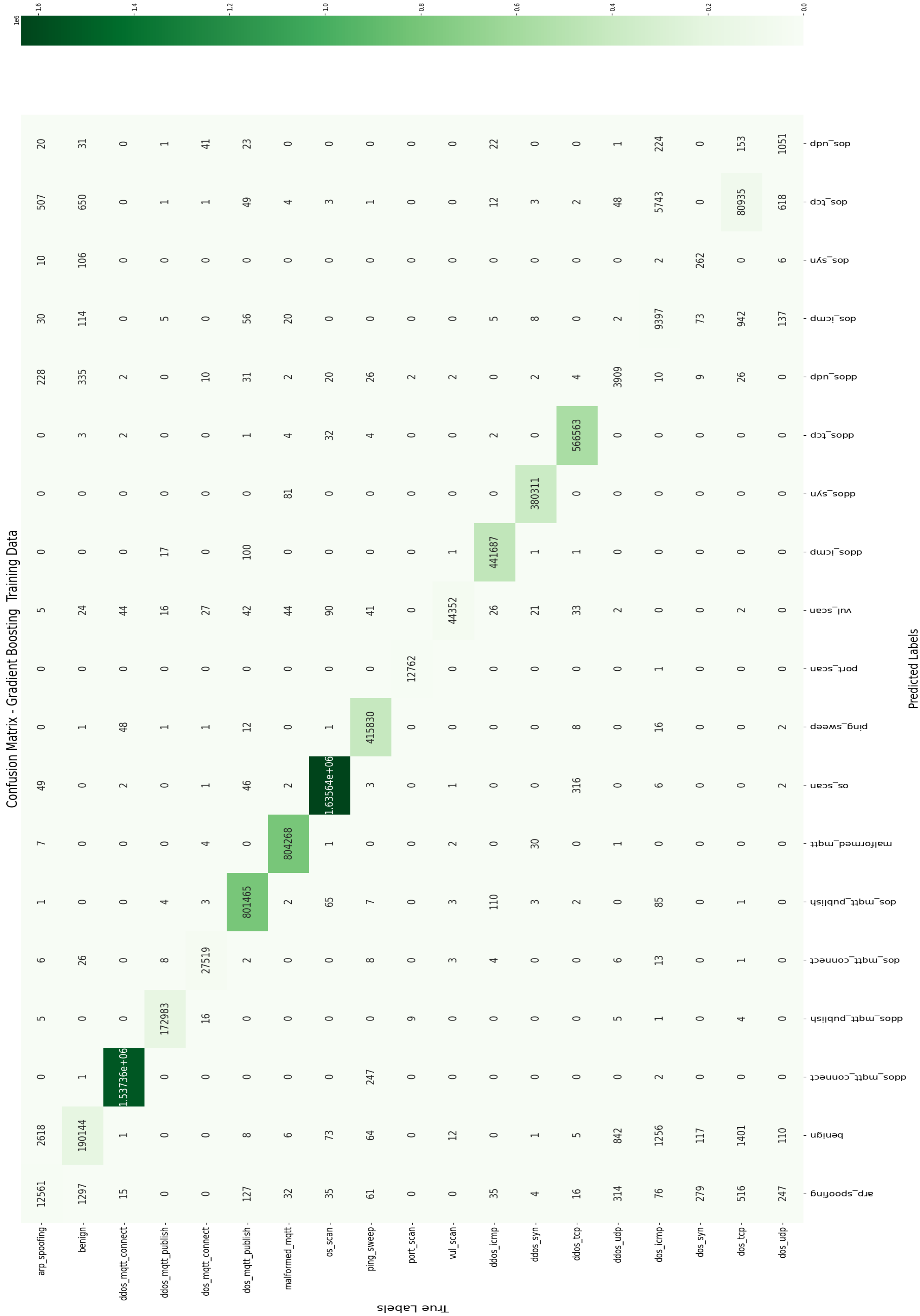

Fig. 6. Confusion Matrix for Gradient Boosting Algorithm on Training Data

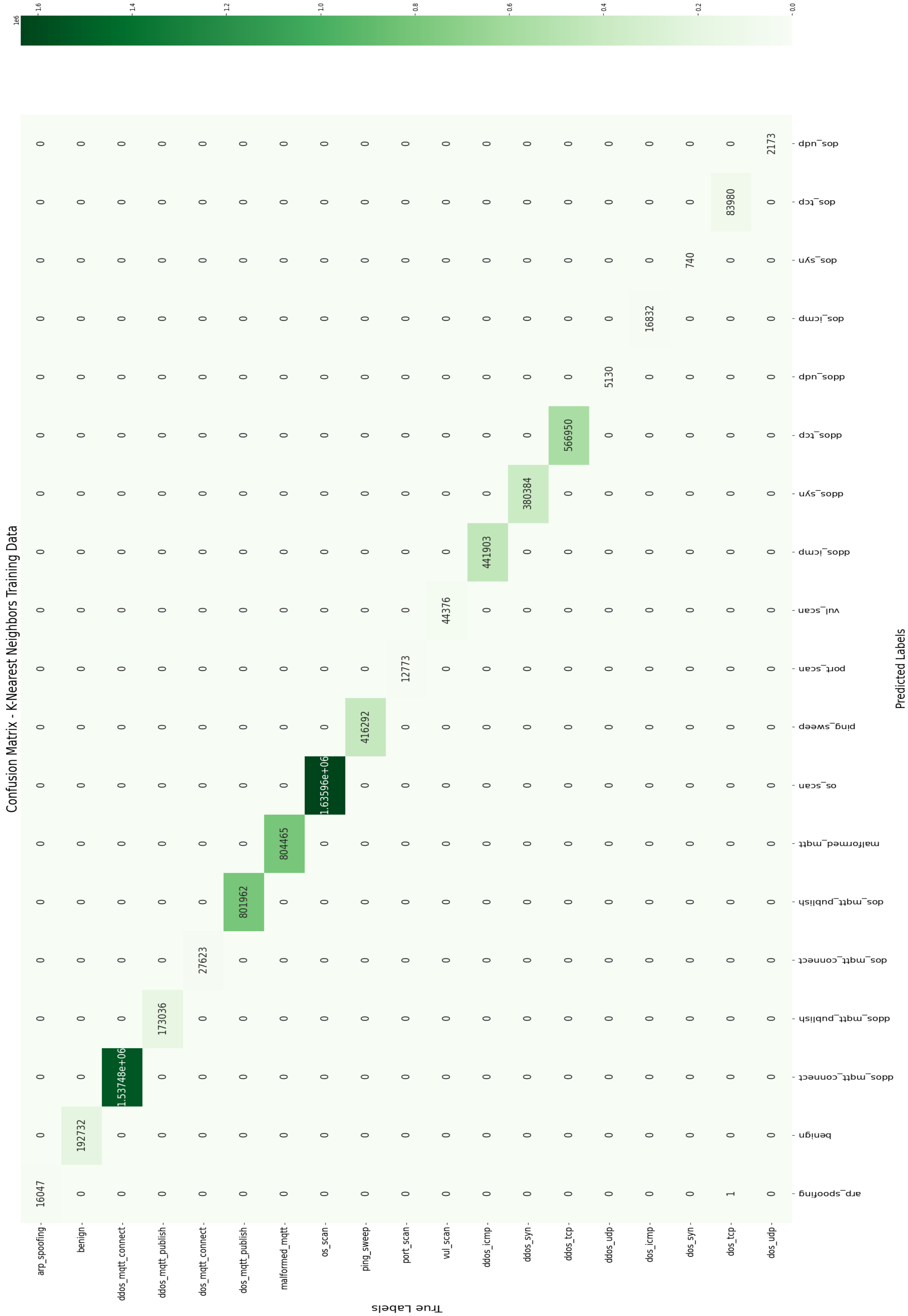

Fig. 7. Confusion Matrix for K-Nearest neighbors Algorithm on Training Data

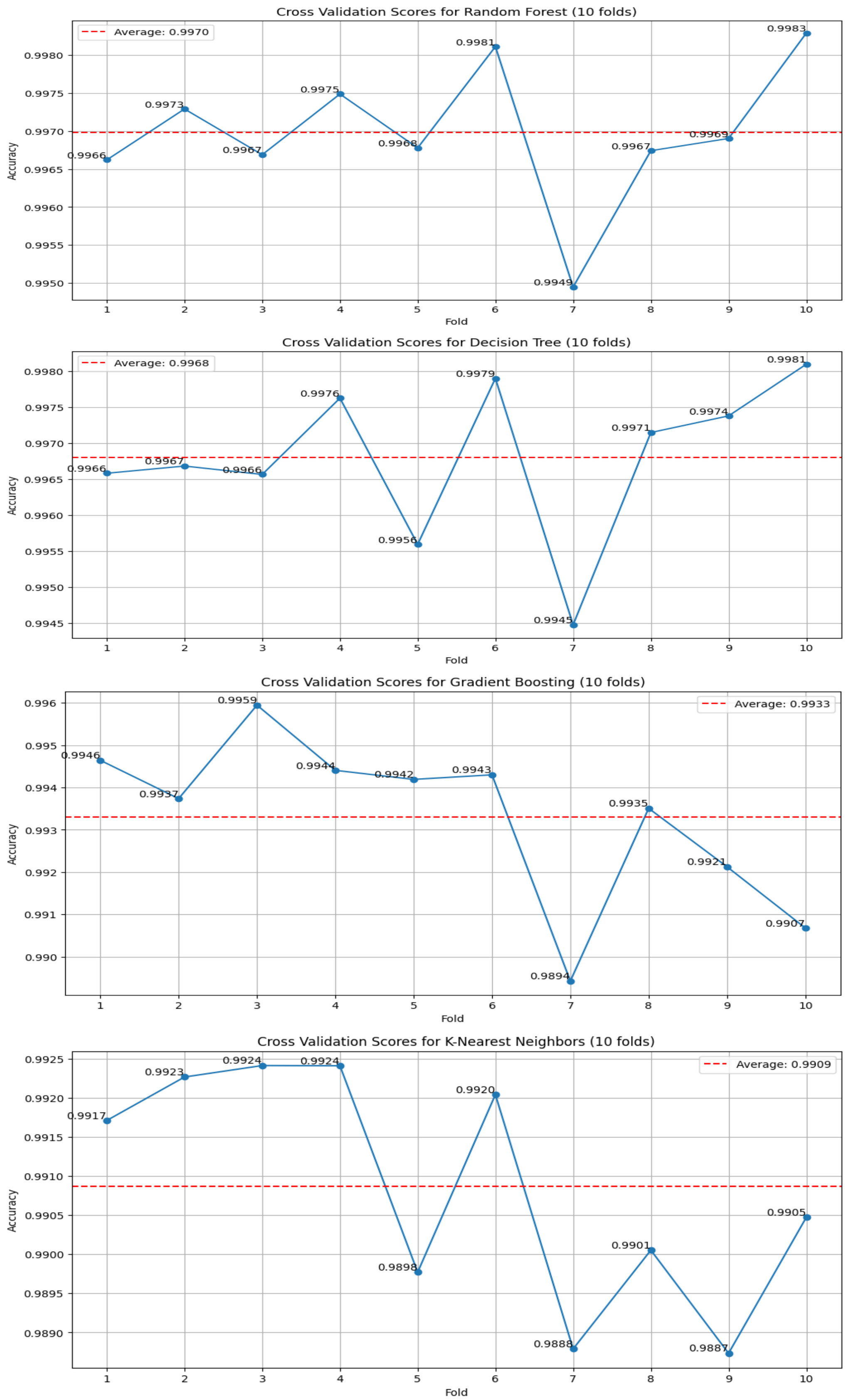

Fig. 8. Comparison of Cross-Validation Results for Each Algorithm

The results of measuring the performance of the IDS model can show that the Gradient Boosting algorithm achieves lower results compared to IDS models with other algorithms. To validate the IDS model, we perform cross-validation to ensure that the IDS model created does not have overfitting. We used 10-fold cross-validation to validate the generated IDS model. Figure 8 shows the graph of IDS model validation results for each algorithm used. The result of cross-validation indicates that there is no overfitting in the IDS model created, this indicates that the IDS model built is valid.

B. Testing the IDS Model

In this study, we tested the IDS model that had been built using the test data that had been separated previously. To ensure relevant testing, the test data was split during the preprocessing of the dataset. Table 7 shows the IDS model accuracy comparison for each algorithm for training data.

TABLE VII
IDS MODEL ACCURACY COMPARISON FOR EACH ALGORITHM ON TESTING DATA

Classifier	Accuracy
Random Forest (RF)	99%
Decision Tree (DT)	78%
Gradient Boosting (GB)	78%
K Nearest Neighbors (KNN)	98%

Based on Table 7, the comparison of IDS model accuracy for each algorithm on the testing data shows that Random Forest (RF) achieved the highest accuracy at 99%, followed by K-Nearest Neighbors (KNN) with 98%. Meanwhile, Decision Tree (DT) and Gradient Boosting (GB) both achieved an accuracy of 78%. These results indicate that the Random Forest and KNN algorithms outperform Decision Tree and Gradient Boosting in identifying patterns in the test data. Further analysis of the performance of each algorithm can be found in the following tables, where Tables 8 to 11 present the IDS model performance for specific algorithms on the test data.

Table 8 shows the IDS model performance using the Random Forest algorithm, while Table 9 shows the IDS model performance using the Decision tree for testing data. Table 10 shows the IDS model performance using the Gradient Boosting algorithm, while Table 11 shows the IDS model performance using K-Nearest neighbors for testing data.

TABLE VIII
IDS MODEL PERFORMACE USING RANDOM FOREST ALGORITHM ON TESTING DATA

Class	Precision	F1-Score	TPR	FPR	FNR	TNR
benign	0.97	0.98	0.98	0.00	0.02	0.99
arp_spoofing	0.72	0.77	0.84	0.00	0.17	0.99
ddos_mqtt_connect	1.00	1.00	1.00	0.00	0.00	1.00
ddos_mqtt_publish	1.00	0.84	0.72	0.00	0.28	1.00
dos_mqtt_connect	1.00	1.00	0.99	0.00	0.00	1.00
dos_mqtt_publish	0.78	0.88	1.00	0.00	0.00	0.99
malformed_mqtt	1.00	0.92	0.00	0.85	0.15	1.00
os_scan	0.86	0.75	0.66	0.00	0.34	0.99
ping_sweep	0.97	0.84	0.75	0.00	0.25	1.00
port_scan	0.95	0.97	0.99	0.00	0.01	0.99
vul_scan	0.86	0.43	0.28	0.00	0.72	1.00
ddos_icmp	1.00	1.00	1.00	0.00	0.00	1.00
ddos_syn	1.00	1.00	0.99	0.00	0.00	1.00
ddos_tcp	1.00	1.00	0.99	0.00	0.00	1.00
ddos_udp	1.00	1.00	0.99	0.00	0.00	0.99
dos_icmp	1.00	1.00	0.99	0.00	0.00	1.00
dos_syn	1.00	1.00	0.99	0.00	0.00	1.00
dos_tcp	1.00	1.00	0.99	0.00	0.00	1.00
dos_udp	1.00	1.00	0.99	0.00	0.00	1.00

TABLE IX
IDS MODEL PERFORMACE USING DECISION TREE ALGORITHM ON TESTING DATA

Class	Precision	F1-Score	TPR	FPR	FNR	TNR
benign	0.98	0.97	0.95	0.00	0.05	0.99
arp_spoofing	0.56	0.67	0.82	0.00	0.19	0.99
ddos_mqtt_connect	1.00	1.00	1.00	0.00	0.00	1.00
ddos_mqtt_publish	1.00	1.00	0.99	0.00	0.00	1.00
dos_mqtt_connect	1.00	1.00	0.99	0.00	0.00	1.00
dos_mqtt_publish	1.00	1.00	0.99	0.00	0.00	1.00
malformed_mqtt	0.93	0.90	0.88	0.00	0.12	0.99
os_scan	0.81	0.75	0.69	0.00	0.31	0.99
ping_sweep	0.82	0.82	0.81	0.00	0.19	1.00
port_scan	0.93	0.95	0.97	0.00	0.03	0.99
vul_scan	0.76	0.66	0.59	0.00	0.41	0.99
ddos_icmp	0.60	0.75	0.99	0.00	0.00	0.88
ddos_syn	1.00	1.00	0.99	0.00	0.00	1.00
ddos_tcp	1.00	1.00	1.00	0.00	0.00	1.00
ddos_udp	0.99	0.28	0.16	0.00	0.84	0.99
dos_icmp	0.42	0.59	0.99	0.12	0.00	0.88
dos_syn	1.00	1.00	0.99	0.00	0.00	1.00
dos_tcp	1.00	1.00	0.99	0.00	0.00	1.00
dos_udp	1.00	0.05	0.024	0.00	0.98	1.00

TABLE X
IDS MODEL PERFORMACE USING GRADIENT BOOSTING ALGORITHM ON TESTING DATA

Class	Precision	F1-Score	TPR	FPR	FNR	TNR
benign	0.96	0.96	0.97	0.00	0.03	0.99
arp_spoofing	0.46	0.56	0.72	0.00	0.28	0.99
ddos_mqtt_connect	1.00	1.00	1.00	0.00	0.00	1.00
ddos_mqtt_publish	1.00	0.93	0.87	0.00	0.13	1.00
dos_mqtt_connect	1.00	1.00	1.00	0.00	0.00	1.00
dos_mqtt_publish	0.89	0.94	1.00	0.00	0.00	1.00
malformed_mqtt	0.92	0.82	0.74	0.00	0.26	0.99
os_scan	0.83	0.87	0.57	0.00	0.43	0.99
ping_sweep	0.43	0.45	0.43	0.00	0.57	0.99
port_scan	0.92	0.95	0.97	0.00	0.03	0.99
vul_scan	0.58	0.35	0.25	0.00	0.75	0.99
ddos_icmp	0.60	0.75	0.99	0.12	0.00	0.88
ddos_syn	1.00	1.00	1.00	0.00	0.00	1.00
ddos_tcp	1.00	1.00	1.00	0.00	0.00	1.00
ddos_udp	0.99	0.29	0.17	0.00	0.83	1.00
dos_icmp	0.42	0.59	0.99	0.12	0.00	0.88
dos_syn	1.00	1.00	1.00	0.00	0.00	1.00
dos_tcp	1.00	1.00	1.00	0.00	0.00	1.00
dos_udp	1.00	0.05	0.02	0.00	0.98	1.00

TABLE XI
IDS MODEL PERFORMACE USING K-NEAREST NEIGHBORS ALGORITHM ON TESTING DATA

Class	Precision	F1-Score	TPR	FPR	FNR	TNR
benign	0.95	0.94	0.93	0.00	0.07	0.99
arp_spoofing	0.38	0.47	0.61	0.00	0.39	0.99
ddos_mqtt_connect	0.98	0.99	0.99	0.00	0.00	0.99
ddos_mqtt_publish	0.81	0.41	0.28	0.00	0.72	0.99
dos_mqtt_connect	1.00	1.00	0.99	0.00	0.00	0.99
dos_mqtt_publish	0.57	0.71	0.93	0.00	0.07	0.99
malformed_mqtt	0.69	0.66	0.64	0.00	0.36	0.99
os_scan	0.75	0.67	0.60	0.00	0.40	0.99
ping_sweep	0.70	0.60	0.53	0.00	0.47	1.00
port_scan	0.91	0.92	0.94	0.00	0.06	0.99
vul_scan	0.79	0.62	0.94	0.00	0.06	0.99
ddos_icmp	1.00	1.00	0.99	0.00	0.00	0.99
ddos_syn	0.99	0.99	0.99	0.00	0.00	0.99
ddos_tcp	1.00	0.99	0.98	0.00	0.02	0.99
ddos_udp	1.00	1.00	0.99	0.00	0.00	0.99
dos_icmp	1.00	1.00	0.99	0.00	0.00	0.99
dos_syn	1.00	1.00	0.99	0.00	0.00	0.99
dos_tcp	1.00	0.99	0.99	0.00	0.00	0.99
dos_udp	1.00	1.00	0.99	0.00	0.00	0.99

Overall, the performance of the four algorithms shows their respective strengths and weaknesses in detecting threats in the Internet of Medical Things (IoMT) network. Random Forest algorithm on testing data demonstrates high performance with excellent F1 scores for most classes. For instance, the benign class achieves an F1-Score of 0.98, while classes ddos_icmp, ddos_syn, ddos_tcp, and dos_icmp all achieve an F1-Score of 1.00. However, some classes like vul_scan show lower performance with an F1-Score of 0.43. The decision Tree algorithm shows good performance, especially for the benign class with an F1-Score of 0.97 and the ddos_icmp class with an F1-Score of 0.75. However, there are some classes with poorer performance such as ddos_udp with an F1-Score of 0.28 and dos_udp with an F1-Score of 0.05.

Gradient Boosting demonstrates high performance for several classes with F1-Scores of 1.00 for classes like ddos_mqtt_connect and ddos_syn. However, some classes like ping_sweep show lower F1-Scores at 0.45 and vul_scan with an F1-Score of 0.35. K-Nearest Neighbors algorithm on testing data shows varied results with some classes like ddos_icmp, ddos_syn, ddos_tcp, and dos_icmp achieving an F1-Score of 1.00, while ddos_mqtt_publish only achieves an F1-Score of 0.41. On the testing data, Random Forest and Gradient Boosting tend to provide better results in terms of consistency and accuracy across various threat classes, while Decision Tree and K-Nearest Neighbors exhibit more varied results depending on the type of threat encountered.

Figure 9 shows the confusion matrix of the Random Forest algorithm for testing data. Figures 10 and 11 show the results of the confusion matrix for the Decision Tree and gradient-boosting algorithms for testing data. Figures 12 display the results of the confusion matrix for the K-Nearest Neighbors algorithm for testing data.

Based on the results of testing the IDS model in detecting cyber threats on the testing data, the IDS model with the Random Forest algorithm performs the best compared to IDS models using other algorithms. There is a decrease in accuracy and performance in the IDS model's ability to detect cyber threats, with the most significant decrease observed in the IDS model using the Decision Tree algorithm.

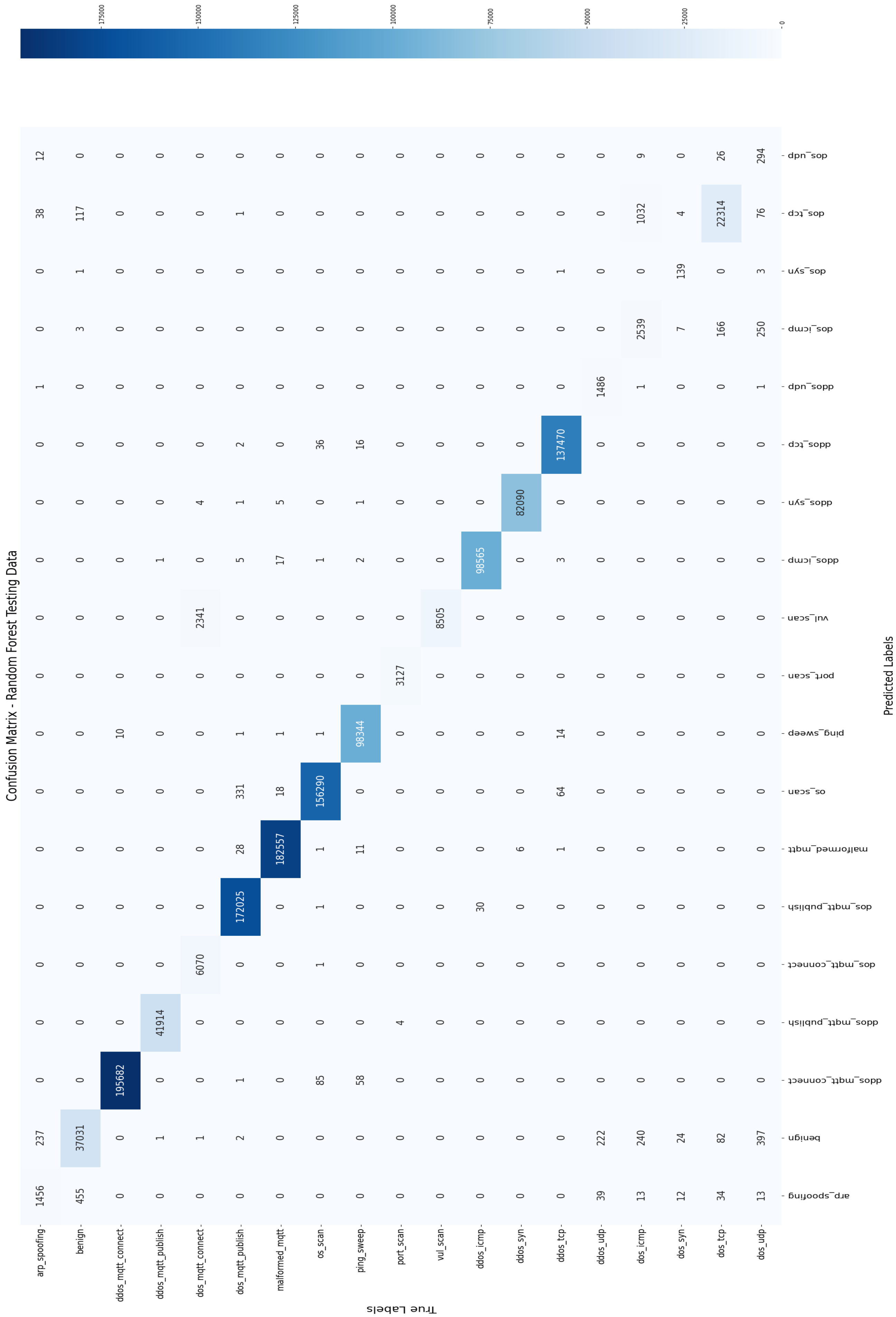

Fig. 9. Confusion Matrix for Random Forest Algorithm on Testing Data

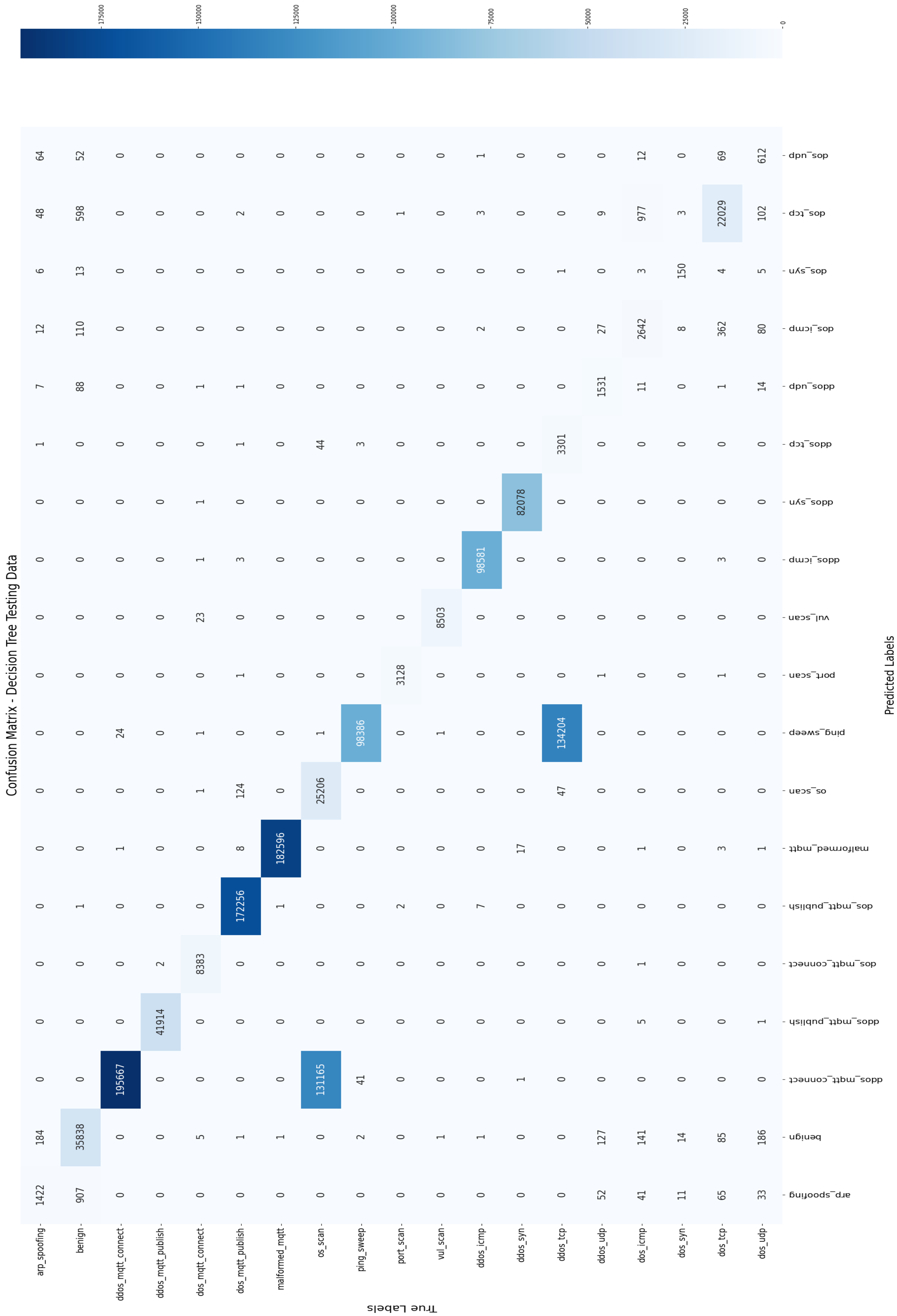

Fig. 10. Confusion Matrix for Decision Tree Algorithm on Testing Data

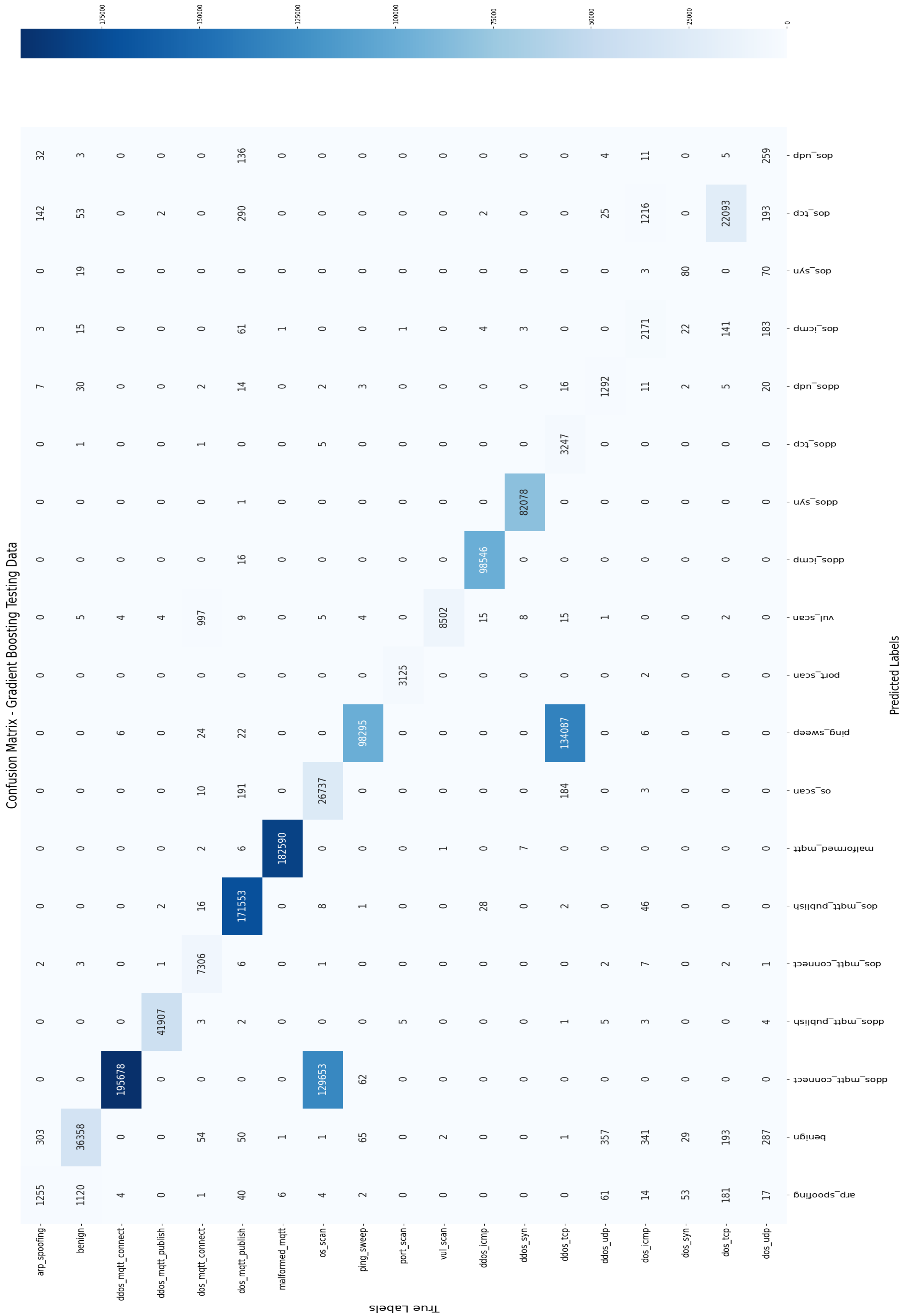

Fig. 11. Confusion Matrix for Gradient Boosting Algorithm on Testing Data

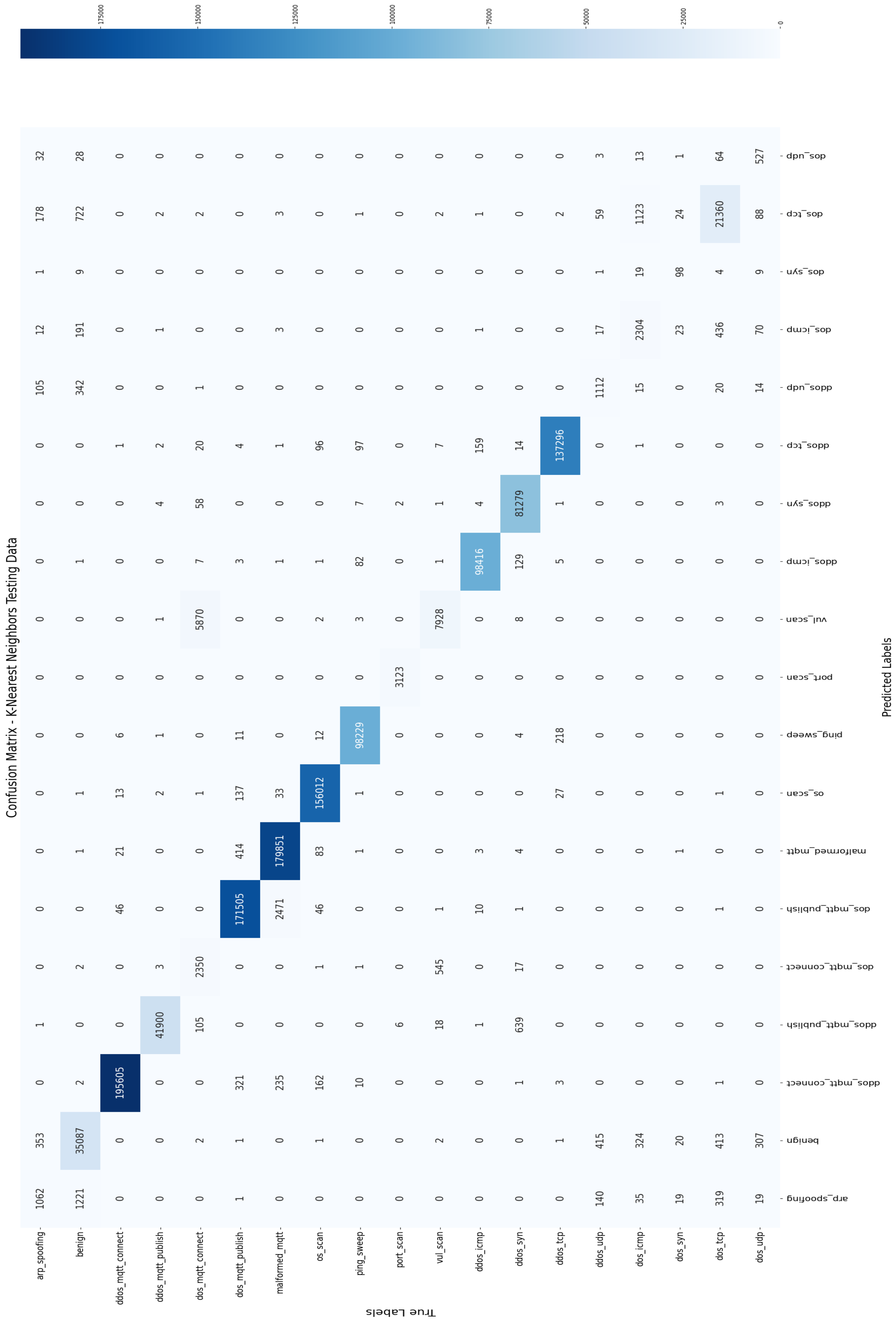

Fig. 12. Confusion Matrix for K-Nearest Neighbors Algorithm on Testing Data

V. Conclusion and Future Work

Our research not only addresses the limitations observed in previous studies but also introduces novel features that enhance the effectiveness and reliability of IDS in IoMT networks. These advancements contribute to ongoing efforts to secure IoMT environments, ensuring they remain resilient against increasingly sophisticated cyber threats.

The experimental results show that the Random Forest algorithm performs the best in detecting cyber threats on IoT networks. The IDS model employing the Random Forest algorithm demonstrates consistent performance on both training and test data. On the training data, it achieves an accuracy of 99.8%, the second highest after the IDS model using the Decision Tree algorithm, which achieves 100% validation through cross-validation, indicating no overfitting in the model.

Tests conducted on the IDS model using the Random Forest algorithm on test data yield superior results compared to the other IDS models in this study, achieving an accuracy of 99%. These findings underscore the viability of using machine learning to develop IDS models for detecting cyber threats on IoMT networks.

Our future work will involve creating an IoMT dataset that includes encrypted normal communication data. This is because the CICIoMT2024 dataset lacks encrypted data for normal communication, leaving open the possibility for attackers to alter the data. Additionally, the dataset lacks scenarios involving attackers manipulating messages. Figure 13 below displays normal communication within the unencrypted CICIoMT dataset.

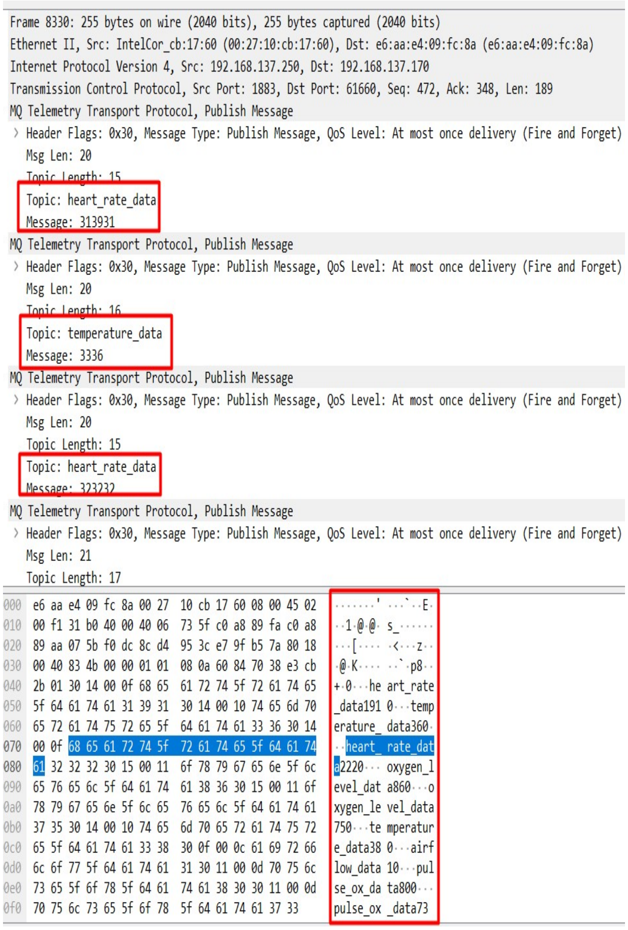

Fig. 13. The unencrypted data on CICIoMT2024 dataset.

Encrypting normal communication in the IoMT network will create a dataset with more diverse features, making it a robust training resource for IDS models to effectively detect cyber threats in IoMT networks.

References

[1] A. Ghubaish, T. Salman, M. Zolanvari, D. Unal, A. Al-Ali, and R. Jain, "Recent Advances in the Internet-of-Medical-Things (IoMT) Systems Security," *IEEE Internet Things J.*, vol. 8, no. 11, pp. 8707–8718, 2021, doi: 10.1109/JIOT.2020.3045653.

[2] U. Tariq, I. Ullah, M. Yousuf Uddin, and S. J. Kwon, "An Effective Self-Configurable Ransomware Prevention Technique for IoMT," *Sensors*, vol. 22, no. 21, pp. 1–18, 2022, doi: 10.3390/s22218516.

[3] C. T. Nnodim, O. M. Arowolo, A. A. Ajani, S. N. Okhuegbe, B. D. Agboola, and C. O. Osueke, "Emerging advances in the internet of things (IoT) technology for fast response to covid-19 outbreak with ANOVA-K-NN implementation," *Eng. Lett.*, vol. 29, no. 3, pp. 856–863, 2021.

[4] R. Hireche, H. Mansouri, and A.-S. K. Pathan, "Security and Privacy Management in Internet of Medical Things (IoMT): A Synthesis," *J. Cybersecurity Priv.*, vol. 2, no. 3, pp. 640–661, 2022, doi: 10.3390/jcp2030033.

[5] S. E. Ali, N. Tariq, F. A. Khan, M. Ashraf, W. Abdul, and K. Saleem, "BFT-IoMT: A Blockchain-Based Trust Mechanism to Mitigate Sybil Attack Using Fuzzy Logic in the Internet of Medical Things," *Sensors*, vol. 23, no. 9, 2023, doi: 10.3390/s23094265.

[6] G. Thamilarasu, A. Odesile, and A. Hoang, "An intrusion detection system for internet of medical things," *IEEE Access*, vol. 8, pp. 181560–181576, 2020, doi: 10.1109/ACCESS.2020.3026260.

[7] J. Nayak, S. K. Meher, A. Souri, B. Naik, and S. Vimal, "Extreme learning machine and bayesian optimization-driven intelligent framework for IoMT cyber-attack detection," *J. Supercomput.*, vol. 78, no. 13, pp. 14866–14891, 2022, doi: 10.1007/s11227-022-04453-z.

[8] G. Sultan Aljumaie, G. Hisham Alzeer, R. Khaild Alghamdi, and H. Alsuwat, "Modern Study on Internet of Medical Things (IOMT) Security," *IJCSNS Int. J. Comput. Sci. Netw. Secur.*, vol. 21, no. 8, p. 254, 2021, [Online]. Available: https://doi.org/10.22937/IJCSNS.2021.21.8.34

[9] S. F. Ahmed, M. S. Bin Alam, S. Afrin, S. J. Rafa, N. Rafa, and A. H. Gandomi, "Insights into Internet of Medical Things (IoMT): Data fusion, security issues and potential solutions," *Inf. Fusion*, vol. 102, no. September 2023, p. 102060, 2024, doi: 10.1016/j.inffus.2023.102060.

[10] D. Koutras, G. Stergiopoulos, T. Dasaklis, P. Kotzanikolaou, D. Glynos, and C. Douligeris, "Security in iomt communications: A survey," *Sensors (Switzerland)*, vol. 20, no. 17, pp. 1–49, 2020, doi: 10.3390/s20174828.

[11] M. L. Hernandez-Jaimes, A. Martinez-Cruz, K. A. Ramírez-Gutiérrez, and C. Feregrino-Uribe, "Artificial intelligence for IoMT security: A review of intrusion detection systems, attacks, datasets and Cloud–Fog–Edge architectures," *Internet of Things (Netherlands)*, vol. 23, no. August, p. 100887, 2023, doi: 10.1016/j.iot.2023.100887.

[12] A. Binbusayyis, H. Alaskar, T. Vaiyapuri, and M. Dinesh, "An investigation and comparison of machine learning approaches for intrusion detection in IoMT network," *J. Supercomput.*, vol. 78, no. 15, pp. 17403–17422, 2022, doi: 10.1007/s11227-022-04568-3.

[13] S. S. and A. A. G. S. Dadkhah, E. C. P. Neto, R. Ferreira, R. C. Molokwu, "CICIoMT2024: Attack Vectors in Healthcare devices-A Multi-Protocol Dataset for Assessing IoMT Device Security," *J. Comput. Commun.*, 2024, doi: 10.20944/preprints202402.0898.v1.

[14] D. Dinculeană and X. Cheng, "Vulnerabilities and limitations of MQTT protocol used between IoT devices," *Appl. Sci.*, vol. 9, no. 5, 2019, doi: 10.3390/app9050848.

[15] C. I. Fan, C. H. Shie, Y. F. Tseng, and H. C. Huang, "An Efficient Data Protection Scheme Based on Hierarchical ID-Based Encryption for MQTT," *ACM Trans. Sens. Networks*, vol. 19, no. 3, 2023, doi: 10.1145/3570506.

[16] A. Ajiboye, M. Olumoye, D. Aleburu, A. Olayiwola, D. Olayiwola, and S. Ajose, "Dimensionality Reduction for Deep Learning Based Intrusion Detection Systems for IoT," *Lect. Notes Eng. Comput. Sci.*, vol. 2245, pp. 76–81, 2023.

[17] A. Yeole, D. R. Kalbande, and A. Sharma, "Security of 6LoWPAN IoT networks in hospitals for medical data exchange," *Procedia Comput. Sci.*, vol. 152, no. December 2020, pp. 212–221, 2019, doi: 10.1016/j.procs.2019.05.045.

[18] A. J. Hintaw, S. Manickam, M. F. Aboalmaaly, and S. Karuppayah, "MQTT Vulnerabilities, Attack Vectors and Solutions in the Internet

of Things (IoT)," *IETE J. Res.*, no. May, 2021, doi: 10.1080/03772063.2021.1912651.
[19] A. J. Hintaw, S. Manickam, S. Karuppayah, M. A. Aladaileh, M. F. Aboalmaaly, and S. U. A. Laghari, "A Robust Security Scheme Based on Enhanced Symmetric Algorithm for MQTT in the Internet of Things," *IEEE Access*, vol. 11, no. May, pp. 43019–43040, 2023, doi: 10.1109/ACCESS.2023.3267718.
[20] F. B. Setiawan and Magfirawaty, "Securing Data Communication Through MQTT Protocol with AES-256 Encryption Algorithm CBC Mode on ESP32-Based Smart Homes," *2021 Int. Conf. Comput. Syst. Inf. Technol. Electr. Eng. COSITE 2021*, no. October, pp. 166–170, 2021, doi: 10.1109/COSITE52651.2021.9649577.
[21] M. Husnain *et al.*, "Preventing MQTT Vulnerabilities Using IoT-Enabled Intrusion Detection System," *Sensors*, vol. 22, no. 2, 2022, doi: 10.3390/s22020567.
[22] M. A. S. Arifin, D. Stiawan, and B. Y. Suprapto, "Oversampling and undersampling for intrusion detection system in the supervisory control and data acquisition IEC 60870 - 5 - 104," *IET Cyber-Physical Syst. Theory Appl.*, no. November 2023, 2024, doi: 10.1049/cps2.12085.
[23] M. Hilda, L. Louk, and B. Adhi, "Dual-IDS : A bagging-based gradient boosting decision tree model for network anomaly intrusion detection system," *Expert Syst. Appl.*, vol. 213, no. PB, p. 119030, 2023, doi: 10.1016/j.eswa.2022.119030.
[24] K. Alissa, T. Alyas, K. Zafar, Q. Abbas, N. Tabassum, and S. Sakib, "Botnet Attack Detection in IoT Using Machine Learning," *Comput. Intell. Neurosci.*, vol. 2022, 2022, doi: 10.1155/2022/4515642.
[25] A. Almogren, I. Mohiuddin, I. U. Din, H. Almajed, and N. Guizani, "FTM-IoMT: Fuzzy-Based Trust Management for Preventing Sybil Attacks in Internet of Medical Things," *IEEE Internet Things J.*, vol. 8, no. 6, pp. 4485–4497, 2021, doi: 10.1109/JIOT.2020.3027440.
[26] R. Punithavathi, K. Venkatachalam, M. Masud, M. A. Alzain, and M. Abouhawwash, "Crypto Hash Based Malware Detection in IoMT Framework," *Intell. Autom. Soft Comput.*, vol. 34, no. 1, pp. 559–574, 2022, doi: 10.32604/iasc.2022.024715.
[27] P. Kulshrestha and T. V Vijay Kumar, "Machine learning based intrusion detection system for IoMT," *Int. J. Syst. Assur. Eng. Manag.*, 2023, doi: 10.1007/s13198-023-02119-4.
[28] U. Zukaib, X. Cui, C. Zheng, M. Hassan, and Z. Shen, "Meta-IDS: Meta-Learning Based Smart Intrusion Detection System for Internet of Medical Things (IoMT) Network," *IEEE Internet Things J.*, p. 1, 2024, doi: 10.1109/JIOT.2024.3387294.
[29] Z. Sun, G. An, Y. Yang, and Y. Liu, "Optimized machine learning enabled intrusion detection 2 system for internet of medical things," *Franklin Open*, vol. 6, no. July 2023, p. 100056, 2024, doi: 10.1016/j.fraope.2023.100056.
[30] N. Oliveira, I. Praça, E. Maia, and O. Sousa, "Intelligent cyber attack detection and classification for network-based intrusion detection systems," *Appl. Sci.*, vol. 11, no. 4, pp. 1–21, 2021, doi: 10.3390/app11041674.
[31] D. Upadhyay, J. Manero, M. Zaman, and S. Sampalli, "Gradient Boosting Feature Selection With Machine Learning Classifiers for Intrusion Detection on Power Grids," *IEEE Trans. Netw. Serv. Manag.*, vol. 18, no. 1, pp. 1104–1116, 2021.
[32] L. A. C. Ahakonye, C. I. Nwakanma, J. M. Lee, and D. S. Kim, "SCADA intrusion detection scheme exploiting the fusion ofmodified decision tree and Chi-square feature selection," *Internet of Things (Netherlands)*, vol. 21, no. September 2022, p. 100676, 2023, doi: 10.1016/j.iot.2022.100676.
[33] G. Liu, H. Zhao, F. Fan, G. Liu, Q. Xu, and S. Nazir, "An Enhanced Intrusion Detection Model Based on Improved kNN in WSNs," *Sensors*, vol. 22, no. 4, pp. 1–18, 2022, doi: 10.3390/s22041407.
[34] M. Aamir and S. M. A. Zaidi, "DDoS attack detection with feature engineering and machine learning: the framework and performance evaluation," *Int. J. Inf. Secur.*, vol. 18, no. 6, pp. 761–785, 2019, doi: 10.1007/s10207-019-00434-1.
[35] A. Gumaei *et al.*, "A robust cyberattack detection approach using optimal features of SCADA power systems in smart grids," *Appl. Soft Comput. J.*, vol. 96, no. November 2020, pp. 1–17, 2020, doi: 10.1016/j.asoc.2020.106658.
[36] H. Shafique, A. A. Shah, M. A. Qureshi, and M. K. Ehsan, "Machine Learning Empowered Efficient Intrusion Detection Framework," *VFAST Trans. Softw. Eng.*, vol. 10, no. 2, pp. 27–35, 2022, doi: http://dx.doi.org/10.21015/vtse.v10i2.1017.
[37] M. Artur, "Review the performance of the Bernoulli Naïve Bayes Classifier in Intrusion Detection Systems using Recursive Feature Elimination with Cross-validated selection of the best number of features," *Procedia Comput. Sci.*, vol. 190, no. 2019, pp. 564–570, 2021, doi: 10.1016/j.procs.2021.06.066.