# 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 crossvalidation. 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 I 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: <u>mas.arifin@univbinsainsan.ac.id; mas.agus1988@gmail.com</u>).

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. Binbusay yis 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. Kulshrest ha 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 Binbusavis 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 characteristics challenges unique and 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.* 

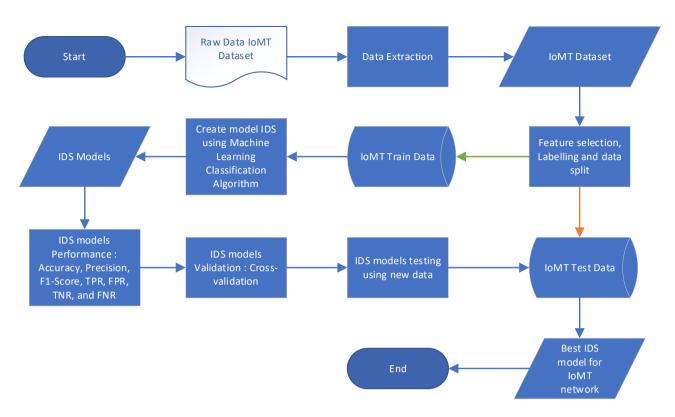


Fig. 1. Proposed method to find the best algorithm for the IDS model in this study

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 gradientboosting 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).

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

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

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

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

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

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

$$TNR = \frac{TN}{(TN+FP)}$$
(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 10fold 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.

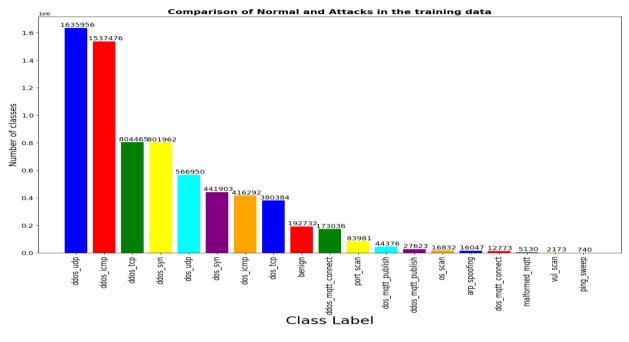


Fig. 2. Comparison of normal data and attacks in the training data

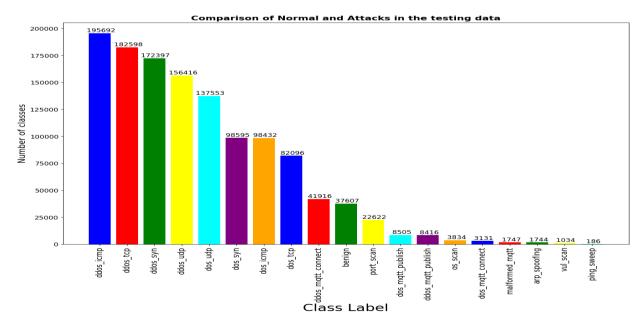


Fig. 3. Comparison of normal data and attacks in the test data

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 MC	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 M	ODEL PERFORMAC	LE USING DECISI	ON TREE ALGORIT	HM ON TRAINING	DAIA
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 DEBEODMACE LIGING CRADIENT POOSTING ALCODITING ON TRADUNC D	A T A

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 mgtt 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 iemp	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, 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.

le6	- 16		- 14			-		- 10		- 0.8			- 0.6		- 0.4		- 0.2			00 -
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2173	- dpn <sup>-</sup> sop
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	83981	0	- dɔī_sop
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	740	0	0	- uʎs <sup>–</sup> sop
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	16830	0	0	0	- dɯɔi_sop
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	5130	0	0	0	0	- dpn <sup>-</sup> sopp
	0	0	0	0	0	0	0	0	0	0	0	0	0	566950	0	0	0	0	0	- dɔə¯sopp
	0	0	0	0	0	0	0	0	0	0	0	0	380384	0	0	0	0	0	0	- uƙs <sup>-</sup> sopp
ng Data	0	0	0	0	0	0	0	0	0	0	0	441903	0	0	0	0	0	0	0	- dmɔi_sobb
orest Trainii	0	0	0	0	0	0	0	0	0	0	44376	0	0	0	0	0	0	0	0	- ueos jnv
Confusion Matrix - Random Forest Training Data	0	0	0	0	0	0	0	0	0	12773	0	0	0	0	0	0	0	0	0	- uɛɔs_bod
on Matrix -	0	0	0	0	0	0	0	0	416292	0	0	0	0	0	0	0	0	0	0	- dəəms <sup></sup> buid
Confusio	0	0	0	0	0	0	0	1.63596e+06	0	0	0	0	0	0	0	0	0	0	0	- นยวร ีรด
	0	0	0	0	0	0	804465	0	0	0	0	0	0	0	0	0	0	0	0	- 11pm_bəm10116m
	0	0	0	0	0	801962	0	0	0	0	0	0	0	0	0	0	0	0	0	- ysilduq_ttpm_sob
	0	0	0	0	27623	0	0	0	0	0	0	0	0	0	0	0	0	0	0	- toonnoc_ttpm_sob
	0	0	0	173036	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	- dsilduq_ttpm_sobb
	0	0	l.53748e+06	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	- גסחחפכל -
	0	192732	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	- uɓịuəq
	16047	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	- ɓuijoods <sup>-</sup> dje
	arp_spoofing - 16047	benign -	ddos_mqtt_connect -	ddos_mqtt_publish -	dos_mqtt_connect -	dos_mqtt_publish -	malformed_mqtt -	os_scan -	ping_sweep -	bort_scan	vul_scan -	ddos_icmp -	- nto_syn	ddos_tcp -	- dpn_sopp	dos_icmp -	- nvs_sob	dos_tcp -	- dpn <sup>-</sup> sop	

Predicted Labels

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

le6	- 1.6		- 1.4			- 12		- 1.0		- 0.8			- 0.6		- 0.4		- 0.2			00 -
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2173	- dpn <sup>-</sup> sop
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	83981	0	- dɔī_sop
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	740	0	0	- uʎs <sup>-</sup> sop
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	16832	0	0	0	- dmɔi_sob
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	5130	0	0	0	0	- dpn <sup>-</sup> sopp
	0	0	0	0	0	0	0	0	0	0	0	0	0	566950	0	0	0	0	0	- dɔī_sopp
	0	0	0	0	0	0	0	0	0	0	0	0	380384	0	0	0	0	0	0	- uʎs <sup>-</sup> sopp
Data	0	0	0	0	0	0	0	0	0	0	0	441903	0	0	0	0	0	0	0	- dmɔi_sobb
ee Training	0	0	0	0	0	0	0	0	0	0	44376	0	0	0	0	0	0	0	0	- ueos <sup>-</sup> inv
Confusion Matrix - Decision Tree Training Data	0	0	0	0	0	0	0	0	0	12773	0	0	0	0	0	0	0	0	0	- nezz_toq
n Matrix - [	0	0	0	0	0	0	0	0	416292	0	0	0	0	0	0	0	0	0	0	- dəəms_priq
Confusio	0	0	0	0	0	0	0	1.63596e+06	0	0	0	0	0	0	0	0	0	0	0	- ueos <sup>-</sup> so
	0	0	0	0	0	0	804465	0	0	0	0	0	0	0	0	0	0	0	0	- Jipm_bəmıoilsm
	0	0	0	0	0	801962	0	0	0	0	0	0	0	0	0	0	0	0	0	- dzilduq_JJpm_zob
	0	0	0	0	27623	0	0	0	0	0	0	0	0	0	0	0	0	0	0	- təənnoə_ttpm_zob
	0	0	0	173036	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	- daildug_jjpm_2obb
	0	0	1.53748e+06	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	- 159nno2_11pm_sobb
	0	192732	0 1.537	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	- пріпэd
		0 192	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	- ɓuijoods_qra
	ing - 16047																			Sagoods die
	arp_spoofing -	benign	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	- dpn <sup>-</sup> sopp	dos_icmp.	dos_syn	dos_tcp ·	- dpn_sob	

Predicted Labels



le6	- 1.6		- 1.4			- 12		- 1.0		- 0.8			- 0.6		- 0.4		- 0.2			00 -
ľ																				
	20	31	0	1	41	23	0	0	0	0	0	22	0	0	1	224	0	153	1051	- dpn <sup>-</sup> sop
	507	650	0	1	1	49	4	m	1	0	0	12	m	2	48	5743	0	80935	618	- dɔī_sop
	10	106	0	0	0	0	0	0	0	0	0	0	0	0	0	2	262	0	9	- uʎs¯sop
	30	114	0	2	0	56	20	0	0	0	0	5	80	0	2	9397	73	942	137	- duɔi_sop
	228	335	2	0	10	31	2	20	26	2	2	0	2	4	3909	10	6	26	0	- dpn <sup>-</sup> sopp
	0	m	2	0	0	1	4	32	4	0	0	2	0	566563	0	0	0	0	0	- dɔī͡sopp
	0	0	0	0	0	0	81	0	0	0	0	0	380311	0	0	0	0	0	0	- uʎs <sup>-</sup> sopp
Confusion Matrix - Gradient Boosting Training Data	0	0	0	17	0	100	0	0	0	0	1	441687	1	1	0	0	0	0	0	- dwoj <sup>–</sup> sopp
oosting Tra	Ω	24	44	16	27	42	44	06	41	0	44352	26	21	33	2	0	0	2	0	- นยวร <sup>-</sup> มกา อ อ
Gradient B	0	0	0	0	0	0	0	0	0	12762	0	0	0	0	0	1	0	0	0	Predicted port_scan -
on Matrix -	0	1	48	1	1	12	0	06 1	415830	0	0	0	0	8	0	16	0	0	2	- dəəms <sup>–</sup> buid
Confusi	49	0	2	0	1	46	2	1.63564e+06	m	0	1	0	0	316	0	Q	0	0	2	- ueos <sup>-</sup> so
	7	0	0	0	4	0	804268	1	0	0	2	0	30	0	1	0	0	0	0	- ttpm_b9motl6m
	1	0	0	4	m	801465	2	65	7	0	m	110	£	2	0	85	0	1	0	- deildug_ffpm_eob
	9	26	0	8	27519	2	0	0	œ	0	Μ	4	0	0	9	13	0	1	0	- toon oo too
	Ω	0	e+06 0	172983	16	0	0	0	0	6	0	0	0	0	Ŋ	1	0	4	0	- deildug tipm_eobb
	0	14 1	1.53736e+06	0	0	0	0	0	247	0	0	0	0	0	0	5 2	0	1 0		- toennoo_ttpm_eobb
	51 2618	7 190144	1	0	0	8	9	73	64	0	12	0	1	5	t 842	1256	117	1401	/ 110	- นธิเนอq
	arp_spoofing - 12561	benign - 1297	nnect - 15	ublish - 0	nnect - 0	ublish - 127	_mqtt - 32	os_scan - 35	sweep - 61	port_scan - 0	vul_scan - 0	ddos_icmp - 35	ddos_syn - 4	ddos_tcp - 16	ddos_udp - 314	dos_icmp - 76	dos_syn - 279	dos_tcp - 516	dos_udp - 247	- 6นมูoods <sup>–</sup> d.e
	arp_sp(	a	ddos_mqtt_connect	ddos_mqtt_publish	dos_mqtt_connect	dos_mqtt_publish	malformed_mqtt	S	ping_sweep -	edel ei		ddos	ddo	ddc	ddo	op	ę	Å	op	

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

le6	- 1.6		- 1.4			- 1.2		- 1.0		- 0.8			- 0.6		- 0.4		- 0.2			00 -
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2173	- dpn <sup>-</sup> sop
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	83980	0	- dɔə͡sop
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	740	0	0	- uʎs¯sop
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	16832	0	0	0	- dmɔi_sob
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	5130	0	0	0	0	- dpn <sup>-</sup> sopp
	0	0	0	0	0	0	0	0	0	0	0	0	0	566950	0	0	0	0	0	- dɔī̄sopp
ta	0	0	0	0	0	0	0	0	0	0	0	0	380384	0	0	0	0	0	0	- u/s¯sopp
Confusion Matrix - K.Nearest Neighbors Training Data	0	0	0	0	0	0	0	0	0	0	0	441903	0	0	0	0	0	0	0	- dwɔi¯sopp
Neighbors <sup>-</sup>	0	0	0	0	0	0	0	0	0	0	44376	0	0	0	0	0	0	0	0	- ueos Ținn e e
· K-Nearest	0	0	0	0	0	0	0	0	2 0	12773	0	0	0	0	0	0	0	0	0	Ped Label Port_scan - Ped
ion Matrix -	0	0	0	0	0	0	0	+06 0	416292	0	0	0	0	0	0	0	0	0	0	- dəəms <sup>–</sup> buid
Confus	0	0	0	0	0	0	55 0	1.63596e+06	0	0	0	0	0	0	0	0	0	0	0	- ueos"so
	0	0	0	0	0	52 0	804465	0	0	0	0	0	0	0	0	0	0	0	0	- malformed_mqtt -
	0	0	0	0	23 0	801962	0	0	0	0	0	0	0	0	0	0	0	0		- dsilduq_ttpm_sob
	0	0	0	)36 0	27623	0	0	0	0	0	0	0	0	0	0	0	0	0		- toonactic
	0	0 0	8e+06 0	0 173036	0 0	0	0 0	0 0	0 0	0 0	0 0	0 0	0 0	0	0 0	0	0 0	0 0	0	- ysildug_typm_sobb
	0 0	192732 0	0 1.53748e+06	0	0	0	0	0	0	0	0	0	0	0	0	0 0	0	0	0 0	- npinəd
		0 192	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	- pnitooq2_q16
	arp_spoofing - 16047	benign - (						os_scan - (	ping_sweep - (	port_scan - (	vul_scan - (	ddos_icmp - (	ddos_syn -	ddos_tcp - (	) - dpn <sup>-</sup> sopp	dos_icmp - (	) - uks_sop	dos_tcp -	) - dpn <sup>-</sup> sop	
	arp_s		ddos_mqtt_connect	ddos_mqtt_publish	dos_mqtt_connect	dos_mqtt_publish	malformed_mqtt	-		8 Balana		ddc	Ğ	q	ğ	ğ	-		5	

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

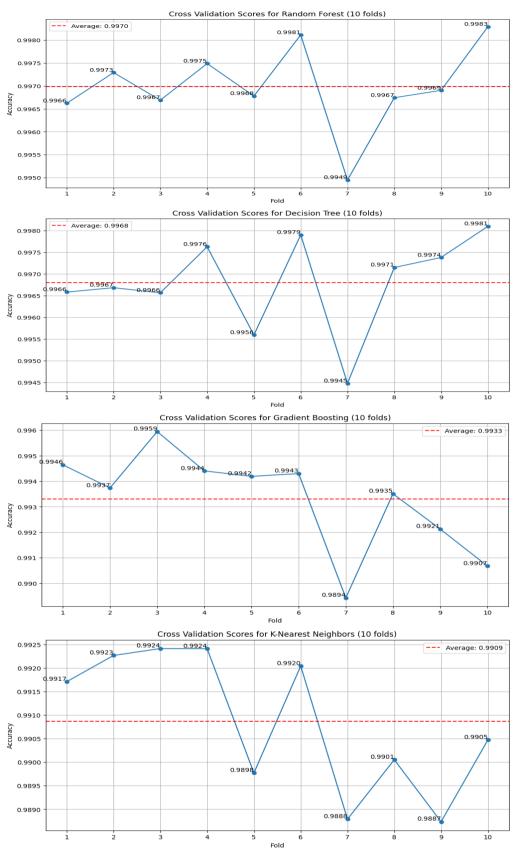


Fig. 8. Comparison of Cross-Validation Results for Each Algorithm

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

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	
S MODEL REPEORMACE LISING PANDOM FOREST ALCORITHM ON TESTING DATA	

	IDS M	DDEL PERFORMAC		M FOREST ALGOR	ITHM 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 N	10DEL PERFORMA	CE USING DECISI	ON TREE ALGORIT	THM ON TESTING I	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
dosudp	1.00	0.05	0.024	0.00	0.98	1.00

	IDS MO	DEL PERFORMACE		BLE A it Boosting Alg	ORITHM ON TESTI	ΝG ΠΑΤΑ
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 mgtt 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

TADIEV

TABLE XI

	IDS MODI	EL PERFORMACE U	ISING K-NEARES	T NEIGHBORS ALC	GORITHM ON TEST	ING 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.

								Confusion	ı Matrix - Rő	andom Fore	Confusion Matrix - Random Forest Testing Data	Data									
arp_spoofing -	1456	237	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	38	12		
benign -	455	37031	0	0	0	0	0	0	0	0	0	0	0	0	0	m	1 1	117	0		
ddos_mqtt_connect -	0	0	195682	0	0	0	0	0	10	0	0	0	0	0	0	0	0	0	0	0006/1	
ddos_mqtt_publish -	0	1	0	41914	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0		
dos_mqtt_connect -	0	1	0	0	6070	0	0	0	0	0	2341	0	4	0	0	0	0	0	0	- 150000	
dos_mqtt_publish -	0	2	1	0	0	172025	28	331	1	0	0	5	1	2	0	0	0	1	0		
malformed_mqtt -	0	0	0	0	0	0	182557	18	1	0	0	17	5	0	0	0	0	0	0	- 125000	
os_scan -	0	0	85	0	1	1	1	156290	1	0	0	1	0	36	0	0	0	0	0		
ping_sweep -	0	0	58	0	0	0	1	0	98344	0	0	2	1	16	0	0	0	0	0		
port_scan -	0	0	0	4	0	0	0	0	0	3127	0	0	0	0	0	0	0	0	0	- 100000	
vul_scan -	0	0	0	0	0	0	0	0	0	0	8505	0	0	0	0	0	0	0	0		
ddos_icmp -	0	0	0	0	0	30	0	0	0	0	0	98565	0	0	0	0	0	0	0	- 75000	
- ddos_syn	0	0	0	0	0	0	9	0	0	0	0	0	82090	0	0	0	0	0	0		
ddos_tcp -	0	0	0	0	0	0	1	64	14	0	0	m	0	137470	0	0	1	0	0		
- dpn <sup>-</sup> sopp	39	222	0	0	0	0	0	0	0	0	0	0	0	0	1486	0	0	0	0	- 20000	
dos_icmp -	13	240	0	0	0	0	0	0	0	0	0	0	0	0	1	2539	0 10	1032	б		
- avs_sob	12	24	0	0	0	0	0	0	0	0	0	0	0	0	0	L 7	139	4	0	- 25000	
dos_tcp -	34	82	0	0	0	0	0	0	0	0	0	0	0	0	0	166	0 22	22314	26		
- dpn <sup>-</sup> sop	13	397	0	0	0	0	0	0	0	0	0	0	0	0	1	250	m	76 2	294		
	- pniìooq2_q16	- นธิเนอต	- toenno_ttpm_sobb	- dsilduq_ttpm_sobb	- toonno_ttpm_zob	- dsilduq_ttpm_sob	- Jipm_b9m10il6m	- ueos"so	- dəəws_priq	ט קיד איז גיי גיי גיי גיי גיי גיי גיי גיי גיי ג	- ueos <sup></sup> ina	- dɯɔi_sopp	- uʎs <sup></sup> sopp	- dɔə̥¯sopp	- dpn <sup>-</sup> sopp	- dmɔi_sob	- u/s¯sop	- dɔɔ̥¯sop	- dpn <sup>−</sup> sop	9 '	
									ricui	ICLEU Laueis											

## IAENG International Journal of Computer Science

			- 175000		- 150000		- 125000			- 100000		- 75000			- 50000		- 25000			° -
	64	52	0	0	0	0	0	0	0	0	0	1	0	0	0	12	0	69	612	- dpn <sup>-</sup> sop
	48	598	0	0	0	2	0	0	0	1	0	m	0	0	6	977	m	22029	102	- dɔɔ̯¯sop
	9	13	0	0	0	0	0	0	0	0	0	0	0	1	0	Μ	150	4	ŝ	- uʎs¯sop
	12	110	0	0	0	0	0	0	0	0	0	2	0	0	27	2642	œ	362	80	- dɯɔi_sop
	Ζ	88	0	0	1	1	0	0	0	0	0	0	0	0	1531	11	0	1	14	- dpn <sup>-</sup> sopp
	1	0	0	0	0	1	0	44	m	0	0	0	0	3301	0	0	0	0	0	- dɔૣīsopp
	0	0	0	0	1	0	0	0	0	0	0	0	82078	0	0	0	0	0	0	- u∕s⁻sopp
וק Data	0	0	0	0	1	m	0	0	0	0	0	98581	0	0	0	0	0	m	0	- duɔi_sobb
Confusion Matrix - Decision Tree Testing Data	0	0	0	0	23	0	0	0	0	0	8503	0	0	0	0	0	0	0	0	- uess <sup>-</sup> inv Mil <sup>-</sup> acan -
x - Decisior	0	0	0	0	0	1	0	0	0	3128	0	0	0	0	1	0	0	1	0	איין איין איין איין איין איין איין איין
usion Matri	0	0	24	0	1	0	0	-1	98386	0	1	0	0	134204	0	0	0	0	0	- dəəms <sup>-</sup> buid
Confi	0	0	0	0	1	124	0	25206	0	0	0	0	0	47	0	0	0	0	0	- นยวร ีรง
	0	0	1	0	0	ω	182596	0	0	0	0	0	17	0	0	1	0	m	1	- 11pm_b9mvo1l6m
	0	1	0	0	0	172256	1	0	0	2	0	7	0	0	0	0	0	0	0	- daildug_ttpm_aob
	0	0	0	2	8383	0	0	0	0	0	0	0	0	0	0	1	0	0	0	- dos_mqtt_connect
	0	0	0	41914	0	0	0	0	0	0	0	0	0	0	0	2	0	0	1	- Azilduq_17pm_2obb
	0	0	195667	0	0	0	0	131165	41	0	0	0	1	0	0	0	0	0	0	- toonnect
	184	35838	0	0	5	1	1	0	2	0	1	1	0	0	127	141	14	85	186	- npinəd
	ng - 1422	gn - 907	ect - 0	sh - 0	ect - 0	sh - 0	att - 0	an - 0	ep - 0	an - 0	an - 0	0 - du	yn - 0	cp -	dp - 52	np - 41	yn - 11	cp - 65	dp - 33	- pnifooq2_q16
	arp_spoofing -	benign -	ddos_mqtt_connect -	ddos_mqtt_publish -	dos_mqtt_connect	dos_mqtt_publish	malformed_mqtt-	os_scan -	ping_sweep	bort scan	vul_scan	ddos_icmp -	- udo_ syn	ddos_tcp -	- dpn <sup>-</sup> sopp	dos_icmp -	- u/s _ sob	dos_tcp -	- dpn <sup>-</sup> sop	

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

### IAENG International Journal of Computer Science

			0005/1 -		- 150000		- 125000			- 100000		- 75000			- 50000		- 25000			ę.
ŕ	32	m	0	0	0	136	0	0	0	0	0	0	0	0	4	11	0	2	259	- dpn <sup>-</sup> sop
	142	53	0	2	0	290	0	0	0	0	0	2	0	0	25	1216	0	22093	193	- dɔɔ̥¯sop
c	0	19	0	0	0	0	0	0	0	0	0	0	0	0	0	m	80	0	70	- uʎs¯sop
ſ	m	15	0	0	0	61	1	0	0	1	0	4	e	0	0	2171	22	141	183	- duɔi_sop
r	7	30	0	0	2	14	0	2	m	0	0	0	0	16	1292	11	2	5	20	- dpn <sup>-</sup> sopp
c	0	1	0	0	1	0	0	ß	0	0	0	0	0	3247	0	0	0	0	0	- dɔī_sopp
c	0	0	0	0	0	1	0	0	0	0	0	0	82078	0	0	0	0	0	0	- uʎs <sup>–</sup> sopp
ng Data ົ	0	0	0	0	0	16	0	0	0	0	0	98546	0	0	0	0	0	0	0	- dɯɔi_sopp
Confusion Matrix - Gradient Boosting Testing Data	0	Ŋ	4	4	<i>1</i> 66	6	0	2	4	0	8502	15	80	15	1	0	0	2	0	- นยวร ี เทง
adient Boo	0	0	0	0	0	0	0	0	0	3125	0	0	0	0	0	2	0	0	0	אפקי דר שסטר־scan - ער בי רום רום רום רום רום רום רום רום רום רום
Matrix - Gr	0	0	9	0	24	22	0	0	98295	0	0	0	0	134087	0	9	0	0	0	- dəəws_priq
Confusion	0	0	0	0	10	191	0	26737	0	0	0	0	0	184	0	m	0	0	0	- ueos"so
c	0	0	0	0	2	9	182590	0	0	0	1	0	٢	0	0	0	0	0	0	- 11pm_bəmro1lsm
c	0	0	0	2	16	171553	0	œ	1	0	0	28	0	2	0	46	0	0	0	- dsildug_jjpm_sob
ſ	2	m	0	1	7306	9	0	1	0	0	0	0	0	0	2	7	0	2	1	- toonnoo_ttpm_sob
c	0	0	0	41907	m	2	0	0	0	Ŋ	0	0	0	1	Ŋ	m	0	0	4	- daildug_JJpm_aobb
c	0	0	195678	0	0	0	0	129653	62	0	0	0	0	0	0	0	0	0	0	- toonnoo_ttpm_sobb
	303	36358	0	0	54	50	1	1	65	0	2	0	0	1	357	341	29	193	287	- uɓiuəq
	1255	1120	4	0	1	40	Q	4	2	0	0	0	0	0	61	14	53	181	17	- ɓuitooq2_q16
	arp_spoofing -	benign -	ddos_mqtt_connect -	ddos_mqtt_publish -	dos_mqtt_connect -	dos_mqtt_publish -	malformed_mqtt -	os_scan -	ping_sweep -	port_scan -	vul_scan -	ddos_icmp -	- uks_sobb	ddos_tcp -	- dpn <sup>-</sup> sopp	dos_icmp -	- u/s_sob	dos_tcp -	- dpn <sup>-</sup> sop	

IAENG International Journal of Computer Science

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

			- 1/2000		- 150000		- 125000			- 100000		- 75000			- 50000		- 25000			° -
	32	28	0	0	0	0	0	0	0	0	0	0	0	0	m	13	1	64	527	- dpn <sup>-</sup> sop
	178	722	0	2	2	0	m	0	1	0	2	1	0	2	59	1123	24	21360	88	- dɔɔ̥¯sop
	1	6	0	0	0	0	0	0	0	0	0	0	0	0	1	19	86	4	6	- u∕is <sup>−</sup> sop
	12	191	0	1	0	0	e	0	0	0	0	1	0	0	17	2304	23	436	70	- dwɔi_sob
	105	342	0	0	1	0	0	0	0	0	0	0	0	0	1112	15	0	20	14	- dpn <sup>-</sup> sopp
	0	0	1	2	20	4	1	96	67	0	Ζ	159	14	137296	0	1	0	0	0	- dɔɔ̥¯sopp
	0	0	0	4	58	0	0	0	7	2	1	4	81279	1	0	0	0	m	0	- u∕is <sup>−</sup> sopp
sting Data	0	1	0	0	7	£	1	1	82	0	1	98416	129	£	0	0	0	0	0	- dɯɔi¯sopp
Confusion Matrix - K-Nearest Neighbors Testing Data	0	0	0	1	5870	0	0	2	m	0	7928	0	8	0	0	0	0	0	0	- ueos_luv Solo
-Nearest N	0	0	0	0	0	0	0	0	0	3123	0	0	0	0	0	0	0	0	0	Predicted Labels
n Matrix - K	0	0	9	1	0	11	0	12	98229	0	0	0	4	218	0	0	0	0	0	- dəəws_pniq
Confusio	0	1	13	2	1	137	33	156012	1	0	0	0	0	27	0	0	0	1	0	- นยวร ีรด
	0	1	21	0	0	414	179851	83	1	0	0	m	4	0	0	0	1	0	0	- malformed_mqtt -
	0	0	46	0	0	171505	2471	46	0	0	1	10	1	0	0	0	0	1	0	- dailduq_JJpm_2ob
	0	2	0	m	2350	0	0	1	1	0	545	0	17	0	0	0	0	0	0	- tɔəunoɔ_ttpm_zob
	1	0	0	41900	105	0	0	0	0	9	18	1	639	0	0	0	0	0	0	- dailduq_ttpm_aobb
	0	2	195605	0	0	321	235	162	10	0	0	0	1	m	0	0	0	1	0	- toennoo_ttpm_sobb
	353	35087	0	0	2	1	0	1	0	0	2	0	0	1	415	324	20	413	307	- npinəd
	- 1062	- 1221	0	0	0	- 1	0	0	0	0	0	0	0	0	- 140	- 35	- 19	319	- 19	- ɓuijoods <sup>–</sup> d.e
	arp_spoofing -	benign -	ddos_mqtt_connect.	ddos_mqtt_publish	dos_mqtt_connect.	dos_mqtt_publish	malformed_mqtt	os_scan -	ping_sweep.	bort_scan	vul_scan-	ddos_icmp -	- uks_sobb	ddos_tcp -	- dpn <sup>-</sup> sopp	dos_icmp -	- uks_sob	dos_tcp -	- dpn <sup>-</sup> sop	

IAENG International Journal of Computer Science

sıəqer ənu 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.

		0.5.5					0.40						1.10								
												capture	•				00 (06)		.1.00.	.f., (	20)
Etherne																9.10.	od (20.	dd.t	24.09.		od)
Interne																	240		100		
Transmi												ort: 010	,000	Seq:	4/2	, ACK	: 348,	Len	: 189		
MQ Tele										-											-
		-	: 0x	30, M	essa	ige I	ype:	Pub	115h	mes	ssage,	QoS Le	vel:	At	most	once	delive	ry (	⊢1re	and	Forge
Msg																					
_		ength			٦.																
		heart		e_dat	а																
_	-	: 313			<b>_</b>			1. 1													
MQ Tele		-	-			-				-			,								-
		-	: 0X	30, 1	essa	ige i	ype:	Pub	1150	mes	ssage,	QoS Le	vel:	AT	most	once	dellve	ry (	Fire	and	Forge
Msg																					
		ength																			
		tempe		re_da	ta																
	-	: 333	_																		
MQ Tele																					
		-	: 0x	30, M	essa	ige T	ype:	Pub	lish	Mes	ssage,	QoS Le	vel:	At	most	once	delive	ry (	Fire	and	Forge
Msg																					
Tori	c le	ength																			
Topi	c: ł	heart	_rat		а																
Topi Mess	c: H age	heart : 323	_rat 232	e_dat	1																
Topi Mess MQ Tele	c: H age met	heart : 323 ry Tr	_rat 232 ansp	e_dat ort F	Proto																
Topi Mess MQ Tele	c: H age met	heart : 323 ry Tr	_rat 232 ansp	e_dat ort F	Proto							QoS Le	vel:	At	most	once	delive	ery (	(Fire	and	Forge
Topi Mess MQ Tele	c:   age met er	heart : 323 ry Tr Flags	_rat 232 ansp	e_dat ort F	Proto							QoS Le	vel:	At	most	once	delive	ry (	(Fire	and	Forge
Topi Mess MQ Tele > Head Msg	c: H age met er H Len:	heart : 323 ry Tr Flags	_rat 232 ansp : 0x	e_dat ort F 30, M	Proto							QoS Le	vel:	At	most	once	delive	ry (	(Fire	and	Forge
Topi Mess MQ Tele > Head Msg Topi 00 e6	c: H age met er H Len: c Le	heart : 323 ry Tr Flags : 21 ength e4 09	_rat 232 ansp : 0x : 17 fc	e_dat ort F 30, M 8a 00	Proto lessa	ige T 10	ype: cb 1	Pub 7 60	lish 08	Mes 00 4	ssage, 45 02	QoS Le		At		once	delive	ry (	(Fire	and	Forge
Topi Mess MQ Tele > Head Msg Topi 100 e6 110 00	c: F age emet er F Len: c Le aa f f1	heart : 323 ry Tr Flags : 21 ength e4 09 31 b0	_rat 232 ansp : 0x : 17 fc 40	e_dat ort F 30, M 8a 00 00 40	Proto lessa	ige T 10 73	ype: cb 1 5f c	Pub 7 60 0 a8	08 89	Mes 00 4 fa d	ssage, 45 02 c0 a8		' ).@.	` s_··	· · E ·	once	delive	ry (	(Fire	and	Forge
Topi Mess MQ Tele > Head Msg Topi 100 e6 110 00 120 89	c:   age met er   Len c Le f1 : aa (	heart : 323 ry Tr Flags : 21 ength e4 09 31 b0 07 5b	_rat 232 ansp : 0x : 17 fc 40 f0	e_dat ort F 30, M 8a 00 00 40 dc 8c	Proto lessa 27 06 d4	10 10 73 95	ype: cb 1 5f c 3c e	Pub 7 60 0 a8 7 9f	08 89 b5	00 4 fa 0 7a 8	55age, 45 02 c0 a8 80 18	···1·@ ···[·	' ).@.	` s .<	••E• •z••	once	delive	ry (	(Fire	and	Forge
Topi Mess. MQ Tele > Head Msg Topi 100 e6 110 00 120 89 130 00	c:   age emet Len c Le aa f1 : aa ( 40	heart : 323 ry Tr Flags : 21 ength e4 09 31 b0 07 5b 83 4b	_rat 232 ansp : 0x : 17 fc 40 f0 00	e_dat ort F 30, M 8a 00 00 40 dc 8c 00 01	Proto lessa 0 27 0 06 : d4 . 01	10 73 95 08	ype: cb 1 5f c 3c e 0a 6	Pub 7 60 0 a8 7 9 <del>f</del> 0 84	08 89 b5 70	Mes 00 4 fa 0 7a 8 38 6	45 02 c0 a8 80 18 e3 cb	···· ···[· ·@·K·	'	s` s	••E• •z•• p8••	once	delive	ry (	(Fire	and	Forge
Topi Mess. MQ Tele > Head Msg Topi 00 e6 10 00 20 89 30 00 40 2b	c: H age met er H Len c Le f1 : aa ( 40 H	heart 323 ry Tr Flags : 21 ength e4 09 31 b0 07 5b 83 4b 30 14	_rat 232 ansp : 0x : 17 fc 40 f0 00 00	e_dat ort F 30, M 8a 00 00 40 dc 8c 00 01 0f 68	27 9 27 9 06 : d4 . 01 65	10 73 95 08 61	ype: cb 1 5f c 3c e 0a 6 72 7	Pub 7 60 0 a8 7 9f 0 84 4 5f	08 89 55 70 72	Mes 00 4 fa 0 7a 8 38 6 61 1	45 02 c0 a8 80 18 e3 cb 74 65	···1·@ ···[· ·@·K· +·0··	).@. .he	s` .< `.	··E· ·z·· p8··	once	delive	ry (	(Fire	and	Forge
Topi Mess. MQ Tele > Head Msg Topi 100 e6 110 00 120 89 130 00 140 2b 150 5f	c:   age met er f Len: c Le f1 : aa ( 40 ) 64 (	heart 323 ry Tr Flags : 21 ength e4 09 31 b0 07 5b 83 4b 30 14 51 74	_rat 232 ansp : 0x : 17 fc 40 f0 00 .00 .61	e_dat ort F 30, M 8a 00 00 40 dc 8c 00 01 0f 68 31 39	Proto iessa 0 27 0 06 : d4 . 01 : 65 . 31	10 73 95 08 61 30	ype: cb 1 5f c 3c e 0a 6 72 7 14 0	Pub 7 60 0 a8 7 9f 0 84 4 5f 0 10	08 89 55 70 72 74	00 4 fa 0 7a 8 61 1 65 0	45 02 c0 a8 80 18 e3 cb 74 65 6d 70	1.@ [. .@.K. +.0 _data	• @ • • he •191	s` .< art_ 0	··E· p8·· rate	once	delive	ry (	(Fire	and	Forge
Topi Mess. MQ Tele > Head Msg Topi 00 e6 10 00 20 89 30 00 40 2b 50 5f 160 65	c:   age met er f Len c Le f1 : aa ( 40 ) 64 ( 72 )	heart : 323 ry Tr Flags : 21 ength e4 09 31 b0 07 5b 83 4b 83 4b 30 14 61 74	_rat 232 ansp : 0x : 17 fc 40 f0 00 .00 .00 .00	e_dat ort F 30, M 8a 00 00 40 dc 8c 00 01 0f 68 31 39 72 65	Proto lessa 06 01 06 01 05 31 5f	10 73 95 08 61 30 64	ype: cb 1 5f c 3c e 0a 6 72 7 14 0 61 7	Pub 7 60 0 a8 7 9f 0 84 4 5f 0 10 4 61	08 89 55 70 72 74 33	00 4 fa 0 7a 8 61 1 65 0 36 1	45 02 c0 a8 80 18 e3 cb 74 65 6d 70 30 14	···1.@ ···[· ·@·K· +·0·· _data eratu	' .he 191	s .< art_ 0 data	··E· p8·· rate temp 360·	once	delive	ry (	(Fire	and	Forge
Topin Mess MQ Tele > Head Msg Topin 100 e6 110 00 120 89 130 00 140 2b 150 5f 160 65 170 00	c:   age met er   Len c Le aa ( 40 01 64 ( 72 01	heart : 323 ry Tr Flags : 21 ength e4 09 31 b0 07 5b 83 4b 30 14 61 74 61 74 61 74	_rat 232 ansp : 0x : 17 fc 40 f0 00 .00 .00 .00 .00 .00 .00 .00 .00	e_dat ort F 30, M 8a 00 8a 00 00 40 dc 8c 00 01 0f 68 31 39 72 65 72 74	Proto lessa 27 06 : d4 : 01 : 5f	10 73 95 08 61 30 64 72	ype: cb 1 5f c 3c e 0a 6 72 7 14 0 61 7	Pub 7 60 0 a8 7 9f 0 84 4 5f 0 10 4 61 4 65	08 89 55 70 72 74 33 5f	00 4 fa ( 7a 8 61 1 65 ( 36 2 64 (	45 02 c0 a8 80 18 e3 cb 74 65 6d 70 30 14 61 74	1-@ [- -@-K- +-0 _data eratu <mark>he</mark> a	).@. .he 1191 irre_	s .< art_ 0 data rate	··E· p8·· rate temp 360· _dat	once	delive	ry (	(Fire	and	Forge
Topin MQ Tele > Head Msg Topin 100 e6 110 00 120 89 130 00 130 00 130 00 130 5f 150 5f 160 65 170 00 180 61	c:   met er   Len: c Le f1 : aa ( 40   64   72   0f 32 :	heart 323 ry Tr Flags : 21 ength e4 09 31 b0 07 5b 83 4b 83 4b 30 14 61 74 61 74 68 65 32 32	_rat 232 ansp : 0x : 17 fc 40 f0 00 61 .75 61 30	e_dat ort F 30, M 8a 00 00 40 dc 8c 00 01 0f 68 31 39 72 65 72 74 15 00	27 9 27 9 06 : d4 . 01 65 9 31 5 f 5 f 9 11	10 73 95 61 30 64 72 6f	ype: cb 1 5f c 0a 6 72 7 14 0 61 7 78 7	Pub 7 60 0 a8 7 9f 0 84 4 5f 0 10 4 61 4 65 9 67	08 89 55 70 72 74 33 5f 65	00 4 fa 0 7a 8 61 1 65 0 36 2 64 0 6e 5	45 02 c0 a8 e3 cb 74 65 64 70 30 14 61 74 55 6c	1.@ [. .@.K. +.0 _data eratu hea a2220	' 	s 	··E· p8·· rate temp 360 <u>dat</u> en_1	once	delive	iry (	(Fire	and	Forge
Topi Mess. MQ Tele > Head Msg Topi 100 e6 110 00 120 89 130 00 140 2b 150 5f 166 65 170 00 180 61 190 65	c:   age: met er   Len: c Le aa ( f1 : aa ( 40 ) 64 ( 72 ( 01 : 76 ( 32 : 76 (	heart 323 ry Tr Flags 21 ength 64 09 31 b0 07 5b 83 4b 30 14 61 74 61 74 68 65 32 32 32 65 66 65 66 65 66 65 66 66 66	_rat 232 ansp : 0x : 17 fc 40 f0 00 61 .75 61 30 5f	e_dat ort F 30, M 8a 00 00 40 dc 8c 00 01 0f 68 31 39 72 65 72 74 15 00 64 61	27 9 06 : d4 . 01 5 f 11 . 74	10 73 95 61 30 64 72 6f	ype: cb 1 5f c 3c e 0a 6 72 7 14 0 61 7 78 7 38 3	Pub 7 60 0 a8 7 9f 0 84 4 5f 0 10 4 61 4 65 9 67 6 30	08 89 b5 70 72 74 33 5f 65 15	00 4 fa 0 7a 8 61 1 65 0 66 1 66 1 66 1	45 02 60 a8 60 18 63 65 64 70 30 14 51 74 55 6c 11 6f	[- [- [- 		s .< art_ 0 data rate oxyg a860	E- -z p8 rate temp 360- _dat en_1 0	once	delive	ry (	(Fire	and	Forge
Topin MQ Tele > Head Msg Topin 100 e6 110 00 120 89 130 00 130 00 130 00 130 5f 150 5f 160 65 170 00 180 61	c:   age: met ler   Len: c Le aa ( f1 : aa ( 40   01 : 64 ( 72 ( 0f 32 : 76 ( 79 (	heart 323 ry Tr Flags : 21 ength e4 09 31 b0 07 5b 83 4b 40 7 5b 83 4b 461 74 61 74 61 74 61 74 61 65 6c 65 6c 67 65	_rat 232 ansp : 0x : 17 fc 40 f0 00 . 61 . 75 61 30 5f 6e	e_dat ort F 30, M 8a 00 00 40 dc 8c 00 01 0f 68 31 39 72 65 72 74 15 00 64 61 55 6c	27 0 27 0 06 : d4 . 01 5 f 0 11 . 74 : 65	10 73 95 08 61 30 64 72 6f 61 76	ype: cb 1 5f c 0a 6 72 7 14 0 61 7 78 7 38 3 65 6	Pub 7 60 0 a8 7 9f 0 84 4 5f 0 10 4 61 4 65 9 67 6 30 c 5f	08 89 55 70 72 74 33 5f 65 15 64	00 4 fa 0 7a 8 61 5 65 0 66 9 66 9 61 5	45 02 45 02 45 02 45 03 80 18 80 18 180 18 180 18 180 18 180 18	1.@ [. .@.K. +.0 _data eratu hea a2220		s  art_ data rate oxyg a860 vel_	··E· p8·· rate temp 360· en_1 ··o data	once	delive	iry (	(Fire	and	Forge
Topi. Mess. MQ Tele > Head Msg   Topi. 100 e6 110 00 120 89 130 00 140 2b 150 5f 166 65 170 00 180 61 190 65 190 65 190 65 190 78	c:   age emet Len c Le f1 aa ( f1 ( f1	heart 323 ry Tr Flags : 21 ength e4 09 31 b0 07 5b 83 4b 40 74 61 74 61 74 61 74 61 74 61 74 61 65 6c 67 65 30 14	_rat 232 ansp : 0x : 17 fc 40 f0 00 61 .75 61 30 5f 6e .00	e_dat ort F 30, M 8a 00 00 40 dc 8c 00 01 831 39 72 65 72 74 15 00 64 61 55 6c 10 74	27 06 06 01 06 01 06 01 05 01 05 01 05 01 05 01 05 05 05 05 05 05 05 05 05 05 05 05 05	10 73 95 61 30 64 72 6f 61 76 6d	ype: cb 1 5f c 3c e 0a 6 72 7 14 0 61 7 78 7 38 3 65 6 70 6	Pub 7 60 0 a8 7 9f 0 84 4 5f 0 10 4 61 9 67 6 30 c 5f 5 72	08 89 55 70 72 74 33 5f 65 15 64 61	00 4 fa 0 7a 8 61 2 65 0 64 0 66 1 66 1 61 2 61 2 61 2 61 2 61 2 61 2	45 02 45 02 45 02 45 03 80 18 80 18 83 cb 74 65 56 70 30 14 51 74 51 6c 11 6f 74 61 75 72			s s art_ 0 data nate oxyg a860 vel_ mper	··E· p8· rate temp 360· dat en_1 ···o data atur	once	delive	iry (	(Fire	and	Forge
Topi Mess. MQ Tele > Head Msg   Topi 100 e6 110 00 120 89 130 00 140 2b 150 5f 156 65 170 00 180 61 190 65 180 61 190 65 180 78 180 37	c:   age emet Len: c Le f1 : aa ( f1 : aaa ( f1 : aa ( f1 : aa) (f1 : aa) (f1 : aa) (f1 : aa (f1 : aa) (f) aa (f1 : aa) (f) (f) aa) (f) (f) (f) (f	heart 323 ry Tr Flags 21 ength e4 09 31 b0 07 5b 83 4b 30 14 61 74 61 74 61 74 65 6c 65 6c 67 65 30 14 64 61	_rat 232 ansp : 0x : 17 fc 40 f0 00 61 . 75 61 30 5f 6e 00 74	e_dat ort F 30, M 8a 00 00 40 dc 8c 00 01 0f 68 31 39 72 65 72 74 15 00 64 61 55 6c 10 74 61 33	27 9 06 65 31 5 5f 5 11 5 5f 111 . 74 65 65 38	10 73 95 08 61 30 64 72 6f 61 76 6d 30	ype: cb 1 5f c 3c e 0a 6 72 7 14 0 61 7 78 7 38 3 65 6 70 6 0f 0	Pub 7 60 0 a8 7 9f 0 84 4 5f 0 10 4 61 4 65 9 67 6 30 c 5f 5 72 0 0c	08 89 b5 70 72 74 33 5f 65 15 64 61 61	00 4 fa ( 7a 8 65 ( 36 5 64 ( 66 5 00 1 74 1 69 1	45 02 45	1.@ [. .@-K. +-0 _data eratu <u>hea</u> a2220 evel_ xygen 750		s art_ 0 data oxyg a860 vel_ mper 0	E- -z p8 temp 360- data atur airf	once	delive	rry (	(Fire	and	Forge
Topi       MQ     Tele       MQ     Tele       MQ     Tele       MQ     Fead       MQ     Topi       Topi     Topi <td>c:   age met Len: c Le aa ( f1 : aa ( f1 : f1 : f1 : f1 : f1 : f1 : f1 : f1 :</td> <td>heart 323 ry Tr Flags : 21 ength e4 09 31 b0 07 5b 83 4b 30 14 61 74 61 74 61 74 61 74 65 32 32 32 32 65 6c 67 65 30 14 64 61 77 5f</td> <td>_rat 232 ansp : 0x : 17 fc 40 f0 00 61 75 61 30 5f 6e 00 74 64</td> <td>e_dat ort F 30, M 8a 00 00 40 dc 8c 00 01 0f 68 31 39 72 65 72 74 15 00 64 61 55 6c 10 74 61 33 61 74</td> <td>27 0 27 0 06 : d4 . 01 5 ff 1 11 . 74 : 65 . 65 . 38 . 61</td> <td>10 73 95 08 61 30 64 72 6f 61 76 6d 30 31</td> <td>ype: cb 1 5f c 0a 6 72 7 14 0 61 7 78 7 38 3 65 6 70 6 0f 0 30 1</td> <td>Pub 7 60 0 a8 7 9f 0 84 4 5f 0 10 4 61 4 65 9 67 6 30 c 5f 5 72 0 0c 1 00</td> <td>08 89 b5 70 72 74 33 5f 65 15 64 61 61 0d</td> <td>00 4 fa 0 7a 8 61 1 65 6 66 9 66 9 61 1 74 2 69 1 70 1</td> <td>45 02 45 0 45 0</td> <td>1-@ [- -@-K- +-0 _data eratu hea 22200 evel_ xygen 750 e_dat</td> <td></td> <td>s art_ 0 data nate oxyg a860 vel_ mper 0 10</td> <td>E- -z p8 rate temp 360- data en_1 -o data atur airf -pul</td> <td>once</td> <td>delive</td> <td>ry (</td> <td>(Fire</td> <td>and</td> <td>Forge</td>	c:   age met Len: c Le aa ( f1 : aa ( f1 : f1 : f1 : f1 : f1 : f1 : f1 : f1 :	heart 323 ry Tr Flags : 21 ength e4 09 31 b0 07 5b 83 4b 30 14 61 74 61 74 61 74 61 74 65 32 32 32 32 65 6c 67 65 30 14 64 61 77 5f	_rat 232 ansp : 0x : 17 fc 40 f0 00 61 75 61 30 5f 6e 00 74 64	e_dat ort F 30, M 8a 00 00 40 dc 8c 00 01 0f 68 31 39 72 65 72 74 15 00 64 61 55 6c 10 74 61 33 61 74	27 0 27 0 06 : d4 . 01 5 ff 1 11 . 74 : 65 . 65 . 38 . 61	10 73 95 08 61 30 64 72 6f 61 76 6d 30 31	ype: cb 1 5f c 0a 6 72 7 14 0 61 7 78 7 38 3 65 6 70 6 0f 0 30 1	Pub 7 60 0 a8 7 9f 0 84 4 5f 0 10 4 61 4 65 9 67 6 30 c 5f 5 72 0 0c 1 00	08 89 b5 70 72 74 33 5f 65 15 64 61 61 0d	00 4 fa 0 7a 8 61 1 65 6 66 9 66 9 61 1 74 2 69 1 70 1	45 02 45 0 45 0	1-@ [- -@-K- +-0 _data eratu hea 22200 evel_ xygen 750 e_dat		s art_ 0 data nate oxyg a860 vel_ mper 0 10	E- -z p8 rate temp 360- data en_1 -o data atur airf -pul	once	delive	ry (	(Fire	and	Forge

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

- 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-
- [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," *Proceedia 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.