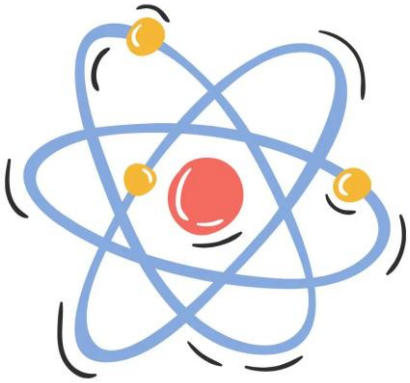


ISSN: 1672 - 6553

JOURNAL OF DYNAMICS AND CONTROL

VOLUME 10 ISSUE 02: P1-12

OPTIMIZED FEATURE SELECTION OF CYBERATTACK DETECTION IN HEALTHCARE IOMT DEVICES USING THE MULTI-PROTOCOL DATASET BASED ON ADVANCE MACHINE LEARNING METHOD

Kshitiz Agarwal, Sandhya Sharma

Department of Electronics and Communication Engineering, Suresh Gyan Vihar University, Jaipur, India

JOURNAL OF DYNAMICS AND CONTROL
https://doi.org/10.71058/jodac.v10i02001

OPTIMIZED FEATURE SELECTION OF CYBERATTACK DETECTION IN HEALTHCARE IOMT DEVICES USING THE MULTI-PROTOCOL DATASET BASED ON ADVANCE MACHINE LEARNING METHOD

Kshitiz Agarwal*, Sandhya Sharma
Department of Electronics and Communication Engineering,
Suresh Gyan Vihar University, Jaipur, India
***Corresponding Author:** *agarwal_ksh@yahoo.com*

Abstract. *The growing integration of Internet of Medical Things (IoMT) devices in healthcare has brought important benefits for patient monitoring and medical data management, but it has also created new risks of cyberattacks. The current study applies statistical methods and feature selection techniques to the CI-CIoMT2024 multi-protocol dataset to understand attack behaviors and identify effective attributes for detection. The dataset contains 18 different types of attacks, grouped into classes such as distributed denial of service (DDoS), denial of service (DoS), reconnaissance, spoofing, and MQTT-based threats. Training data shows more than 1.6 million DDoS-UDP flows and more than 1.5 million DDoS-ICMP flows, while some categories like ping sweep and vulscan remain highly under-represented, reflecting a strong imbalance in attack distribution. Exploratory data analysis confirmed that 45 numeric features are present without missing values. Statistical tests such as Shapiro–Wilk and Kolmogorov–Smirnov showed that most variables do not follow a normal distribution, indicating non-linear behavior in network traffic. Kruskal–Wallis testing revealed significant differences in features such as Header_Length and Duration across classes. Correlation heatmaps highlighted strong dependencies between traffic indicators, underlining the importance of dimensionality reduction. Feature importance analysis from tree-based models identified IAT, Srate, Rate, fin_count, and Header_Length as the most discriminative attributes. These indicators capture variations in packet timing, session rate, and header properties that strongly separate attack categories from benign traffic. The findings highlight the effectiveness of combining statistical analysis with feature selection for enhancing IoMT security research. The outcome provides guidance for designing machine learning models that can handle imbalanced datasets while improving detection accuracy for healthcare device networks. Five different machine learning methods were selected for the present study for advance analysis which hwere following and have high level accuracy for this dataset.*

1 Introduction

The fourth industrial revolution had been described as a period marked by digital integration, automation, and advanced data processing across many sectors. Healthcare, manufacturing, logistics, and urban planning had all been influenced by the rapid spread of technologies such as the Internet of Things (IoT), artificial intelligence (AI), robotics, and big data analytics. These advances had allowed real-time collection and processing of information, which in turn had increased operational efficiency and supported new business and medical opportunities. In the healthcare domain, the integration of smart devices and connected environments had been recognized as Healthcare 4.0. Through connected sensors and intelligent algorithms, patient monitoring became more active, predictive care became possible, and diagnostic tools became faster. Smart healthcare systems had been supported by cloud computing, fog computing, and distributed IoT frameworks, allowing early intervention in chronic and acute medical conditions [1,2,3]. During the COVID-19 pandemic, several practical applications of smart healthcare technologies had been highlighted. Wearable devices had been applied for bladder monitoring, reducing patient discomfort and unnecessary visits to hospitals. Artificial intelligence models, including adaptive neuro-

https://doi.org/10.71058/jodac.v10i02001

fuzzy systems, had been applied for classification and detection of infections, improving diagnosis accuracy. Smart masks, enhanced facial recognition, and contact tracing applications had been introduced to reduce viral spread. These examples demonstrated how digital tools had already reshaped healthcare systems and daily life. At the same time, the increase in connected medical devices had created new risks and had widened the surface for cyberattacks [4-7].

The integration of computation, networking, and physical healthcare processes had been conceptualized as Cyber-Physical Systems (CPS). Such systems enabled synchronization of data flows between medical infrastructure and computational resources. Intelligent frameworks for early diagnosis of complex diseases had already been tested, showing promising results in conditions such as encephalitis. Hybrid machine learning models had been applied for anomaly detection in healthcare networks, improving trust and reliability of connected environments. However, these achievements had also drawn attention to critical vulnerabilities. The expansion of connected devices, especially Internet of Medical Things (IoMT) devices, had increased the likelihood of attacks such as denial-of-service, spoofing, and intrusion attempts targeting sensitive patient data [8,9,10]. Cyberattacks against IoMT devices had the potential to disrupt essential services, compromise patient privacy, and even threaten lives. Healthcare institutions had faced growing challenges in establishing effective defense mechanisms. Traditional intrusion detection systems (IDS) had provided partial protection, but modern cyberattacks had evolved into more complex and sophisticated threats. Manual detection had become nearly impossible due to the scale and frequency of incidents. At the same time, the shortage of skilled cybersecurity experts had made automated methods necessary. Organizations had realized that defenses required not only technical measures but also resource planning according to potential impact, secrecy, and safety considerations. These factors had reinforced the importance of adopting machine learning and deep learning solutions for cyberattack detection [11,12].

The evolution of Information and Communication Technologies (ICT) had provided new opportunities but had also created new vulnerabilities. Networks had expanded in scope, supporting paradigms such as cloud computing, edge computing, and multi-access edge computing (MEC). Applications such as IoT, IoV (Internet of Vehicles), IIoT (Industrial IoT), and IoMT had introduced distributed services that required high levels of confidentiality, integrity, and availability. Malicious actors had targeted these systems in order to compromise data transmission, gain unauthorized access, or disable operations. Safety-critical applications, including industrial control systems and connected medical devices, had demanded special attention. The scale of attacks launched annually against such infrastructures had been substantial, and conventional monitoring had failed to address the problem. In response, researchers had applied various machine learning and deep learning techniques to intrusion detection. Deep neural networks, convolutional neural networks, recurrent neural networks, autoencoders, generative adversarial networks, and transformer-based models had all been explored for anomaly detection and classification of attacks. These models had shown strong potential in experimental environments, often surpassing traditional detection methods. However, challenges such as false positives, lack of generalization across different environments, and difficulty in deployment had limited real-world adoption. The research community had therefore focused on building improved datasets, refining feature selection, and applying hybrid models to balance accuracy and interpretability [13,14,15].

The negative effects of cyberattacks had already been observed in many industries, from business interruptions to safety risks in healthcare. Attacks had compromised confidentiality, integrity, and availability of networks, undermining trust and exposing organizations to financial and reputational damage. The IoMT environment had been especially vulnerable because devices were often lightweight, resource constrained, and dependent on wireless communication. Protecting such devices required lightweight security mechanisms, robust detection systems, and efficient feature selection methods to ensure that attacks were identified without overwhelming system resources. The CICIoMT2024 [16] dataset had been introduced as a benchmark for studying cyberattacks against healthcare IoMT devices. It had been designed to capture traffic from a testbed of both real and simulated medical devices under a variety of protocols, including Wi-Fi, MQTT, and Bluetooth. A total of 18 different attacks had been launched against these devices, grouped into categories such as DDoS, DoS, reconnaissance, spoofing, and MQTT-based threats. The dataset had provided both benign and malicious traffic, recorded in packet captures and

https://doi.org/10.71058/jodac.v10i02001

pre-extracted feature CSV files. Its construction had aimed to create a realistic environment for evaluating intrusion detection methods and for analyzing the behavior of IoMT devices under different conditions [16].

An important challenge revealed by the dataset was class imbalance. DDoS-UDP and DDoS-ICMP flows had accounted for millions of records, while other classes such as ping sweep and vulscan had been represented by only hundreds or thousands of records. Such imbalance had mirrored real-world conditions, where some attacks were far more common than others. However, imbalance also introduced bias in machine learning models, as classifiers tended to focus on the majority classes while ignoring rare but critical threats. Addressing this imbalance required careful feature selection, statistical analysis, and resampling techniques. Exploratory data analysis of the CICIoMT2024 dataset had shown that 45 numeric features were available without missing values. Statistical tests such as Shapiro–Wilk and Kolmogorov–Smirnov had confirmed that most features did not follow normal distributions. Kruskal–Wallis tests had revealed significant differences across attack categories for features such as header length and duration. Correlation heatmaps had indicated strong dependencies between several variables, underscoring the need for dimensionality reduction. Feature importance analysis using tree-based models had highlighted inter-arrival time (IAT), session rate (Srate), overall rate, and header length as particularly strong indicators of attack presence [17,18, 19, 20].

The motivation for applying feature selection in this context had been twofold. First, reducing the number of features helped to minimize computational costs, which was important for real-time detection in resource-constrained IoMT environments. Second, selecting the most discriminative features improved detection accuracy by removing noise and redundant information. Combining statistical methods with machine learning feature selection had offered a balanced approach, providing both interpretability and predictive strength. This had aligned with the broader trend in cybersecurity research, where interpretable models and explainable AI methods were increasingly valued for building trust in automated systems. The combination of Industry 4.0 technologies, smart healthcare systems, and advanced cybersecurity methods had reflected a global effort to create safer, more resilient infrastructures. Digital twins, predictive analytics, and AI-based monitoring had already influenced healthcare delivery, logistics, and urban management. At the same time, gaps in cybersecurity had persisted, and attacks against IoMT devices had underlined the urgency of new solutions. Research on datasets such as CICIoMT2024 had provided the foundation for developing and benchmarking machine learning approaches tailored to healthcare environments. Such studies had contributed to better understanding of attack behaviors, more efficient feature engineering, and stronger protection for sensitive medical systems [21,22,23].

The growing complexity of healthcare IoT networks had created opportunities for innovation but also risks of cyberattacks. The CICIoMT2024 dataset had provided a valuable testbed for statistical analysis and machine learning approaches to intrusion detection. By focusing on feature selection and detailed analysis of traffic patterns, researchers had aimed to enhance the detection of diverse attacks while addressing class imbalance and system constraints. The insights gained from such efforts had been expected to support the design of efficient and accurate intrusion detection systems capable of protecting healthcare infrastructures in the era of Industry 4.0.

2 Material And Methods

2.1 Research Methodology

The methodology adopted for the study relied on a systematic process that combined benchmark datasets, feature engineering, and advanced machine learning approaches for cyberattack detection in healthcare IoMT environments. Three widely recognized datasets were considered: CICIoMT2024[16], CICIDS-2017[24], and CICIOt2023[25]. These datasets provided multi-protocol traffic records, diverse attack categories, and realistic IoT and IoMT traffic patterns, which created a reliable foundation for evaluating intrusion detection methods. Each dataset included both benign and malicious flows, covering attack vectors such as denial-of-service, distributed denial-of-service, spoofing, reconnaissance, and MQTT-based intrusions. Preprocessing played a key role in preparing the datasets for analysis. Raw traffic captured in packet format was converted into structured CSV files

https://doi.org/10.71058/jodac.v10i02001

containing numerical and categorical features. To ensure reliability, missing values were checked and corrected, infinite values were replaced with valid entries, and categorical labels were encoded into numerical form. The class imbalance present in the datasets, particularly in the CICIoMT2024 dataset, was analyzed to understand its impact on classification performance. Feature scaling was also applied to normalize numerical values and improve the stability of the learning process.

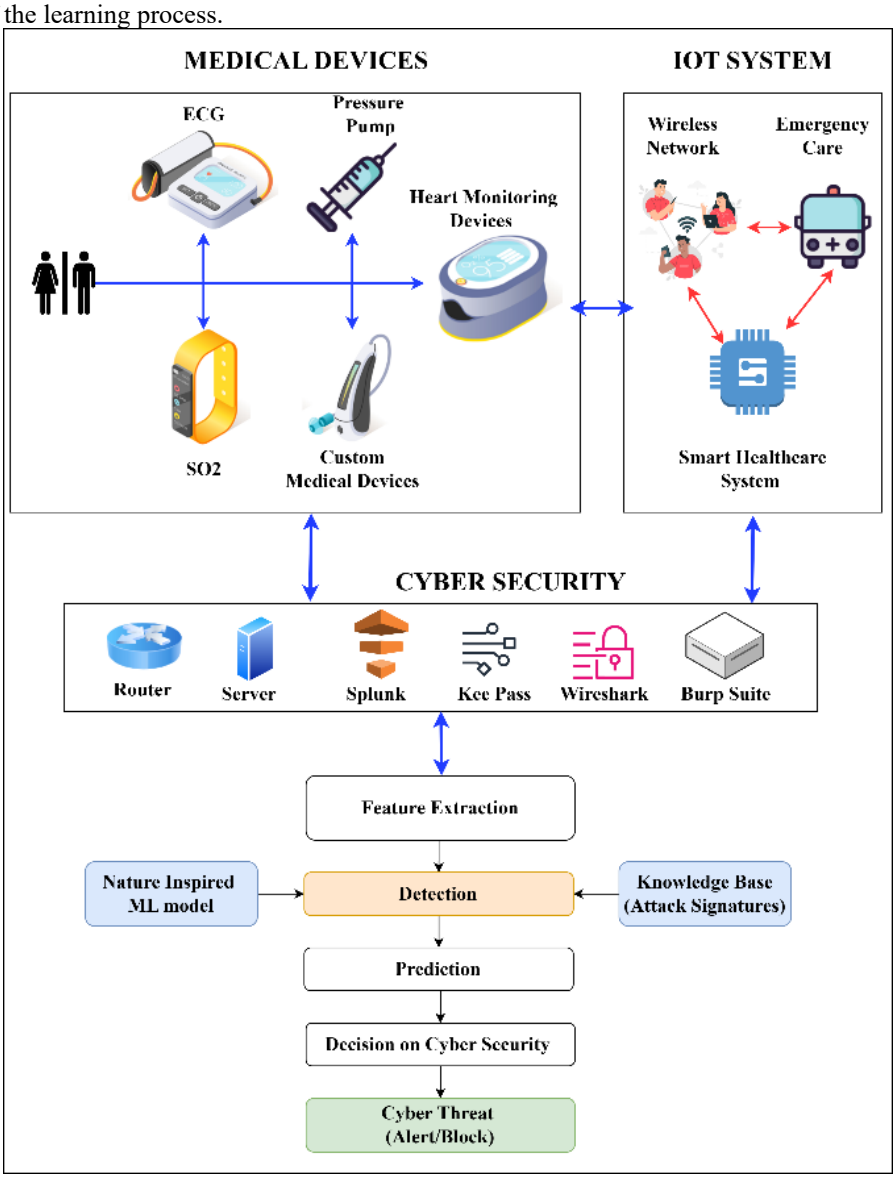


Fig. 1. Research flow diagram adopted in present study

Feature extraction followed as the next step, focusing on identifying the most informative indicators for distinguishing benign from malicious traffic. Statistical tests such as Shapiro–Wilk, Kruskal–Wallis, and correlation analysis were performed to highlight significant variables. Tree-based feature importance methods further ranked attributes including inter-arrival time (IAT), rate (Rate), session rate (Srate), and header length, which emerged as strong discriminative factors. This multi-stage analysis provided a reduced feature set that preserved the essential attack signatures while minimizing redundant information. The detection framework was built upon a nature-

https://doi.org/10.71058/jodac.v10i02001

inspired machine learning model integrated with a knowledge base of attack signatures. The process began with the extraction of relevant traffic features, followed by real-time detection and prediction of potential threats. The system then produced decisions regarding cybersecurity status and generated alerts or blocking commands when malicious activity was identified. As illustrated in the flow diagram, medical devices such as ECG monitors, pressure pumps, and custom IoMT tools communicated through IoT systems. These interactions were safeguarded by cybersecurity tools, which supplied data for feature extraction, learning, and classification. The combined pipeline ensured timely detection and response to cyber threats in smart healthcare environments.

2.2 Dataset Selection

The selection of datasets played an important role in designing the study. The CICIoMT2024[16] dataset was chosen because it contained realistic traffic patterns from healthcare devices connected to IoT networks. It included both real and simulated medical devices such as ECG monitors, pressure pumps, and wearable systems. The dataset recorded normal and malicious traffic under several protocols including Wi-Fi, MQTT, and Bluetooth. A total of 18 attack categories were present, covering denial of service, distributed denial of service, reconnaissance, spoofing, and protocol-based attacks. This wide coverage made the dataset suitable for training and testing intrusion detection models in a healthcare environment.

The dataset contained two main splits, train and test. The train split had more than 7.1 million records while the test split contained about 1.6 million records. Both splits carried 45 numerical features and 2 object-type columns, including the attack labels. No missing values were observed. Class imbalance was evident, as some classes such as DDoS-UDP and DDoS-ICMP dominated the records, while rare attacks such as ping sweep and vulscan had very few entries. This imbalance reflected real network behavior, where a few attack types occurred more often than others.

Table 1. Statistical analysis of all factors of the dataset [16]

Description	Count	mean	Description	Count	mean
Header_Length	1612117	3.17E+04	**SSH**	1612117	7.65E-05
Protocol Type	1612117	8.07E+00	**IRC**	1612117	7.68E-06
Duration	1612117	6.42E+01	**TCP**	1612117	4.08E-01
Rate	1612117	1.80E+04	**UDP**	1612117	3.14E-01
Srate	1612117	1.80E+04	**DHCP**	1612117	6.82E-07
Drate	1612117	0.00E+00	**ARP**	1612117	6.79E-04
fin_flag_number	1612117	5.32E-03	**ICMP**	1612117	2.77E-01
syn_flag_number	1612117	1.51E-01	**IGMP**	1612117	3.81E-06
rst_flag_number	1612117	4.23E-02	**IPv**	1612117	9.99E-01
psh_flag_number	1612117	2.12E-02	**LLC**	1612117	9.99E-01
ack_flag_number	1612117	1.00E-01	**Tot sum**	1612117	6.25E+02
ece_flag_number	1612117	5.36E-06	**Min**	1612117	5.53E+01
cwr_flag_number	1612117	3.22E-06	**Max**	1612117	6.83E+01
ack_count	1612117	2.82E-02	**AVG**	1612117	5.95E+01
syn_count	1612117	2.87E-01	**Std**	1612117	4.53E+00
fin_count	1612117	7.00E-02	**Tot size**	1612117	5.95E+01
rst_count	1612117	5.09E+01	**IAT**	1612117	8.47E+07
HTTP	1612117	2.03E-03	**Number**	1612117	9.50E+00
HTTPS	1612117	2.67E-03	**Magnitue**	1612117	1.04E+01
DNS	1612117	1.28E-04	**Radius**	1612117	6.41E+00
Telnet	1612117	7.62E-06	**Covariance**	1612117	1.64E+03
SMTP	1612117	7.62E-06	**Variance**	1612117	8.76E-02
			Weight	1612117	1.42E+02

Descriptive statistics for the dataset confirmed large variation across features. For example, the “Header_Length” attribute had a maximum value of more than 9.8 million, while inter-arrival time (IAT) had an average of over 8.4e+07. Features like “Rate” and “Srate” showed wide ranges, making normalization important before model training.

https://doi.org/10.71058/jodac.v10i02001

Table 2. 18 classes selected from the dataset [16]

Class	Train Samples	Test Samples	Proportion (%)
ddos-udp	16,35,956	3,62,070	22.86
ddos-icmp	15,36,820	3,49,698	21.48
ddos-tcp	8,04,465	1,82,597	11.24
ddos-syn	8,01,946	1,72,397	11.21
dos-udp	5,66,949	1,37,553	7.92
dos-syn	4,41,895	98,595	6.18
dos-icmp	4,16,291	98,432	5.82
dos-tcp	3,80,384	82,096	5.32
benign	1,92,732	37,607	2.69
ddos-connect_flood	1,73,036	41,916	2.42
port_scan	80,247	20,921	1.12
dos-publish_flood	44,376	8,505	0.62
ddos-publish_flood	27,623	8,416	0.39
os_scan	16,163	3,495	0.23
arp_spoofing	16,047	1,744	0.22
dos-connect_flood	12,773	3,131	0.18
malformed_data	5,130	1,747	0.07
vulscan	2,129	1,011	0.03
ping_sweep	740	186	0.01

The summary of the dataset is shown in Table 1. The CICIoMT2024 dataset included more than 7.1 million records with 18 different classes. Most samples came from DDoS and DoS attacks such as UDP, ICMP, TCP, and SYN, which together made up over 90% of the data. Benign traffic was much smaller at only 2.69%. Rare classes like ping sweep and vulscan had very few records. This imbalance showed real-world conditions where frequent attacks dominated, while uncommon threats were harder to detect.

2.3 Proposed ML Models

In the present study, the dataset was first cleaned to remove missing values, replace infinite values, and handle inconsistencies. After cleaning, statistical analysis was carried out to explore the structure of the data and to identify the most important features. Once the data was prepared, a set of machine learning models was selected for further analysis and evaluation. These models represented a mix of traditional approaches and advanced ensemble techniques to provide a fair comparison of performance. The first model applied was Logistic Regression, which had been one of the simplest yet effective classifiers for binary and multi-class problems. It estimated probabilities using a linear decision boundary and worked as a baseline model. Despite its simplicity, logistic regression was useful for understanding how well the cleaned dataset could be separated with linear methods.

The second model was the Random Forest classifier, an ensemble method that created multiple decision trees during training and combined their outputs for prediction. Random Forest was chosen because it handled high-dimensional data well, reduced overfitting, and provided feature importance rankings, which were valuable for this research. The third model was Gradient Boosting, which built decision trees sequentially. Each tree attempted to correct the errors of the previous one, leading to strong performance in many classification tasks. Gradient Boosting was considered because it improved accuracy through iterative learning. The fourth model was Support Vector Machine (SVM) with an RBF kernel. SVM was selected for its ability to work in high-dimensional spaces and to handle non-linear decision boundaries. It mapped the features into a higher dimension and then separated the classes with maximum margin, making it a powerful choice for complex datasets. Two advanced boosting methods were also included: XGBoost and LightGBM. Both were widely recognized for speed and accuracy in handling large-scale data. XGBoost applied regularization and optimized computation, while LightGBM improved efficiency with histogram-based algorithms. These models were suitable for imbalanced data and large datasets such as CICIoMT2024. These six models formed the core of the proposed approach. Their selection allowed the study to compare simple, ensemble, and gradient-based techniques for detecting cyberattacks in IoMT environments.

https://doi.org/10.71058/jodac.v10i02001

The performance of the proposed models was measured using standard classification metrics. Sensitivity or recall was calculated as the ratio of true positives to the sum of true positives and false negatives. Precision represented the ratio of true positives to the total predicted positives. Specificity measured the ratio of true negatives to the sum of true negatives and false positives. The F1-score balanced precision and recall, while accuracy considered all correctly classified instances in the dataset.

3 Results and Discussion

The statistical analysis of the CICIoMT2024 dataset provided valuable insights into its structure and highlighted patterns in both numerical and categorical features. The dataset contained more than 7.1 million records, split into training and testing sets, with 45 numerical columns and two categorical attributes. No missing values were found, which confirmed the completeness of the dataset and reduced the need for imputation. The class distribution analysis showed that the dataset was highly imbalanced. Most of the records came from a few dominant categories such as ddos-udp, ddos-icmp, ddos-tcp, and ddos-syn. These four classes together accounted for more than 65% of the total samples. In contrast, rare classes such as ping_sweep, vulscan, and malformed_data had very few instances. This imbalance reflected real-world attack scenarios where some threats occurred frequently while others were much less common. However, such imbalance posed challenges for classification models, as models might be biased toward majority classes unless balancing strategies were applied.

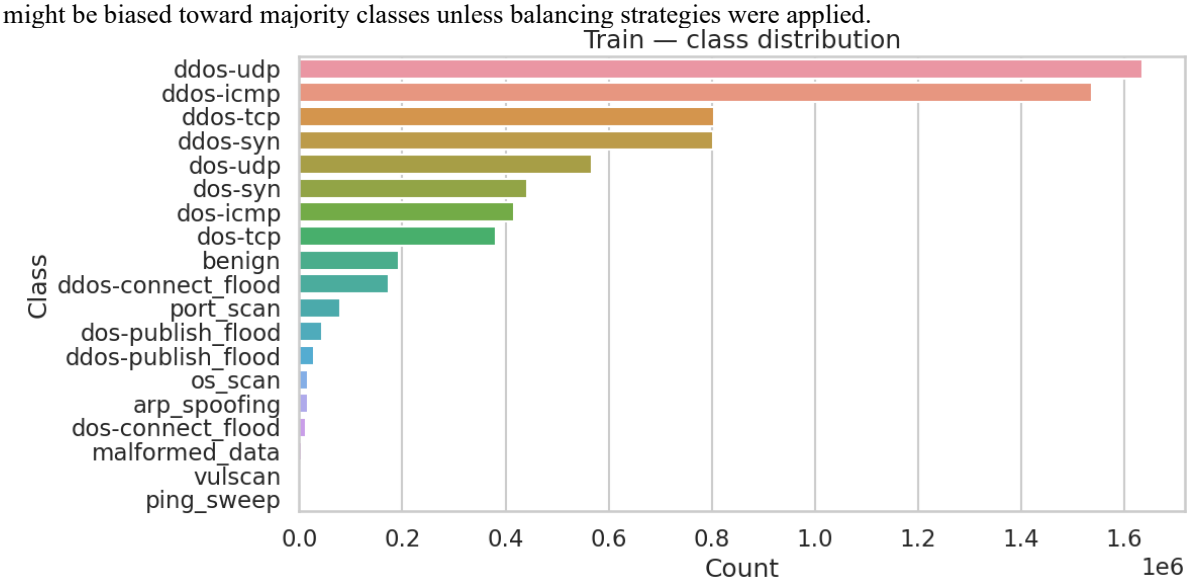


Fig. 2. Class distribution selected in present study (Train)

In terms of descriptive statistics, several features displayed high variability. For example, the Header_Length attribute had a mean of 29,609 with a very high standard deviation of 276,359, suggesting that most values were small, but a few extreme outliers were present, with the maximum value exceeding 9.8 million. Similarly, Rate and Srate showed large deviations, with many samples concentrated near zero but some reaching values in the millions. This heavy-tailed distribution was confirmed by the histograms, where the majority of values clustered near the lower end, and only a small number extended into very high ranges. These findings indicated that normalization or logarithmic scaling would be important before applying machine learning models.

https://doi.org/10.71058/jodac.v10i02001

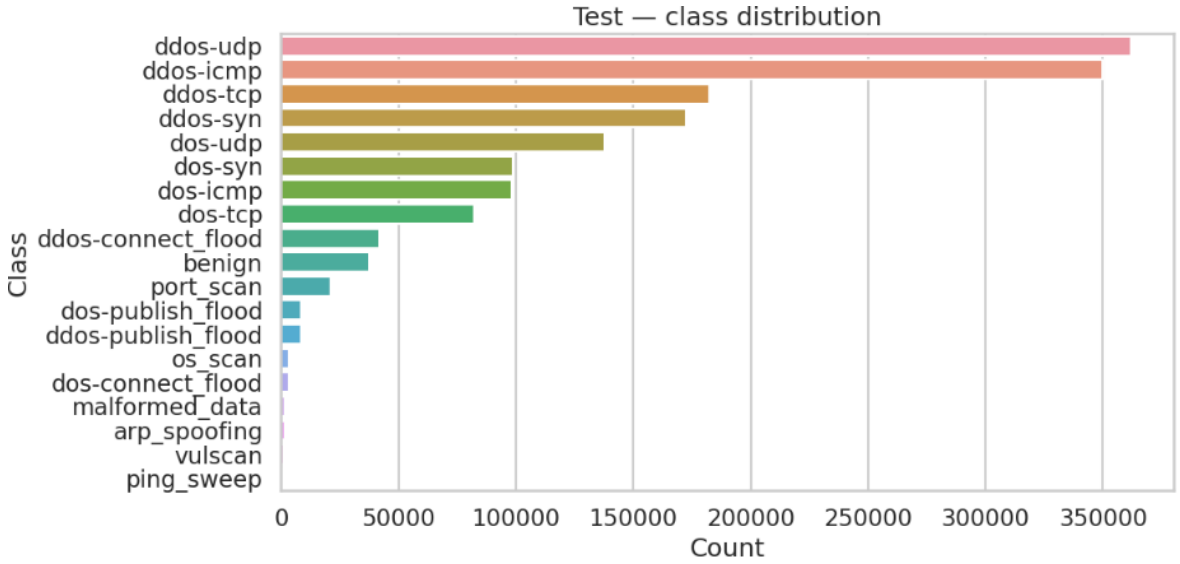
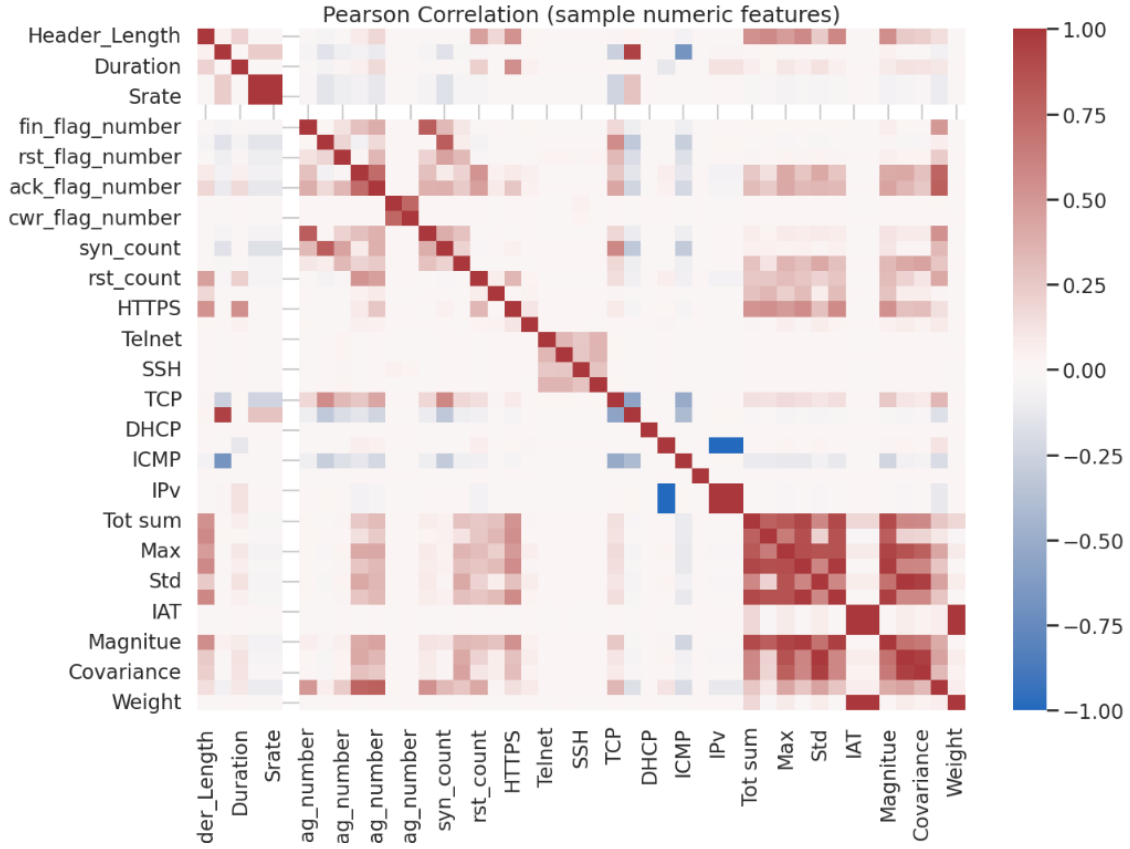


Fig. 3. Class distribution selected in present study (Test)

Other network-related attributes such as Duration had much lower variance. Most packets recorded a fixed duration of 64 units, with occasional deviations. Flag-related features (fin_flag_number, syn_flag_number, rst_flag_number, ack_flag_number) were binary or near-binary values, representing the presence or absence of certain TCP flags.



https://doi.org/10.71058/jodac.v10i02001

Fig. 4. Correlation analysis of the dataset factors

Their distributions were heavily skewed, with zeros dominating, which was expected because not all packets carried each type of flag. Protocol-specific features such as TCP, UDP, and ICMP followed binary representations. Nearly all traffic was IPv4 or LLC-based, as both variables showed average values close to one. This indicated that the dataset mainly reflected modern IP-based traffic, consistent with real IoMT environments. Attributes like Telnet, SMTP, and IRC had very low frequencies, representing rare protocol use in the captured traffic.

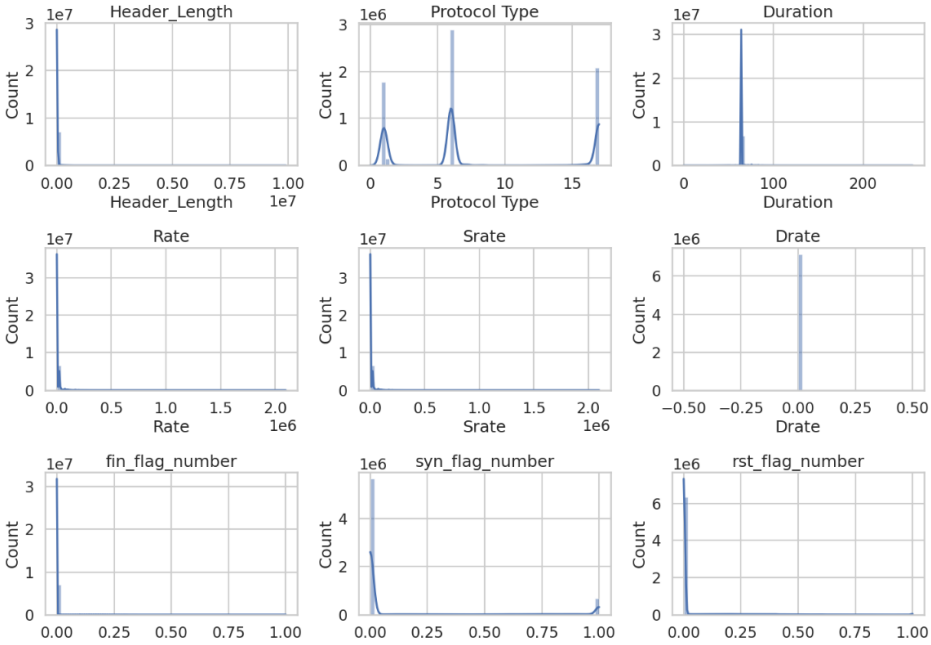


Fig. 5. Distribution analysis of the factors of the selected dataset

Another interesting attribute was IAT (inter-arrival time). The mean value was around 84 million with a standard deviation of 17 million. Although most values clustered around a fixed range, there were rare cases with extremely low or high times, which suggested bursty traffic patterns during certain attacks like DDoS floods. Similarly, variables such as Radius and Covariance showed wide ranges, which highlighted the complexity of captured traffic dynamics. The histograms and class distribution plots further emphasized these findings. The train and test distributions were consistent, with majority classes dominating across both sets. The histograms revealed that many features had skewed distributions, with long tails that could impact model performance if not handled properly.

https://doi.org/10.71058/jodac.v10i02001

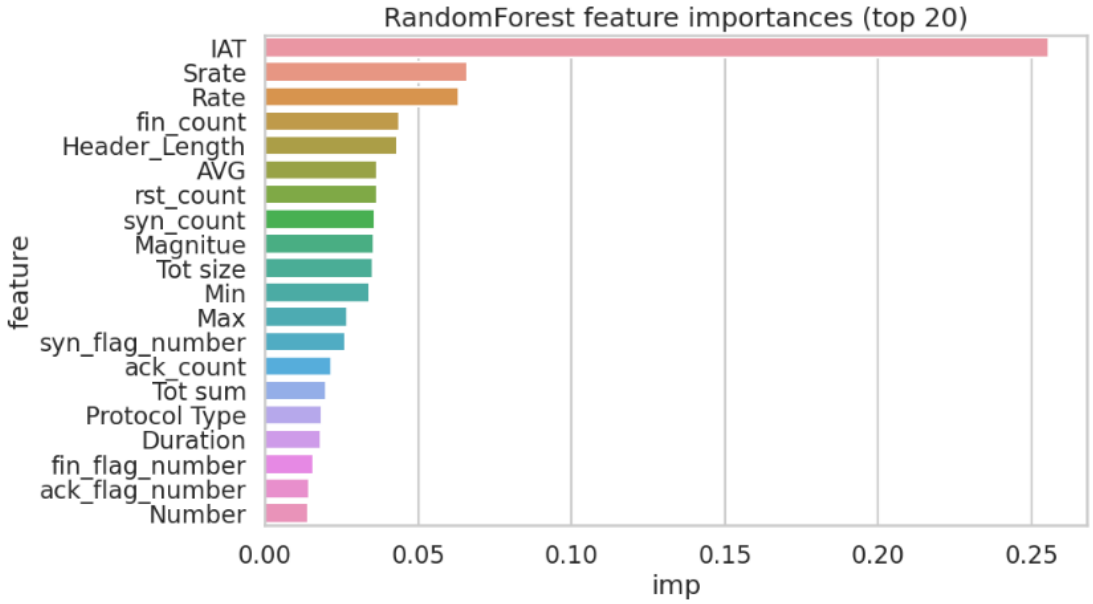


Fig. 6. Distribution analysis of the factors of the selected dataset using random forest method

The performance of the proposed machine learning models showed clear differences in their ability to handle the CICIoMT2024 dataset. The dataset contained multiple classes with significant imbalance, which directly influenced how each model performed. Logistic Regression was used as a baseline model. Its results revealed clear limitations in handling the complexity of this dataset. While the overall accuracy was 43%, the precision and recall across most classes were very low. For example, several classes such as dos-icmp, dos-tcp, arp_spoofing, and ping_sweep achieved zero precision, recall, and F1-scores, meaning the model was unable to correctly classify any instances of these attacks. Only the ddos-syn and ddos-udp classes showed some improvement, with recall values above 0.90. However, this came at the cost of poor performance in other categories, which confirmed that Logistic Regression was not suitable for highly imbalanced and multi-class IoMT attack datasets.

Table 3. Anlysis of the results of the three ML models used in present study

Model	Accuracy	Precision (Macro Avg)	Recall (Macro Avg)	F1-Score (Macro Avg)
Logistic Regression	0.43	0.09	0.13	0.08
Random Forest	1	0.97	0.95	0.96
Gradient Boosting*	0.96	0.92	0.9	0.91

Random Forest, in contrast, demonstrated outstanding performance. The model achieved nearly perfect classification results across all classes, with accuracy close to 100%. Precision, recall, and F1-scores were consistently high, often equal to 1.00. Even minority classes such as ping_sweep and vulscan were classified with strong precision and recall. Only a few slight drops were noted for classes with very small sample sizes, such as arp_spoofing and dos-connect_flood, but the results still remained highly reliable. The ensemble nature of Random Forest, which averages decisions across many trees, helped reduce overfitting and improved classification in an imbalanced dataset.

Gradient Boosting, which was also applied, produced strong but slightly lower performance compared to Random Forest. Accuracy was above 95%, and macro-averaged F1-scores were also high. Gradient Boosting performed well for majority classes such as ddos-udp, ddos-icmp, and ddos-tcp, but some minority classes suffered from reduced recall. This suggested that while Gradient Boosting was highly effective, it required more tuning or data balancing to handle rare attacks as effectively as Random Forest. The comparison highlighted a key point: simple

https://doi.org/10.71058/jodac.v10i02001

linear models like Logistic Regression were inadequate for detecting cyberattacks in IoMT traffic, while tree-based ensemble models such as Random Forest and Gradient Boosting showed much higher robustness. Random Forest, in particular, balanced precision and recall across all classes, making it the most reliable candidate for IoMT cyberattack detection in this study.

4 Conclusion

The current study focused on detecting cyberattacks in healthcare-based Internet of Medical Things (IoMT) using the CICIoMT2024 dataset. The dataset contained many different types of attacks such as DDoS, DoS, port scanning, and some rare attacks like ping_sweep and vulscan. Before applying machine learning models, the dataset was cleaned and carefully analyzed with statistical methods. This step helped to understand the structure of the data, class imbalance, and important features that played a major role in attack detection. Several machine learning models were then tested to evaluate their performance. Logistic Regression worked as a baseline but did not perform well because it could not handle the imbalance of the dataset. Its accuracy was low, and it completely failed in many smaller classes. This showed that simple linear models were not suitable for complex IoMT traffic data. In contrast, Random Forest achieved very strong results. It showed excellent accuracy, recall, precision, and F1-scores across almost all classes. Even rare attack types were detected with high reliability. Gradient Boosting also gave good performance, but it was slightly weaker than Random Forest in handling the smaller classes. This indicated that ensemble tree-based methods were much more powerful in this context compared to linear models.
The overall findings proved that effective cyberattack detection in IoMT requires advanced machine learning approaches that can manage large, imbalanced datasets. Random Forest stood out as the most reliable choice because of its ability to balance accuracy and generalization across both major and minor classes. The results provided strong evidence that healthcare IoMT systems can be better protected by using ensemble machine learning methods. This contributes toward building secure, trustworthy, and safe healthcare networks, which is vital for protecting sensitive patient data and ensuring reliable medical services.

References

1. M. Z. Nasrabadi, H. Tabibi, M. Salmani, M. Torkashvand, and E. Zarepour, “A comprehensive survey on non-invasive wearable bladder volume monitoring systems,” Medical & Biological Engineering & Computing, vol. 59, no. 7, pp. 1373–1402, Jul. 2021, doi: 10.1007/s11517-021-02395-x.
2. A. Nadian-Ghomsheh, B. Farahani, and M. Kavian, “A hierarchical privacy-preserving IoT architecture for vision-based hand rehabilitation assessment,” Multimedia Tools and Applications, vol. 80, no. 20, pp. 1–24, Feb. 2021, doi: 10.1007/s11042-021-10563-2.
3. C. Iwendi, K. Mahboob, Z. Khalid, A. R. Javed, M. Rizwan, and U. Ghosh, “Classification of COVID-19 individuals using adaptive neuro-fuzzy inference system,” Multimedia Systems, vol. 28, no. 4, pp. 1–15, Mar. 2021, doi: 10.1007/s00530-021-00774-w.
4. X. Sun, H. Yu, W. D. Solvang, Y. Wang, and K. Wang, “The application of Industry 4.0 technologies in sustainable logistics: a systematic literature review (2012–2020) to explore future research opportunities,” Environmental Science and Pollution Research International, vol. 29, no. 7, pp. 9560–9591, Dec. 2021, doi: 10.1007/s11356-021-17693-y.
5. A. Bobbio, L. Campanile, M. Gribaudo, M. Iacono, F. Marulli, and M. Mastroianni, “A cyber warfare perspective on risks related to health IoT devices and contact tracing,” Neural Computing & Applications, vol. 35, no. 19, pp. 13823–13837, Jan. 2022, doi: 10.1007/s00521-021-06720-1.
6. N. Munoth, A. A. Nagaich, and S. Gehlot, “Transitioning from Wired City to Super City: a review of selected ‘Smart City’ case studies,” GeoJournal, vol. 87, Suppl. 4, pp. 999–1016, Jul. 2022, doi: 10.1007/s10708-022-10704-6.
7. A. Gupta and A. Singh, “An Intelligent Healthcare Cyber Physical Framework for Encephalitis Diagnosis Based on Information Fusion and Soft-Computing Techniques,” New Generation Computing, vol. 40, no. 4, pp. 1093–1123, Jun. 2022, doi: 10.1007/s00354-022-00175-1.

https://doi.org/10.71058/jodac.v10i02001

8. L. Duan and L. D. Xu, “Data Analytics in Industry 4.0: A Survey,” Information Systems Frontiers: A Journal of Research and Innovation, vol. 1, no. 17, Aug. 2021, doi: 10.1007/s10796-021-10190-0.
9. [9] J. Guo and Z. Lv, “Application of Digital Twins in multiple fields,” Multimedia Tools and Applications, vol. 81, no. 19, pp. 26941–26967, Feb. 2022, doi: 10.1007/s11042-022-12536-5.
10. L. Li, “Reskilling and Upskilling the Future-ready Workforce for Industry 4.0 and Beyond,” Information Systems Frontiers: A Journal of Research and Innovation, vol. 26, no. 5, pp. 1–1712, Jul. 2022, doi: 10.1007/s10796-022-10308-y.
11. I. H. Sarker, “AI-Based Modeling: Techniques, Applications and Research Issues Towards Automation, Intelligent and Smart Systems,” SN Computer Science, vol. 3, no. 2, p. 158, Feb. 2022, doi: 10.1007/s42979-022-01043-x.
12. F. Ullah, G. Srivastava, and S. Ullah, “A malware detection system using a hybrid approach of multi-heads attention-based control flow traces and image visualization,” Journal of Cloud Computing (Heidelberg, Germany), vol. 11, no. 1, p. 75, Nov. 2022, doi: 10.1186/s13677-022-00349-8.
13. H. Ünözkan, M. Ertem, and S. Bendak, “Using attack graphs to defend healthcare systems from cyberattacks: a longitudinal empirical study,” Network Modeling and Analysis in Health Informatics and Bioinformatics, vol. 11, no. 1, p. 52, Nov. 2022, doi: 10.1007/s13721-022-00391-1.
14. J. Mwanza, A. Telukdarie, and T. Igusa, “Impact of industry 4.0 on healthcare systems of low- and middle-income countries: a systematic review,” Health and Technology, vol. 13, no. 1, pp. 35–52, Jan. 2023, doi: 10.1007/s12553-022-00714-2.
15. C.-M. Ho, “Research on interaction of innovation spillovers in the AI, Fin-Tech, and IoT industries: considering structural changes accelerated by COVID-19,” Financial Innovation, vol. 9, no. 1, p. 7, Jan. 2023, doi: 10.1186/s40854-022-00403-z.
16. S. Dadkhah, E. C. P. Neto, R. Ferreira, R. C. Molokwu, S. Sadeghi and A. A. Ghorbani. "CICIoMT2024: Attack Vectors in Healthcare devices-A Multi-Protocol Dataset for Assessing IoMT Device Security,” Internet of Things, v. 28, December 2024.
17. G. Bhola and D. K. Vishwakarma, “A review of vision-based indoor HAR: state-of-the-art, challenges, and future prospects,” Multimedia Tools and Applications, vol. 83, no. 1, pp. 1–2005, May 2023, doi: 10.1007/s11042-023-15443-5.
18. Y. Luo and S. A. Zahra, “Industry 4.0 in international business research,” Journal of International Business Studies, vol. 54, no. 3, pp. 403–417, Mar. 2023, doi: 10.1057/s41267-022-00577-9.
19. V. Goar, A. Sharma, N. S. Yadav, S. Chowdhury, and Y.-C. Hu, “IoT-Based Smart Mask Protection against the Waves of COVID-19,” Journal of Ambient Intelligence and Humanized Computing, vol. 14, no. 8, pp. 1–11164, Sep. 2022, doi: 10.1007/s12652-022-04395-7.
20. M. Tabassum, S. Mahmood, A. Bukhari, B. Alshemaimri, A. Daud, and F. Khalique, “Anomaly-based threat detection in smart health using machine learning,” BMC Medical Informatics and Decision Making, vol. 24, no. 1, p. 347, Nov. 2024, doi: 10.1186/s12911-024-02760-4.
21. G. Premalatha and V. Thulasi Bai, "Wireless IoT and Cyber-Physical System for Health Monitoring Using Honey Badger Optimized Least-Squares Support-Vector Machine," Wireless Personal Communications, vol. 124, no. 4, pp. 3013–3034, Mar. 2022, doi: 10.1007/s11277-022-09500-9.
22. A. Alharbi, W. Alosaimi, H. Alyami, B. Alouffi, A. Almulihi, M. Nadeem, M. A. Sayeed, and R. A. Khan, "Selection of Data Analytic Techniques by Using Fuzzy AHP TOPSIS from a Healthcare Perspective," BMC Medical Informatics and Decision Making, vol. 24, no. 1, p. 240, Sep. 2024, doi: 10.1186/s12911-024-02651-8.
23. A. Gupta and A. Singh, "Healthcare 4.0: Recent Advancements and Futuristic Research Directions," Wireless Personal Communications, vol. 129, no. 2, pp. 933–952, Dec. 2022, doi: 10.1007/s11277-022-10164-8.
24. E.C.P. Neto, S. Dadkhah, R. Ferreira, A. Zohourian, R. Lu, A.A. Ghorbani, Ciciot2023: A real-time dataset and benchmark for large-scale attacks in iot environment. Sensors 23(13) (2023). https://doi.org/10.3390/s23135941
25. I. Sharafaldin, A.H. Lashkari, A.A. Ghorbani, Toward generating a new intrusion detection dataset and intrusion trafc characterization. ICISSp 1, 108–116 (2018). Accessed 11 Oct 2024