Botnet Attacks Detection in Internet of Medical Things Network

Sophiya Kangjam[1,*], *Nongthombam Joychandra* Singh[1,**], *Leishangthem Sashikumar* Singh[1,***], *Yumnam* Nirmal[1,****], and *Khumukcham Robindro* Singh[2,†]

[1]Brainware University, Barasat, Kolkata, West Bengal 700125, India
[2]Manipur University, Canchipur, Imphal, Manipur 795003, India

Abstract. With the rapid applications of the Internet of Things (IoT) in the areas of Healthcare, the threats to IoT in healthcare is increasing significantly. Attackers always try to compromise the less secured devices connected to IoT and form a large botnet of compromised devices. The IoT botnet-based attacks are very severe and cause significant impacts on healthcare applications. If the attacker manipulates medical sensor readings and generates false data, it might cause havoc during diagnosis. So, it is an utmost security concern to protect IoT networks from vulnerabilities and attacks. This paper analyzes the effectiveness of Machine Learning (ML) and Deep Learning (DL) methods on the CICIoMT2024 IoT healthcare dataset. We undertake an experimental evaluation of this dataset, employing a spectrum of ML and DL methods. Evaluation of these models encompasses a range of performance metrics such as Accuracy, Precision, Recall, F1-score, Area Under the Curve, Matthews Correlation Coefficient, and Kappa score, thereby facilitating a thorough understanding of their efficacy in detecting intrusions within IoT networks. Our findings reveals that advaced ML models such as XGBoost and RF outperforms DL models with an accuracy of 99.85% and 99.87% respectively. This paper reveals valuable insights and will help future research in the same domain.

1 Introduction

The IoT refers to a network of interconnected hardware, including processors, sensors, and software, that enable data exchange and communication among objects [1]. This interconnected system collects and analyses large amounts of data, enabling task automation in various disciplines. The IoT revolutionizes various sectors, including smart homes, healthcare, industrial IoT, smart cities, agriculture, transportation, energy, and environmental monitoring [2]. In the present era, there is a growing focus on the IoT in the healthcare industry due to its potential to transform the healthcare sector [3, 4]. Integrating healthcare-related sensors and devices into the IoT has led to the development of the Internet of Medical Things (IoMT). IoT applications in healthcare cover a broad spectrum of features, such as boosting

*e-mail: sophiya7kangjam@gmail.com
**e-mail: joy140nong@gmail.com
***e-mail: saskulei@gmail.com
****e-mail: yumnamnirmal@gmail.com
†e-mail: rbkh@manipuruniv.ac.in

© The Authors, published by EDP Sciences. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/).

patient-provider communication, monitoring medical parameters, providing remote patient monitoring, and optimizing hospital treatment systems. The IoMT has improved patient outcomes and healthcare delivery by improving the accuracy (Acc) and capabilities of electronic equipment [3]. This evolution represents a significant advancement in healthcare, aiming to meet patients' needs more efficiently and effectively. IoMT is progressively replacing traditional healthcare systems by offering numerous benefits by providing innovative solutions for real-time patient care, disease management, telemedicine, medical research, etc. [1, 5].

The IoMT is a rapidly growing field within healthcare, leveraging IoT technologies to enhance patient care and outcomes. Sensitive health data is collected by IoMT devices, facilitating better monitoring and treatment [6]. With this advancement, the widespread adoption of IoT infrastructures, notably in IoMT, has raised significant cybersecurity concerns [7]. The vulnerabilities in IoMT threats not only the IoMT infrastructure, it also gives severe risks to the entire healthcare ecosystem and potentially life threatening. Recently, the threat landscape targeting IoMT systems has been significantly evolving and becoming more extensive, complex, and diverse [8]. IoMT sensors are more vulnerable to attackers in forming a large Botnet as such devices are less powered, memory-contained, and plug-and-play. Botnet-based attacks present a serious threat to the IoMT by enabling large-scale assaults using compromised devices [9]. A botnet is a network of compromised devices that is created by a hacker called a botmaster, and these bots are given commands and controlled remotely by the botmaster. Botnet attacks exploit vulnerabilities in connected devices, leveraging them to execute large-scale malicious activities [1]. The variety and volume of security threats and attacks targeting these systems have increased significantly. Threats such as routing attacks, Recon, MQTT, spoofing, Denial of Service (DoS), and Distributed Denial of Service (DDoS) attacks are becoming more prevalent, making it crucial to develop and implement robust Intrusion Detection Systems (IDSs) tailored specifically for IoMT environments [10].

2 Background Study

The integration of ML or DL techniques into IDS for IoMT environments is indeed gaining significant attention in recent research [11]. Recent studies reveals that ML and DL-based IDS systems have the potential to effectively identify the attacks [14]. DL models can adapt and learn the evolving attack patters, thus continuously improving their ability to identify potential threats in real-time, however it demands more computational resources [1, 13]. Table 1 illustrates summary of the recent research on IoMT network intrusion detection. IoMT environments, characterized by their complex architecture and device heterogeneity, present unique challenges for traditional intrusion detection methods [7, 12]. Vinayakumar Ravi et al. [19] propose a DL model integrating network flow data and patient biometrics with attention mechanisms and cost-sensitive learning. Their method achieves an Acc of 99% when combining both feature types. Likewise, Panagiotis et al. [20] propose an SDN-based IDS focusing on IEC 60870-5-104 protocol, demonstrating effective detection and mitigation of cyberattacks using ML-based analysis. Hybrid DL architectures have also gained popularity, study such as, Nuruzzaman Faruqui et al. [21] propose SafetyMed combining CNN and LSTM. Their model achieves 97.63% Acc and 98.47% F1. Likewise, Jafar A. Alzubi et al. [24] propose a hybrid CNN-LSTM framework for detecting attacks at the network edge with improved accuracy. Umamaheswaran et al. [22] address data imbalance using a hybrid CGAN-CNN approach, achieving high precision and F1-scores above 97%. These hybrid models gives better results however the concern is the deployability, since they demands more computation resources. By considering deployability, many studies focus on lightweight IDS which suits the lightweight nature of the IoT infrastructure. Aswani Devi

Aguru et al. [23] propose an mGRU-based IDS for multi-vector DDoS detection with reduced computational overhead, while Faisal Hussain et al. [15] introduce a context-aware framework and the IoT-Flock dataset, where RF demonstrating better performance.

The development of realistic dataset close to the real IoMT environment and architecture are also an important factor in the development of an effective IDS. Mohammed Zubair et al. [16] propose the BlueTack dataset for Bluetooth-based IoMT attacks alongside a DL-based IDS achieving over 99% accuracy. Mohiuddin Ahmed et al. [17] develop the ECU-IoHT dataset, showing that nearest neighbor methods outperform other approaches. Rajasekhar Chaganti et al. [18] introduce a PSO-DNN model combining network and biometric data, achieving 96% Acc. In the next section, We briefly highlight the recent publicly available IoMT-based datasets.

Table 1: Recent studies on IoMT network intrusion detection

Year	**Dataset**	**IoMT based dataset**	**Models**	**Area of Study**	**Refs.**
2020	WUSTL-EHMS-2020	✓	RF, KNN, SVM, ANN	Enhanced Healthcare Monitoring System (EHMS): Integrating IoT systems in healthcare for remote patient monitoring.	[29]
2021	IoT Healthcare Dataset	✓	NB, KNN, RF, AdaBoost, LR,DT	A framework for developing IoT context-aware security solutions to detect malicious traffic.	[15]
2022	BlueTack	✓	ML-LR,DT,SVM,RF DL-DNN	Bluetooth-based attacks detection on IoMT using deep learning techniques	[16]
2022	IoMT network traffic and patient biometrics dataset	✓	ML- LR, KNN, DT, RF,AdaBoost, SVM; DL-DNN, CNN, LSTM	Particle swarm optimization deep neural network PSO-DNN model for intrusion detection in IoMT	[18]
2023	IEC 60870-5-104	✓	ML-RF, OneR, J48, IBk, and NB DL-Dense DNN Relu and Dense DNN Tanh	Intrusion Detection and Prevention System on IoMT utilizing ML and Software Defined Networking (SDN) technologies	[20]
2023	CICIDS 2017	X	CNN-LSTM	CNN-LSTM based IDS to protect IoMT devices.	[21]
2023	WUSTL-EHMS-2020, KDDCup-99, SDN-IoT	✓	CNN-LSTM	DL-based approach for network intrusion detection in IoMT systems, utilizing network flows and patient biometrics.	[19]

2024	CICDDoS 2019	X	GAN-CNN	Addressing network intrusion detection challenges in IoMT systems with imbalanced data, a deep learning-based approach.	[22]
2024	CICIoT 2023, CICDDoS 2019	X	GRU	Multi-vector DDoS attacks in mobile healthcare informatics systems using stacked modified Gated Recurrent Units (mGRU)	[23]
2024	CICIoMT 2024	✓	LR,RF,AdaBoost, DNN	CICIoMT2024 dataset to evaluate the security of IoMT devices	[10]
2024	CSE-CIC-IDS 2018	X	CNN-LSTM	Blended Intrusion Detection System for the edge-centric Internet of Medical Things	[24]

3 IoMT Datasets

Table 2 highlights the available datasets over the past five years for developing IoT security solutions in healthcare. Developing effective intrusion detection systems for IoT devices in healthcare is crucial for ensuring the security and privacy of sensitive patient data [25, 26]. ML and DL algorithms have demonstrated significant potential in enhancing the security of IoT networks by identifying anomalous behavior indicative of potential threats [11]. However, the success of these algorithms heavily depends on the availability of high-quality datasets. In the context of healthcare, this becomes even more challenging due to the sensitive nature of the data involved and the stringent regulations surrounding its use and sharing [27].

Efforts are underway to address the scarcity of IoMT datasets. Initiatives such as data sharing among research institutions, collaboration between academia and industry, and the development of synthetic datasets are helping to mitigate this challenge [11]. With the high-quality, large volume and realistic datasets, researchers can develop sophisticated IDS capable of effectively capturing the evolving botnet threats. The next section presents the experimental analysis using the most recent IoMT dataset, CICIoMT-2024, to evaluate the effectiveness of ML and DL models.

Table 2: Summary of IoMT datasets

Year	Dataset	Devices Involved	Attack types	Publicly available	Refs.
2020	WUSTL-EHMS-2020	medical sensors attached to the patent's body, gateway, network and control with visualization	man-in-the-middle attacks: spoofing and data injection	Yes	[29]
2021	IoT Healthcare Dataset	Nine patient monitoring devices (i.e., sensors) and one control unit called as Bedx-Control-Unit	MQTT distributed denial-of-service, MQTT publish flood, brute force, and SlowITE	Yes	[15]

2021	ECU-IoHT	Patient monitoring sensors: Temperature, Blood pressure and Heart Rate	Nmap attack, Smurf attack, ARP spoofing, DoS attack using Ettercap, Script injection using the MITMf framework, Bettercap attack	Yes	[17]
2022	Blue-Tack	SpO2, heart rate,and ECG	DDoS, Bluesmack, MITM, and DoS on the L2CAP layer of the Bluetooth protocol stack	Yes	[16]
2023	IEC 60870-5-104	seven virtual machines (VMs) with IEC-TestServer, one VM with Qtester104, and three VMs equipped with Metasploit, OpenMUC j60870, and Ettercap to represent different entities in the system	replay attacks, DoS attacks, and address resolution protocol spoofing attacks	Yes	[20]
2024	CICIoMT-2024	40 IoMT devices (25 real devices and 15 simulated devices), considering the plurality of protocols used in healthcare (e.g., Wi-Fi, MQTT and Bluetooth)	DDoS, DoS, Recon, MQTT, and spoofing	Yes	[10]

4 Experimental Analysis on CICIoMT2024 dataset

Detecting botnet-based attacks using ML and DL involves a structured experimental analysis framework to ensure effective detection performance. As illustrated in Figure 1, our framework involves several important steps, including gathering dataset, data preprocessing, model selection, and training, evaluating the model using various evaluation matrices, fine-tuning the model, and classification using the trained model. The first important step is gathering the dataset. Developing an efficient botnet detection system heavily relies on the dataset's quality. The next step is preprocessing the dataset; it involves several steps and various techniques. Exploratory analysis, handling missing values, handling categorical values, data normalization or scaling, splitting training and testing sets, feature selection, etc., are included in the preprocessing steps. Feature selection is one of the most crucial steps in the preprocessing. IoT network traffic datasets often contain many features and are highly dimensional due to irrelevant or redundant features. Feature selection helps identify and select the most relevant features, reducing the dimensionality of the data. This, in turn, improves the efficiency of the learning algorithm and reduces computational complexity [34]. After preprocessing, the next crucial step is choosing the most suitable model or classifier. Then, the model will be trained with different parameters and architectures to find the best-performing one. Then evaluate, the model using various evaluation metrics like Acc, Pre, Rec, F1s, kappa-scores, Mathew's correlation coefficient, roc-run, etc. Finally, attacks are detected using the trained model.

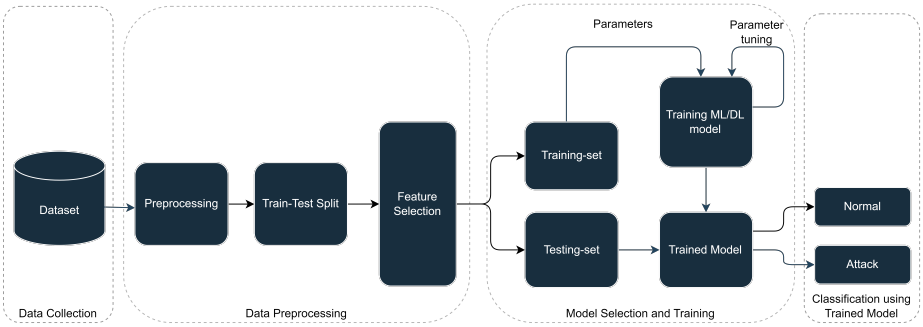

Figure 1. Conceptual Framework

4.1 Experimental Results

We conducted an experimental analysis on the CICIoMT2024 dataset using various ML methods such as Logistic Regression (LR), Random Forest (RF), Decision Tree (DT), Naive Bayes (NB), Adaptive Boosting (AdaBoost), Gradient Boosting (GBoost), and Extreme Gradient Boosting (XGBoost). Additionally, we employed DL methods such as Deep Neural Network (DNN), Convolutional Neural Network (CNN), Recurrent Neural Network (RNN), Long Short Term Memory (LSTM), Gated Recurrent Unit (GRU) and hybrid CNN-LSTM models. We evaluated these methods using performance metrics like Acc, Pre, Rec, F1, AUC, Matthews Correlation Coefficient (MCC), and Kappa. Our experiments were executed on GPU-enabled Google Colab.

Table 3. Experimental results of various ML models on CICIoMT dataset

Model	Acc	Pre	Rec	F1	AUC	MCC	Kappa
LR	99.47%	99.47%	94.94%	94.96%	95.0%	89.91%	89.91%
RF	99.87%	99.30%	99.40%	99.35%	99.0%	98.70%	98.70%
DT	99.75%	99.65%	95.46%	97.46%	95.0%	95.02%	94.92%
NB	98.69%	83.60%	99.22%	89.82%	99.0%	81.33%	79.66%
AdaBoost	99.79%	97.98%	99.21%	98.59%	99.0%	97.18%	97.17%
Gboost	99.77%	99.57%	95.96%	97.69%	96.0%	95.45%	95.37%
XGBoost	99.85%	98.86%	99.63%	99.24%	100.0%	98.48%	98.48%

Experimental results of various ML models are illustrated in Figure 3, RF, AdaBoost, and XGBoost standing out as the top performers. XGBoost achieves a balanced overall performance, including a perfect AUC. LR demonstrates high Acc and Pre but lags slightly in Rec and F1 compared to other models. RF perform exceptionally well across all metrics, making it the most suitable ML model on this dataset. XGBoost achieves the highest AUC and excellent performance across all other metrics, making it the top performer in this analysis. This analysis emphasizes the importance of evaluating multiple models to determine the best fit for specific data characteristics.

Experimental results of various DL models are show in Table 4, DNN, LSTM, and CNN models stand out due to their balanced and high values across all performance metrics. The CNN-LSTM hybrid, while performing well, shows slightly lower Pre, indicating it might generate more false positives compared to DNN and LSTM. DNN exhibits excellent performance, with high values across all metrics. It achieves a balanced trade-off between Pre and

Table 4. Experimental results of various DL models on CICIoMT dataset

Model	Acc	Pre	Rec	F1	AUC	MCC	Kappa
DNN	99.75%	96.89%	98.36%	97.62%	98.0%	95.24%	95.23%
RNN	99.40%	93.44%	95.31%	94.35%	95.0%	88.73%	88.70%
GRU	99.74%	96.10%	99.12%	97.56%	99.0%	95.16%	95.11%
LSTM	99.75%	96.99%	98.31%	97.64%	98.0%	95.29%	95.28%
CNN	99.73%	96.21%	98.90%	97.52%	99.0%	95.07%	95.03%
CNN-LSTM	99.79%	95.58%	98.90%	97.18%	99.0%	94.42%	94.35%

Rec, indicating it can effectively classify both positive and negative cases. CNNs show the best performance in terms of Rec as compared to other validation measures. However, its slightly lower Pre compared to DNN and LSTM.

Overall comprehensive analysis of ML and DL models on the CICIoMT2024 dataset reveals that while advanced machine learning models like XGBoost and RF excel in overall performance, certain deep learning models like DNN and LSTM also achieve impressive results. XGBoost and RF outperforms other models throughout all the metrics, underscoring their robustness and effectiveness in the CICIoMT2024 dataset.

4.2 Comparative Analysis and Discussion

We compare our top performing models with the study of [10], the comparison is shown in Table 5. Our experimental results highlight better performances, this variations may be due to different preprocessing stratagies and hyperparameter settings. We experimented using different sets of hyperparameters and presented the best options. In the LR model, we emphasise on the maximum number of parameters and best result is found when $max\_iter = 1000$. For the AdaBoost, we adjust the number of weak learners and found the best results when $n\_estimators = 150$. We consider the number of trees and tree depth for the RF, and gives best result when $max\_depth = 6$. For the DNN model, the architecture has three fully connected neurons, 128, 64 and 32 with ReLU and a dropout at the rate of 0.4 and 0.3 in the first two hidden layers for the regularization. The output layer is of single neuron with the sigmoid activation function. With this settings, our experimental results exhibit better performance in terms of Acc in LR, AB, and DNN. In terms of Rec, ours models uniformly demonstrate higher scores across all classifiers. The improvements are significant particularly in AB reching 99.21%, RF - 99.40% and DNN 98.36%. The improvements in Rec, Pre, and F1 suggest that our method has potentially improved the model's ability to detect effectively.

Table 5. Comparative Analysis

Refs.	Metrics	LR	AB	RF	DNN
[10]	Acc	99.46%	99.80%	99.83%	99.61%
	Rec	93.50%	97.78%	97.64%	95.23%
	Pre	94.60%	97.97%	98.75%	96.27%
	F1	94.04%	97.88%	98.19%	95.74%
Ours	Acc	99.47%	99.79%	99.87%	99.75%
	Rec	94.94%	99.21%	99.40%	98.36%
	Pre	99.47%	97.98%	99.30%	96.89%
	F1	94.96%	98.59%	99.35%	97.62%

5 Conclusion

IoMT is omnipresent and rapidly proliferating due to its signigicance in the healthcare sector. However it posses significant threats due to the lightweight and weak security mechanisms of the IoT devices. To develop an efficient IDS requries quality dataset comprising real IoMT scenarios. The CICIoMT 2024 dataset is a valuable resource for developing IDS in IoMT, which includes diverse collection of IoMT-related scenarios and devices. Our experimental analysis of various ML and DL models on this dataset highlights the efficiency of ML models such as XGBoost and RF reaching an Acc of 99.85% and 99.87% respectively and demonstrate their robustness and effectiveness with high Pre, Rec, and AUC scores. In fact, on this dataset, ML methods outperform DL models, however, DNN and LSTM also gives competitive performances, when considering a balanced combination of Pre and Rec. Future research should focus on further refining these models incorporating feature selection techniques and exploring new datasets to keep pace with the dynamic landscape of cybersecurity threats in the IoMT domains.

References

[1] Singh, N. Joychandra, et al. "Botnet-based IoT network traffic analysis using deep learning." Security and Privacy 7.2 (2024): e355.

[2] Chataut, Robin, Alex Phoummalayvane, and Robert Akl. "Unleashing the power of IoT: A comprehensive review of IoT applications and future prospects in healthcare, agriculture, smart homes, smart cities, and industry 4.0." Sensors 23.16 (2023): 7194.

[3] Wu, Ju-Yu, et al. "IoT-based wearable health monitoring device and its validation for potential critical and emergency applications." Frontiers in Public Health 11 (2023): 1188304.

[4] Ejiyi, Chukwuebuka, et al. "The internet of medical things in healthcare management: a review." Journal of Digital Health (2023): 30-62.

[5] Nissar, Gousia, et al. "IoT in healthcare: a review of services, applications, key technologies, security concerns, and emerging trends." Multimedia Tools and Applications (2024): 1-62.

[6] Huang, Chenxi, et al. "Internet of medical things: A systematic review." Neurocomputing (2023): 126719.

[7] Ksibi, Sondes, Faouzi Jaidi, and Adel Bouhoula. "IoMT security model based on machine learning and risk assessment techniques." 2023 International Wireless Communications and Mobile Computing (IWCMC). IEEE, 2023.

[8] Rasool, Raihan Ur, et al. "Security and privacy of internet of medical things: A contemporary review in the age of surveillance, botnets, and adversarial ML." Journal of Network and Computer Applications 201 (2022): 103332.

[9] Kumar, A. Karthick, K. Vadivukkarasi, and R. Dayana. "A Novel Hybrid Deep Learning Model for Botnet Attacks Detection in a Secure IoMT Environment." 2023 International Conference on Intelligent Systems for Communication, IoT and Security (ICISCoIS). IEEE, 2023.

[10] Dadkhah, Sajjad, et al. "CICIoMT2024: Attack Vectors in Healthcare devices-A Multi-Protocol Dataset for Assessing IoMT Device Security." Raphael and Chukwuka Molokwu, Reginald and Sadeghi, Somayeh and Ghorbani, Ali, CiCIoMT2024: Attack Vectors in Healthcare Devices-A Multi-Protocol Dataset for Assessing IoMT Device Security (2024).

[11] Hernandez-Jaimes, Mireya Lucia, et al. "Artificial intelligence for IoMT security: A review of intrusion detection systems, attacks, datasets and Cloud-Fog-Edge architectures." Internet of Things (2023): 100887.

[12] Sowmya, T., and EA Mary Anita. "A comprehensive review of AI based intrusion detection system." Measurement: Sensors 28 (2023): 100827.

[13] Singh, Nongthombam Joychandra, et al. "Massive IoT network traffic analysis using ML and DL methods: an empirical evaluation: N. Joychandra Singh et al." The Journal of Supercomputing 81.10 (2025): 1107.

[14] Neto, Euclides Carlos Pinto, et al. "A review of Machine Learning (ML)-based IoT security in healthcare: A dataset perspective." Computer Communications (2023).

[15] Hussain, Faisal, et al. "A framework for malicious traffic detection in IoT healthcare environment." Sensors 21.9 (2021): 3025.

[16] Zubair, Mohammed, et al. "Secure Bluetooth communication in smart healthcare systems: a novel community dataset and intrusion detection system." Sensors 22.21 (2022): 8280.

[17] Ahmed, Mohiuddin, et al. "ECU-IoHT: A dataset for analyzing cyberattacks in Internet of Health Things." Ad Hoc Networks 122 (2021): 102621.

[18] Chaganti, Rajasekhar, et al. "A particle swarm optimization and deep learning approach for intrusion detection system in internet of medical things." Sustainability 14.19 (2022): 12828.

[19] Ravi, Vinayakumar, Tuan D. Pham, and Mamoun Alazab. "Deep learning-based network intrusion detection system for Internet of medical things." IEEE internet of things magazine 6.2 (2023): 50-54.

[20] Radoglou-Grammatikis, Panagiotis, et al. "Modeling, detecting, and mitigating threats against industrial healthcare systems: a combined software defined networking and reinforcement learning approach." IEEE Transactions on Industrial Informatics 18.3 (2021): 2041-2052.

[21] Faruqui, Nuruzzaman, et al. "SafetyMed: a novel IoMT intrusion detection system using CNN-LSTM hybridization." Electronics 12.17 (2023): 3541.

[22] Umamaheswaran, S., et al. "Smart intrusion detection system with balanced data in IoMT infra." Journal of Intelligent & Fuzzy Systems Preprint (2024): 1-17.

[23] Aguru, Aswani Devi, and Suresh Babu Erukala. "A lightweight multi-vector DDoS detection framework for IoT-enabled mobile health informatics systems using deep learning." Information Sciences 662 (2024): 120209.

[24] Alzubi, Jafar A., et al. "A blended deep learning intrusion detection framework for consumable edge-centric iomt industry." IEEE Transactions on Consumer Electronics (2024).

[25] Sun, Zhenyang, et al. "Optimized machine learning enabled intrusion detection 2 system for internet of medical things." Franklin Open 6 (2024): 100056.

[26] Akram, Faiza, et al. "Trustworthy intrusion detection in e-healthcare systems." Frontiers in public health 9 (2021): 788347.

[27] Gong, Youdi, et al. "A survey on dataset quality in machine learning." Information and Software Technology 162 (2023): 107268.

[28] Khalid, Nazish, et al. "Privacy-preserving artificial intelligence in healthcare: Techniques and applications." Computers in Biology and Medicine 158 (2023): 106848.

[29] Hady, Anar A., et al. "Intrusion detection system for healthcare systems using medical and network data: A comparison study." IEEE Access 8 (2020): 106576-106584.

[30] Hoque, Nazrul, Dhruba K. Bhattacharyya, and Jugal K. Kalita. "MIFS-ND: A mutual information-based feature selection method." Expert systems with applications 41.14 (2014): 6371-6385.

[31] Hoque, Nazrul, Mihir Singh, and Dhruba K. Bhattacharyya. "EFS-MI: an ensemble feature selection method for classification: An ensemble feature selection method." Complex & Intelligent Systems 4 (2018): 105-118.

[32] Shekhar, Shashank, Nazrul Hoque, and Dhruba K. Bhattacharyya. "PKNN-MIFS: a parallel KNN classifier over an optimal subset of features." Intelligent systems with applications 14 (2022): 200073.

[33] Kingma, Diederik P., and Max Welling. "Auto-encoding variational bayes." arXiv preprint arXiv:1312.6114 (2013).

[34] Singh, N. Joychandra, et al. "Significance of feature selection on IoT-based botnet attacks identification using machine learning." 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT). IEEE, 2024.