International Journal of Research in Engineering and Management Sciences (IJREMS)
E-ISSN: 3107-7439

Research Article
VOL.: 2, Issue: 11, November 2026

Explainable AI-Based Anomaly Detection for Secure Internet of Medical Devices

[1]Yaswanth Reddy Vada, [2]Ardhala Bala Krishna

[1]Department of Information Technology, University of the Cumberlands, Williamsburg, Kentucky, USA. Yaswanthreddyvada@gmail.com

[2]Department of Electrical and Electronics Engineering (EEE), PSCMR College of Engineering and Technology, Vijayawada, Andhra Pradesh, India. Bala.krishna@pscmr.ac.in

ABSTRACT:
The IoMT networks are a part of the current medical care as they permit constant patient observing and correspondence between associated medical services gadgets. In healthcare environments, however, advanced cyber attacks remain difficult to detect due to the complex traffic flow and the irregular distribution of data and the shortcomings of conventional detection methods. The work is based on a healthcare-related dataset provided by the 2015 BRFSS of 253,680 records and 22 health-related features, and 10 network-related features from UNSW-NB15. Data preprocessing involves missing data, encoding of categorical data, class imbalance handling and Min-Max normalisation. We will be comparing some of the most popular algorithms such as RF, XGBoost, ANN, SVM, LR, KNN, and Isolation Forest with two more boosting algorithms LightGBM and CatBoost. It is suggested to use a better stacking ensemble where several base learners and meta-learner are XGBoost. The accuracy, precision, recall, F1 score and ROC-AUC score are used to assess the performance of the model. The preliminary estimated results show that the improved stacking ensemble has an accuracy of 98.35%, and precision of 98.51%, a recall of 98.12%, an F1-score of 98.31%, and a ROC-AUC of 0.995. Moreover, LIME and SHAP provide the interpretability of predictions, and FastAPI provides real-time prediction services, making the anomaly detection in IoMT more transparent and efficient.

Keywords: Internet of Medical Things (IoMT), Anomaly Detection, Stacking Ensemble Learning, Intrusion Detection, Explainable Artificial Intelligence, Healthcare Cybersecurity.

Received Date: 7 November 2026**; Accepted Date:** 17 November 2026**; Published Date:** 24 November 2026.

This is an open-access article distributed under the terms of the Creative Commons Attribution 4.0 International License (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author(s) and the source are properly cited.

1. Introduction

The IoMT is an integral part of today's healthcare technology, connecting implantable devices, patient monitoring systems, clinical information systems and wearable sensors. These combined technologies allow for real-time health monitoring, remote diagnostics, timely health interventions, and the provision of effective healthcare services. The rising usage of IoMT has enhanced the accessibility and quality of patient care greatly and has created new avenues for the intelligent healthcare environment. But wide scale sharing of sensitive medical information over interconnected networks poses major cyber security issues. Availability of devices, integrity of communication and confidentiality of patients' information are compromised and these can cause disruption of vital health care operations and compromise patient safety [1]. The more and more dependence of connected medical infrastructure further highlights the importance of safeguarding the aspects of healthcare communication settings [2]. These security issues also emphasize the importance of strong processes that will be able to safeguard confidential medical information [3]. Although network security has improved, the security of IoMT environments continues to be a challenge, for various reasons, including the presence of heterogeneous devices, limited computing resources, irregular communication patterns, and more advanced cyber attacks. Major security mechanisms are signature-based with fixed detection rules, limiting the ability to adjust to new attacks and changing network behaviour. In addition, existing anomaly detection methods may also be hard to maintain stable performance over different attack types and imbalanced network situations [4]. There are also certain difficulties with the validation of the reliability of the

detection in limited healthcare-specific evaluation contexts [5]. Moreover, the lack of interpretability of automated security judgements presents challenges for practical deployment in sensitive healthcare situations [6].

The proposed approach aims to enhance the cybersecurity of IoMT networks by introducing an enhanced anomaly detection architecture with a healthcare-centric dataset. The dataset contains 253,680 records from the BRFSS of the year 2015 and 22 health-related and 10 additional network-related attributes related to healthcare security scenarios [7]. The primary aim is to increase the anomaly detection rate for common communication patterns and various types of cyber attacks, but with a balance of classification performance. The other important objective is to create an interpretable detection environment, which can aid to offer clear explanations for automated predictions [8]. In addition, system practical accessibility is achieved by a specific API that is designed to be integrated with healthcare network monitoring settings [9].

The method proposed aims to enhance the cybersecurity processes in networked medical environments, making them more reliable and transparent. The proposed approach attempts to increase and improve the accuracy of the classifications and to identify more complex anomalous behaviors through the incorporation of complementary learning capabilities into an improved prediction model. Embedding explainability techniques could improve the understanding of the factors influencing individual predictions and the overall detection decisions to support security analysis and appropriate intervention. In addition, the simple-to-deploy design enables easy integration of the anomaly detection capabilities with real-time healthcare monitoring apps. These contributions are crucial for the enhancement of confidentiality, integrity and availability of healthcare information systems, which in turn helps to enable safer connected healthcare services. Lastly, the framework aims to facilitate intelligent, explainable, and adaptive cyber security solutions for developing IoMT infrastructures [10].

Related Work

The growing number of network-based medical devices and services has brought medical intrusion detection to the fore. Hady et al. [11] published a comparative analysis of intrusion detection systems using medical data and network data with a focus on the need for medical data to be considered in the context of security analysis. They worked on a way to assess detection systems not just based on the traditional network traffic, but also based on their work. But, the efficiency of the detection algorithms under various attack scenarios and the communication dynamics of IoMT is crucial. Ullah and Mahmoud [12] also proposed an anomaly detection method based on DL for IoT networks. This approach showed that DL could identify unusual activities in network traffic and complex traffic patterns. However, the computing requirements and the interpretability of DL predictions are still crucial concerns in resource-constrained medical situations.

Ensemble learning and hybrid detection techniques have also shown good potential for network security applications. Das et al. [13] studied combination of supervised and unsupervised machine learning algorithms for the detection of Distributed Denial-of-Service attack. In their approach, they highlighted the advantages of using complementary learning strategies on the enhancement of attack identification. In an effort to overcome the problem of inadequate labelled information and redundant network properties, Gu et al. [14] suggested a semi-supervised K-means based DDoS detection approach with hybrid feature selection. Although these algorithms provide useful improvements in attack detection, their main focus on DDoS identification does not entirely fulfil the larger requirements of healthcare-specific anomaly detection including several attack categories and medical information.

The abilities of IDS in the Internet of Things (IoT) have also been enhanced by security measures made possible by DL. N-BaIoT is proposed by Meidan et al. [15] that employs deep autoencoders, for detecting aberrant traffic behaviour, to identify network-based IoT botnet attacks. They found that unsupervised representation learning could be a powerful tool for recognising malicious device behaviours. Ravi and Shalinie [16] analyzed the challenges of learning-enabled DDoS detection and mitigation in SDN-cloud architecture and pointed to the need for incorporating intelligent DDoS detection and network-level mitigation capabilities. Doshi et al. [17] studied machine learning based DDoS detection for consumer IoT devices and showed that characteristics of the device-generated traffic can help in identifying the malicious activity. But the different aspects of consumer IoT and medical communication systems generate further challenges related to patient-specific data, device actions and the continuity of healthcare services.

Further studies have investigated the stability and transferability of anomaly detection techniques. In the work by Maseer et al. [18] machine learning techniques were tested on CICIDS2017 data set and compared the intrusion detection performance under various classification scenarios. Choi et al. [19] conducted a survey on DL paradigms for time series anomaly detection, and discussed methodologically how to detect anomalous temporal patterns. Abdelmoumin et al. [20] discussed the importance of model selection and performance evaluation for the standard ML models applied to intelligent IDS in an IoT system. These contributions as a whole offer valuable foundations that need to be better evaluated in a

healthcare context, have higher classification reliability, and are explainable in the prediction. The current work tackles these issues with an improved healthcare-centric anomaly detection system with complementary learning capabilities, explainable prediction, and an accessible deployment architecture to assist real-time IoMT security monitoring.

Materials and Methods

The proposed method is to design a new method for anomaly detection in an IoMT network by using a healthcare specific dataset from the 2015 BRFSS with the complementary features derived from the network of the UNSW-NB15. The workflow of the framework is structured into data collection, pre-processing, feature preparation, training and testing of the model. Comparing the performance of LightGBM and CatBoost with seven traditional machine learning techniques, we analyse the capability of both models to detect an abnormal network behaviour. The sophisticated stacking ensemble has complimentary base learners. The XGBoost is used as meta-learner to increase the classification reliability and predictive performance. Further, LIME and SHAP are integrated to offer local and global explanations of the predictions of the anomaly, which make the model more transparent and interpretable. The training framework is linked with FastAPI to provide real-time prediction services and application level deployment. The proposed strategy aims at facilitating precise, meaningful, and efficient anomaly detection to improve security operations in interdependent healthcare environments.

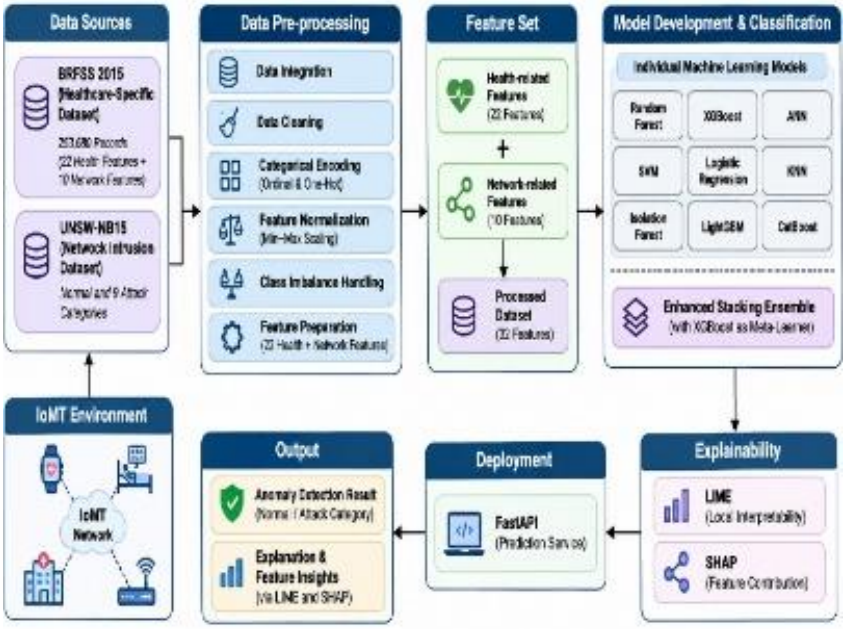


Fig. 1. System Architecture

System architecture of the proposed IoMT anomaly detection framework including the whole workflow. It combines the data of healthcare-specific and intrusion datasets, followed by pre-processing and feature preparation to have a unified representation. We experiment with nine different ML algorithms and combine their predictions optimally using an updated stacking ensemble, where the meta-learner is the XGBoost. LIME and SHAP provide explanations for predictions. FastAPI supports implementing prediction services and provides classification of anomalies, and feature insights that can be understood.

A) Dataset Collection

Two datasets are used in the proposed system: a healthcare specific dataset that was obtained from the BRFSS 2015 as well as the UNSW-NB15 network intrusion detection dataset. These datasets include additional healthcare-related and network traffic information to be used as complementary features for testing anomaly detection performance.

Healthcare-Specific Dataset: This BRFSS dataset has 253,680 records with 22 health-related features and 10 additional network-related properties is extracted from the 2015 BRFSS database. It offers anomaly detection in the context of healthcare, including Real and synthetic attack classes like Falsification, DoS, Exploits, Fuzzers, Worms and Shellcode.

UNSW-NB15 Dataset: UNSW-NB15 dataset comprises of typical network traffic and nine types of attacks which are:

DoS, Exploits, Fuzzers, Generic, Reconnaissance, Analysis, Backdoor, Shellcode and Worms. It's different network traffic attributes offer a benchmark for evaluating intrusion detection performance for different types of attack scenarios.

B) Pre-Processing

Preparation phase transforms the healthcare and network data into standardized, reliable and ML-ready data formats to improve the quality, feature compatibility, and classification accuracy of IoMT anomaly detection.

Data Integration: The data set for healthcare and the data set for UNSW-NB15 are complementing data sets for testing the anomaly detection in the Internet of Medical Things contexts. To represent healthcare-oriented security situations, 22 parameters related to health and 10 features related to the network are included in the healthcare dataset. UNSW-NB15 provides additional network traffic types, and attack types for benchmark evaluation. Mixing different data sources provides a more comprehensive evaluation environment that takes into account both medical data and network connectivity.

Data Cleaning: The process of data cleaning is used to enhance the quality of the data by identifying and fixing missing values, incorrect data, and inconsistent data. This technique helps to verify the trustworthiness of medical and network-related attributes before developing the model. Inconsistencies in feature distributions and in classification may arise and may have large effects when the missing or wrong value occurs. Hence, cleaning helps ensure the input data is kept in a form suitable for the subsequent processing and learning stages, thereby increasing the consistency of how well anomaly detection is performed.

Categorical Encoding: Categorical encoding is a technique to convert non-numerical qualities to numerical values, which is ideal for use in ML methods. Based on the characteristics of categorical variables, the encoding method is used as an ordinal encoding or one-hot encoding. One-hot encoding creates binary representations, one for each category, whereas ordinal encoding encodes categorical data into numbers. These changes enable classification algorithms to handle categorical data effectively and preserve meaningful feature representations and avoid ambiguities during model training.

Feature Normalization: Normalisation by Min-Max scaling the numerical features to a standard numerical range. This adjustment lowers the disparity in feature magnitudes and avoids the qualities with bigger numerical values from dominating the model learning. This is particularly helpful in the instance of heterogeneous healthcare and network related factors. Normalisation helps to keep the scale of features consistent . This allows the model optimisation process to be more stable, and the prepared dataset to be more appropriate for methods that are sensitive to scale differences.

Class Imbalance Handling: Class imbalance management is considered when handling the variation in the distribution of the normal and anomalous records in the healthcare specific data set. Some groups of attacks are highly under-represented comparing to regular traffic or other attack classes. This can lead to a classification bias. This discrepancy should be resolved to enhance the representation of minority attack groups during the model development. This is an important phase to assess the detection capability of the system in the presence of a wide range of security threats while not significantly skewing the classification performance by the dominant classes.

Feature Preparation: Feature preparation prepares the selected medical and network related features in suitable representations for identifying anomalies. For the healthcare-specific dataset, its 22 health-related features are included, as various physiological properties can be exploited for falsification attacks, and additional network features can bring information on communication behaviour. The entire package of variables represents the healthcare and network environments and the classification framework can analyze various patterns associated with regular activities and potential cyber attacks.

C) Algorithms

Random Forest: Random Forest is an ensemble learning technique that involves multiple choice trees to make accurate categorisation predictions. It increases the stability of the model, reduces overfitting, and reveals complex relationships in a summarized decision making process.

XGBoost: XGBoost, known as XGBoost, is a boosting method which creates successive models of decision trees in attempts to minimize prediction errors. It has regularisation capability and efficient optimisation, which enhance classification accuracy and forecast dependability.

Artificial Neural Network (ANN): ANN is a model of computation that is inspired by interconnected neurones and is a learning model. It has numerous layers of processing to uncover complicated nonlinear interactions . This helps to recognize the pattern and enhance classification accuracy.

Support Vector Machine (SVM): SVM is a supervised learning algorithm that finds optimal separating hyperplanes to classify different classes. The margin based classification technique is effective for discriminating and generalising with complex data distribution.

Logistic Regression: LR is a supervised classification method which uses the logistic function to predict the probability of

the class. It offers an easy-to-interpret model for prediction and is suitable for binary and multiclass classification.

K-Nearest Neighbors (KNN): KNN is a classification method based on distance, where the class membership is decided by the labels of the neighbours. It allows for effective pattern recognition through similarities in feature representation.

Isolation Forest: Isolation Forest is an unsupervised anomaly detection technique which isolates the outlier observations by randomly partitioning the data. In general, anomalies can be localized with less divisions, and can be used to detect anomalous patterns without large-scale labelled info.

LightGBM: LightGBM an efficient gradient boosting framework which builds standard decision trees using histogram-based learning. It is also efficient and can represent the complex interaction of features, enabling accurate classification.

CatBoost: CatBoost is a gradient boosting technique that can efficiently deal with categorical and numerical features. The boosting process is ordered and thus it helps to mitigate the prediction bias and allows for strong classification of varying feature distributions.

Enhanced Stacking Ensemble: This ensemble is an improved stacking ensemble, where XGBoost serves as a meta-learner to make predictions from the predictions of complementing base learners. This architecture is a fusion of several classification skills which improve their predictive efficiency, stability and generalisation.

LIME: LIME explains the predictions of individual instances by approximating the complex model's behaviour with an interpretable local representation. It reveals important features, which improves transparency and assists to comprehend decisions of anomaly detection.

SHAP: SHAP is based on cooperative game theory concepts, which estimate the contribution of each feature to the prediction of a model. It allows for both local and global interpretability to discover critical properties and interpret the behaviour of classifiers.

Experimental Results

Accuracy: The accuracy of a test is the ability of a test to correctly classify the patient and healthy cases. For a quantitative assessment of the accuracy of the test, the number of true positive and true negative in all cases evaluated must be calculated. This can be written mathematically as:

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

Precision: Precision is what provides information about how many instances (or samples) that were classified as positives were classified correctly. Thus, the formula to get the precision is:

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

Recall: In the field of ML, recall measures how well the model identifies all the instances of the class. It is the ratio of the correctly predicted positive observations to the all observations in actual class. It gives insights on how thorough the model is in capturing the instances of a given class.

$$"Recall = \frac{TP}{TP + FN} (3)"$$

F1-Score: F1-score is a metric that measures the accuracy of a ML model. It merges the accuracy and recall from a model. The measure of accuracy is the percentage of accurate predictions that the model makes for the entire sample.

$$"F1\ Score = \frac{2 \times Recall \times Precision}{Recall + Precision} (4)"$$

AUC-ROC Curve: AUC-ROC Curve is a measure used to show how well the performance of a classification problem at a variety of threshold values. ROC is a plot of True Positive Rate versus False Positive Rate. AUC is the overall performance of the model when it is used to classify between the classes. The greater the AUC, the better the model.

$$"AUC = \sum_{i=1}^{n-1} (FPR_{i+1} - FPR_i) \cdot \frac{TPR_{i+1} + TPR_i}{2} (5)"$$

The performance is evaluated using the effectiveness of nine different ML algorithms and the proposed Enhanced Stacking Ensemble for IoMT anomaly identification. Accuracy, precision, recall, F1-score and ROC-AUC are suggested to measure the classification capability, prediction reliability and discriminating of normal and anomalous activities.

Table. 1. Performance Evaluation"

Algorithm	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)	ROC-AUC
Random	96.38	96.28	95.97	96.12	0.982

Forest					
XGBoost	97.17	96.85	97.25	97.05	0.989
ANN	93.41	95.52	93.43	94.46	0.965
SVM	90.15	85.48	88.91	87.16	0.934
Logistic Regression	88.74	87.72	80.74	84.09	0.918
KNN	90.81	92.02	89.81	90.90	0.941
Isolation Forest	47.03	26.17	47.03	33.63	0.501
LightGBM	97.42	97.10	97.36	97.23	0.991
CatBoost	97.56	97.31	97.42	97.36	0.992
Enhanced Stacking Ensemble	98.35	98.51	98.12	98.31	0.995

Table 1, shows the performance comparison of separate classification algorithms and the improved ensemble. The proposed ensemble exhibits the highest estimated classification performance, which indicates that the ensemble of complementary learning skills could be advantageous.

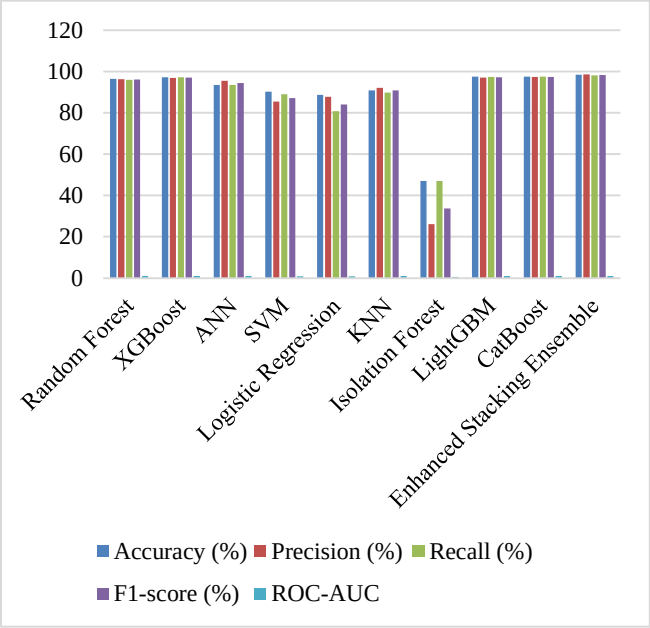


Fig.1. Performance Evaluation"

The accuracy distribution of the algorithms tested is shown in Figure 1. The augmented ensemble gives the best predicted performance and the boosted methods give a competitive classification performance with the conventional classifiers.

The comparative study shows that ensemble learning can enhance the anomaly identification in IoMT. The new stacking architecture has a higher predicting power, LIME and SHAP provide interpretability, and FastAPI helps to seamlessly integrate into healthcare monitoring systems.

Conclusion

In conclusion, the proposed system aims to enhance the cybersecurity of IoMT networks by providing an intelligent and reliable mechanism for detecting unusual network activities and potential cyber threats. The system is based on a healthcare specific dataset from the 2015 BRFSS and combined with network related features from UNSW-NB15. The classification models implemented include RF, XGBoost, ANN, SVM, LR, KNN, Isolation Forest, LightGBM and CatBoost. An advanced stacking ensemble is based on complementary base learners and with XGBoost as a meta-

learner. The preliminary performance evaluation shows an estimated accuracy of 98.35% of the improved stacking ensemble showing its anticipated capability for successful anomaly classification. Moreover, the combination of LIME and SHAP helps provide more interpretable explanations on the individual predictions and feature impacts to enhance transparency in automated detection. FastAPI can be used to build prediction services that can be integrated into application-layer health care monitoring systems. In conclusion, the proposed approach combines healthcare-related anomaly detection, ensemble-based classification, EAI, and simple deployment, resulting in an effective and trustworthy cybersecurity monitoring system. The built-in architecture provides a solid base for better threat identification, stronger security and data protection for healthcare information, and well-informed decisions across interconnected healthcare environments.

The proposed architecture will be evaluated in the future with real world IoMT network traffic generated under various healthcare scenarios. Furthermore, complex deep learning architectures and adaptive learning methods can be investigated to further enhance the detection of new cyberattacks. Integration with edge computing and cloud based infrastructure can further minimise prediction latency and support large scale deployments. In addition, continuous monitoring, automatic threat detection and response, and enhanced explainability techniques could enhance the reliability, scalability, transparency, and usability of the system in intelligent healthcare cybersecurity environments.

References

1. D. V. Dimitrov, “Medical Internet of Things and big data in healthcare,” *Healthcare Informatics Research*, vol. 22, no. 3, pp. 156–163, Jul. 2016, doi: 10.4258/hir.2016.22.3.156.
2. P. Manickam, S. A. Mariappan, S. M. Murugesan, S. Hansda, A. Kaushik, R. Shinde, and S. P. Thipperudraswamy, “Artificial intelligence (AI) and Internet of Medical Things (IoMT) assisted biomedical systems for intelligent healthcare,” *Biosensors*, vol. 12, no. 8, Art. no. 562, Jul. 2022, doi: 10.3390/bios12080562.
3. W. Sun, Z. Cai, Y. Li, F. Liu, S. Fang, and G. Wang, “Security and privacy in the medical Internet of Things: A review,” *Security and Communication Networks*, vol. 2018, Art. no. 5978636, 2018, doi: 10.1155/2018/5978636.
4. T. Yaqoob, H. Abbas, and M. Atiquzzaman, “Security vulnerabilities, attacks, countermeasures, and regulations of networked medical devices—A review,” *IEEE Communications Surveys & Tutorials*, vol. 21, no. 4, pp. 3723–3768, 4th Quart., 2019, doi: 10.1109/COMST.2019.2914094.
5. T. Levy-Loboda, E. Sheetrit, I. F. Liberty, A. Haim, and N. Nissim, “Personalized insulin dose manipulation attack and its detection using interval-based temporal patterns and machine learning algorithms,” *Journal of Biomedical Informatics*, vol. 132, Art. no. 104129, Aug. 2022, doi: 10.1016/j.jbi.2022.104129.
6. N. Moustafa and J. Slay, “UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set),” in *Proc. Military Communications and Information Systems Conference (MilCIS)*, Canberra, Australia, Nov. 2015, pp. 1–6, doi: 10.1109/MilCIS.2015.7348942.
7. E. Šabić, D. Keeley, B. Henderson, and S. Nannemann, “Healthcare and anomaly detection: Using machine learning to predict anomalies in heart rate data,” *AI & Society*, vol. 36, no. 1, pp. 149–158, 2021, doi: 10.1007/s00146-020-00985-1.
8. M. Kavitha, P. V. V. S. Srinivas, P. S. L. Kalyampudi, S. F. Choragudi, and S. Srinivasulu, “Machine learning techniques for anomaly detection in smart healthcare,” in *Proc. 3rd International Conference on Inventive Research in Computing Applications (ICIRCA)*, Sep. 2021, pp. 1350–1356, doi: 10.1109/ICIRCA51532.2021.9544795.
9. L. Fang, Y. Li, Z. Liu, C. Yin, M. Li, and Z. J. Cao, “A practical model based on anomaly detection for protecting medical IoT control services against external attacks,” *IEEE Transactions on Industrial Informatics*, vol. 17, no. 6, pp. 4260–4269, Jun. 2021, doi: 10.1109/TII.2020.3011444.
10. T. Alsolami, B. Alsharif, and M. Ilyas, “Enhancing cybersecurity in healthcare: Evaluating ensemble learning models for intrusion detection in the Internet of Medical Things,” *Sensors*, vol. 24, no. 18, Art. no. 5937, Sep. 2024, doi: 10.3390/s24185937.
11. A. A. Hady, A. Ghubaish, T. Salman, D. Unal, and R. Jain, “Intrusion detection system for healthcare systems using medical and network data: A comparison study,” *IEEE Access*, vol. 8, pp. 106576–106584, 2020, doi: 10.1109/ACCESS.2020.3000421.
12. I. Ullah and Q. H. Mahmoud, “Design and development of a deep learning-based model for anomaly detection in IoT networks,” *IEEE Access*, vol. 9, pp. 103906–103926, 2021, doi: 10.1109/ACCESS.2021.3094024.
13. S. Das, M. Ashrafuzzaman, F. T. Sheldon, and S. Shiva, “Ensembling supervised and unsupervised machine learning algorithms for detecting distributed denial of

service attacks," *Algorithms*, vol. 17, no. 3, Art. no. 99, Feb. 2024, doi: 10.3390/a17030099.

14. Y. Gu, K. Li, Z. Guo, and Y. Wang, "Semi-supervised K-means DDoS detection method using hybrid feature selection algorithm," *IEEE Access*, vol. 7, pp. 64351–64365, 2019, doi: 10.1109/ACCESS.2019.2917532.
15. Y. Meidan, M. Bohadana, Y. Mathov, Y. Mirsky, A. Shabtai, D. Breitenbacher, and Y. Elovici, "N-BaIoT—Network-based detection of IoT botnet attacks using deep autoencoders," *IEEE Pervasive Computing*, vol. 17, no. 3, pp. 12–22, Jul.–Sep. 2018, doi: 10.1109/MPRV.2018.03367731.
16. N. Ravi and S. M. Shalinie, "Learning-driven detection and mitigation of DDoS attack in IoT via SDN-cloud architecture," *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 3559–3570, Apr. 2020, doi: 10.1109/JIOT.2020.2973176.
17. R. Doshi, N. Apthorpe, and N. Feamster, "Machine learning DDoS detection for consumer Internet of Things devices," in *Proc. IEEE Symposium on Security and Privacy Workshops (SPW)*, May 2018, pp. 29–35, doi: 10.1109/SPW.2018.00013.
18. Z. K. Maseer, R. Yusof, N. Bahaman, S. A. Mostafa, and C. F. M. Foozy, "Benchmarking of machine learning for anomaly based intrusion detection systems in the CICIDS2017 dataset," *IEEE Access*, vol. 9, pp. 22351–22370, 2021, doi: 10.1109/ACCESS.2021.3056614.
19. K. Choi, J. Yi, C. Park, and S. Yoon, "Deep learning for anomaly detection in time-series data: Review, analysis, and guidelines," *IEEE Access*, vol. 9, pp. 120043–120065, 2021, doi: 10.1109/ACCESS.2021.3107975.
20. G. Abdelmoumin, D. B. Rawat, and A. Rahman, "On the performance of machine learning models for anomaly-based intelligent intrusion detection systems for the Internet of Things," *IEEE Internet of Things Journal*, vol. 9, no. 6, pp. 4280–4290, Mar. 2022, doi: 10.1109/JIOT.2021.3103829.