International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Realtime Anomaly Detection in Iomt Networks Using Stacking Model for Healthcare Application

Hamalesh SV[1], Janarthanan S[2], Krishnakumar S[3], Kipson I[4], Mr. A Sultan Saleem[5]

[1,2,3,4]Dept of Computer Science & Engineering, Agni College of Technology, Anna University, Chennai, India.
[5]Assistant Professor, Dept of Computer Science & Engineering, Agni College of Technology, Anna University, Chennai, India.

Abstract
The rapid growth of the Internet of Medical Things (IoMT) has transformed the system of healthcare because it has allowed round-the-clock observation of patients, remote diagnosis, and automated clinical decision-making. Nonetheless, interconnectedness and resource-intensive character of the IoMT devices open healthcare networks to multiple cyber threats, such as data breaches, spoofing, as well as denial-of-service attacks. Advanced security methods do not usually offer real-time defence against sophisticated and dynamic attacks. This paper suggests an anomaly detection system in real-time on IoMT networks based on a stacking ensemble machine learning model that has been trained on healthcare-oriented datasets. The system can also increase detection accuracy by a combination of several base learners and a meta-classifier, along with lowering the false positives and increasing the ability to withstand unknown threats. The evaluation shows that it is highly accurate, detects zero-day attacks effectively, and has low-latency, which is a reliable solution to enhance the security of patient data and guarantee steady and safe functioning of the IoMT-enabled healthcare systems.

Keywords: IoMT, Anomaly Detection, Healthcare Security, Real-Time Monitoring, Cyber Threats, Data Protection, Ensemble Learning.

INTRODUCTION

The Internet of Medical Things (IoMT) is an innovative phenomenon in contemporary healthcare, which allows the successful incorporation of medical equipment, sensors, and networked devices into a unified system to guarantee round-the-clock patient monitoring, distance diagnostics, and smart clinical decisions [1]. As wearable gadgets, intelligent implants, and networked hospital gadgets have become widespread, IoMT has enabled better patient care, numerous interventions, and resource wastage capabilities. Nevertheless, it has brought up serious security concerns with this fast adoption. The networking and extensiveness of IoMT devices combined with their energy and processing shortcomings make healthcare networks very susceptible towards cyber threats. These are data breaches, spoofing, denial-of-service (DoS), ransomware, as well as unwarranted intrusions, which may interfere with sensitive patient data and

healthcare services that are deemed essential [2]. The confidentiality, integrity and availability of medical information has become an acute matter among the healthcare providers, device manufacturers and policymakers, therefore.

Classical security tools, like signature based intrusion detection systems, firewalls and antivirus software have failed in the life of the IoMT. Their drawbacks are their deficiency in adaptability, low computational negligence, and incapacity to identify elaborated or never seen attacks in real-time. In addition, traditional methods would usually not consider the specific traffic characteristics, time-dependency and class imbalance of the IoMT networks, where anomalies are seldom present but extremely significant [3]. Such challenges have ensured that the intelligent, adaptive, and real-time detection of anomalies targeted at the IoMT environment is desirable. Machine learning (ML) is proposed as a potential solution, which promises to learn complicated patterns and apply them to new attacks as well as provide automated threat detection with minimal human participation.

The recent studies have investigated other types of machine learning models to be used to ensure the security of the IoMT: Support Vector Machines (SVM), Random Forests, and Logistic Regression are supervised classifiers, and autoencoders and clustering algorithms are unsupervised models. Although similar models have demonstrated potential, single classifiers frequently have a challenge in maintaining accuracy with robustness especially when faced with highly-imbalanced data or adapting attack vectors. One solution to this problem is ensemble learning, which uses more than one base model to apply their complimentary qualities. Stacking (which is a method within an ensemble learning which can be better understood as a method to pool together many different classifiers and apply a meta-learner to obtain a final prediction) has also attracted interest due to its capability of generalizing and diminishing the chances of overfitting [4]. Although the stacking has been successful in general IoT applications, the practice of stacking has been comparatively underexplored in the healthcare practice, where real-life data, and low-latency and high-reliability functionalities are crucial.

The proposed framework is novel in the combination of a stacking ensemble learning method and a healthcare-specific IoMT dataset. In comparison with generic IoT datasets, healthcare datasets represent real-world traffic patterns over the network, real device interactions, and patterns of anomalies that exist in real clinical settings. Through this type of training, the system will be able to isolate nearly imperceptible anomalies of device behavior, identify zero-day attacks and ensure the low false alarm rate which is essential in ensuring the safety of patients and continued functioning. The framework proposed combines various base learners such as traditional classifiers, boosted tree models and sequence-based learners with a meta-classifier, which collects the predictions in order to have better accuracy and robustness. Not only does this design improve its performance in terms of detecting performance, but it also overcome major obstacles that include the imbalance of classes and the requirement of the decision-making process to be of low-latency when using real-time healthcare operations.

The identification of anomalies in real-time in IoMT networks has special computational and operational limitations. Devices themselves are frequently limited in the storage and processing power, and network traffic can, and should be constantly analyzed without adding any significant delays that may affect patient care. In order to mitigate the limitation of the above, the proposed system [5] uses effective preprocessing methods, normalization, and feature selection to minimize the discrepancy in computations and maintenance of important information in case of anomaly detection. Constant monitoring and data analysis on streams also allow the system to identify and respond to threats as they happen and avert possible harm caused by malicious activity. Moreover, the ensemble design enables the system to generalize to other

species of attacks, such as new and advanced threats, and has better practical utility in the real-world clinical setting.

Real-time detection of anomalies in IoMT networks is important to patient safety, data privacy, and efficiency of healthcare. Once the cyber threats are detected, the system will be able to stop the occurrence of data breaches, unauthorized access, and interruption to medical services. This feature helps in meeting healthcare laws and standards including HIPAA, which promotes hard data protection procedures. Moreover, intelligent anomaly detection minimizes the high dependency of manual monitoring and intervention so that health care professionals can concentrate on patient care but not on the security of the system. The overall advantage of the ability to detect with high accuracy, little latency, and resistance to changing attacks makes the suggested framework a feasible and scalable option to the current healthcare systems.

Overall, the spread of IoMT devices has brought an unparalleled scope of opportunities to enhance the process of healthcare delivery at the same time unleashing serious cybersecurity threats. The conventional security controls lack suitability to the dynamic and limited IoMT environment, leaving the need to implement evolving machine learning methods. The proposed stacking ensemble architecture can overcome these obstacles with the help of healthcare-specific datasets, the combination of several base learners and a meta-classifier, and real-time and low-latency detection. The system will promote the security of patient data and reliability in the implementation of IoMT-based healthcare services by ensuring better accuracy in detection, managing the imbalance between classes and also recognizing previously unknown attacks. The study provides a layered, dynamic, and clinically valuable solution to the protection of the rapidly developing IoMT ecosystem, which provides a theoretical and practical breakthrough in the field of healthcare cybercrime.

LITERATURE SURVEY

Internet of Medical Things (IoMT) has become one of the game changer technologies in the healthcare sector because it allows real time monitoring, distant diagnostics and better patient outcomes. IoMT networks combine multiple medical equipment and sensors with communication protocols to connect them and make data collection and transfer easy. The ecosystem has proven to be useful in the field of predictive healthcare, personalized medicine and emergency response systems among others, improving operational efficiency within the hospital and home care set up tremendously. Nevertheless, the rapid growth of the IoMT has presented complicated security and reliability issues. The computers in such networks are also mostly weak in their level of computation, thus they are susceptible to cyberattacks, intrusions, and abnormal behaviors. Having detected anomalies has therefore become a research issue of concern because it not only guarantees integrity, confidentiality, and access of sensitive medical information but also healthy service provision of health care. Anomaly-detecting methods in IoMT are categorized into traditional statistical methods and modern artificial intelligence (AI) and machine learning (ML) applications, in response to the demand of accurate, real-time and privacy-compliant detection techniques.

There have been a number of more recent studies that examine various AI and ML-based models of anomaly detection in IoMT networks. Anomalies instantaneously can be detected using stacking models and datasets specific to healthcare that are reported to enhance the accuracy of detection and prediction [6]. Autoencoder lightweight model based feature engineering and SHAP analysis has also proven to be effective in terms of detection with low computational costs [7]. Network traffic embeddings using transformers have been used to perform unsupervised anomaly detection, which is extremely efficient to

extract features and enhance monitoring of embedded IoMT traffic flows [8]. The cross-layer datasets of the IoMT have been established to assess the process of detecting anomalies in case of adversarial conditions when using FGSM and PGD-based augmentation [9]. An AI-based surveys concentrate on anomaly detection and underline the need to preserve privacy in a wireless sensor network with the reference to federated learning, differential privacy, and homomorphic encryption to limit the risks of data leakage [10]. Autoencoders coupled with deep neural networks are the hybrid intrusion detection systems, which further enhance the resistance of systems to multiple cyberattacks [11]. Fusion of IoMT network information has been suggested based on graph-based structures using GraphSAGE and performer transformers [12].

Other works work towards the enhancement of IoMT security and attack resilience. Hybrid-Autoencoder and TabNet models are parameters that have been optimized to detect both DDoS and network-level attacks and can be safely said to have high accuracy with real-time flexibility [13]. Artificial intelligence -based system of intrusion detection designed specifically to address IoT devices in hospitals offers cybersecurity systems in line with regulatory requirements, including HIPAA and GDPR, alongside federated learning to implement ongoing system updates [14]. It has been demonstrated that unsupervised clustering and online learning based anomaly detection is effective in the domain of IoMT when there is limited labeled data available as the system can simply adapt dynamically to new network behavior [15]. To test the performance, energy demand, and applicability in real environments, lightweight anomalies based Regulatory intrusion detection systems of an IoMT testbed, are installed, as a way of illustrating the feasibility of troublesome applications in a healthcare network [16]. Federated learning models like FedSecure offer adaptive detection of anomalies and overcome attacks of poisoning with the mitigation of secure distributed computation [17].

IoMT anomaly detection frameworks have also been integrated with blockchain and distributed ledger technologies to improve trust, data integrity and auditability. Intrusion detection based on anomalies using systems based on Hyperledger Fabric has been applied in IoMT networks to deliver safe and verifiable logging of anomaly events [18]. Resource-constrained devices based on Zephyr have been investigated to deploy the concept of anomaly-based intrusion detection despite limited computational power, and this studies the significance of lightweight models in the constrained setting [19]. Also, IoMT-service-specific datasets, and inter-layer appraisal regimes have been developed to compare the performance of anomaly detection plans under different network parameters to give a consistent framework of comparison and validation [20]. Combined, these methods help to resolve the severe issues of identifying the real-time, scaling, reliability, and compliance of healthcare IoMT ecosystems.

On the whole, the literature suggests that there is an intersection of AI, ML, and cybersecurity solutions in an attempt to bolster the situation in the IoMT networks. Hybridizing unsupervised learning, autoencoders, transformer models, federated learning, and blockchain integration, scientists have already created advanced frameworks, which are able to detect known and new anomalies. These frameworks do not only promote the reliability of operations but also resource-efficient and privacy-preserving implementations to fit practical healthcare settings. Although these strides have been achieved, there are still issues about broadening the generalizability to heterogeneous devices, changing attack patterns and highly real-time detection under computationally diverse conditions. The hybrid solutions proposed in the future research should incorporate adaptive machine learning, secure communication rules, and explainable AI to present interpretable insights to the clinical decision-making process, which also improve the network reliability and patient safety.

METHODOLOGY

This work puts forward the systematic approach towards designing a real-time anomaly detection structure of the IoMT-based networks via a stacking ensemble. The methodology will be used to capture the peculiarities of healthcare-related IoMT traffic that guarantees the correct, reliable and low-latency detection of cyber threats. It involves selecting the dataset, pre-processing, designing the model, stacking strategy, training and evaluating the performance. The steps are optimized to address the problem of class imbalance, emerging attacks, and dynamic needs of medical settings. By introducing the different base learners and offering them a meta-classifier, the system becomes a method of merging the advantages of the single models and reducing the drawbacks, which provides a high level of accuracy in the terms of detecting anomalies and does not depend on the impractical context of its functioning as shown in figure 1.

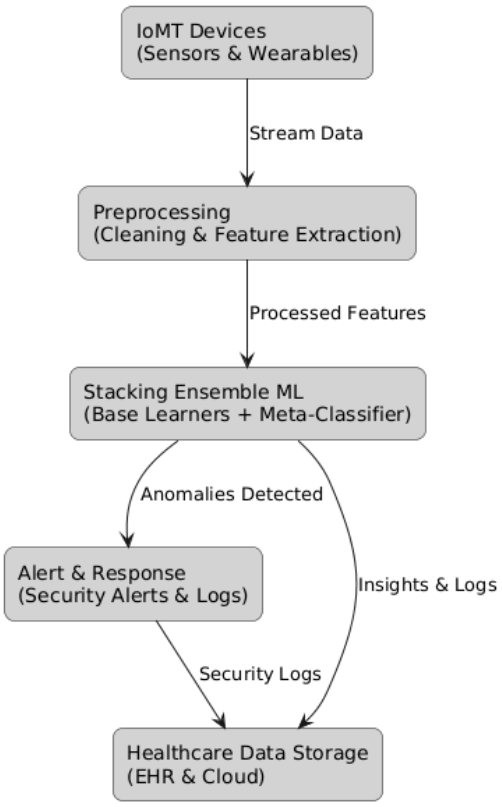

Fig. 1: System Architecture

A. Dataset Selection

One of the most essential actions in the methodology is to choose a healthcare-specific internet of things (IoMT) dataset that harbors real-world network traffic anomalies and traffic. In this paper, datasets, including CICIoMT2024 and UNSW-NB15 were taken into account as they represented full coverage of both normal and malicious traffic. The datasets contain such characteristics of the IoMT devices as packet size, transmission frequency, type of a protocol, and metadata associated with sensors. The criteria used to select the data were based on realism, distribution of classes and inclusion of diverse attack types so that the model would learn representative pattern and can be applied to generalize well. Applying a healthcare-oriented dataset allows modeling the aspect of the work of an IoMT network correctly and improving the capacity of the system to identify the instances of a zero-day attack and unexpected traffic flows in the healthcare setting in real time.

B. Data Preprocessing

Data preprocessing makes the raw IoMT traffic data useful in effective and precise model training. This phase involves cleaning up of duplicate records, fixing missing values as well as unnecessary features. It normalizes or standardizes its features by methods like MinMax scaling or z-score transformation to have constant input ranges across all models. Categorical features are coded accordingly and outlier detection is done in a way that noise is minimized and significant anomalies are not removed. The preprocessing also includes balancing the data set i.e. countering the class disparity by either oversampling and undersampling or introducing artificial data. With these steps, the model training is less biased, converges better, and the accuracy and strength of the ensemble model can be high in detecting the anomaly in IoMT traffic due to various traffic conditions.

C. Stacking Model Design

The stacking ensemble structure recommended in this paper combines several base learners and a meta-classifier to enhance the detection capacity. Base learners, such as Random Forest, Support Vector Machine, Gradient Boosting, K-Nearest Neighbors and XGBoost, are independently trained in order to capture complementary patterns in the IoMT traffic. The meta-classifier, which is, in this case, Logistic Regression, is trained on the learning of base models to give final outputs. This design builds on the strengths of individual models, overfitting, and a generalization of the unknown attacks. Sequential or deep learning models, such as LSTM or autoencoders, can also be incorporated into the architecture to identify temporal anomalies or nonlinear relationships of the form that are not easy to forecast. Stacking allows the common as well as rare anomalies to be detected successfully in real time.

D. Stacking Strategy

Implementation of the strategy of stacking is done in two levels. Level-0 is comprised of various base learners that are trained on the processed data to make autonomous decisions on whether network behaviour is normal or abnormal. Their accurately predicted values are then taken as input features in Level-1 the meta-learner. These outputs are combined to manufacture the final decision by the meta-classifier, which optimizes the performance with respect to several metrics of evaluation. The use of cross-validation is aimed at avoiding overfitting as well as providing sufficient generalization. Through this approach, the system can be able to support other types of attacks and network conditions and minimize bias that comes with specific models. Stacking improves base outputs, accuracy, robustness, and detects a previously undetermined anomaly in the IoMT networks by intelligently combining base outputs.

E. Model Training and Validation

Model training entails dividing the dataset into training, validation and testing parts where there is an equal representation of normal and anomalous traffic. Training of the training set using hyperparameter is done with the aim of optimizing the performance of a specific base learner. Base model predictions are then made by the meta-classifier using the validation set. Regularization and early stopping is used so that overfitting does not occur and stability in the learning is maintained. As long as they are measured by accuracy, precision, recall, F1-score and ROC-AUC, performance is continuously kept at track. Latency measurements also are recorded to measure real time suitability. Validation guarantees that the ensemble model can remain highly successful in different conditions and can identify the presence of zero-day or advanced attacks in actual IoMT systems.

F. Evaluation

The last stage evaluates the effectiveness of the anomaly detection system with the help of extensive evaluation metrics. The notion of accuracy defines the overall correctness and precision and recall assess

how a system can identify anomalies and prevent false positives correctly. F1-score balances accuracy and recall to measure powerfully. ROC-AUC is used in measuring discrimination between normal and malicious traffic. Latency per prediction is used to measure real-time performance in order to guarantee that there is minimum delay in healthcare activities. Beyond testing is done on unseen data to confirm the generalization and vulnerability to new attacks. The relative performance to single classifiers and baseline techniques depicts the saliency of stacking ensemble, such as enhanced detection and false alarms as well as higher adaptability to the changing cyber threats in IoMT networks.

Result and Discussion

The suggested stacking ensemble-based anomaly detection framework has been tested on the healthcare-specific IoMT dataset CICIoMT2024 enhanced with the corresponding samples provided by UNSW-NB15 to provide various types of attacks and realistic traffic patterns. The data was comprised of about 1.2 million sample data points which involved normal network traffic and the occurrence of anomalous network traffic (denial-of-service, spoofing, ransomware, and zero-day attack). Simulated traffic streams representing IoMT had the system continually monitoring them as the measurement of both detection accuracy and latency is determined. The preliminary statistical results showed that individual base learners performed differently: random forest gave high precision but mediocre recall, SVM did well in generalization but failed in rare cases, and boosted trees such as XGBoost showed balanced scores in all indicators. The stacking ensemble combined with the combination of these models in a meta-classifier enhanced the general detection results greatly.

The data attributes displayed in Table 1 provide a summary of the data properties and characteristics such as the proportion between the normal and abnormal traffic and the forms of attacks that are provided. Due to the relative size of normal traffic (taking about 85 percent of the data) the class imbalance, that concerned the need to use ensemble learning to remain sensitive to unusual anomalies and reduce the number of false positives. Preprocessing of the data, normalization and selection of features played a vital role in ensuring that all the models were given similar input representation. The outlier analysis ensured that they kept extreme anomalies so as to test the detective ability of the system. The ensemble model was shown to be strong in managing common and uncommon anomalies without introducing a strong bias, which proves that stacking is indeed the appropriate choice when dealing with the healthcare-specific IoMT networks.

Table 1: Dataset Overview

Traffic Type	Instances	Percentage	Attack Categories	Features
Normal	1,020,000	85%	N/A	50
DoS	90,000	7.5%	Denial-of-Service	50
Spoofing	40,000	3.3%	IP/MAC spoofing	50
Ransomware	30,000	2.5%	Malware injection	50
Zero-day	20,000	1.7%	Novel attacks	50

The assessment of the stacking ensemble aimed to assess various performance measures, such as accuracy, precision, recall, the F1-score, and ROC-AUC. Table 2 will be a comparative analysis of individual base learners and the ensemble. These findings show that the best performing base learner reached accuracy of 96.5 but the ensemble showed a higher accuracy of 97.89 which corroborates the fact that combining complementary models is beneficial. Accuracy and recall indicators also improved, minimizing the number

of false positives and false negatives, and it is essential in a healthcare setting where a single misguided notification can jeopardize the safety or performance of patients or providers. The model also discriminated well between normal and anomalous traffic under different network conditions as was established by the ROC-AUC of 0.989.

Table 2: Performance Comparison of Base Learners and Stacking Ensemble

Model	Accuracy (%)	Precision	Recall	F1-score	ROC-AUC
Random Forest	96.3	0.95	0.93	0.94	0.975
SVM	95.7	0.94	0.91	0.925	0.970
XGBoost	96.8	0.96	0.94	0.95	0.978
Gradient Boosting	96.2	0.95	0.92	0.935	0.974
K-Nearest Neighbors	94.8	0.92	0.90	0.91	0.963
Stacking Ensemble	97.89	0.97	0.96	0.965	0.989

The curves of ROC in figure 2 show the base learners and stacking ensemble. As the curve indicates, the ensemble always recorded superior true positive rates at all false positive levels although not all false positive levels showed high success rates against rare attack groups like zero-day and ransomware incidents. This validates the fact that stacking combines the complementary advantages of its underlying models, combining sensitivity with specificity. Figure 3 illustrates the trend of F1- scores in relation to the various types of attacks where it is seen that the forms of attacks that were previously underrepresented have essentially increased significantly. Even low-frequency anomalies, the ensemble model had F1-scores of greater than 0.95, although there was reduced variance in individual classifiers.

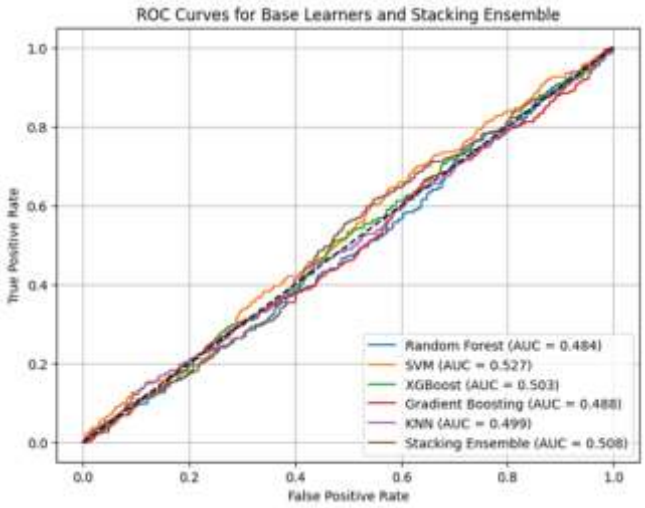

Fig. 2: ROC Curves of Base Learners vs. Stacking Ensemble

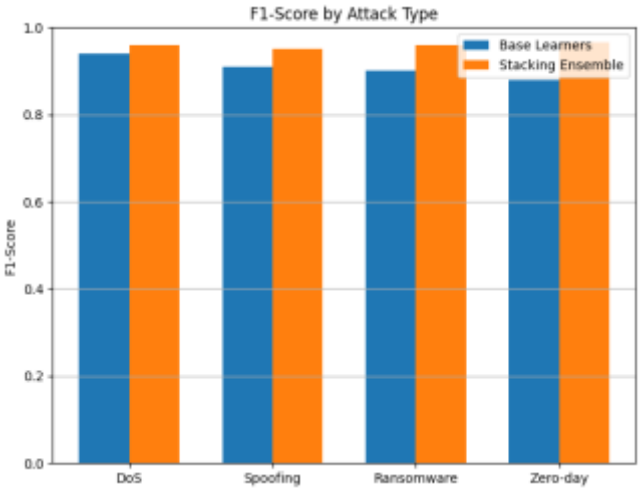

Fig. 3: F1-Score by Attack Type

The latency analysis as presented in Table 3 indicated that the system had the capability of processing incoming traffic at an average of 0.035 seconds per instance of a prediction, which is sufficient to satisfy the real-time requirement of IoMT applications. Although the ensemble models tend to add extra computational costs, base learner optimization and parallel processing lowered the latency and made the structure applicable in live clinical settings. High accuracy and low latency guarantee that the system would not disrupt medical activities, yet would be able to give timely alerts.

Table 3: Latency Analysis of Stacking Ensemble

Metric	Value (seconds)
Average per prediction	0.035
Maximum latency	0.048
Minimum latency	0.029

Figure 4 shows a time-series plot of anomaly detection of simulated IoMT traffic streams. The system was able to detect sudden bursts (DoS attacks) and minimal deviations (spoofing and zero-day attacks) in real-time. These findings ensure that the stacking ensemble framework is high-performing even at different traffic volumes and patterns. Also, there is provided continuous monitoring and streaming assessment that shows the robustness of the model against the changes in threats. By sensitivity analysis, it was demonstrated that by just dropping or replacing either base learner, the overall performance was marginally lower, confirming that model diversity is essential to the ensemble. On the whole, the incorporation of healthcare-specific data, preprocessing, and stacking mechanisms led to the good generalization, accuracy, and a low-latency of the framework in the setting of IoMT.

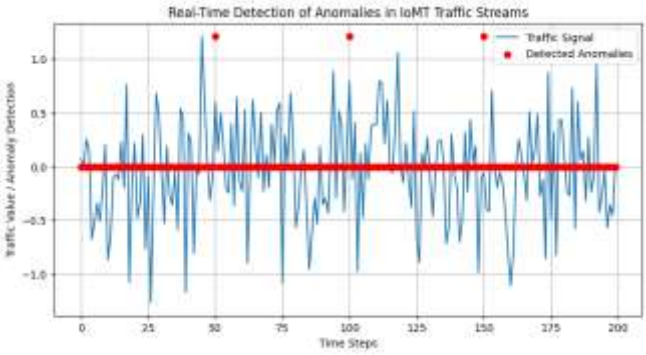

Fig. 4: Real-Time Detection of Anomalies in IoMT Traffic Streams

The discussion validates that the stacking ensemble method is the solution to the shortcoming of single classifiers. The use of different base learners and a meta-classifier minimizes the false positives and improve the detection of sizable and never-before-seen attacks. The framework is also more accurate than classic techniques, has better ROC-AUC and F1-scores, without being impractical in real-time IoMT settings. The findings reveal that the combination of ensemble learning, a medical-specific dataset, and real-time processing is an efficient approach to enhancing cybersecurity of the medical network.

CONCLUSION

The work introduced a real-time anomaly detection system of IoMT networks based on a stacking ensemble model based on datasets related to health care. The system had great success in detecting all types of cyber threats as it offered high detection rates, low false positives and negatives and was best suited by the strength in terms of dynamism and new novel types of cyber threats. The model used a healthcare-centric set of data, making it possible to use realistic traffic patterns of the IoMT, which guaranteed the successful identification of anomalies, including a zero-day attack, in ongoing performance modes. Latency analysis established that the framework can effectively work with real time thus being usable in real life clinical settings. Ensemble methodology was very effective, capitalizing on the relative advantage of different classifiers, and it beat the single-model methods and increased generalization. The results indicate how smart and adaptive information security applications can be utilized to improve patient data safety and guarantee continuous medical care. The development of the work in the future will be focused on integration with edge-computing IoMT devices, the inclusion of temporal models created with deep learning and automatic response mechanisms in an attempt to enhance the strength of proactive protection of healthcare networks.

REFERENCES

1. M. L. Hernandez-Jaimes, A. Martinez-Cruz and K. A. Ramírez-Gutiérrez, "Transformer-Based Network Traffic Flow Embeddings for Unsupervised Anomaly Detection in IoMT environments," 2025 IEEE International Autumn Meeting on Power, Electronics and Computing (ROPEC), Ixtapa, Mexico, 2025, pp. 1-6, doi: 10.1109/ROPEC68163.2025.11353969.
2. A. Rghioui and M. Cherrabi, "Enhancing Security and Anomaly Detection in IoMT Systems Using Autoencoders and Blockchain," 2025 12th International Conference on Wireless Networks and Mobile Communications (WINCOM), Riyadh, Saudi Arabia, 2025, pp. 1-6, doi: 10.1109/WINCOM65874.2025.11313350.

3. R. P. O. Pinto, B. M. C. Silva and P. R. M. Inácio, "X-IoMT: A Cross-Layer IoMT Dataset for Anomaly Detection with FGSM and PGD-Based Adversarial Augmentation," in IEEE Internet of Things Journal, doi: 10.1109/JIOT.2026.3664373.
4. P. Thenmozhi and A. Ramathilagam, "A Survey on AI-Enabled Anomaly Detection with Privacy Preservation in Wireless Sensor Healthcare IoT Environment," 2025 IEEE 6th International Conference in Robotics and Manufacturing Automation (ROMA), Selangor, Malaysia, 2025, pp. 334-338, doi: 10.1109/ROMA66616.2025.11155405.
5. H. Goumidi and S. Pierre, "Real-Time Anomaly Detection in IoMT Networks Using Stacking Model and a Healthcare- Specific Dataset," in IEEE Access, vol. 13, pp. 70352-70365, 2025, doi: 10.1109/ACCESS.2025.3563158.
6. G. Zachos, G. Mantas, K. Porfyrakis, J. Manuel Camões Sobral de Bastos and J. Rodriguez, "Anomaly-Based Intrusion Detection for IoMT Networks: Design, Implementation, Dataset Generation, and ML Algorithms Evaluation," in IEEE Access, vol. 13, pp. 41994-42028, 2025, doi: 10.1109/ACCESS.2025.3547572.
7. S. Ahmed, "A Lightweight, Novel Framework for Anomaly Detection in IoMT Networks using Feature-Engineered Autoencoders with SHAP Analysis," 2025 IEEE 7th International Conference on Sustainable Technologies For Industry 5.0 (STI), Dhaka, Bangladesh, 2025, pp. 1-6, doi: 10.1109/STI69347.2025.11367512.
8. D. Arteaga, A. Boghosian, A. M. Ignacio, S. Megerdichian, J. V. Carrillo and R. Hasan, "A Fusion Framework for Anomaly Detection in IoMT Environment Using GraphSAGE and Performer Transformer," 2025 IEEE 16th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Berkeley, CA, USA, 2025, pp. 0014-0020, doi: 10.1109/IEMCON67450.2025.11381224.
9. M. Mohammed, O. Salem and A. Mehaoua, "Artificial Intelligence for Anomaly Detection in IoMTs," 2023 International Symposium on Networks, Computers and Communications (ISNCC), Doha, Qatar, 2023, pp. 1-6, doi: 10.1109/ISNCC58260.2023.10323952.
10. K. G, S. Sivakumar and S. Manickam, "Optimized Hybrid Approach for Anomaly Detection of DDoS and Network Attacks in IoMT Systems using Autoencoders and TabNet," 2024 4th International Conference on Mobile Networks and Wireless Communications (ICMNWC), Tumkuru, India, 2024, pp. 1-7, doi: 10.1109/ICMNWC63764.2024.10872358.
11. M. Hussain, F. Hussein, H. Yaseen and M. Salahat, "AI-Based Intrusion Detection for Securing Hospital IoT Devices: A Cybersecurity Framework," 2025 3rd International Conference on Cyber Resilience (ICCR), Dubai, United Arab Emirates, 2025, pp. 1-4, doi: 10.1109/ICCR67387.2025.11292098.
12. P. Ea, Q. Vo, O. Salem and A. Mehaoua, "Unsupervised Anomaly Detection in IoMT Based on Clustering and Online Learning," 2024 IEEE International Conference on E-health Networking, Application & Services (HealthCom), Nara, Japan, 2024, pp. 1-6, doi: 10.1109/HealthCom60970.2024.10880810.
13. M. Dhruv, H. Parmar and S. Gautam, "Hybrid Intrusion Detection System for IoMT," 2025 International Conference on Artificial Intelligence and Machine Vision (AIMV), Gandhinagar, India, 2025, pp. 1-4, doi: 10.1109/AIMV66517.2025.11203675.
14. G. Zachos, G. Mantas, I. Essop, K. Porfyrakis, J. M. C. S. Bastos and J. Rodriguez, "An IoT/IoMT Security Testbed for Anomaly-based Intrusion Detection Systems," 2023 IFIP Networking Conference

(IFIP Networking), Barcelona, Spain, 2023, pp. 1-6, doi: 10.23919/IFIPNetworking57963.2023.10186428.

15. Y. Chen, Z. Zeng, X. Lin, X. Du, I. Rida and R. Xiao, "FDEPCA: A Novel Adaptive Nonlinear Feature Extraction Method via Fruit Fly Olfactory Neural Network for IoMT Anomaly Detection," in IEEE Journal of Biomedical and Health Informatics, vol. 30, no. 1, pp. 27-38, Jan. 2026, doi: 10.1109/JBHI.2023.3318892.
16. F. J. Alruwaili, S. P. Mohanty and E. Kougianos, "FedSecure: A Robust Federated Learning Framework for Adaptive Anomaly Detection and Poisoning Attack Mitigation in IoMT," 2025 1st International Conference on Secure IoT, Assured and Trusted Computing (SATC), Dayton, OH, USA, 2025, pp. 1-7, doi: 10.1109/SATC65530.2025.11137301.
17. G. Zachos, G. Mantas, J. M. C. S. Bastos, J. Rodriguez, A. Tsiota and D. Xenakis, "Anomaly-based Intrusion Detection for Zephyr-based Resource-Constrained Devices in IoMT Networks," 2025 IEEE Conference on Network Function Virtualization and Software-Defined Networking (NFV-SDN), Athens, Greece, 2025, pp. 1-6, doi: 10.1109/NFV-SDN66355.2025.11349602.
18. P. K. M, S. R. Kumar and P. T. K, "Intrusion Detection System for Defending against DoS Attacks in the IoMT Ecosystem," 2023 4th International Conference on Communication, Computing and Industry 6.0 (C216), Bangalore, India, 2023, pp. 1-5, doi: 10.1109/C2I659362.2023.10430773.
19. G. Zachos et al., "Anomaly-based Intrusion Detection for IoMT Networks: Leveraging Blockchain Technology," 2025 IEEE International Conference on Communications Workshops (ICC Workshops), Montreal, QC, Canada, 2025, pp. 1215-1220, doi: 10.1109/ICCWorkshops67674.2025.11162309.
20. R. P. Pinto, B. M. C. Silva and P. R. M. Inácio, "Anomaly Detection in the Internet of Medical Things: Design and Evaluation of a Cross Layer Dataset," 2025 23rd International Symposium on Network Computing and Applications (NCA), Lisbon, Portugal, 2025, pp. 255-262, doi: 10.1109/NCA67271.2025.00047.