iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** V **Month of publication:** May 2026

DOI: https://doi.org/10.22214/ijraset.2026.82594

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue V May 2026- Available at www.ijraset.com

Internet of Medical Things (IoMT): Anomaly Detection in Real Time on Healthcare Dataset Using Stack Model

A. Jyothi[1], M. Tilak[2], B. Shakeena[3]
[1, 2, 3]*Computer Science Engineering, Bonam Venkata Chalamayya Institute of Technology and Science*

Abstract: ***The Internet of Medical Things (IoMT) has transformed healthcare by enabling interconnected medical devices, wearable sensors, and healthcare systems to exchange patient information in real time. Although IoMT improves patient monitoring and healthcare efficiency, it also introduces serious cybersecurity challenges due to insecure communication channels and vulnerable medical devices. Detecting abnormal network behavior is essential to ensure secure healthcare operations and protect sensitive patient information. This paper presents a real-time anomaly detection system for IoMT networks using a stacking ensemble machine learning model. The proposed system combines multiple machine learning algorithms including Random Forest, Support Vector Machine (SVM), and Gradient Boosting to improve anomaly detection accuracy. A meta-classifier integrates predictions from the base models to provide final classification results. The system performs data preprocessing, feature extraction, model training, and real-time detection using healthcare-specific datasets. Experimental results demonstrate improved detection accuracy, reduced false positives, and better adaptability compared to traditional single-model approaches.***

Keywords: IoMT, Anomaly Detection, Machine Learning, Stacking Ensemble, Random Forest, SVM, Gradient Boosting, Cybersecurity, Healthcare Dataset.

I. INTRODUCTION

The Internet of Medical Things (IoMT) represents a modern healthcare ecosystem where medical devices, wearable sensors, and hospital systems communicate through internet technologies. IoMT enables remote patient monitoring, real-time diagnostics, and efficient healthcare management. However, due to continuous connectivity and limited security mechanisms in medical devices, IoMT systems are highly vulnerable to cyberattacks such as unauthorized access, malware injection, denial-of-service attacks, and data manipulation.

Traditional intrusion detection systems rely on predefined signatures and fail to identify unknown attacks. Machine learning-based anomaly detection techniques provide better solutions by learning patterns from network traffic and identifying abnormal activities automatically. Ensemble learning approaches further improve detection performance by combining multiple classifiers.

This paper proposes a stacking ensemble-based anomaly detection system for IoMT healthcare networks. The model integrates Random Forest, Support Vector Machine, and Gradient Boosting algorithms to improve prediction accuracy and reduce false alarms in real-time healthcare environments.

II. RELATED WORK

Several researchers have proposed Machine Learning and Deep Learning techniques for anomaly detection in Internet of Medical Things (IoMT) networks. Deepti Gupta et al. developed a federated learning-based anomaly detection system using Digital Twin technology for secure healthcare monitoring. Goumidi et al. proposed a real-time anomaly detection framework using a stacking ensemble model combining Random Forest, SVM, and Gradient Boosting algorithms to improve detection accuracy.

Easa Alalwany et al. introduced a stacking deep learning intrusion detection system capable of detecting attacks such as DoS and ARP spoofing in IoMT environments. Mourad Benmalek et al. proposed SNN-IoMT, which combines CNN, LSTM, and MLP models for efficient intrusion detection in healthcare systems. Other studies used autoencoders, ensemble AI models, and unsupervised deep learning methods to identify abnormal patterns in IoMT network traffic.

Although existing systems improve cybersecurity, many suffer from high false positives, computational complexity, and limited real-time adaptability. The proposed stacking ensemble model overcomes these limitations by providing higher accuracy, reduced false alarms, and efficient real-time anomaly detection for healthcare IoMT networks.

III.EXISTING SYSTEM

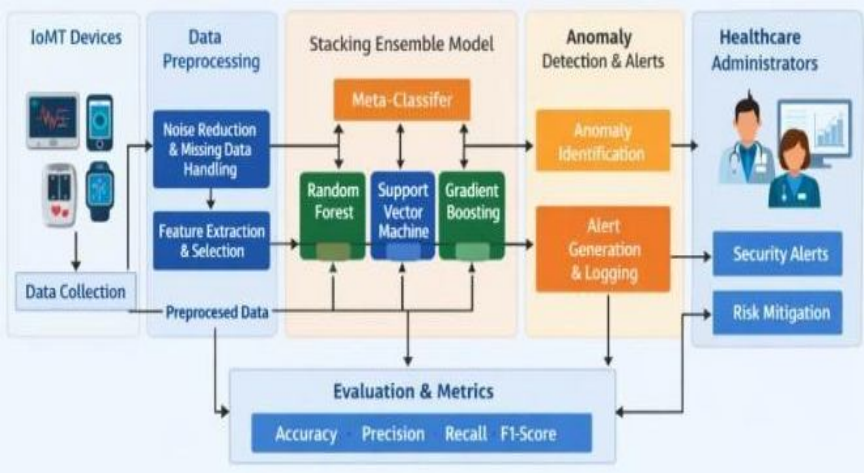
The existing systems for anomaly detection in Internet of Medical Things (IoMT) networks mainly use traditional Intrusion Detection Systems (IDS) and single Machine Learning algorithms such as Decision Tree, KNN, SVM, and Random Forest. These systems detect attacks based on predefined signatures and network traffic patterns. Although they can identify known attacks, they often fail to detect new or unknown cyber threats. Existing models also suffer from low accuracy, high false positive rates, poor scalability, and lack of real-time detection capability in healthcare environments.

IV.PROPOSED SYSTEM

The proposed system introduces a real-time anomaly detection framework for IoMT networks using a stacking ensemble machine learning model. The system combines Random Forest, Support Vector Machine (SVM), and Gradient Boosting algorithms to improve detection accuracy and reliability. A meta-classifier integrates predictions from all base models to identify abnormal network behavior effectively. The proposed approach supports real-time monitoring, reduces false alarms, improves scalability, and provides better adaptability to healthcare-specific IoMT environments.

V. SYSTEM ARCHITECTURE

The above architecture represents a real-time anomaly detection system for Internet of Medical Things (IoMT) networks using a stacking ensemble machine learning model. Initially, data is collected from IoMT devices such as wearable sensors and smart medical equipment. The collected data undergoes preprocessing, where noise removal, missing value handling, and feature extraction are performed to improve data quality. The processed data is then provided to the stacking ensemble model, which combines Random Forest, Support Vector Machine (SVM), and Gradient Boosting algorithms. A meta-classifier integrates the outputs of these models to make accurate predictions. The anomaly detection module identifies abnormal network activities and generates alerts and logs for healthcare administrators. Finally, the system evaluates performance using metrics such as Accuracy, Precision, Recall, and F1-Score to ensure efficient and reliable anomaly detection in healthcare environments.



VI.ALGORITHMS USED

The proposed system uses three important Machine Learning algorithms: Random Forest, Support Vector Machine (SVM), and Gradient Boosting, which are combined using a stacking ensemble model for accurate anomaly detection in IoMT networks. Random Forest is an ensemble learning algorithm that creates multiple decision trees using different subsets of data and combines their outputs through majority voting. It improves accuracy and reduces overfitting while handling complex healthcare network data efficiently. Support Vector Machine (SVM) is a supervised learning algorithm used for classification tasks. It works by finding an optimal boundary called a hyperplane that separates normal and abnormal network behavior with maximum margin, making it highly effective for detecting anomalies. Gradient Boosting is another ensemble algorithm that builds multiple weak prediction models sequentially, where each new model corrects the errors of the previous one. This process improves prediction accuracy and enhances the model's ability to detect complex attack patterns. In the proposed system, these three algorithms act as base classifiers, and their predictions are combined using a meta-classifier in a stacking ensemble model to provide highly accurate and reliable real-time anomaly detection in healthcare IoMT environments.

VII. RESULTS AND DISCUSSION

The proposed stacking ensemble model achieved improved anomaly detection accuracy compared to traditional machine learning models. The system effectively identified abnormal network behavior in healthcare datasets while reducing false positive rates.

A. Advantages

- High Detection Accuracy
- Reduced False Positives
- Real-Time Detection
- Better Scalability
- Improved Generalization

VIII. CONCLUSION

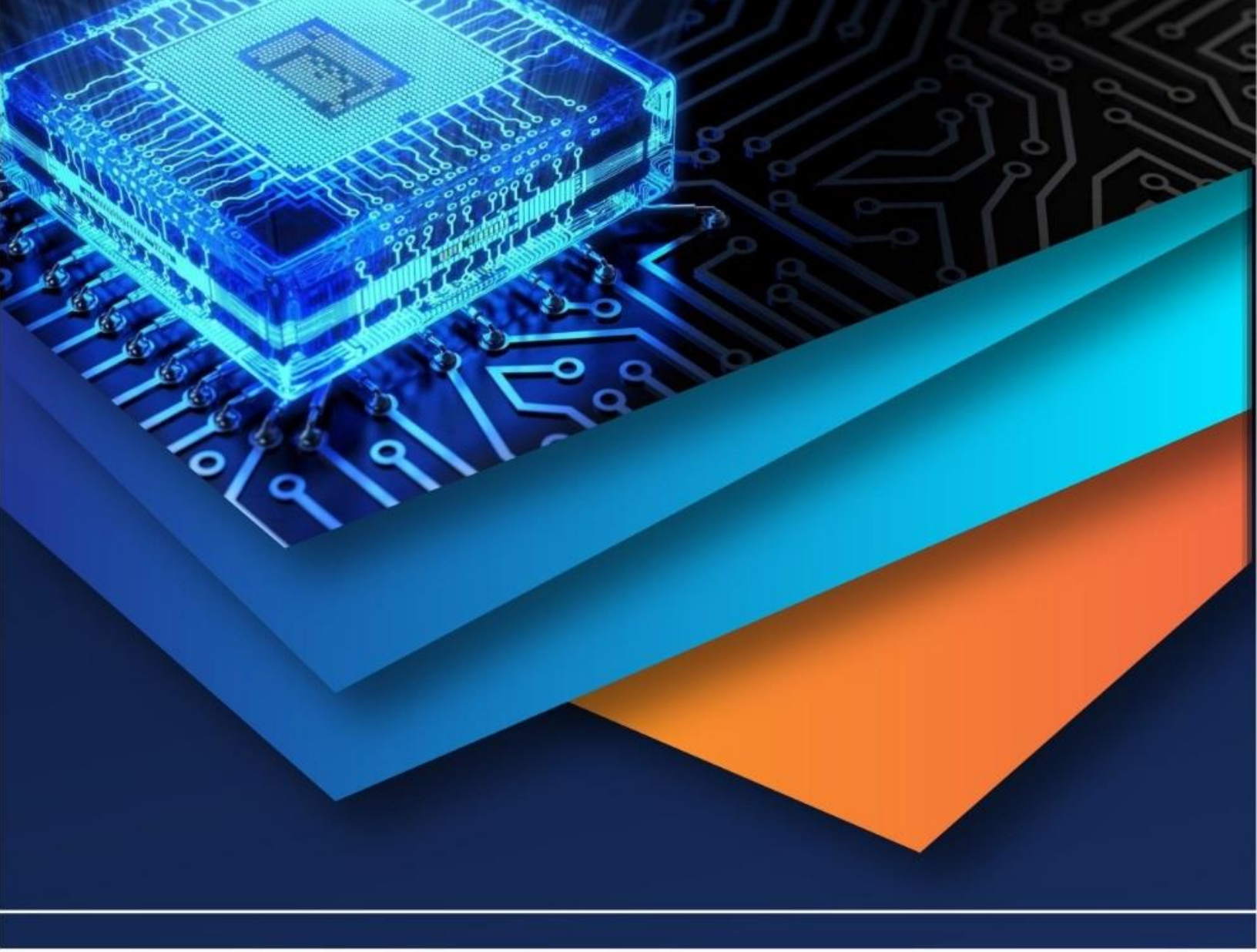
This paper presented a real-time anomaly detection system for IoMT networks using a stacking ensemble machine learning model. The proposed approach combines Random Forest, SVM, and Gradient Boosting algorithms to improve detection accuracy and reduce false alarms. The system provides secure and reliable healthcare network monitoring with better adaptability to dynamic IoMT environments.

IX. FUTURE ENHANCEMENT

The proposed anomaly detection system can be further enhanced by integrating advanced Deep Learning techniques such as CNN, RNN, and LSTM to improve detection accuracy and identify complex cyberattacks in IoMT networks. Future improvements may also include cloud-based deployment for better scalability, real-time streaming data analysis with lower latency, and intelligent alert systems using email or SMS notifications. Additionally, advanced feature selection methods and larger healthcare datasets can be used to improve system performance, adaptability, and security in smart healthcare environments.

REFERENCES

[1] S. M. Metev and V. P. Veiko, Laser Assisted Microtechnology, 2nd ed., R. M. Osgood, Jr., Ed. Berlin, Germany: Springer-Verlag, 1998.
[2] J. Breckling, Ed., The Analysis of Directional Time Series: Applications to Wind Speed and Direction, ser. Lecture Notes in Statistics. Berlin, Germany:
[3] H. Goumidi and S. Pierre, “Real-Time Anomaly Detection in IoMT Networks Using Stacking Model and a Healthcare-Specific Dataset,” IEEE Access, vol. 13, pp. 70352–70365, 2025.
[4] E. Alalwany, B. Alsharif, Y. Alotaibi, A. Alfahaid, I. Mahgoub, and M. Ilyas, “Stacking Ensemble Deep Learning for Real-Time Intrusion Detection in IoMT Environments,” Sensors, vol. 25, no. 3, Art. no. 624, 2025, doi: 10.3390/s25030624.
[5] P. Chandekar, M. Mehta, and S. Chandan, “Enhanced Anomaly Detection in IoMT Networks Using Ensemble AI Models on the CICIoMT2024 Dataset,” arXiv, Feb. 2025.
[6] J. A. Shaikh et al., “RCLNet: An Effective Anomaly-Based Intrusion Detection for Securing the IoMT System,” Frontiers in Digital Health, vol. 6, Art. 1467241, 2024.
[7] F. Pastore, R. W. Anwar, N. H. Jabeur, and S. Ali, “Intelligent Fusion: A Resilient Anomaly Detection Framework for IoMT Health Devices,” Information, vol. 17, no. 2, Art. 117, 2026.
[8] Y. Zhang, Y. Chen, J. Wang, and Z. Pan, “Unsupervised Deep Anomaly Detection for Multi-Sensor Time Series Signals,” arXiv, Jul. 2021.
[9] A. Vinayakumar, S. Soman, and K. Poornachandran, “Deep Learning Approach for Intrusion Detection in IoMT Networks,” Procedia Computer Science, vol. 132, pp. 103–110, 2018.
[10] N. Sharma, A. Kumar, and S. Singh, “Ensemble Machine Learning Models for Anomaly Detection in Healthcare IoT,” Journal of Healthcare Engineering, vol. 2022, Article ID 9876543, 2022.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY