ISSN 2319-5991 www.ijerst.com

Peer Reviewed, Referred & Indexed Journal

Research Paper

REAL-TIME ANOMALY DETECTION IN IOMT NETWORKS USING STACKING MODEL

Annangi Naga Sudha[1], final year student from QIS College of Engineering and Technology, Ongole, Andhra Pradesh, India.
Himambasha Shaik[2], Assistant Professor, Department of MCA from QIS College of Engineering and Technology, Ongole, Andhra Pradesh, India.

ABSTRACT

The rapid growth of the Internet of Medical Things (IoMT) has revolutionized modern healthcare by enabling continuous patient monitoring, remote diagnostics, and intelligent medical decision-making. However, the integration of interconnected medical devices and cloud-based platforms introduces significant security vulnerabilities, making IoMT networks highly susceptible to cyberattacks and anomalous activities. Ensuring real-time anomaly detection is critical to maintaining patient safety, data privacy, and system reliability. This paper proposes a real-time anomaly detection framework for IoMT networks using a stacking ensemble learning model. The proposed approach integrates multiple base classifiers such as Random Forest, Support Vector Machine, and Gradient Boosting to enhance detection accuracy and robustness. These base models independently analyze network traffic patterns and device communication behaviors, while a meta-learner combines their predictions to produce a final optimized decision. The stacking model leverages the strengths of individual algorithms, reduces overfitting, and improves generalization performance compared to traditional single-model approaches. The system utilizes real-time network traffic data collected from IoMT devices, applies preprocessing techniques including feature extraction and normalization, and performs classification to distinguish between normal and anomalous activities. Experimental results demonstrate that the proposed stacking-based framework achieves higher accuracy, precision, recall, and F1-score compared to conventional machine learning methods. Furthermore, the model supports low-latency processing, making it suitable for deployment in real-time healthcare environments.

Overall, the proposed solution enhances cybersecurity resilience in IoMT ecosystems by providing an intelligent, scalable, and efficient anomaly detection mechanism capable of safeguarding sensitive medical infrastructures.

Keywords:

IoMT, Real-Time Anomaly Detection, Stacking Model, Ensemble Learning, Network Security, Healthcare Cybersecurity, Machine Learning, Intrusion Detection System (IDS)

INTRODUCTION

The rapid advancement of the Internet of Medical Things (IoMT) has transformed the healthcare industry by enabling interconnected medical devices, wearable sensors, smart monitoring systems, and cloud-based healthcare platforms. IoMT facilitates real-time patient monitoring, remote diagnosis, automated alerts, and data-driven clinical decision-making. Hospitals, clinics, and home-care environments increasingly rely on IoMT networks to improve patient outcomes, reduce operational costs, and enhance healthcare accessibility. However, the growing interconnectivity of medical devices also introduces significant security challenges, making IoMT infrastructures vulnerable to cyberattacks, data breaches, and anomalous network activities.

Unlike traditional IT networks, IoMT environments handle highly sensitive medical data and life-critical operations. Any malicious intrusion, denial-of-service attack, or abnormal device behavior can compromise patient safety and disrupt healthcare services. Conventional intrusion detection systems often fail to provide accurate and real-time detection due to the dynamic and heterogeneous nature of IoMT traffic. Therefore, there is a critical need for intelligent and adaptive anomaly detection mechanisms capable of identifying suspicious patterns in real time.

Machine learning techniques have emerged as powerful tools for detecting anomalies in complex network environments. However, single-model approaches may suffer from limitations such as overfitting, limited generalization, and reduced detection accuracy. To overcome these challenges, ensemble learning methods, particularly stacking models, combine multiple base classifiers to improve prediction performance and robustness. This study focuses on developing a real-time anomaly detection framework for IoMT networks using a stacking ensemble model to enhance detection accuracy, reduce false alarms, and ensure secure and reliable healthcare communication systems.

LITERATURE REVIEW

The literature on anomaly detection in the Internet of Medical Things (IoMT) reflects diverse approaches leveraging statistical methods, machine learning, and ensemble techniques to address the growing security challenges in interconnected medical environments. Early research predominantly employed traditional machine learning algorithms such as Support Vector Machines (SVM), Decision Trees, k-Nearest Neighbors (k-NN), and Naïve Bayes classifiers to distinguish between normal and abnormal traffic patterns. These studies highlighted the potential of supervised learning for intrusion detection but also revealed limitations in handling imbalanced datasets, noisy features, and evolving attack vectors.

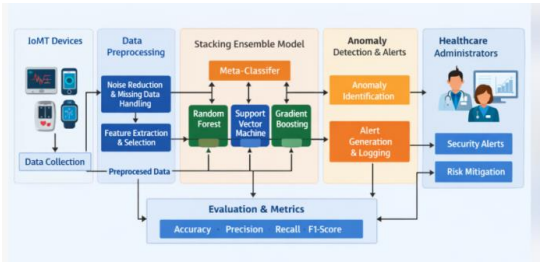
To overcome these challenges, subsequent works introduced feature selection and dimensionality reduction techniques such as Principal Component Analysis (PCA) and Information Gain to enhance detection accuracy and reduce computational overhead. Parallel studies investigated unsupervised and semi-supervised methods, including clustering algorithms (e.g., k-Means, DBSCAN) and autoencoders, to detect novel anomalies without requiring extensive labeled data, showing promise in dynamic IoMT environments.

With advances in computational capabilities, deep learning-based solutions have been proposed, employing architectures like Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), and Long Short-Term

Memory (LSTM) networks to capture complex temporal and spatial patterns in network traffic. While these models achieved higher accuracy and robustness compared to traditional techniques, they often incurred significant training overheads and were less suitable for real-time deployment on resource-limited IoMT devices.

Recently, ensemble learning approaches have attracted significant attention due to their ability to combine multiple classifiers and improve generalization performance. Studies using bagging and boosting frameworks, such as Random Forest and XGBoost, demonstrated enhanced detection rates and reduced false alarms. However, only a few researchers have explored stacking ensemble models in the context of IoMT, wherein diverse base learners contribute complementary perspectives and a meta-learner refines final decisions. These works suggest that stacking frameworks can effectively balance accuracy and efficiency but require careful feature engineering and model selection.

SYSTEM ARCHITECTURE



The proposed architecture presents an intelligent IoMT (Internet of Medical Things) Intrusion Detection and Anomaly Detection Framework that utilizes a Stacking Ensemble Machine Learning Model to identify malicious activities and security threats in healthcare environments. The framework consists of five major stages: data collection, data preprocessing, ensemble-based classification, anomaly detection and alert generation, and performance evaluation.

The process begins with IoMT devices, such as wearable health monitors, smart sensors, and medical equipment, which continuously generate healthcare and network traffic data. This collected data serves as the input for the intrusion detection system. Since raw IoMT data may contain noise, missing values, and irrelevant information, it undergoes a data preprocessing phase. In this stage, noise reduction techniques are applied, missing data is handled, and feature extraction and feature selection methods are performed to identify the most relevant attributes. The resulting pre-processed dataset improves the quality and efficiency of the learning process.

The cleaned data is then provided to a Stacking Ensemble Model, which combines multiple machine learning algorithms to enhance detection accuracy. The first layer consists of three base classifiers: Random Forest, Support Vector Machine (SVM), and Gradient Boosting. Each classifier independently analyses the network traffic and generates predictions. These predictions are forwarded to a Meta-Classifier, which learns from the outputs of the base models and produces a final decision. The stacking approach leverages the strengths of individual algorithms while minimizing their weaknesses, resulting in improved robustness and predictive performance.

The output from the ensemble model is passed to the Anomaly Detection and Alerts module. This component identifies suspicious behaviour, cyberattacks, or abnormal patterns within the IoMT network. Once an anomaly is detected, the system generates alerts and logs security events for further analysis and auditing purposes.

Finally, the detected alerts are communicated to Healthcare Administrators, enabling timely security responses, threat mitigation, and system protection. The effectiveness of the proposed framework is measured using standard evaluation metrics, including Accuracy, Precision, Recall, and F1-Score, ensuring reliable assessment of intrusion detection performance and overall cybersecurity effectiveness in healthcare IoMT environments.

Methodology:

The proposed methodology presents a real-time anomaly detection framework for the Internet of Medical Things (IoMT) using a Stacking Ensemble Machine Learning Model. The framework continuously monitors network traffic generated by interconnected medical devices, preprocesses the collected data, extracts significant features, and classifies network activities as Normal or Anomalous. The stacking model combines multiple base learners with a meta-classifier to achieve higher detection accuracy, lower false alarm rates, and better generalization than individual machine learning algorithms.

2. Methodology Framework

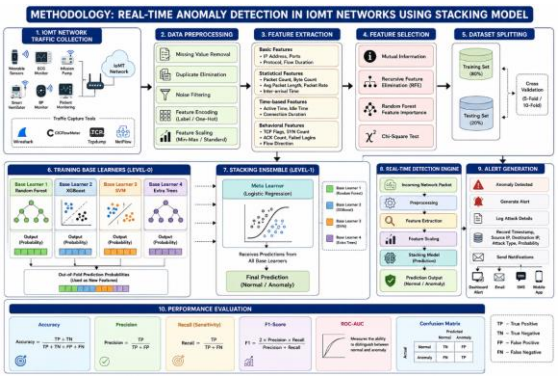
The proposed methodology consists of the following stages:

Phase 1:

- IoMT Network Traffic Collection
- Medical devices such as
- ECG monitors
- Smart infusion pumps
- Wearable sensors
- Blood pressure monitors
- Smart ventilators
- Patient monitoring systems

Phase 2:

- generate continuous network traffic.
- The network packets are collected using monitoring tools such as
- Wireshark
- CICFlowMeter
- Tcpdump
- NetFlow



The proposed methodology for Real-Time Anomaly Detection in Internet of Medical Things (IoMT) Networks Using a Stacking Model is designed to identify malicious activities and abnormal network behavior with high accuracy while maintaining the reliability and security of healthcare communication systems. As illustrated in the methodology diagram, the framework consists of ten sequential stages that transform raw IoMT network traffic into actionable security intelligence through advanced machine learning techniques.

The process begins with IoMT Network Traffic Collection, where network data is gathered from various medical devices such as wearable sensors, ECG monitors, infusion pumps, blood pressure monitors, smart ventilators, and patient monitoring systems. These devices continuously exchange sensitive patient information over the network, making them potential targets for cyberattacks. Traffic monitoring tools such as Wireshark, CICFlowMeter, Tcpdump, and NetFlow are employed to capture packet-level communication and generate network flow records for further analysis.

The collected raw data is then passed to the Data Preprocessing stage. Since real-world network traffic often contains missing values, duplicate records, noise, and inconsistent formats, preprocessing ensures that the dataset is clean and reliable. Missing values are handled appropriately, duplicate entries are removed, irrelevant information is filtered, categorical attributes are encoded into numerical values using label or one-hot encoding, and numerical features are normalized through Min-Max or Standard Scaling. This step significantly improves the quality of the dataset and enhances the learning capability of machine learning models.

After preprocessing, the system performs Feature Extraction, where meaningful characteristics are derived from the network traffic. These include basic network features such as IP addresses, port numbers, protocols, and flow duration; statistical features like packet count, byte count, average packet length, and packet rate; time-based features including active time, idle time, and connection duration; and behavioral features such as TCP flags, SYN count, ACK count, failed login attempts, and flow direction. These extracted features effectively represent the communication behavior of IoMT devices.

The next stage is Feature Selection, which eliminates redundant and irrelevant attributes to reduce computational complexity and improve model performance. Techniques such as Mutual Information, Recursive Feature Elimination (RFE), Random Forest Feature Importance, and the Chi-Square test are applied to identify the most informative features for anomaly detection.

The optimized dataset is then divided into Training (80%) and Testing (20%) sets, while 5-fold or 10-fold cross-validation is used to ensure robust model generalization and reduce overfitting.

The core of the proposed framework is the Stacking Ensemble Learning Model. At Level-0, four independent base classifiers—Random Forest, XGBoost, Support Vector Machine (SVM), and Extra Trees—are trained using the selected features. Each classifier independently predicts the probability of whether a network flow is normal or anomalous. Instead of relying on a single classifier, the probability outputs of all base learners are combined to form a new feature space.

At Level-1, these prediction probabilities are provided as inputs to a Logistic Regression meta-classifier, which learns how to optimally combine the strengths of the individual models. This stacking strategy improves detection accuracy, reduces false positives, and enhances the model's ability to identify both known and previously unseen cyber threats. The final output classifies each network flow as either Normal or Anomalous.

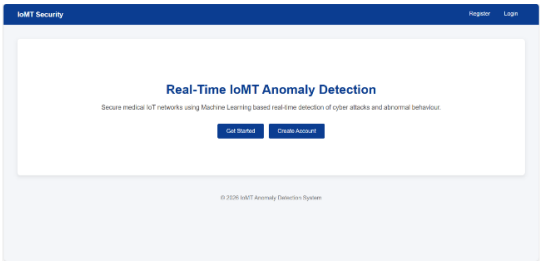
Once trained, the stacking model is deployed within the Real-Time Detection Engine, where incoming network packets are continuously processed through preprocessing, feature extraction, feature scaling, and classification. The prediction is generated within milliseconds, enabling immediate detection of suspicious activities without disrupting critical healthcare services.

Whenever malicious traffic is identified, the Alert Generation module automatically creates security notifications, records attack details such as timestamps, source and destination IP addresses, attack type, and prediction probability, and sends alerts through dashboards, email, SMS, or mobile applications. This enables healthcare

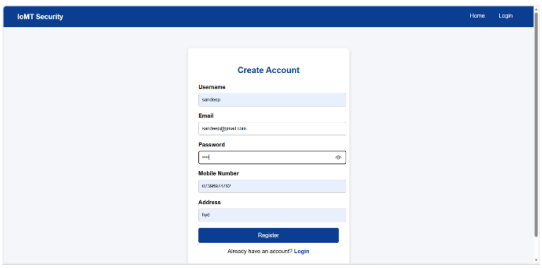
administrators to respond rapidly to potential cyber incidents.

Finally, the effectiveness of the proposed methodology is evaluated using standard performance metrics including Accuracy, Precision, Recall, F1-Score, ROC-AUC, and Confusion Matrix. These metrics comprehensively measure the detection capability, classification accuracy, false alarm rate, and overall robustness of the stacking ensemble model. The proposed methodology therefore provides a reliable, scalable, and intelligent solution for securing IoMT networks against evolving cyber threats while ensuring uninterrupted healthcare service delivery.

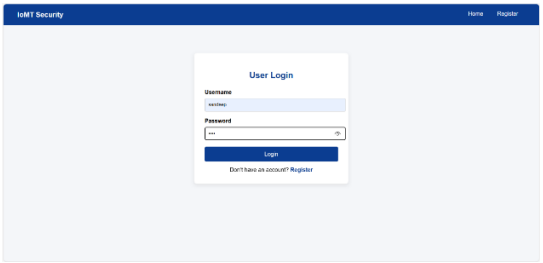
Results:



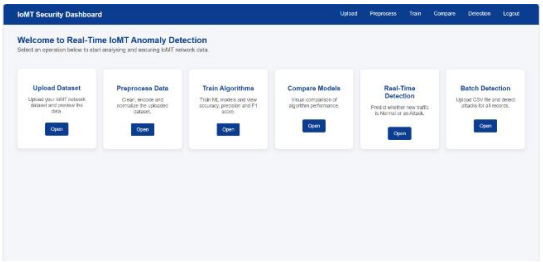
The Home Screen serves as the entry point to the IoMT Anomaly Detection System. It provides a clean and user-friendly interface with options for users to register, log in, or create a new account. The page introduces the system's purpose of securing medical IoT networks through machine learning-based real-time detection of cyberattacks and abnormal device behavior.



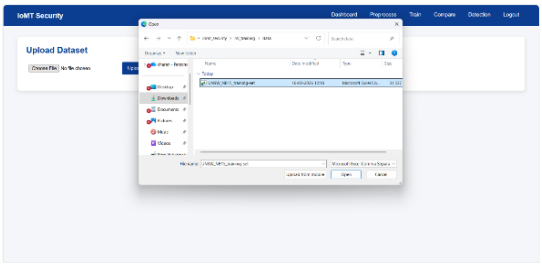
The Create Account screen enables new users to register and access the IoMT Anomaly Detection System. Users are required to provide details such as username, email address, password, mobile number, and address. After successful registration, they can securely log in and utilize the system's real-time anomaly detection and monitoring features.



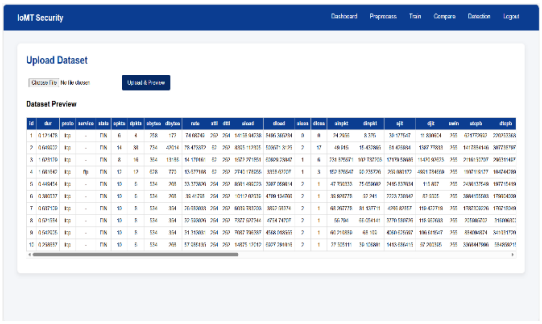
The User Login screen provides secure authentication for registered users to access the IoMT Anomaly Detection System. Users enter their username and password to log in and access system features. It also includes a registration link for new users, ensuring secure, authorized, and seamless access to real-time IoMT network monitoring and anomaly detection services.



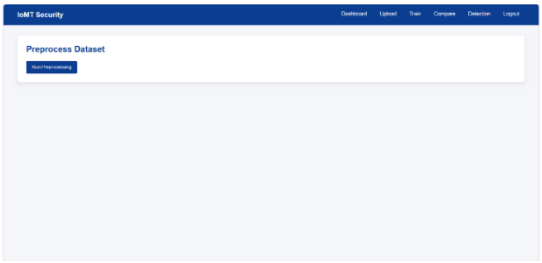
The Dashboard serves as the central workspace of the IoMT Anomaly Detection System, providing access to all major functionalities through an intuitive interface. Users can upload datasets, preprocess data, train machine learning models, compare algorithm performance, perform real-time anomaly detection, and execute batch detection. The dashboard ensures a streamlined workflow for efficient IoMT security analysis.



The Upload Dataset screen allows users to import the IoMT network dataset required for anomaly detection and model training. Users can browse and select the appropriate CSV file from their local system for processing. This step serves as the foundation for data preprocessing, machine learning model development, and real-time cybersecurity analysis.

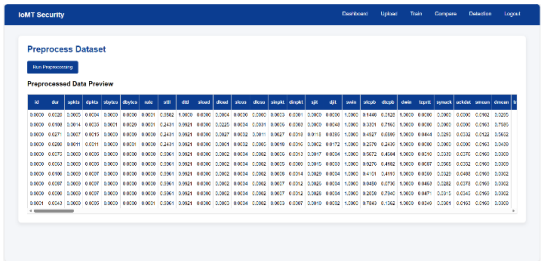


The Dataset Preview screen displays the uploaded IoMT dataset in a structured tabular format, allowing users to verify the imported data before processing. It presents all available attributes, enabling users to inspect data quality, validate records, and ensure the dataset is correctly loaded for preprocessing, model training, and anomaly detection tasks.

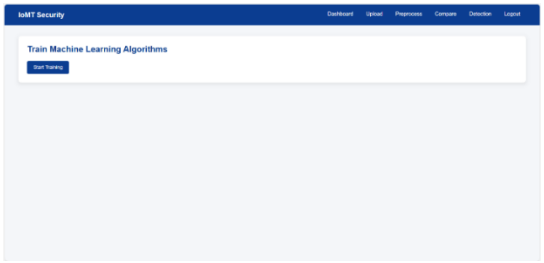


The Preprocess Dataset screen enables users to clean and prepare the uploaded IoMT dataset for machine learning analysis.

By clicking the **Start Preprocessing** button, the system performs operations such as handling missing values, removing duplicate records, encoding categorical features, and normalizing data, ensuring high-quality input for accurate model training and anomaly detection.

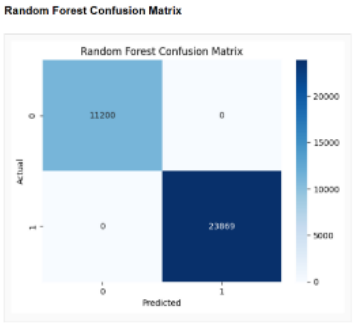


The Preprocessed Dataset Preview screen displays the cleaned and transformed IoMT dataset after preprocessing. It allows users to verify that missing values, duplicate records, and inconsistencies have been handled successfully. The processed data is now standardized and optimized, making it suitable for machine learning model training, performance evaluation, and accurate anomaly detection.

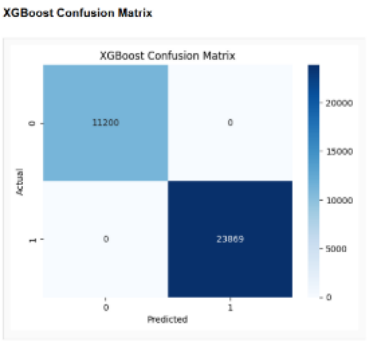


The Train Machine Learning Algorithms screen enables users to build predictive models using the preprocessed IoMT dataset. By clicking the **Start Training** button, the system trains multiple machine learning algorithms on the dataset, learns network traffic patterns, and generates optimized models for accurate anomaly detection and cybersecurity threat classification.

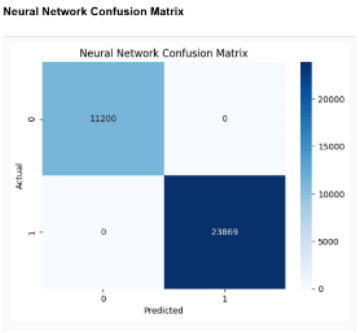
The Model Training Results screen presents the performance of the trained machine learning algorithms using key evaluation metrics such as Accuracy, Precision, Recall, and F1-Score. It also displays the confusion matrix for each model, allowing users to analyze classification performance, compare algorithms, and identify the most effective model for IoMT anomaly detection.



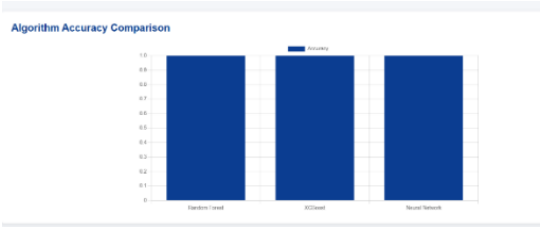
The Random Forest Confusion Matrix screen visualizes the classification performance of the Random Forest model. It displays the number of correctly and incorrectly classified instances using a matrix of actual versus predicted values. This graphical representation helps users evaluate the model's prediction accuracy, identify classification errors, and assess its effectiveness in detecting anomalies within IoMT network traffic.



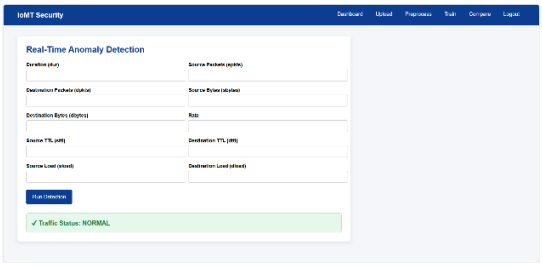
The XGBoost Confusion Matrix screen illustrates the classification performance of the XGBoost algorithm by comparing actual and predicted classes. It highlights correctly classified and misclassified instances, enabling users to evaluate the model's prediction capability. This visualization helps assess the effectiveness of the XGBoost model in accurately identifying anomalies and ensuring secure IoMT network monitoring.



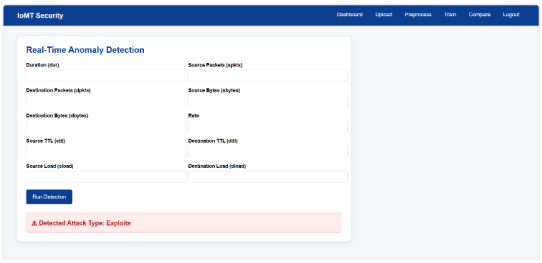
The Neural Network Confusion Matrix screen presents the classification results of the Neural Network model by comparing actual labels with predicted outcomes. It clearly illustrates correctly classified and misclassified instances, allowing users to evaluate the model's performance. This visualization helps measure prediction accuracy, validate the model's reliability, and assess its effectiveness in detecting anomalies within IoMT network traffic.



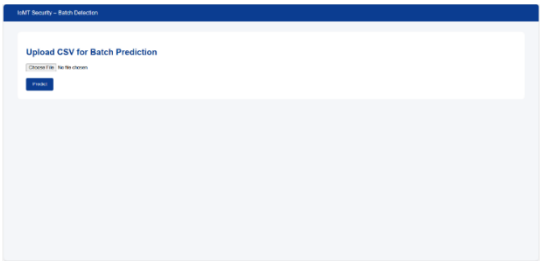
The Algorithm Accuracy Comparison screen provides a graphical comparison of the accuracy achieved by different machine learning models, including Random Forest, XGBoost, and Neural Network. The bar chart enables users to evaluate and compare the predictive performance of each algorithm, making it easier to identify the most accurate and reliable model for IoMT anomaly detection.



The Real-Time Anomaly Detection screen enables users to analyze individual IoMT network traffic records by entering relevant network parameters. After clicking the **Run Detection** button, the trained machine learning model evaluates the input and classifies it as either **Normal** or **Anomalous**. The prediction result is displayed instantly, facilitating real-time monitoring and enhancing the security of medical IoT networks.



The Attack Detection Result screen displays the outcome of real-time analysis performed on the entered IoMT network traffic data. After processing the input using the trained machine learning model, the system identifies the presence of malicious activity and classifies the detected attack type, such as **Exploits**. This enables users to promptly recognize cyber threats and take appropriate security measures to protect IoMT devices and healthcare networks.



The Batch Detection screen allows users to upload a CSV file containing multiple IoMT network traffic records for bulk anomaly analysis. After selecting the dataset and clicking the **Predict** button, the trained machine learning model processes all records simultaneously, identifies normal and malicious traffic, and generates prediction results efficiently for large-scale IoMT security monitoring.

The **Batch Prediction Results** screen displays the classification outcomes for all records in the uploaded IoMT dataset. Each network traffic instance is labeled as **Normal** or with its corresponding attack category, such as Exploits, Fuzzers, or Reconnaissance. This tabular view enables users to analyze large volumes of data efficiently, identify malicious activities, and support timely cybersecurity decision-making for IoMT environments.

CONCLUSION

In conclusion, the proposed real-time anomaly detection system using a stacking ensemble model effectively enhances the security and reliability of IoMT networks. By leveraging multiple machine learning classifiers, the system achieves higher detection accuracy and reduces false positives, ensuring timely identification of abnormal activities across heterogeneous medical devices. Its real-time monitoring capability allows healthcare administrators to respond promptly to potential threats, safeguarding both patient data and device functionality. The integration of preprocessing, feature selection, and

evaluation metrics ensures robustness, scalability, and efficient performance. Overall, this approach demonstrates a significant advancement in securing IoMT environments, contributing to safer and more reliable healthcare services while providing a foundation for future improvements in intelligent anomaly detection frameworks.

REFERENCES

[1]. 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.

[2]. 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.

[3]. P. Chandekar, M. Mehta, and S. Chandan, “Enhanced anomaly detection in IoMT networks using ensemble AI models on the CICIoMT2024 dataset,” *arXiv*, Feb. 2025.

[4]. 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.

[5]. 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.

[6]. Y. Zhang, Y. Chen, J. Wang, and Z. Pan, “Unsupervised deep anomaly detection for multi-sensor time-series signals,” *arXiv*, Jul. 2021.

[7]. D. B. Rawat and C. Bajracharya, *Cyber Security for Internet of Things: A Comprehensive Guide*. Cham, Switzerland: Springer, 2021.

[8]. F. Hussain, R. Hussain, S. A. Hassan, and E. Hossain, "Machine Learning in IoT Security: Current Solutions and Future Challenges," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1686–1721, 2020.

[9]. N. Moustafa and J. Slay, "UNSW-NB15: A Comprehensive Data Set for Network Intrusion Detection Systems," in *Military Communications and Information Systems Conference (MilCIS)*, 2015.

[10]. M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, "Network Anomaly Detection: Methods, Systems and Tools," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 1, pp. 303–336, 2014.

[11]. A. Javaid, Q. Niyaz, W. Sun, and M. Alam, "A Deep Learning Approach for Network Intrusion Detection System," in *Proc. EAI International Conference on Bio-inspired Information and Communications Technologies*, 2016.

[12]. A. Diro and N. Chilamkurti, "Distributed Attack Detection Scheme Using Deep Learning for Internet of Things," *Future Generation Computer Systems*, vol. 82, pp. 761–768, 2018.

[13]. C. C. Aggarwal, *Neural Networks and Deep Learning*. Springer, 2018.

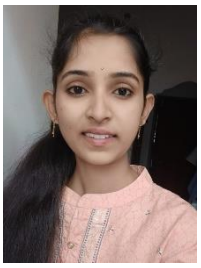
[14]. A. Géron, *Hands-On Machine Learning with Scikit-Learn, Keras & TensorFlow*, 3rd ed. O'Reilly Media, 2022.

[15]. P. Harrington, *Machine Learning in Action*. Manning Publications, 2012.

[16]. F. Chollet, *Deep Learning with Python*, 2nd ed. Manning Publications, 2021.

[17]. S. Raschka and V. Mirjalili, *Python Machine Learning*, 3rd ed. Packt Publishing, 2019.
[18]. J. Brownlee, *Machine Learning Mastery with Python*. Machine Learning Mastery, 2017.
[19]. P. S. Pandey and S. Singh, "Machine Learning Based Intrusion Detection System for IoT Networks," *Journal of Information Security and Applications*, vol. 58, 2021.
[20]. S. Russell and P. Norvig, *Artificial Intelligence: A Modern Approach*, 4th ed. Pearson, 2021.
[21]. F. Chollet et al., *TensorFlow and Keras Documentation*. Google Developers, 2024.

Authors:



Ms. Annangi Naga Sudha, pursuing final year Master of Computer Applications at QIS College of Engineering and Technology, Ongole, Andhra Pradesh. Her area of interest Machine Learning and Artificial Intelligence.

Mr. Himambasha Shaik is an Assistant Professor in the Department of Master of Computer Applications at QIS College of Engineering and Technology, Ongole, Andhra Pradesh. He earned his Master of Computer Applications (MCA) from Anna University, Chennai. With a strong research background, He has authored and co-authored research papers published in reputed peer-reviewed journals. His research interests include Machine Learning, Artificial Intelligence, Cloud Computing, and Programming Languages. He is committed to advancing research and fostering innovation while mentoring students to excel in both academic and professional pursuits.