RESEARCH & INNOVATION DIVISION
IJIST

NeuroSecure-IoMT: Deep Learning Meets Cyber Defense in the Internet of Medical Things

Urwa Bibi, Hafiz Gulfam Ahmad Umer, Rimsha Jamil Ghilzai, and Muskan Maryam
Ghazi University D.G Khan
*** Correspondence:** Urwa Bibi, urwatariqkhosa@gmail.com

Citation | Bibi. U, Umar. H. G. A, Ghilzai. R. J, Maryam. M, "NeuroSecure-IoMT: Deep Learning Meets Cyber Defense in the Internet of Medical Things", IJIST, Vol. 07 Issue. 02 pp 1179-1199, June 2025
DOI | https://doi.org/10.33411/ijist/20257211791199
Received | April 12, 2025 **Revised |** June 03, 2025 **Accepted |** June 06, 2025 **Published |** June 08, 2025.

Intrusion deduction systems (IDS) are crucial to preserving sensitive medical information from cyber threats. However, issues with multi-class intrusion detection include an imbalanced data set, poor accuracy for minority classes, and a lack of flexibility in handling complex real-world situations. To address these issues, we provide a hybrid framework that combines machine learning and deep learning methods to address these problems. The model uses a random forest classifier for anomaly detection after reducing dimensionality using an autoencoder. The Synthetic Minority Oversampling Technique (SMOTE) was used during processing to ensure equitable class representation and reduce class imbalance. A multi-class intrusion detection dataset tailored to healthcare applications was used to thoroughly test the suggested framework, which provides an impressive 99% accuracy rate. In addition to its excellent accuracy, the model addresses important issues in multi-class Intrusion detection by exhibiting remarkable precision for minority classes and consistent performance across all categories. These results highlight the framework's effectiveness in providing dependable and effective normal detection solutions, which makes it ideal for implementation in crucial sectors like healthcare, their accuracy and data security are crucial.

Keywords: Intrusion Detection System (IDS), Machine Learning (ML), Deep Learning (DL), Autoencoder, Random Forest, Dimensionality Reduction


DRJI


Crossref


ResearchGate


WIKIDATA


HEC

Introduction:

The rapid transmission has been driven by various technologies, especially the Internet of Medical Things (loMT). The growing use of Internet of Things (IoT) technology in the healthcare sector is emphasized by (IoMT), which is commonly referred to as a healthcare IoT. Various sensors in IoMT systems gather real-time, sensitive patient data, enabling healthcare providers to gain deeper insights into critical situations and giving patients greater awareness of their healthcare condition [1].

The Internet of Medical Things IoMT has many benefits, according to authorincluding remote monitoring of infectious diseases, enhanced diagnostics, and treatments, instant access to medical history, automated reminders, and seamless data analysis through advanced algorithms that detect abnormalities.[2] The COVID-19 pandemic significantly accurate this adoption, making IoMT essential for minimizing physical attraction and improving healthcare services [3]. However, the rapid expansion of IOMT has also significantly increased the risk of cyber-attacks targeting sensitive medical data and connected devices. Table 1 presents the projected growth of IoT-connected devices from 2010 to 2030, highlighting the massive expansion of the IoT ecosystem, including medical devices.

Table 1. Projected Growth of IoT-Connected Devices (2010–2030)

Year	Estimated IoT Connected Devices (in billions)
2010	5.0
2015	15.4
2020	35.0
2025	75.4
2030	125.0

The IoMT landscape is expanding significantly and quickly. The global Internet of Medical Things was valued at 108.5 billion in 2020 and is expected to reach 1100 billion in 2028 to grow at a component annual growth rate (CAGR) of 22.3%. IoMT systems are vulnerable to cyber-attacks due to Open wireless communication, weak authentication, and poor design. There can be serious financial consequences if security is not given top priority during IoT development. To reduce threats, strong security management must be put in place right away. IoMT security with machine learning-powered, privacy-focused ideal solution. This will encourage wild adoption of IoMT and unlock its full potential to enhance healthcare delivery.

Attack and compose patient safety by manipulating devices or data. The challenge is to detect intrusion effectively while minimizing computational overhead and false alarms. In response to increasing security challenges, IDS has become a critical element of the security of things (SOT) framework, showing promise in addressing IoMT-related problems including restricted resource availability, data transmission delays, scalability, and diversity [4][5]. Machine learning (ML) and Deep learning (DL) solution to improve the attack detection.[6][7]. Intrusion detection strengthens the protection of computer systems against possible cyber threats. The three main categories of machine learning methods for Intrusion detection are supervised, unsupervised, and semi super supervised learning. Each of these methods offers different strategies for locating and fixing security flaws [8]. Traditional detection methods frequently fail because hackers are always improving their tactics and using more sophisticated hacking tools [6][9][10]. These traditional security methods are not suitable for the limited resources of IoMT amenities due to their limited scalability and high computational resource requirements.[11][12].

Machine learning algorithm used an Intrusion detection system (IDS) to find patterns associated with both benign and hostile activities. The large-scale set of network traffic and device behavior can be used to train learning algorithms. IDS is more effective than standard

security methods since these algorithms can identify danger that has not been identified yet. For more as a cyber threat change machine learning enabled ideas to automatically adjust to new attack types and often continuously protect protections.[13][14]. Deep learning improves threat detection in IDS by examining the massive data set to find complex sophisticated assault veterans. Ideas that are more adaptable and resilient to complex attacks become deep learning, which uses neural networks to detect new and changing cyber threats with higher accuracy. Passing network traffic and patient biometric data through multiple hidden deep-learning layers is a popular method.[6].

As illustrated in **Figure 1**, IDS systems monitor network traffic and sensor data, classify patterns using ML/DL models, and trigger alerts upon detecting malicious activity.

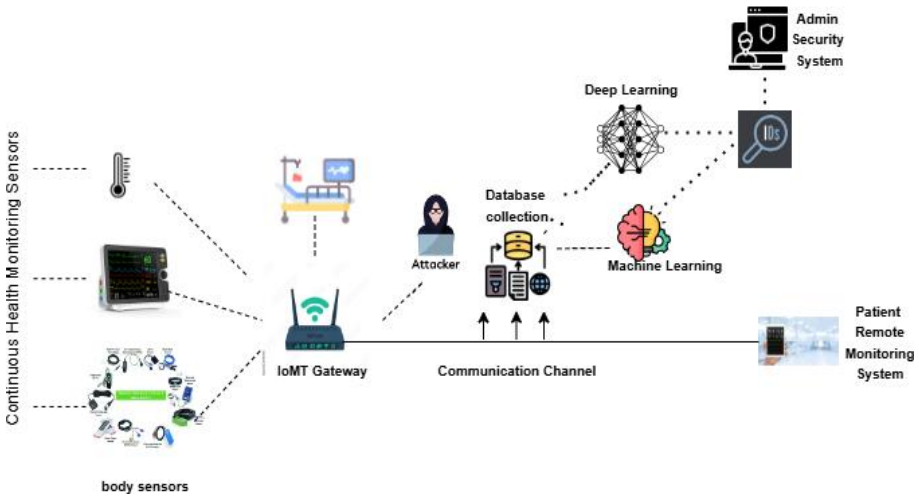

Figure 1. IDS Working Diagram

Incidents such as the ransomware cyber-attack on an Indian hospital system in 2018 demonstrate the serious operational and financial consequences of such security breaches [15]. In another incident in 2023, Prospect Medical Holdings had a ransomware attack that shut down and disrupted emergency services in multiple U.S. states, requiring FBI action. The incident shows how the healthcare industry is susceptible to cybercrime. Consequently, the attack resulted in substantial interruptions to critical services, including elective surgeries, outpatient visits, blood drives, and ambulance operations [16]. Singapore health data breach hackers accessed the personal data of 1.5 million patients, including details of the prime minister 's medical records, highlighting the sensitive nature of IOMT data.

Despite its benefits, the quick development of the IoMT system has exposed serious flaws, leaving numerous devices vulnerable to cyber-attacks that might threaten patient lives. Further, the cost of cybercrime will rise by 1.5 times from 2022. The cost of cybercrime is projected to exceed 10.5 trillion potentially reaching 20 trillion by 2026.

To meet the CIA requirements (Confidentiality, Integrity, Availability) for IoMT at the data level, some researchers have recently begun investigating some security mechanisms, such as Radio Frequency Identification (RFID), Elliptic Curve Cryptography (ECC), Homomorphic Encryption, and Physically Unclonable Function (PUF). Advances in computer and processing power have made it possible to apply machine learning and deep learning approaches widely to more accurately forecast harmful events.

This paper proposes are novel hybrid framework for multiple classes of detection, tailored specially for health applications. The flavor addresses the critical limitation of traditional methods by combining the learning and machine learning techniques. An autoencoder is employed for dimensionality reduction to simplify high-dimensional data, while a random forest classifier ensures robust and accurate classification. The purpose of this paper is to present an effective and reliable IDS model that not only has high overall accuracy but

also ensures equitable performance across all classes, including minority categories. The proposed framework is designed to handle the complexity of the rail world healthcare network, offering a dependable solution for safeguarding sensitive medical. This research aims to contribute to the field of ideas by providing a scalable and adaptable. A solution capable of enhancing security in the critical healthcare environment.

Related Work:

Privacy and safety are fundamental duties in IoMT since the patient data is sensitive and private. This session discussed the efforts related to cyber-attack detection in IoMT utilizing machine and deep learning techniques.

In [17] a model based on a swarm neural network identifies intrusions in the data-driven IoMT system. By detecting intruders during data transfer, the suggested approach enables accurate and efficient analysis of medical data at the edge of the network. Our real-time NF-ToN-IoT data set for IoT applications that gathered network, operating system, and telemetry data was used to test the system's performance. Using a variety of performance indicators, the outcomes of the suggested model are contrasted with those of the conventional intuition detection classification models that employ the same data set. The suggested model achieves 89.0% accuracy over the ToN-IoT data according to the testing results. The limitations of this paper include the relatively modest accuracy of 89.0%, which may not be sufficient for critical healthcare applications requiring higher reliability. The reliance on a single dataset, ToN-IoT, limits the generalizability of the findings to more diverse and complex real-world scenarios. While addressing intrusion detection, the paper does not sufficiently tackle broader privacy concerns or regulatory compliance issues related to transferring patient data to the cloud. Additionally, the feasibility of deploying the model on resource-constrained IoMT devices and its scalability with larger datasets or evolving attack patterns are not discussed. The comparative analysis lacks depth, failing to evaluate the model against state-of-the-art architectures like transformers.

In [18] the implementation of an efficient and precise intrusion detection system IDS in IoMT, suggests the particle swarm optimization deep neural network PSO – DNN. Using the combined network traffic and patient sensing data set, the over method detects the network intrusion with an accuracy of 96% surpassing the state of the art. Additionally, thorough examination of the use of different machine learning and deep learning techniques for network intrusion detection in IoMT, and we verified that the ML model outperforms the machine learning model by a small margin. Future Work We leveraged PSO-based feature selection and the DNN model to predict the IoMT attacks. Although our work improved the performance of the IoMT intrusion detection, the dataset used for our evaluation mainly addresses the patient's confidentiality and integrity-based attacks. The denial-of-service attacks are not considered in our evaluation. One of our future works will be performing IoMT attack classification using ML and DL models, including the DoS, data injection, man-in-the-middle attacks, etc. Data analytics plays a significant role in the smart health industry. The secured implementation of machine learning operations (MLOps) is essential to align with the health industry regulations and maintain compliance requirements. The combination of patient data with network data in our approach requires securely collecting, processing, and transforming the data in real-time applications. Hence, additional security measures are needed in MLops implementation to apply our approach in real-time healthcare industry applications. Various sensing-related patient data are generated in the IoMT networks.

In [19] to create the learning models using Ridge regression and Recursive feature elimination RFE along with machine learning paradigm in order to provide precise anomaly intrusion detection using the real-time data set WUSTL – EHMS. Among the paradigms employed, the suggested method demonstrates that the RFE-based decision tree DL works better than the cutting adjective method with a 99% training accuracy and 97.85% testing

accuracy while keeping the FAR at 0.03 it has been demonstrated the methodology may be used to develop anomalous in Russian detection, strengthening IoMT against pervasive cyber-attacks and preserving the integrity of cutting-edge health care system. The main limitations include an overgeneralization of data augmentation, as its impact on noise and overfitting depends on the context, with the contradictory claim that it increases overfitting when it typically reduces it. The proposed recall improvement methods, such as voting classifiers, stacking ensembles, and active learning, may introduce additional complexity, costs, or trade-offs, such as reduced precision, which are not discussed. Furthermore, the limitations of RFE, such as sensitivity to noise, computational expense, and reliance on the base model, are overlooked. Additionally, there is a lack of empirical evidence to support the claims, and the trade-offs between recall and precision are not addressed, which weakens the argument.

In [2] building more reliable security solutions by addressing these issues with hyperparameter optimized machines and deep learning models. Six cutting-edge machine learning (ML) and Deep Learning (DL). DL architecture was trained using a representative anomaly intrusion detection IDS data set. Class imbalance in the training data set was addressed by the Synthetic Minority over the assembling technique SMOTE. All six models can accurately classify normal situations as a sequence of over-hyperparameter optimization using the random research technique with random forest and K-nearest neighbors exhibiting the highest accuracy. The hybrid Convolution Neural network and long short-term memory CNN-LSTM model did the poorest, while the attention-based LSTM model came in second. However, there was not a single model that worked best for categories of all assault labels.

In [20] an intrusion detection system that uses AdaBoost algorithms and particle swarm optimization to identify and categorize malware-related data in cutting-edge health app platforms. The study uses the NSL-KDD data set which is divided into training 20% and testing 80% set and has 125973 instant and 41 correct texts. 11 important correct texts for induction detection are found through a feature selection for a procedure that uses particle swarm optimization. Numerous attack types, such as Denial-of-Service DoS, user-to-route U2R, route to local R2L, and probe attacks, are effectively categorized by the intuition detection system. Ab boost has the highest recall value 0.96 in terms of classifier performance demonstrating its potent intuition detection power. The experimental finding shows that the PSO-AdaBoost methods outperform other methods in intuition detection in terms of accuracy, precision, and recall. By cooperating intuition detection systems with machine learning into intelligence. The intrusion detection research limitations include data imbalance, generalization, scalability, and false positives. In contrast, future research may involve adaptive models, privacy-preserving techniques, federated learning, explainability, real-time detection, and device-specific models tailored to different medical IoT devices. These directions could help guide further research in the field of optimized machine learning-enabled intrusion detection systems for the Internet of Medical Things.

In [21] exams, the effectiveness of machine learning models for the Internet of medical things in Russian detection with the goal of strengthening cyber security defenses and safeguarding private medical information. The analysis uses the random forest and support vector machines as basis models on the WUSTL-EHMS-2020 data to assess the performance of assembling learning techniques, particularly stacking bagging and boosting with an accuracy rate of 98.88%, stacking exhibits remarkable accuracy and dependability in identifying and categorizing cyber-attack occurs occurrence based on a thorough analysis of performance may like accuracy, precision, recall, and F1 score. With an accuracy percentage of 97.83% backing income in second while boosting provided the lowest accuracy rate at 88.68%. Limitations in intrusion detection using ensemble learning should focus on mitigating overfitting in Boosting algorithms through regularization techniques and ensemble pruning. Investigating the balance between model complexity and performance can enhance adaptability across diverse data

scenarios. Additionally, integrating Boosting algorithms with advanced regularization mechanisms offers the potential to create more robust and precise intrusion detection models for IoMT environments. These efforts aim to develop highly accurate, reliable, and adaptive IDS for healthcare cybersecurity.

In [22] self-tuning long-short-term memory LSTM intrusion detection system IDS for the Internet of medical things that is based on physiologic. For a wide overfitting and underfitting method use early halting and dynamically modify the number of epochs. In order to compare over suggested model performance with that of other ideas models for the Internet of Medical Things, we carry out some testers. The outcome demonstrates over-model efficiency in detecting intrusion by demonstrating a high detection rate, low fall positive rate, and excellent accuracy. We also got over the drawback of employing batch size and static epochs in deep learning models and stressed the significance of dynamic adjustment. The result of this study aids in the creation of IDS models for Internet of Medical Things scenarios that are more accurate and efficient. The accuracy (ACC) of the proposed FST-LSTM model in this paper peaks at 96.7% when using 25 features during the training phase, as mentionedin the document, limitation could focus on optimizing fuzzy logic rules, adaptive self-tuning of hyperparameters, and applying self-tuning mechanisms to advanced architectures like transformers for better handling of IoMT data. Integrating self-tuning with online learning could enable continuous adaptation to evolving threats while reducing computational overhead and energy use for resource-constrained IoMT devices. Developing benchmarking frameworks to compare self-tuning models with traditional approaches can further advance autonomous and efficient intrusion detection systems for secure IoMT environments.

Some of the IoMT Malware Detection Approaches: Analysis and Research Challenges and directions of malware detection in IoT/IoMT environment are also highlighted.

Objectives:

The objective of this Study are:

1. Enhance Multi-Class Intrusion Detection Accuracy:

Move beyond binary classification by effectively detecting multiple types of cyberattacks in healthcare networks.

2. Address Class Imbalance in IDS Datasets:

Use SMOTE to ensure minority classes are properly represented, thus improving the detection of less frequent but critical attack types.

3. Reduce Feature Dimensionality:

Apply autoencoders for dimensionality reduction to retain essential features while reducing computational complexity.

4. Improve Classification Robustness

Use Random Forest classifiers to ensure reliable and high-performance classification across all intrusion types.

5. Ensure Real-World Applicability in Healthcare IoT

Design a system that meets the Confidentiality, Integrity, and Availability (CIA) requirements essential for healthcare data security.

Novelty statement:

This study proposes a novel hybrid intrusion detection framework tailored for the Internet of Medical Things (IoMT), addressing key limitations of existing security models in healthcare environments. The framework uniquely integrates autoencoders for dimensionality reduction with random forest classifiers for efficient multi-class classification. By incorporating SMOTE, it effectively handles class imbalance, ensuring fair detection across both majority and minority classes. Unlike traditional IDS approaches, this model is designed to operate under real-world constraints, offering improved adaptability, reduced false

positives, and robust performance across diverse and complex intrusion patterns, making it well-suited for sensitive and resource-constrained healthcare networks.

Material and Methods:

The proposed Hybrid Intrusion Detection System (HIDS) aims to enhance the detection of cyberattacks and anomalous behaviors in healthcare IoT systems, integrating Autoencoders for dimensionality reduction and Random Forest classifiers for accurate classification. The model follows a structured approach to data processing, feature extraction, classification, and evaluation. The detailed components of the model are described below:

Deep Learning Component: Autoencoder for Dimensionality Reduction:

The deep learning component in this framework is an autoencoder, a type of neural network used for unsupervised learning. Autoencoders are particularly suited for dimensionality reduction as they can identify and retain the most important features of the dataset while eliminating irrelevant or redundant information.

Architecture of the Autoencoder:

Input Layer: The autoencoder takes the high-dimensional feature set from the dataset as input. Each feature represents a specific network characteristic.

Encoding Layer: The input is compressed into a lower-dimensional latent space using dense layers with a ReLU activation function. This layer ensures the most relevant patterns are retained while reducing computational complexity.

Decoding Layer: The compressed representation is reconstructed back to its original dimension using dense layers with a sigmoid activation function. The reconstruction process ensures minimal loss of information. Table 2 summarizes the architecture of the Autoencoder.

Table 2. Autoencoder Architecture

Layer	Description
Input Layer	Number of features in the dataset
Encoding Layer	20 neurons (latent space representation)
Decoding Layer	Same size as the input layer

Autoencoder Hyperparameters:

The autoencoder is trained using the following hyperparameters to optimize its performance:

- Input Size: Number of features in the dataset (original dimensionality).
- Latent Space Size: 20 (dimensionality of the encoded representation).
- Loss Function: Mean Squared Error (MSE).
- Optimizer: Adam optimizer with a learning rate of 0.001.
- Number of Epochs: 50.
- Batch Size: 32.

Machine Learning Component: Random Forest for Classification:

The machine learning component of the framework is a Random Forest classifier, an ensemble-based algorithm that excels in multi-class classification tasks. Random Forest creates a collection of decision trees during training and aggregates their outputs to make predictions.

What a Random Forest Works:

- **Training Phase:** Multiple decision trees are constructed using random subsets of the training data and features. Each tree learns to classify the data independently.
- **Prediction Phase:** For a given input, each tree predicts a class. The final classification is determined using majority voting across all trees.

Hyperparameter Tuning:

The tuned hyperparameters are presented in **Table 3**.

Table 3. Random Forest Hyperparameters

Parameter	Value
Number of Trees	100
Max Depth	None
Criterion	Gini
Minimum Samples Leaf	1

Random Forest Hyperparameters:

To maximize performance, the following hyperparameters were fine-tuned:

- **Number of Trees:** 100. Number of decision trees in the ensemble, ensuring diverse predictions.
- **Criterion:** Gini Impurity. The measure used to split nodes in each tree
- **Maximum Depth:** None. Allows trees to grow fully, capturing all patterns in the data.
- **Minimum Samples per Leaf:** 1. Minimum number of samples required to form a leaf node.

Overview of the Proposed Hybrid Framework:

This research presents a hybrid framework designed to address challenges in multi-class intrusion detection systems, particularly in healthcare data. The model leverages the combined strengths of deep learning (autoencoders) for dimensionality reduction and machine learning (Random Forest) for classification. To handle imbalanced datasets, the Synthetic Minority Oversampling Technique (SMOTE) was applied to generate balanced data, ensuring improved precision and recall for minority classes.

The proposed framework integrates three primary steps: data preprocessing, dimensionality reduction, and classification. (see **Figure 2**). These steps are executed sequentially to ensure the efficiency and accuracy of the intrusion detection system (IDS). The overall workflow is depicted in Figure 2.

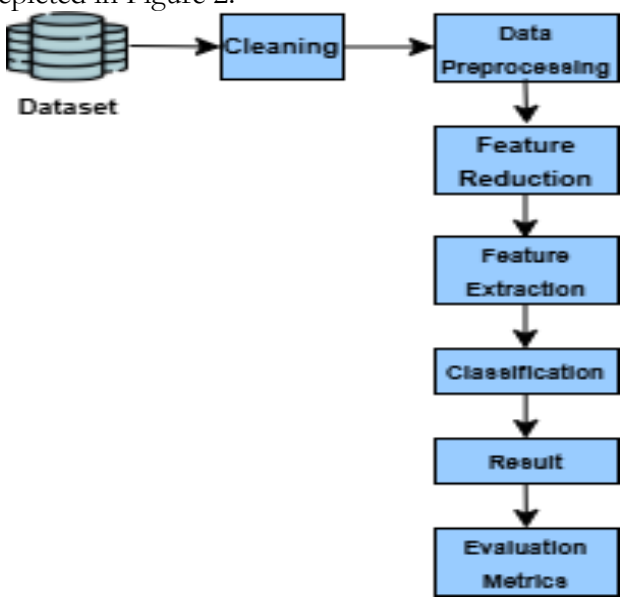

Figure 2. illustrates the architecture and workflow of the proposed hybrid IDS framework.

Dataset Analysis and Preprocessing:

Dataset Overview:

The dataset consists of 4998 samples and 35 features. These features represent network traffic metrics, and the target column (last column) contains labels indicating the type of intrusion or normal traffic. The dataset is multi-class, with various attack types such as DoS,

Botnet, and others. The dataset includes numeric features and requires preprocessing to handle missing values, outliers, and categorical variables.

Dataset Description:

The study utilizes a multi-class intrusion detection dataset tailored to healthcare applications. A summary of key features is provided in Table 4.

Table 4. Feature Descriptions of the Intrusion Detection Dataset

Feature Name	Description
Duration	Duration of the network connection.
Protocol Type	Type of protocol used (e.g., TCP, UDP).
Service	Network service on the destination port (e.g., HTTP, FTP).
Src_Bytes	Number of bytes transferred from the source to the destination.
Dst_Bytes	Number of bytes transferred from the destination to the source.
Flag	Status flag of the connection (e.g., SF, REJ).
Land	Binary feature indicating if the source and destination IPs/ports are the same.
Wrong_Fragment	The number of wrong fragments in the packet.
Urgent	Number of urgent packets in the connection.
Hot	Number of hot indicators (e.g., login attempts, sensitive data access).
Num_Failed_Logins	Count of failed login attempts.
Root_Shell	Binary feature indicating if a root shell was obtained.
Count	Number of connections to the same host as the current connection in 2s.
Srv_Count	Number of connections to the same service as the current connection in 2s.
Class	A label indicating the type of traffic (e.g., Normal, DoS, Probe, Botnet).

Analysis of Feature Distributions in the Intrusion Detection Dataset:

Figure 3. Feature Distributions Across the Intrusion Detection Dataset

To better understand the data distribution, Figure 3 visualizes the frequency distributions of selected features across all samples. As observed, several features exhibit skewed distributions, such as ifOutOctets11 and ifOutDiscards11, which may affect model performance. Other features, including icmpInMsgs and tcpRetransSegs, display concentrated distributions, indicating lower variability. Recognizing these patterns helps in applying appropriate preprocessing steps, such as normalization and dimensionality reduction.

Feature Distributions:

Interpretation:

- Each subplot represents the distribution of a feature across the dataset.
- Skewed distributions or outliers may impact model performance.

Observations:

- Features like ifOutOctets11 and ifOutDiscards11 are highly skewed.
- Features such as icmpInMsgs and tcpRetransSegs have concentrated distributions, which might indicate lower variability.

Preprocessing Steps:

- **Data Cleaning**: The dataset was cleaned by removing any rows with missing values and outliers.
- **Label Encoding:** The target labels (such as Normal, DoS, Botnet, etc.) were encoded using Label Encoder to convert them into numerical format.
- **Standardization:** The features were standardized using the Standard-Scaler to ensure all features were on the same scale, which is important for both Autoencoders and Random Forest.

Data Cleaning and Pre-Processing:

Data preprocessing is essential to ensure that the model performs optimally. The steps involved include the main components of the proposed framework and their functions are summarized in Table 5.

Table 5. Key Components and Their Functional Roles in the Proposed IDS Model

Step	Description
Missing Value Handling	Missing values are handled through imputation techniques or removing instances with missing data.
Feature Scaling	All input features are normalized to a range (e.g., 0-1) to ensure that no feature dominates due to scale differences.
Label Encoding	The target labels are converted into numeric format (0 for benign, 1 for attacks) to make the data compatible with the model.
Class Imbalance Handling	Oversampling the minority class (attacks) using SMOTE to balance the dataset and prevent biased model training.

Class Distribution and Imbalance:

Figure 4 shows the distribution of samples across different traffic classes. Some classes, such as tcp-syn and slowLoris, have significantly more samples than others, like bruteForce, which appears much less frequently. This imbalance can negatively affect model performance by biasing predictions toward majority classes. To address this, the SMOTE technique was applied during preprocessing to synthetically oversample minority classes and improve classification balance.

Observations:

Classes like tcp-syn and slow Loris have the highest counts, while brute force has the lowest. The imbalance could lead to biased predictions favoring majority classes.

Handling Class Imbalance with SMOTE:

After dimensionality reduction, SMOTE was applied to the reduced dataset. This technique generated synthetic samples for minority classes, ensuring balanced representation

across all classes. SMOTE is particularly effective for addressing issues of imbalanced datasets, which often lead to biased classification.

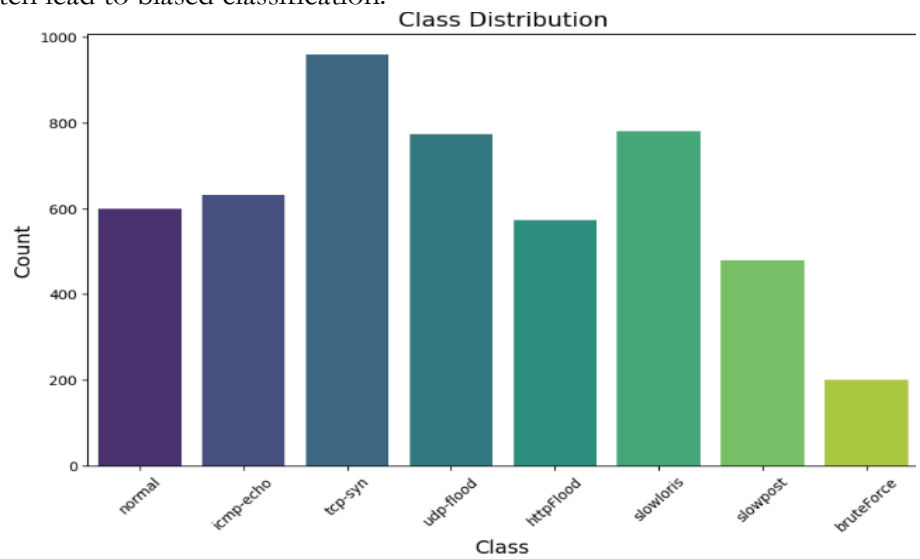

Figure 4. Class Distribution in the Intrusion Detection Dataset Interpretation

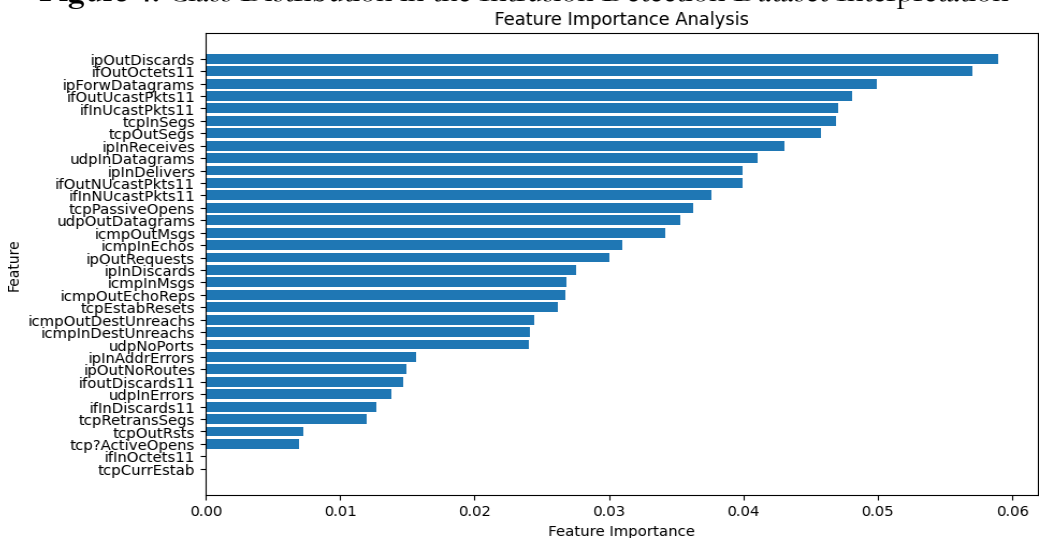

Figure 5. Feature Importance Scores from Random Forest Classifier

Feature Selection:

Feature selection plays a vital role in improving model accuracy by ensuring that only the most relevant features are used for training the model. After preprocessing, the Autoencoder is applied to reduce the dimensionality of the data and extract a latent representation of the most important features. The reduced features are then used to train the Random Forest classifier.

Framework Workflow:

The complete workflow of the proposed framework is described step-by-step:

- **Input Data:** Raw intrusion detection dataset is provided as input.
- **Preprocessing:** The data is cleaned, normalized, and oversampled using SMOTE to address imbalances.
- **Feature Extraction:** The autoencoder reduces the dataset's dimensionality, extracting the most relevant features.
- **Classification:** Random Forest classifies the reduced, balanced dataset into normal and multiple intrusion classes.

- **Evaluation:** Model performance is assessed using metrics such as accuracy, precision, recall, and F1-score.

Table 6. Functional Roles of Key Components in the Proposed IDS Framework

Model Component	Functionality
Autoencoder	Reduce feature dimensions for efficient processing.
SMOTE	Handle class imbalance by oversampling minorities.
Random Forest	Classify input samples into appropriate categories.

Table 6 summarizes the functional role of each core component in the proposed intrusion detection framework. The Autoencoder reduces the dimensionality of input features, retaining only the most informative representations. SMOTE addresses class imbalance by generating synthetic samples for minority attack types, ensuring balanced classification. Finally, the Random Forest classifier uses these refined features to accurately categorize network traffic into normal and various intrusion types.

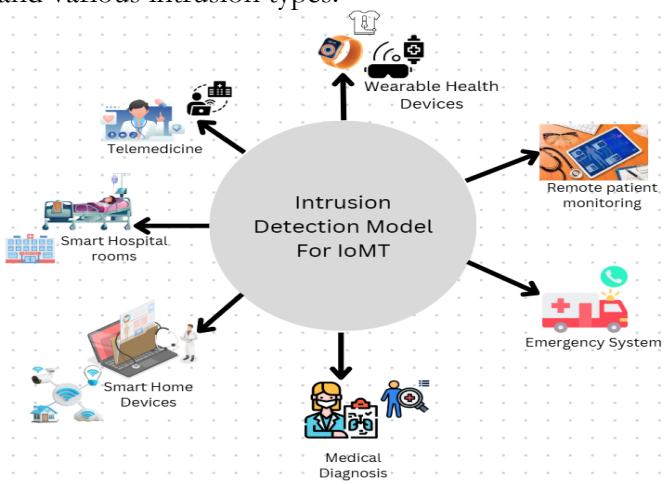

Figure 6. Application Scope of the Proposed Intrusion Detection Model in IoT Environments

As illustrated in Figure 6, the proposed Intrusion Detection System (IDS) can be deployed across various Internet of Medical Things (IoMT) environments, including smart hospitals, telemedicine platforms, wearable health devices, smart home monitoring systems, and emergency response infrastructure. The model's versatility makes it a strong candidate for real-time, healthcare-specific cybersecurity solutions.

Evaluation Metrics:

The performance of the proposed IDS is evaluated using various metrics, which allow a comprehensive assessment of the model's effectiveness:

- **Accuracy**: Measures the overall classification performance. It is calculated using the formula:

$$\mathbf{ACC} = \frac{TP+TN}{TP+TN+FP+FN}$$

Where TP, TN, FP, and FN represent the true positives, true negatives, false positives, and false negatives, respectively.

- **Recall**: Also known as detection rate or sensitivity, it measures the model's ability to detect attacks, calculated as:

$$\mathbf{Recall} = \frac{TP}{TP+FN}$$

Precision: Represents the proportion of correctly predicted attack instances among all predicted positives, calculated as:

$$\mathbf{Precision} = \frac{TP}{TP+FP}$$

- **F1-Measure**: Balances precision and recall, providing a single value that reflects both aspects. It is calculated as:

$$\text{F1-Measure} = \frac{2 * \text{Recall} * \text{Precision}}{\text{Recall} + \text{Precision}}$$

- **False Positive Rate (FPR)**: This metric evaluates the rate at which benign instances are misclassified as attacks. It is calculated as:

$$\text{FPR} = \frac{FP}{FP + TN}$$

- **True Positive Rate (TPR)**: Represents the probability of correctly identifying a true attack, calculated as:

$$\textbf{TPR} = \frac{TP}{TP + FN}$$

- **ROC-AUC**: The Area Under the Receiver Operating Characteristic curve indicates the model's ability to discriminate between benign and malicious traffic across different thresholds. A higher ROC-AUC value signifies a more effective classification model.
- **Specificity**: Measures the ability of the model to correctly identify normal (benign) traffic, calculated as:

$$\textbf{Specificity} = \frac{TN}{FP + TN}$$

Each of these metrics helps to assess different aspects of model performance, from detecting attacks (recall) to minimizing false positives (precision and specificity).

Result and Discussion:

The proposed hybrid intrusion detection framework was evaluated on a multi-class intrusion detection dataset tailored for healthcare applications. The results were assessed based on multiple metrics, including accuracy, precision, recall, F1-score, specificity, and ROC-AUC, to ensure a comprehensive evaluation of the model's performance across all classes.

Accuracy:

The framework achieved an overall accuracy of 99%, demonstrating its ability to correctly classify the majority of instances in the dataset. This high accuracy indicated the robustness of the combined autoencoder and Random Forest approach in handling multi-class intrusion detection scenarios.

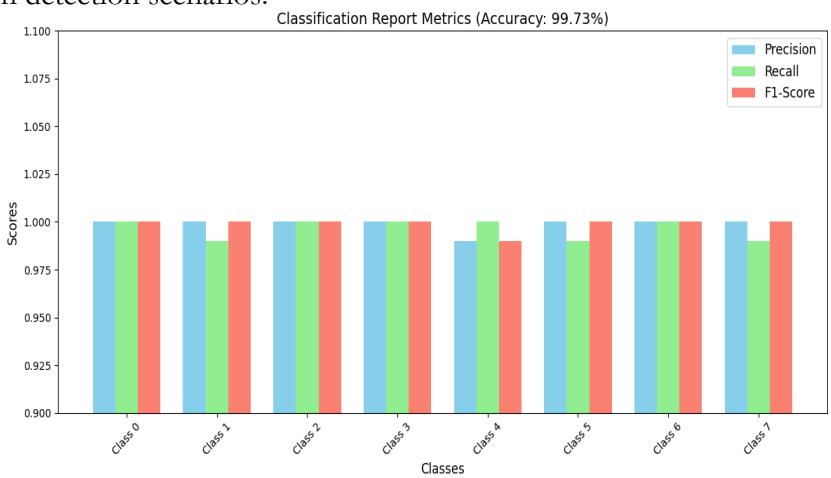

Figure 7. Accuracy of the Proposed Hybrid IDS Model on Multi-Class IoMT Dataset

Precision:

Precision was calculated for each class to evaluate the model's ability to correctly identify true positives among predicted positives. The results showed excellent precision for both majority and minority classes, indicating the model's ability to minimize false positives. The use of SMOTE during preprocessing played a critical role in ensuring equitable performance across all classes.

Recall (Sensitivity):

The recall values for each class were consistently high, reflecting the model's effectiveness in detecting actual intrusions. This metric highlighted the framework's capability to correctly identify both common and rare attack types in the dataset.

F1-Score:

The F1-score, which balances precision and recall, further confirmed the model's reliability. High F1 scores across all classes, including minority classes, underscored the framework's ability to maintain a balance between detecting attacks and minimizing false positives.

ROC-AUC:

The Receiver Operating Characteristic (ROC) curve and its corresponding Area Under theCurve (AUC) value were used to evaluate the model's overall classification ability. The framework achieved an AUC value close to 1.0, signifying excellent discrimination between benign and malicious traffic across different threshold values.

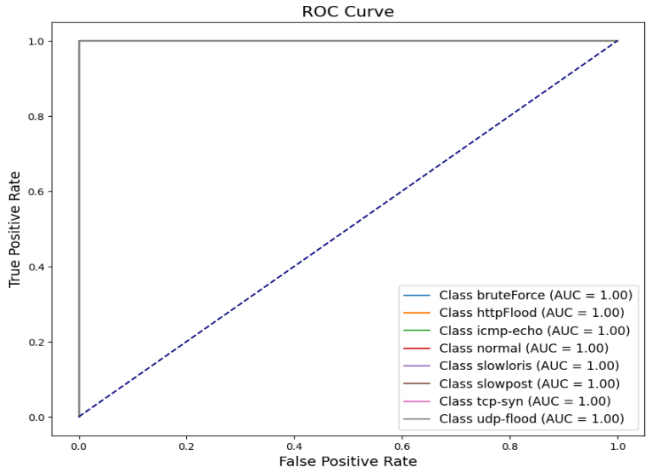

Figure 8. ROC Curve Showing the Discriminative Ability of the Proposed IDS Model

Confusion Matrix Analysis:

The Y-axis (True Class) represented the actual classes (ground truth) of the data, labeled from Class 0 to Class 7. The X-axis (Predicted Class) represented the predicted classes assigned by the model, also labeled from Class 0 to Class 7.

Diagonal Values:

These represented correctly classified instances where the predicted class matched the true class. For example:

- Class 0: 60 samples were correctly classified.
- Class 6: 276 samples were correctly classified.

The values on the diagonal indicated the model's strength in classification.

Off-Diagonal Values:

These were the misclassified samples, where the predicted class differed from the actual class. For instance:

- For Class 1, one sample was misclassified as Class 4.
- For Class 5, one sample was misclassified as Class 6.

Insights from the Confusion Matrix:

- High Accuracy: Most samples were correctly classified, as evidenced by the high diagonal values and sparse off-diagonal entries.
- Class Distribution: The model demonstrated robustness across all classes, with strong performance for Classes 2, 3, 4, 6, and 7.

- Few Misclassifications: As noted, Class 1 had one sample misclassified as Class 4, and Class 5 had one sample misclassified as Class 6.

The matrix reflected a weighted average accuracy of 99.73%.

False Positive Rate (FPR):

The False Positive Rate (FPR) measures the proportion of benign traffic incorrectly classified as attacks. In the proposed model, Class 4 (HTTP flood) exhibited the highest false alarm rate (~0.012), while Class 6 (slowest) showed a smaller but notable false positive value. The overall low FPR across all classes demonstrates the model's ability to minimize unnecessary alerts, a critical requirement in sensitive healthcare environments where precision is essential for system reliability.

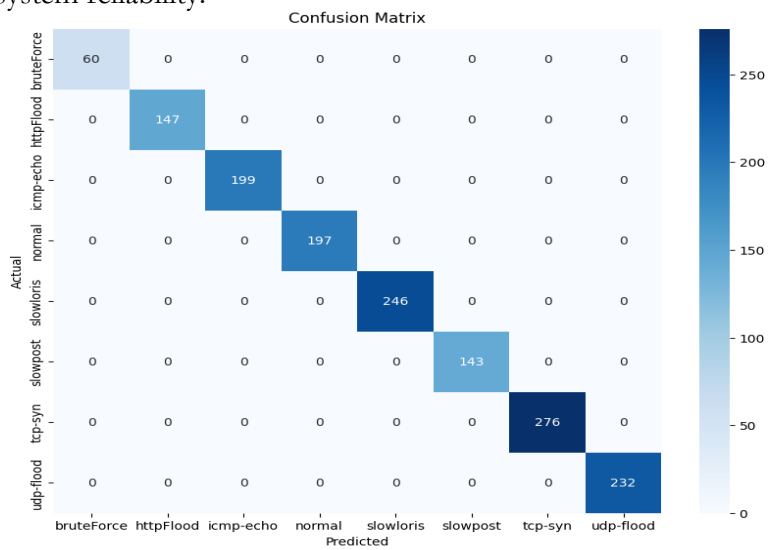

Figure 9. Confusion Matrix of the Proposed IDS Model for Multi-Class Classification

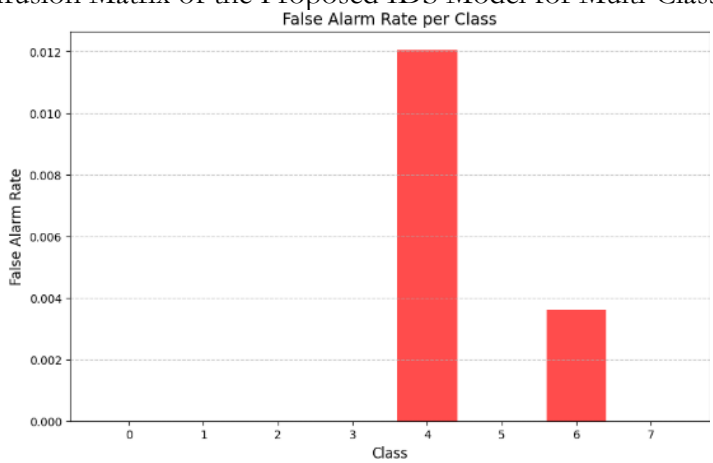

Figure 10. False Positive Rates for Individual Classes in the IDS Model

Model Performance Comparison:

This graph visually compares how well each model performs in terms of accuracy, which is the percentage of correctly classified intrusion or normal traffic samples. Each bar represents the performance level of a machine learning or deep learning model used for intrusion detection in the IoMT environment.

Autoencoder + Random Forest (99%)

This hybrid model combines a deep learning autoencoder for dimensionality reduction and a Random Forest classifier for final decision-making.It outperforms all other models due to:

- Its ability to extract compact, noise-free features (via the autoencoder)
- Robust, ensemble-based classification (via Random Forest)

- This high accuracy suggests it can reliably detect both known and unknown attack patterns across multiple intrusion types in healthcare systems.

CNN (98%):

- CNNs are known for detecting patterns in structured data like sequences and matrices.
- Though originally designed for image data, CNNs work well in IDS tasks by identifying patterns in network flow and traffic behavior.
- Slightly lower than the hybrid model, CNNs are strong but may struggle with deeper feature learning in tabular data compared to autoencoders.

LSTM (94%):

- LSTM networks are effective for sequential data, especially where time patterns matter.
- In IoMT, LSTMs can capture time-based attack patterns.
- However, LSTM may suffer from:
- Overfitting in small datasets
- High training time and sensitivity to noise in non-sequential features

SVM (90%):

- SVM is a traditional ML algorithm that works well in smaller, linearly separable problems.
- It has the lowest performance here because:
- It's not well-suited for high-dimensional, complex intrusion patterns
- It lacks adaptability for multi-class, large-scale intrusion types

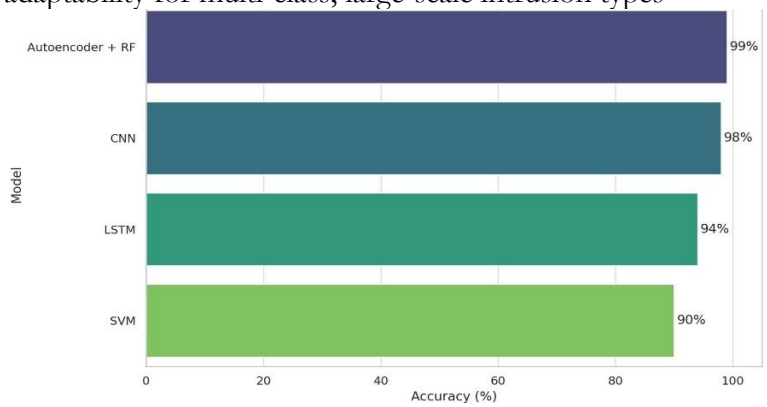

Figure 11. Accuracy Comparison of Intrusion Detection Models in IoMT

Figure 11 illustrates the classification accuracy of four intrusion detection models applied to Internet of Medical Things (IoMT) data: Autoencoder + Random Forest (Hybrid), Convolutional Neural Network (CNN), Long Short-Term Memory (LSTM), and Support Vector Machine (SVM). The hybrid model achieves the highest accuracy at 99%, followed by CNN (98%), LSTM (94%), and SVM (90%). This comparison demonstrates the superior detection capability and learning efficiency of the hybrid model in handling complex, high-dimensional healthcare data.

Feature Importance Analysis:

To understand which features most influence the classification results, the Random Forest model was analyzed for feature importance. The importance score indicates how much each feature contributes to the decision-making process in detecting different types of intrusions.

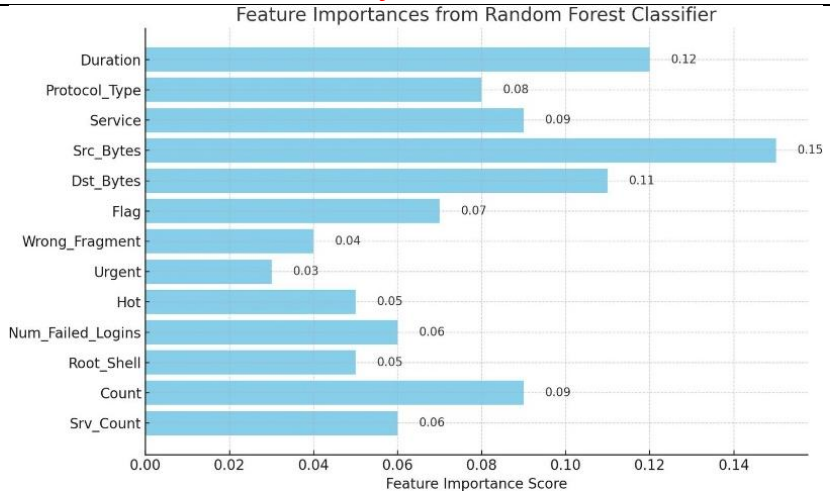

Figure 12. Feature Importances from Random Forest Classifier

Figure 12 displays the importance of individual features in classifying intrusion types using the Random Forest model. The highest contributing features included Src_Bytes, Duration, and Dst_Bytes, highlighting their significance in detecting anomalies in healthcare network traffic.

Reconstruction Error Distribution Analysis:

The figure 13 shows the reconstruction error for both training and test data. A clear separation is visible, where test data includes higher errors, likely corresponding to abnormal or attack patterns. This supports the use of reconstruction error as a threshold for anomaly detection in healthcare intrusion detection systems.

Separation of Train and Test Errors: The training reconstruction error (blue) is concentrated at lower values, indicating the model has learned the training data well. The test reconstruction error (orange) overlaps but slightly shifts towards higher values, which could indicate some generalization issues or the presence of anomalies in the test set.

Anomalies: The tail of the test reconstruction error distribution (higher values) likely corresponds to anomalies or data points the model struggles to reconstruct accurately. This distribution can be used to set a threshold for anomaly detection. For example, if the reconstruction error exceeds a certain value (e.g., 2.5 or 3.0), it can be flagged as an anomaly.

Skewness: Both distributions are skewed towards lower errors, which is expected in well-trained models. However, the long tail of test errors might warrant further investigation into specific test samples.

Impact of Smote:

The application of SMOTE during preprocessing effectively addressed the issue of class imbalance. It ensured that the minority classes received sufficient representation, resulting in improved detection rates and reduced bias.

Evaluation of Dimensionality Reduction:

The use of autoencoders for dimensionality reduction proved to be highly effective. By reducing the dataset to its most essential features, the autoencoder not only enhanced computational efficiency but also improved the overall classification accuracy by eliminating noise and redundant features.

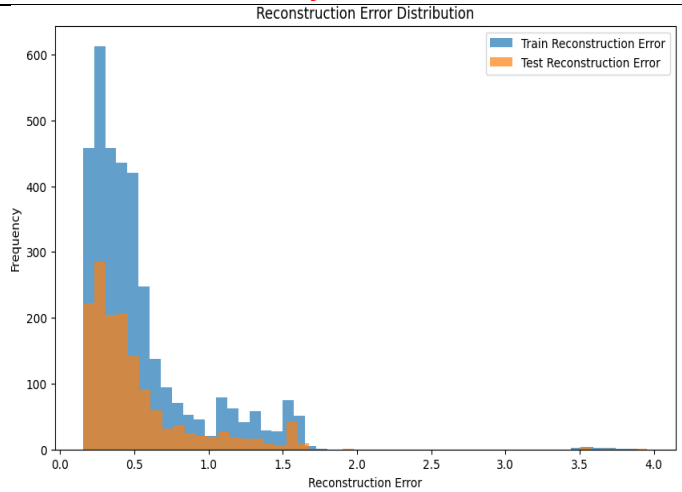

Figure 13. Reconstruction Error Distribution for Training and Test Data

Random Forest Classifier:

The Random Forest classifier, through its ensemble approach, delivered robust classification performance across all classes. The diversity of decision trees contributed to the high accuracy and generalization of the model.

Classification Report:

Performance metrics (Precision, Recall, F1-Score) for each intrusion class in the multi-class classification task. The model demonstrates high accuracy across all classes, indicating balanced and effective detection.

Table 7. Classification Report of the Proposed Hybrid Intrusion Detection System

Class	Precision	Recall	F1-Score	Support
0	1.00	1.00	1.00	60
1	1.00	0.99	0.99	147
2	0.99	1.00	1.00	199
3	1.00	1.00	1.00	197
4	0.99	1.00	1.00	246
5	1.00	1.00	1.00	143
6	1.00	1.00	1.00	276
7	1.00	1.00	1.00	232

Overall Observations:

The hybrid framework successfully addresses the challenges of multi-class intrusion detection in IoMT environments. The results highlight the following strengths: **Equitable Performance:** The model maintains consistent accuracy across all classes, including minority ones. **High Precision and Recall:** Ensures reliable detection of both common and rare attack types. **Scalability and Adaptability:** The framework is well-suited for real-world healthcare networks with complex and high-dimensional data. **Low False Positives:** Reduces unnecessary alerts, making the system practical for deployment in healthcare environments.

Conclusion:

This study presents a robust and efficient hybrid machine learning and deep learning framework aimed at enhancing security in Internet of Medical Things (IoMT) environments through improved intrusion detection capabilities. By integrating autoencoders for dimensionality reduction with a Random Forest classifier for multi-class classification, the framework effectively addresses key challenges associated with existing IDS approaches namely, handling high-dimensional data, detecting minority-class intrusions, and adapting to the dynamic nature of network threats in healthcare systems. The use of SMOTE for balancing class distribution proved instrumental in overcoming the issue of class imbalance, ensuring

equitable model performance across both majority and minority classes. Experimental evaluation using a healthcare-focused multi-class intrusion dataset demonstrated the framework's strong performance across multiple metrics:99% overall accuracy. The confusion matrix revealed minimal misclassifications, indicating a highly discriminative model capable of precise threat categorization. Moreover, the reconstruction error analysis offered insights into the autoencoder's ability to distinguish anomalous patterns, making the model suitable for real-time anomaly detection as well. In practical terms, this framework achieves a rare balance: it is both computationally efficient and highly accurate, making it scalable for real-world deployment in complex, high-dimensional IoMT networks. Its modular design enables adaptability to various healthcare security needs, including the detection of novel or evolving threats.

Future recommendations:

To further enhance the framework's capabilities: Online/Incremental learning can be explored to adapt to real-time evolving threats. Integration with federated learning could enable privacy-preserving collaborative training across distributed healthcare institutions. Explainability techniques (like SHAP or LIME) can be incorporated to make intrusion detection decisions more transparent for healthcare professionals and system administrators. Ultimately, the proposed model offers a viable, scalable, and effective solution to one of the most pressing challenges in smart healthcare, ensuring the security of interconnected medical devices and sensitive patient data in the IoMT landscape. To ensure real-world applicability, the proposed IDS must comply with privacy regulations such as HIPAA and GDPR. It should also support low-latency detection for real-time healthcare systems.

Acknowledgement: Acknowledgements are considered necessary.

Author's Contribution: The corresponding author should explain the contribution of each co-author completely.

Project details: If this research was conducted as a result of a project, please give details like project number, project cost completion date, etc.

References:

[1] I. S. M. Ali Tunc, Emre Gures, "A Survey on IoT Smart Healthcare: Emerging Technologies, Applications, Challenges, and Future Trends," *arXiv:2109.02042*, 2021, doi: https://doi.org/10.48550/arXiv.2109.02042.

[2] Eichie FranklinBernardi Pranggono, "Anomaly-Based Intrusion Detection System for the Internet of Medical Things," *Int. J. Informatics Dev.*, vol. 12, no. 2, 2023, doi: https://doi.org/10.14421/ijid.2023.4308.

[3] A. A. Bernardi Pranggono, "COVID-19 pandemic cybersecurity issues," *Internet Technol. Lett.*, 2020, doi: https://doi.org/10.1002/itl2.247.

[4] D. N. Celestine Iwendi, Joseph Henry Anajemba, Cresantus Biamba, "Security of Things Intrusion Detection System for Smart Healthcare," *Electronics*, vol. 10, no. 12, p. 1375, 2021, doi: https://doi.org/10.3390/electronics10121375.

[5] F. T. S. Khalid Albulayhi, Qasem Abu Al-Haija, Suliman A. Alsuhibany, Ananth A. Jillepalli, Mohammad Ashrafuzzaman, "IoT Intrusion Detection Using Machine Learning with a Novel High Performing Feature Selection Method," *Appl. Sci.*, vol. 12, no. 10, p. 5015, 2022, doi: https://doi.org/10.3390/app12105015.

[6] N. B. Ayoub Si-Ahmed, Mohammed Ali Al-Garadi, "Survey of Machine Learning based intrusion detection methods for Internet of Medical Things," *Appl. Soft Comput.*, vol. 140, p. 110227, 2023, doi: https://doi.org/10.1016/j.asoc.2023.110227.

[7] A. Alamleh *et al.*, "Federated Learning for IoMT Applications: A Standardization and Benchmarking Framework of Intrusion Detection Systems," *IEEE J. Biomed. Heal. Informatics*, vol. 27, no. 2, pp. 878–887, Feb. 2023, doi: 10.1109/JBHI.2022.3167256.

[8] L. P. W. G. Tehseen Mazhar, Inayatul Haq, Allah Ditta, Syed Agha Hassnain Mohsan,

Faisal Rehman, Imran Zafar, Jualang Azlan Gansau, "The Role of Machine Learning and Deep Learning Approaches for the Detection of Skin Cancer," *Healthcare*, vol. 11, no. 3, p. 415, 2023, doi: https://doi.org/10.3390/healthcare11030415.

[9] B. A. S. Al-rimy, M. A. Maarof, and S. Z. M. Shaid, "Crypto-ransomware early detection model using novel incremental bagging with enhanced semi-random subspace selection," *Futur. Gener. Comput. Syst.*, vol. 101, pp. 476–491, 2019, doi: https://doi.org/10.1016/j.future.2019.06.005.

[10] F. A. Aboaoja, A. Zainal, F. A. Ghaleb, and B. A. S. Al-Rimy, "Toward an Ensemble Behavioral-based Early Evasive Malware Detection Framework," *2021 Int. Conf. Data Sci. Its Appl. ICoDSA 2021*, pp. 181–186, 2021, doi: 10.1109/ICODSA53588.2021.9617489.

[11] S. P. T. Pandiaraj Manickam, Siva Ananth Mariappan, Sindhu Monica Murugesan, Shekhar Hansda, Ajeet Kaushik, Ravikumar Shinde, "Artificial Intelligence (AI) and Internet of Medical Things (IoMT) Assisted Biomedical Systems for Intelligent Healthcare," *Biosensors*, vol. 13, no. 8, p. 562, 2022, doi: https://doi.org/10.3390/bios12080562.

[12] S. A. Nora El-Rashidy, Shaker El-Sappagh, S. M. Riazul Islam, Hazem M. El-Bakry, "Mobile Health in Remote Patient Monitoring for Chronic Diseases: Principles, Trends, and Challenges," *Diagnostics*, vol. 11, no. 4, p. 607, 2021, doi: https://doi.org/10.3390/diagnostics11040607.

[13] N. N. Tamar Levy-Loboda, Eitam Sheetrit, Idit F. Liberty, Alon Haim, "Personalized insulin dose manipulation attack and its detection using interval-based temporal patterns and machine learning algorithms," *J. Biomed. Inform.*, vol. 132, p. 104129, 2022, doi: https://doi.org/10.1016/j.jbi.2022.104129.

[14] V. C. Parjanay Sharma, Siddhant Jain, Shashank Gupta, "Role of machine learning and deep learning in securing 5G-driven industrial IoT applications," *Ad Hoc Networks*, vol. 123, p. 102685, 2021, doi: https://doi.org/10.1016/j.adhoc.2021.102685.

[15] Luke Irwin, "Indiana hospital pays $55,000 after ransomware attack," *IT Gov. a GRCI Solut. Co.*, 2018, [Online]. Available: https://www.itgovernanceusa.com/blog/indiana-hospital-pays-55000-after-ransomware-attack

[16] Luke Irwin, "FBI Investigates Cyberattack on US Healthcare Systems," *IT Gov. a GRCI Solut. Co.*, 2023, [Online]. Available: https://www.itgovernanceusa.com/blog/fbi-investigates-cyberattack-on-us-healthcare-systems

[17] J. B. Awotunde, K. M. Abiodun, E. A. Adeniyi, S. O. Folorunso, and R. G. Jimoh, "A Deep Learning-Based Intrusion Detection Technique for a Secured IoMT System," *Commun. Comput. Inf. Sci.*, vol. 1547 CCIS, pp. 50–62, 2022, doi: 10.1007/978-3-030-95630-1_4.

[18] B. B. Rajasekhar Chaganti, Azrour Mourade, Vinayakumar Ravi, Naga Vemprala, Amit Dua, "A Particle Swarm Optimization and Deep Learning Approach for Intrusion Detection System in Internet of Medical Things," *Sustainability*, vol. 14, no. 19, p. 12828, 2022, doi: https://doi.org/10.3390/su141912828.

[19] G. Lazrek, K. Chetioui, Y. Balboul, S. Mazer, and M. El Bekkali, "An RFE/Ridge-ML/DL based anomaly intrusion detection approach for securing IoMT system," *Results Eng.*, vol. 23, p. 102659, 2024, [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2590123024009149?via%3Dihub

[20] Z. Sun, G. An, Y. Yang, and Y. Liu, "Optimized machine learning enabled intrusion detection 2 system for internet of medical things," *Franklin Open*, vol. 6, p. 100056,

2024, doi: https://doi.org/10.1016/j.fraope.2023.100056.

[21] M. I. Theyab Alsolami, Bader Alsharif, "Enhancing Cybersecurity in Healthcare: Evaluating Ensemble Learning Models for Intrusion Detection in the Internet of Medical Things," *Sensors*, vol. 24, no. 18, p. 5937, 2024, doi: https://doi.org/10.3390/s24185937.

[22] S.-C. H. Mousa Alalhareth, "An Adaptive Intrusion Detection System in the Internet of Medical Things Using Fuzzy-Based Learning," *Sensors*, vol. 23, no. 22, p. 9247, 2023, doi: https://doi.org/10.3390/s23229247.