RESEARCH PAPER

A Hybrid Machine Learning and Deep Learning Framework for Intrusion Detection in IoMT Using Grey Wolf Optimizer.

Dr. Thenmozhi T [1], Makesh L [2], Sabarish Gopal K [3], Sree Dharsan S [4], Vasanth M [5]

[1]Professor, HOD, Department of CSE
Email ID : hodcse@kgkite.ac.in
[2]Department of CSE
Email ID : makeshl023@gmail.com
[3]Department of CSE
Email ID : sabarishkovalan@gmail.com
[4] Department of CSE
Email ID : sreedharsancbe@gmail.com
[5]Department of CSE
Email ID : vasanth8447@gmail.com
KGISL Institute of Technology, Coimbatore, 641035, TamilNadu, India

ABSTRACT
Internet of Medical Things (IoMT) continues to be increasingly integrated in modern healthcare systems as a form of real-time specialist healthcare along with data exchange among medical equipment. Nevertheless, the high rate of interconnected medical equipment development also preconditions the emergence of a range of cybersecurity threats that can alarm patient safety and confidentiality of their data. This study suggests a hybrid intrusion detection agenda to solve these concerns, a pool of machine learning and deep learning processes. The suggested system combines the feature selection based on a Grey Wolf Optimizer (GWO), a Random Forest classifier to determine known attacks, and an autoencoder model to detect unknown attacks or zero-day attacks. GWO algorithm eliminates redundant features in the network traffic dataset without losing significant information needed to do the accurate detection. Random Forest model is applied to classify known patterns of attack with categorized data, and the autoencoder is trained to learn the normal work of the IoMT traffic and identify anomalies without the necessity of labelled attack samples. On the whole, the hybrid framework advances the reliability and effectiveness of intrusion detection on the IoMT setting through the fusion of the feature optimization and machine learning and anomaly detection algorithms. The suggested method can assist in enhancing the security of healthcare networks and assist in safer disposition of IoMT systems

Keywords: Internet of Medical Things, Intrusion Detection System, Grey Wolf Optimizer, Hybrid Machine Learning and Deep Learning, Autoencoder, Anomaly Detection, Zero-Day Attacks, healthcare security, Feature Selection, random forest.
How to cite this article: Thenmozhi T, Makesh L, Gopal KS, Dharsan SS, Vasanth M., A Hybrid Machine Learning and Deep Learning Framework for Intrusion Detection in IoMT Using Grey Wolf Optimizer...Int J Drug Deliv Technol. 2026; 16(11s): 745-768; DOI: 10.25258/ijddt.16.11s.76
Source of support: Nil.
Conflict of interest: None

INTRODUCTION

The rapid growth of digital healthcare technologies has resulted in the introduction of the Internet of Medical Things (IoMT), in which the medical devices, sensors, and healthcare systems are linked via the internet [1]. IoMT allows continuous monitoring of patients, standalone diagnosis, and effective healthcare services. Connected medical utensils, wearable sensors, and smart monitors are devices that generate and exchange vast capacities of medical data in real time [2], [3]. Even though this equipment has enhanced healthcare delivery and treatment to patients, they have brought new security issues.

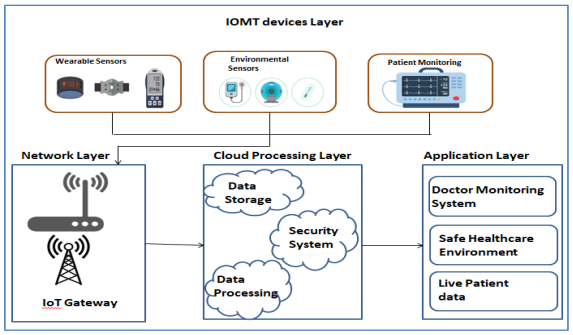

Figure 1. IoMT Healthcare System Architecture

Figure 1 illustrates an average IoMT healthcare system, Patient monitoring sensors and wearables transmit real time data via the IoT gateways to the cloud storage and analytics services. The hybrid intrusion detection system that we proposed is used here to monitor network traffic and intercept zero-day attacks and known attacks.

*Author for Correspondence: Dr Bindu T Nair

The designers of IoMT devices make interactive use of them, which makes them potential victims of cyberattacks. Cancellation of sensitive patient data and disruption of healthcare services through unauthorized accessibility, manipulation of data, and denial-of-service attacks, and other security issues can consider the data [4], [5]. Patient security may be directly impacted in critical healthcare scenarios by such attacks [6]. Consequently, the opposition of the IoMT systems to cyber threats is a significant demand of modern healthcare infrastructure.

Intrusion detection has of late been addressed with machine learning practices in order to enhance the accuracy of detection. These methods examine network traffic trends and identify them as either ordinary or suspicious [7], [6]. Nevertheless, the majority of machine learning models rely on categorized data and attack names, and they are not able to detect unseen attacks [8]. Conversely, deep learning models are able to detect uncharacteristic patterns without labelled attack data, but require more computational resources.

In order to overcome these obstacles, the present research suggests a hybrid intrusion detection charter, which incorporates machine learning and deep learning algorithms with bio-inspired feature optimization. The Gray Wolf Optimizer (GWO) is employed in choosing the most relevant features of the IoMT network traffic that simplifies computational complexity and does not affect detection performance. An autoencoder-based deep learning model is then trained to detect unknown attacks or zero-day attacks using anomaly detection and a Random Forest classifier is used to detect the known attacks. Having absorbed such methods, the suggested framework is expected to enhance the accuracy of detection, decrease the number of features, and increase the level of overall security of ionically magnetic telehealth care networks [9], [10]. This hybrid solution offers a balanced solution, which is a combination of the advantages of both supervised learning and anomaly detection, to achieve effective intrusion detection under resource-constrained IoMT environments [12].

Security Requirements in IoMT Environments

Keeping IoMT-based healthcare systems protected means ensuing basic information security principles. Because medicinal data is so delicate and patient monitoring happens in real-time, we need these security requirements:

Confidentiality:
Keep patient data safe from unauthorized access when it's being sent or stored.

Integrity:
Make sure medical records and sensor readings stay accurate and trustworthy.

Availability:
Healthcare services and monitoring systems must keep running, especially during emergencies.

Authentication:
Only authorized users and devices should get into IoMT networks.

Authorization:
Access control policies should limit what users can do based on their roles.

Non-Repudiation:
Track all system transactions so nobody can deny what they did.

If we don't meet these requirements, we risk patient safety, service disruptions, and breaking healthcare data laws.

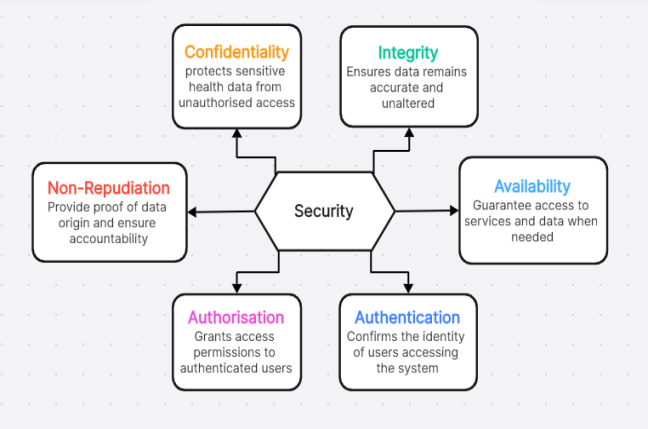

Figure 2. Security Requirements in IoMT Healthcare Systems

This research presents a hybrid ML-DL framework for IoMT Intrusion Detection. In addition to proposing a **GWO/ML** approach to feature selection to reduce size and increase performance, our work also includes an implementation of an Autoencoder to learn the normal behavior of an IoMT device in order to detect zero-day attacks.

1.1 Structure of the Manuscript

The structure of this paper will proceed as follows. Section 2 contains a background of IDS within IoT and IoMT with a summary of current IDS technologies. In Section 3, we provide an overview of our proposed hybrid machine learning/deep learning (ML/DL) framework with regard to its architecture and workflow. Section 4 focuses on the mathematical basis for Grey Wolf Optimizer feature selection (GWO-FS). In Section 5, we detail the ML portion of our IDS system. In Section 6, we detail the DL portion of our IDS that aids in the detection of zero-day attacks. Section 7 provides details for the experiment setup, datasets, and performance metrics that were used to evaluate how well our proposed ML/DL framework performs relative to current IDS technologies. Section 8 provides a discussion about the results of our experiments related to the IDS set up through our proposed ML/DL framework relative to existing systems. Section 9 concludes the paper and provides speculation on how future research

will enhance and continue the evolution of our proposed ML/DL framework..

1.2 Problem Statement

Cyber threats pose a significant danger to healthcare systems because of increased connectivity due to the Internet of Medical Things (IoMT), which provides access to significant amounts of health data and allows for real-time controls over these data. All stakeholders in healthcare organizations including provider organizations, care givers and patients experience negative impacts from losing knowledge from a data breach, including reputation and financial loss. Data breaches occur in many different forms, and often from combinations of root causes such as employee errors, software issues or inadequate security measures. The IoMT consists of smart devices and smartphones that are used for access to information, so they present many opportunities for unauthorised access to and data breaches [13]. Therefore, to sufficiently protect medical data and maintain patient confidentiality, a strong intrusion detection system (IDS) must be fully implemented.

Intrusion detection systems (IDS) currently provide a good level of defense for healthcare systems, but cannot adequately identify new types of attacks (zero-day). Using deep learning-based abnormality detection methods in the resource-constrained health care setting will have a large computational delay in the IDS. Furthermore, using high-dimensional feature sets from IoMT network traffic may hurt detection results and future processing times will be higher than they should be. A hybrid detection model that leverages the best of supervised machine learning and anomaly detection methods would serve to increase operational efficiency and decrease false positive rates.

2. Background and Related Work

As IoT Medical Technologies become more common, finding ways to secure healthcare data and networks from attack is becoming increasingly vital. Many researchers are pursuing the use of machine learning, deep learning, and bio-inspired optimization algorithms to create intrusion detection systems that can adjust and keep pace with new cyber threats across both IoT and IoMT. This section aims to provide a broad summary of the current state of the art in Intrusion Detection within IoMT, including existing research into the usage of machine learning based detections, deep learning seemingly anomaly based detections, and bio-inspired optimization for feature selection in relation to Intrusion Detection Systems (IDS) used for both IoT and IoMT.

2.1 Intrusion Detection in IoT and IoMT

As the Internet of Things (IoT) continues to rapidly develop, we see a proliferation of connected devices. In the healthcare field, this proliferation is reflected by the use of connected medical devices such as Sensors, Wearables, and Remote Patient Monitoring systems to actively monitor patients and share patient information across various healthcare providers. While the use of IoMT will help make healthcare more efficient and improve delivery of healthcare services in real time, it also creates a myriad of security challenges. Because of the open and distributed nature of IoMT networks, they are at risk to a multitude of attacks including denial of service [2], [3], data modification and misrepresentation, and unauthorized access.

Network traffic is monitored by Intrusion Detection Systems (IDS) to detect suspicious activity [4]. However, traditional IDS solutions designed for use on conventional networks cannot be effectively used in IoMT, as there is a wide variation among different devices, computing power is constrained, and latency requirements are very strict. As a result, researchers have developed intelligent methodologies for providing intrusion detection capabilities to support the evolution of IoMT traffic and to detect malicious behavior without interfering with healthcare systems..

2.2 Machine Learning–Based Intrusion Detection Systems

Machine-learning-based IDS have been the main focus of attention as an alternative to signature-based security, by using machine-learning (ML) algorithms that utilize historical data on realized network traffic to form patterns of normal behavior and abnormal behavior and to classify incoming network traffic as either normal or abnormal. Many machine learning techniques, including decision trees, random forests, support vector machines, and ensemble learning [4], [6], have been used extensively for intrusion detection of IoT and IoMT traffic because they can provide high accuracy for attacks that are already known.

However, there are limitations to the use of ML for intrusion detection [4]. Because model training in ML requires a large amount of labelled data and has an identified attack pattern, they tend to struggle with identifying new and evolving attack vectors. In addition, IoMT traffic has a large number of features, many of which are redundant and/or irrelevant to the determination of an attack. The increase of features adds to overall processing complexity and slows network-level attack detection, particularly when operating in real-time healthcare. Therefore, ML-based IDS may require optimization to scale effectively and operate efficiently..

2.3 Deep Learning for Anomaly and Zero-Day Attack Detection

Intrusion detection systems (IDS) do a great job of protecting healthcare facilities but aren't able to detect the newest types of attacks called "zero-day" attacks or have a large amount of time delay for performing decisions based on deep learning algorithms in a resource-constrained environment [8], [13]. The high dimensionality of Internet of Medical Things (IoMT) network traffic data will also decrease detection and increase processing time. To meet the needs of healthcare facilities, it is important that the IDS used to protect them utilize a hybrid detection framework that will combine the strengths of supervised machine learning detection with the strengths of anomaly detection

so that the efficiency of both methods is maximized and false positives are minimized in the healthcare environment [8], [14].

Using deep-learning models for anomaly-detection has been shown to be successful at identifying unknown zero-day attacks. However, this type of detection will not provide aid in making decisions about unknown attacks since they do not provide actual historical data on attacks to base their detection. They are capable of learning what should normally be done without knowing the specifics of the signatures tied to any types of associated attacks; however, these types of models typically require large amounts of computational resources and training time to build. Because of these limitations with regards to limited resources available in an IoMT environment, exclusively using deep-learning based functionality to implement an IDS may result in problems and will likely require a hybrid approach that balances an acceptable level of accuracy against resource use.

2.4 Bio-Inspired Optimization in Intrusion Detection Systems

The numerous numbers of researches that have been conducted regarding the application of bio-inspired optimization algorithms to enhance the performance of Intrusion Detection Systems (IDSs) through improved feature selection, parameter tuning and model optimization reflect the ever-growing use of bio-inspired optimization algorithms. Bio-inspired optimization algorithms are based upon behavior's seen in nature, such as evolutionary processes and swarm behavior's; as such they allow researchers to search large solution spaces reasonably effectively. Many bio-inspired optimization algorithms, including genetic algorithms, particle swarm optimization, firefly algorithms, and Grey Wolf Optimization (GWO), have been found to enhance the performance of an IDS on many types of networks [9], [16].

GWO has become increasingly popular as of late due in large part to its simplicity and ease of use, rapid convergence rate, and the very few parameters required to be set [10], [17]. GWO is based upon a model of the social hierarchy and hunting behaviors of grey wolves, thus enabling the exploration of the trade-off between exploration and exploitation during the optimization process. When implemented as a feature selection method in an IDS framework, GWO can achieve dimensionality reduction while maintaining classification accuracy, making it an excellent choice for use within intelligent IoT (IoMT) systems where both fast detection and computation efficiency are of great importance.

2.5 Research Gap and Motivation

Research studies that use Machine Learning, Deep Learning, and Bio-inspired Optimization as the basis of Intrusion Detection Systems and their interaction have not yet been published since a significant amount of research has focused on each of these technologies independently. The majority of Intrusion Detection Systems based on Machine Learning are able to identify previously known attacks, but they are less effective at detecting zero-day attacks. In contrast, Deep Learning based Intrusion Detection Systems have the advantage of providing greater accuracy in identifying anomalous behaviors; however, they require substantial computational resources to achieve that level of accuracy. The amount of features used in today's Intrusion Detection System technologies are far beyond what is appropriate to deploy in an environment with limited resource availability such as the Internet of Medical Things.

Based upon this, we identify future directions and create a combined machine learning/deep learning-based intrusion detection system framework that has been designed specifically for use by IoMT environments, uses significantly fewer features than existing solutions, processes data through computations with while maintaining high levels of accuracy in the detection of both known and unknown attacks.

The is basis for this research project is to exploit BIO optimization techniques to assist us in developing a new machine learning/deep learning-based model for improving the performance of today's current technologies utilized by health care institutions to detect intrusions on Home IoT devices.

2.6 Literature Survey

SI. No	Paper Name	Objective of Paper	Paper Outcomes	Drawbacks
1	(IoT) Network intrusion detection system using optimization algorithms (Shan, 2025)	The purpose of this research project will be to design an intrusion detection system (IDS) for IoT networks based on metaheuristic algorithms that use optimization.	In addition, it has been indicated that utilizing metaheuristic algorithms to improve the overall quality of the intrusion detection process has the potential to improve the overall success of detection, while also reducing the number of false positives	It is likely that these methods may have significant computational complexity, which could impede their implementation in real-time systems. Future research could potentially involve exploring a number of additional larger and more heterogeneously distributed types of attacks,

			compared to more traditional methods.	along with attempts to reduce the computational and storage requirements for remote systems.
2	A deep reinforcement learning-based robust intrusion detection system for securing IoMT healthcare networks (Shaikh et al., 2025)	The aim is to create a robust and deep identification (ID) system to identify Internet of Medical Things (IoMT) network attacks using Deep Reinforcement Learning (DRL) that will develop the ability to adapt to different types of attacks.	A functional adaptive identification system has been developed, which can learn and grow with new attack methods to enhance security on IoMT networks.	Some challenges that may occur during development will be maintaining stable training conditions and convergence of the ID system to the endpoint of interest. Future researchers may wish to investigate optimizing the reward function and testing on zero-day vulnerabilities.
3	A modified Grey Wolf Optimization algorithm for an intrusion detection system (Alzaqebah et al., 2022)	To develop an enhanced Grey Wolf Optimizer (GWO) Algorithm for better performing feature selection and classification of Intrusion Detection Systems (IDS).	The resulting E-GWO Algorithm has resulted in the selection of more relevant features and improved classification accuracy as well as a reduction in computational time needed to classify an IDS.	The improvement of the GWO Algorithm may depend upon the characteristics of the dataset used in developing it; thus, future studies may validate the continued use of the E-GWO Algorithm with many current datasets containing Modern attack types and the application of the E-GWO Algorithm to different classification methods.
4	A novel hybrid method using Grey Wolf algorithm and genetic algorithm for IoT botnet DDoS attacks detection (Maazalahi & Hosseini, 2025)	To combine the E-GWO Algorithm with the GWO GA to accurately detect Botnet-based DDoS attacks within IoT networks.	The hybrid E-GWO-GA approach will be very successful in identifying Complex Botnet-Based DDoS attack patterns, compared to other algorithms using the GWO Approach.	The hybrid model may have increased complexity; therefore, reducing the amount of time needed to process and identify the DDoS attacks. Future studies could optimize the hybrid model for deployment within Actors on IoT devices with limited computational capabilities.
5	A novel intrusion detection system based on a hybrid quantum support vector machine and improved Grey Wolf optimizer (Elsedimy et al., 2024)	A fusion of quantum machine learning and enhanced GWO (Grey Wolf Optimiser) is aimed at enhancing intrusive detection accuracy as well.	Quantum-enhanced Support Vector Machines (SVM) in conjunction with GWO feature selection have been shown to outperform traditional methods in their ability to detect intrusions by exploiting the principles of quantum computing.	Although these findings can be implemented practically, such as verifying that such hardware exists (i.e., at present there is not enough quantum computer hardware available for access or use), continuing to run simulations of larger networks will help lessen existing reliance on purely classical computing systems.
6	SafetyMed: A novel IoMT intrusion detection system using CNN-LSTM hybridization (Faruqui et al., 2023)	To develop a hybrid deep learning architecture which will use both convolutional neural networks (CNNs) and long short term memory (LSTM) networks	The use of this new type of CNN-LSTM model permitted detection of medical device data flows by taking into account both the spatial	One area for potential failure of the model is when highly imbalanced datasets exist. Ongoing work could explore other forms of advanced data

		for securing communications of medical devices within the Internet of Medical Things (IoMT).	(from CNNs) and temporal (from LSTMs) characteristics of the network traffic related to the devices.	augmentation techniques or applying cost-sensitive learning approaches to correct for this situation.
7	A voting grey wolf optimizer-based ensemble learning model for intrusion detection in the Internet of Things (Saheed & Misra, 2024)	An ensemble learning framework will utilize a voting-based approach to optimize IoT intrusion detection through the use of the GWO algorithm.	A voting-based ensemble, optimized by GWO, provides a stronger and more accurate IDS than using any of the individual classifiers on their own.	Ensemble methods tend to increase the complexity of models and the amount of resources they consume. Future work could concentrate on methods to reduce the amount of classifiers in an ensemble to make it more lightweight for use with IoT/IoMT edge devices.
8	An adaptive intrusion detection system in IoMT using fuzzy-based learning (Alalhareth & Hong, 2023)	The creation of an adaptive IDS can be accomplished using fuzzy logic to deal with the inherent uncertainty of traffic patterns on the IoMT.	By managing imprecise and ambiguous data from network traffic, the IDS was able to become an adaptive method of recognizing normal variations of IoMT traffic, in addition to reducing the number of false positives.	The development of fuzzy membership functions and rules is difficult and requires considerable expertise in the subject matter. Future efforts would be focus on automated learning of these rules.
9	An intrusion detection system for Internet of Medical Things (Thamilarasu et al., 2020)	The purpose of this study is to develop a lightweight, efficient IDS that can be used in IoMT systems.	The development of this functional and low-overhead IDS allows it to be deployed onto resource-constrained devices within limited processing power/batteries, which is vital for the success of IoMT systems.	Due to its lightweight nature, the performance of the proposed IDS will be limited by its ability to detect sophisticated, multi-phase attacks, compared to other complex and resource-intensive systems.
10	Deep learning enabled intrusion detection system for IoT security (Jablaoui et al., 2025)	To utilize deep learning architectures to detect potential threats in an IoT environment, we explored the potential capability of deep learning to automatically learn high-level representations of IoT traffic in order to develop adequate threat detection capabilities for known and potential unknown threats in a comprehensive method.	However, while deep learning models can effectively detect threats within IoT ecosystems, the nature of deep learning models as "black boxes" makes it difficult to understand the basis upon which the model made a particular decision.	As such, our future work will focus on explainable AI (XAI) in order to enhance the model's transparency and trust.
11	Deep learning-based network intrusion detection system for Internet of Medical Things (Ravi et al., 2023)	A deep-learning model was created to detect advanced attacks on the Internet of Medical Things (IoMT) networks.	eep learning for modeling complex behavior and detecting advanced and stealthy IoMT attacks is challenging and often results in higher-quality results than traditional	Developing an appropriate training set can be challenging to produce due to the privacy issues concerning medical data in the sensitive healthcare industry.

			attack detection methods.	
12	Efficient cyber attack detection on IoMT using deep recurrent neural networks and machine learning (Saheed & Arowolo, 2021)	To perform efficient cyberattack detection in IoT medical devices, a hybrid approach of both RNN's and traditional machine learning was developed.	The hybrid approach used the advantages of RNN's to process and classify complex sequential information (i.e. network traffic flows) in conjunction with traditional classifiers to provide an efficient and accurate method of detecting cyberattacks.	The hybrid approach may require further investigation into the balance of speed and accuracy provided by each classification method. Future research will investigate other architectures, such as transformers, for processing sequential information better than RNN's.
13	Hybrid intrusion detection models based on Grey Wolf Optimizer optimized deep learning (Elsaid et al., 2024)	Improving intrusion detection capabilities relies on deep learning model optimization via GWO (Grey Wolf Optimization).	The application of GWO for hyperparameter optimization during deep learning model development (e.g. determining number of layers/neuron count) was shown to result in significantly higher detection rates when compared to hyperparameters being set manually or through default values.	Hyperparameter optimization is also an expensive computational process and future work may look into enhancing GWO-based searches for hyperparameters so that they are done in a more efficient manner.
14	Intrusion detection system for healthcare systems using medical and network data: A comparison study (Hady et al., 2020)	The comparative study of intrusion detection systems was conducted using both medical data as well as network-based data from healthcare organizations.	Combining network-based and medical based data (e.g., patient vital signs) into one data set provides a much improved overall and accurate security posture from a healthcare perspective than if only network-based data was included.	The difficulty in successfully combining heterogeneous (and potentially incompatible) data environments into one dataset (network packets with medical data readings etc.) to perform the analysis of IDS performance and the absence of standardized datasets (data from network packets and medical data readings) to conduct the analysis that was the focus of this study will provide opportunities for future research within the healthcare industry as organizations seek to improve their IDS performance.
15	Intrusion detection system with Grey Wolf Optimizer (Kouidri et al., 2021)	To apply and assess the GWO method for selecting features in intrusion detection system applications.	Illustrated that using the GWO method alone results in a smaller, optimal feature set that provides quicker and more accurate detection of intrusions.	The data sets included in this research were probably dated; the next phase of work will involve testing current IoMT-related datasets on an annual basis and comparing them with current variants of GWO.

16	Multi-objective feature selection for intrusion detection systems: A comparative analysis of bio-inspired optimization algorithms (Sezgin et al., 2025)	To use multiple types of BIOS inspired methodologies to compare multi-objective feature selection methods for intrusion detection systems.	Compared the various types of BIOS inspired algorithms (GWO, GA, PSO) for the purpose of determining those that are best suited to achieve a balance between competing goals such as maximizing detection rate and limiting the number of features included.	The results are relative and will not be presenting an absolute answer. Future research will continue to concentrate on creating a hybrid that combines the most positive characteristics of those algorithms performing best in this study.
17	Network intrusion detection by optimized feature engineering using hybridization of Grey Wolf Optimizer and nonlinear activation function (Malik, 2024)	The GWO method for feature engineering in network-based Intrusion Detection Systems (IDS) and nonlinear inverse functions of features.	can increase the number of distinct feature representations, thus improving the ability of IDS to categorize data as either benign or malicious.	Future research could explore how well this technique generalizes across various network architectures due to the potential reduced interpretability of these new engineered features.
18	Optimized intrusion detection for IoMT networks with tree-based machine learning and filter-based feature selection (Balhareth & Ilyas, 2024)	The tree-based machine learning model optimizes for data security for IoMT through the use of filter-based methods of feature selection.	The combination of fast filter-based feature selection with a powerful tree based model, such as Random Forest or XGBoost, provides a high level of performance on both detection and data processing.	Filter based techniques may produce features that are not optimally aligned with the actual tree model being used. Future research could focus on developing an improved version of the Hybrid Filter Wrapper approach to increase alignment between filter-based and tree-based feature selection techniques.
19	Real-time anomaly detection in IoMT networks using stacking models and a healthcare-specific dataset (Goumidi, 2025)	To create a solution to detect anomalies in real-time utilizing ensemble stacking methods designed specifically for IoMT environments.	Successfully developed an ensemble stacking solution that was capable of near real-time processing on a health-related dataset while providing reliable accuracy that could be utilized in possible real-world implementations.	The purpose of the proposed solution will be limited by highest throughput network traffic. Future efforts may include investigating hardware acceleration or compressing the model for use with lower network throughput.
20	Securing the Internet of Medical Things: A machine learning approach for cyber threat detection (Arifin & Martadinata, 2024)	To execute a complete cyber-attack detection system for the Internet of Medical Things (IoMT) using machine learning methodologies.	Broadly described the results of many different ML methods were validated as a viable option for use as a primary method of cyber-attack detection in an IoMT security framework.	This study could be classified more as a general summary or report on cyber-attack detection and would likely be limited by either absence of a defined threat, or evaluation on a non-specific dataset pertaining to an IoMT application.
21	A Comprehensive Survey on Security and Privacy Challenges in Internet of Medical Things Applications: Deep Learning and	Evaluating the security and privacy challenges associated with IoMT systems, as well as assessing how both machine learning and deep	This research comprises an exhaustive taxonomy of the various security threats that exist in IoMT systems. The authors have identified	Additionally, the authors identify several key limitations to current IoMT systems, including: the lack of realistic datasets; difficulties associated with

	Machine Learning Solutions, Obstacles, and Future Directions (Nithyavani G, Naga Raja G, 2024)	learning approaches can be utilized to mitigate those challenges.	several security threats and detailed how both ML and DL techniques can enhance intrusion detection and safeguard the privacy of patient data in healthcare.	deploying ML and DL models on edge devices; and regulatory compliance challenges specific to the healthcare market.
22	A Survey on Intelligent Internet of Things: Applications, Security, Privacy, and Future Directions (Aouedi et al., 2024)	An overview of intelligent IoT technology is provided with a focus on applications, security threats, privacy challenges, and potential future directions for research in this area.	The authors classifying the IoT security approaches they reviewed according to the use of ML, DL, federated learning, and reinforcement learning; as well as providing an extensive discussion of each of those classes along with the corresponding IoT secure framework.	Lastly, the study is primarily theoretical in nature and does not include any actual implementation or experimental testing for validation of results in real-world IoT systems.
23	Binary Optimization Using Hybrid Grey Wolf Optimization for Feature Selection (Al-Tashi et al., 2019)	A hybrid binary Grey Wolf Optimization (GWO) algorithm is developed to achieve high classification performance for feature selection in an intrusion detection system (IDS).	The hybrid GWO algorithm successfully reduced the number of features while maintaining a high level of performance in classifying data (the main goal of the experiment).	The hybrid GWO algorithm also has very high computational complexity compared with other machine learning algorithms and has not been evaluated experimentally on Internet of Medical Things (IoMT) datasets or real-time healthcare environments.
24	Comprehensive Review of IDS Techniques: ML and DL in Different Networks (Rakine et al., 2025)	The purpose of the review of intrusion detection techniques with both machine learning (ML) and deep learning (DL) algorithms is to summarize the existing intrusion detection techniques implemented in various network environments (IoT, cloud, and SDN networks).	The results of this review include a comparison of ML and DL algorithms (SVM, Random Forest, CNN, LSTM) for the purpose of detecting network intrusions.	In addition, the review does not provide any evaluation of the challenges associated with real-time deployment of algorithms or consider any resource constraints when using these algorithms in IoMT environments.
25	Improved Grey Wolf Optimization Algorithm and Application (Hou et al., 2024)	This project aims to improve upon existing versions of the Grey Wolf Optimization algorithm by enhancing their ability to find optimal solutions to various optimization problems through improved initialization and convergence methods.	Through extensive benchmarking and path-finding applications using the enhanced GWO algorithm, researchers found that this revised version converges significantly faster than standard versions of GWO, as well as yields better optimization results.	The current research studies the effectiveness of the GWO algorithm only within a simulated environment; therefore, it does not provide information about its applicability in the area of cybersecurity or intrusion detection systems.
26	Intrusion Detection and Real-Time Adaptive Security in Medical IoT Using a Cyber-Physical	This project will provide a framework for building an advanced Cyber-Physical System (CPS) designed to facilitate real-time intrusion	The proposed CPS demonstrated very high quality results in how well it was able to detect an intrusion with the	The performance of this system has not yet been validated in any real-world hospital scenarios or how well it would scale if

	System Design (Serhani, 2025)	detection for Medical Internet of Things (IoMT) systems utilizing Machine Learning algorithms.	highest quality monitoring results when applied to valid ToN-IoT datasets.	applied in a large scale healthcare network.
27	Intrusion Detection in the Internet of Things Using Convolutional Neural Networks: An Explainable AI Approach (Ebrahimi et al., 2025)	An integrated CNN-Based IDS and Explainable AI Techniques in IDS as a Mean of Providing Transparency into IDS and Model Results.	The model has produced high detection accuracy with Interpretable Results through the use of Feature Importance Using SHAP and LIME.	Although the model has a high level of accuracy, there's still a need for further evaluation regarding the Model's Scalability and Performance Related to Heterogeneous IoT Environments.
28	SNN-IoMT: A Novel AI-Driven Model for Intrusion Detection in Internet of Medical Things (Benmalek et al., 2025)	To Develop a Stacked NN Model from Multiple Deep Learning Architectures that can be Used to Detect Intrusions Within an IoMT Environment.	Through the use of Stacked Architectures, the Detection Performance of the Model Enhanced the Detection Accuracy by Capturing Spatial and Temporal Traffic Patterns as they Relate to IoMT Network Data.	The Model has been Trained on Small Sized IoMT Data Sets and will require further evaluation for Potential Use in Real-Time Deployment Within Healthcare Settings.
29	Stacking Ensemble Deep Learning for Real-Time Intrusion Detection in IoMT Environments (Alalwany et al., 2025)	Developing a system in real time of detecting unauthorized network traffic on IoMT (Internet of Medical Things) can be done with the integration of multiple deep learning models together (stacking ensemble).	The model created for this research had a very accurate detection rate as well as provided the ability for IoMT networks' traffic analysis to be done using real-time information.	There are currently no defined datasets to evaluate the effectiveness of the proposed model and further research is needed into the applicability of the model in large scale heterogeneous IoMT networks.
30	Survey of Machine Learning Based Intrusion Detection Methods for Internet of Medical Things (Si-Ahmedad et al., 2023)	Conduct a review of different types of machine learning algorithms/techniques used in intrusion detection systems across multiple layers of an IoMT architecture.	The survey provides information regarding how effective machine learning-based models are being used to identify potential cybersecurity threats in IoMT networks and it classifies those solutions by their architectural layer.	Some of the limitations/challenges identified with state-of-the-art machine learning intrusion detection systems in IoMT are the availability of existing datasets for IoMT security purposes and the challenge of deploying machine learning models on constrained resource medical devices.

Table 1: Literature Review of Intrusion Detection Systems for IoMT

3. Proposed Hybrid Intrusion Detection Framework

This section presents our hybrid intrusion detection framework for IoMT environments. The framework combines machine learning and deep learning with bio-inspired feature optimization to detect both known and unknown attacks [17]. We focus on reducing computational complexity, improving detection accuracy, and building strength against zero-day threats in healthcare networks.

3.1 System Architecture Overview

Multi-layered architecture for intrusion detection systems consists of a pre-processing layer (for data and traffic), feature optimization layer, machine learning classification layer (for detecting known attack patterns), and an ML classification layer utilizing deep learning via autoencoders for detecting unknown attacks [18]. This architecture was specifically created for IoMT. In the IoMT environment, both the ability to perform attack detection in real-time and effectively manage resources will be essential.

The first layer of this architecture, the pre-processing layer, receives raw traffic from IoMT devices through this layer. At this stage, raw traffic from IoMT devices is pre-processed for use in training. The pre-processed data are then forwarded to the next layer of the architecture, which is the Feature Selection Layer (FSL). FSL applies the Grey Wolf Optimizer to reduce the total required number of features needed to perform intrusion detection, therefore successfully reducing the overall number of dimensions of the data set used for intrusion detection while still providing sufficient numbers of dimensions to perform accurate intrusion detection.

The optimised features will then be forwarded to the ML classification methods that are capable of identifying known patterns of attack in the data. Concurrently, the same features will also be forwarded to a deep learning-based autoencoder ML classification method that performs anomaly detection by learning about the normal behaviours associated with IoMT traffic.

.

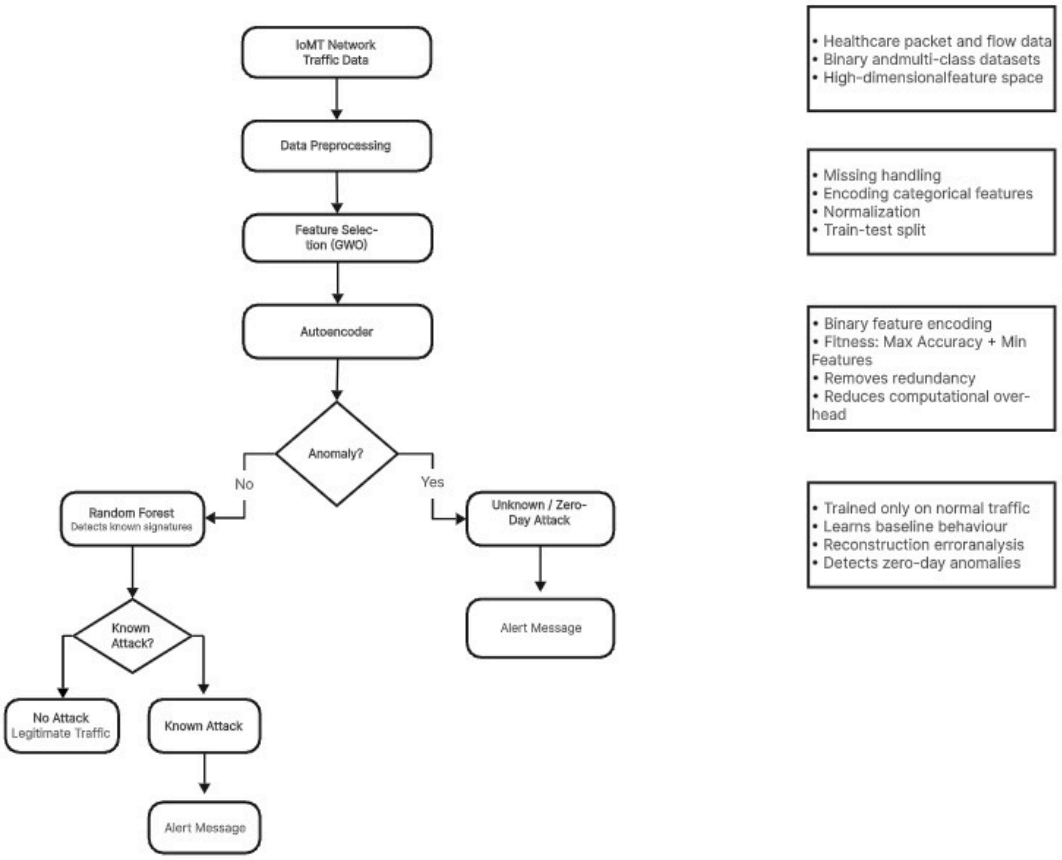

Figure 3. Flow Diagram

3.1.1 Detailed Architecture Description

Hybrid intrusion detection framework follows a multi-layered architecture built for IoMT healthcare. It combines optimization, supervised learning, and anomaly detection into one security model.

First layer is **Data Acquisition**. Here we collect raw network traffic from IoMT devices like patient monitoring sensors, environmental sensors, and control units. This traffic includes packet-level and protocol-level features.

Second layer does **Data Preprocessing**. This includes cleaning data, encoding categorical attributes, normalizing, and splitting the dataset. This stage makes sure everything works with both ML and DL models.

Third layer does **Feature Selection using Grey Wolf Optimizer**. Here we remove redundant and irrelevant features to cut computational complexity and improve model generalization.

Fourth layer is the **Machine Learning Detection Module**. A Random Forest classifier trains on the optimized feature subset. This module detects known attack patterns using labeled data.

Fifth layer is the **Deep Learning Anomaly Detection Module**, implemented with an autoencoder. The autoencoder trains only on normal IoMT traffic to learn baseline behavior. During testing, high reconstruction errors point to possible zero-day attacks.

Finally, a **Hybrid Decision Module** combines outputs from Random Forest and the autoencoder. If the supervised model says traffic is malicious, it's a known attack. If the supervised model says normal but reconstruction error is above threshold, it's a possible zero-day attack. This layered design catches everything while keeping computational efficiency for healthcare IoMT.

3.2 Workflow of the Proposed Framework

Hybrid intrusion detection framework workflow has several stages:

Data Preprocessing: Raw IoMT network traffic often has noise, missing values, and inconsistent formats. In preprocessing, we remove irrelevant attributes, encode categorical values, and normalize data so it works with both ML and DL models. Then we split the dataset into training and testing sets.

Feature Selection Using GWO: To handle all the features in IoMT traffic, we use Grey Wolf Optimizer for feature selection. GWO mimics grey wolf social hierarchy and hunting behavior to search the feature space efficiently. By testing candidate feature subsets with a fitness function based on detection performance, GWO finds a reduced set of useful features. This cuts redundancy, lowers computational load, and improves detection efficiency.

Machine Learning–Based Intrusion Detection: The selected features train a machine learning classifier that detects known attack patterns. ML models learn to separate normal and malicious traffic when labeled data is available. This part gives high accuracy for known attacks.

Deep Learning–Based Anomaly Detection: To find unknown and zero-day attacks, we add a deep learning-based autoencoder. The autoencoder trains only on normal IoMT traffic to learn patterns of normal behavior. During testing, samples with high reconstruction errors get flagged as anomalies. This lets the framework find new attack patterns without needing labeled attack data.

Hybrid Decision Logic: We get the final detection by combining outputs from the ML classifier and autoencoder. If the ML model says a sample is malicious, it's a known attack. If the ML model says normal but the autoencoder shows high reconstruction error, the sample gets flagged as a possible zero-day attack. This hybrid approach uses strengths from both ML and DL.

3.3 Mathematical Formulation of the Proposed Framework

This section presents the calculation for Grey Wolf Optimizer and autoencoder -based anomaly detection.

3.3.1 Grey Wolf Optimizer Mathematical Model

The Grey Wolf Optimizer impressionists the way that real-life grey wolves hunt and show supremacy amongst each other within their established social order. One of their unique physiognomies is the manner in which they circumscribe their target; mathematically, this relationship can be epitomized by the following:

$$D = | C \cdot Xp(t) - X(t) | \quad (1)$$

$$X(t+1) = Xp(t) - A \cdot D \quad (2)$$

Where:

X(t) = Current position vector of a grey wolf at iteration ttt

Xp(t) = Position vector of the prey (best solution found so far)

D = Distance vector between wolf and prey

A, C = Coefficient vectors controlling exploration and exploitation

t = Current iteration number

The coefficients A and C are defined by:

$$A = 2a.r_1 - a \quad (3)$$

$$C = 2r_2$$

Where:

a = linearly diminishing parameter from 2 to 0, as iterations increase

r1,r2 ∈ [0,1] = Random variables

A = Step size & direction of exploration

C = Stochastic effect involved with prey

Fnal position of the wolf after updating the positions of the 3 best wolves (α, β, & δ) is represented by:

$$X(t+1) = (X\alpha + X\beta + X\delta)/3 \quad (4)$$

This allows for balanced exploration and exploitation within the feature search space.

3.3.2 Fitness Function for Feature Selection

Maximizing classification accuracy while minimizing the number of features selected is the goal of the feature selection process. A fitness function to measure the fitness of feature sets is used for this study, which is formulated as follows:

$$Fitness = \alpha(accuracy) - \beta(| FTotal | / FSelected) \quad (5)$$

where:

Accuracy is the classification accuracy achieved with the selected features.

FSelected is the number of features selected.

FTotal is the total number of original features..

α and β are weight coefficients (i.e., they provide an effect on how much either accuracy or the number of features would contribute to the overall fitness of the features).

3.3.3 Autoencoder Reconstruction Loss

To train the autoencoder, it is necessary to reduce the reconstruction error of the original input with respect to the reconstruction of the input by the encoder. The reconstruction loss will be defined using the mean squared error (MSE):

$$MSE = (1/n)\Sigma i=1n \ (xi-x\hat{}i)^2 \quad (6)$$

where:

x_i is an original input sample,

$x\hat{}_i$ is a reconstructed output,

n is the total number of samples.

3.3.4 Threshold-Based Anomaly Detection

In order to detect zero-day attacks, a threshold has been defined based on the distribution of reconstruction errors from the normal samples within the data. The formula for this threshold is:

$$Threshold = \mu + K\sigma \quad (7)$$

where:

μ is the mean reconstruction error of the normal samples,
σ is the standard deviation,
K is a constant controlling sensitivity.
If the reconstruction error of the sample exceeds this defined threshold, it will be classified as an anomalous sample.

3.3.5 Binary Encoding of Feature Subsets

The gray wolf-based feature selection process will employ binary vectors to represent the prospective feature subsets. Each gray wolf will represent a prospective feature subset in binary form:

X = [x1, x2, x3, …, xn], (8)

Where

xi = {1, if the ith feature has been accepted; 0, if not}.

The use of binary representations allows the gray wolf optimization algorithm to efficiently search the feature space and evaluate multiple combinations of features. After the positions are updated, the position values, which are continuous, will be converted to binary decisions through the use of a sigmoid transformation.

3.3.6 Computational Complexity Analysis

The overall computation complexity of the proposed framework will consist of three principal components:

(1) Grey Wolf Optimizer

Let N = the number of gray wolves;
T = the number of iterations;
F = the number of features.

The complexity of gray wolf optimized feature selection is:

O(N×T×F) (9)

The computational complexity established by the GWO will be manageable in IoMT datasets with moderate feature dimensions.

(2) Random Forest Classifier

where

M = the number of decision trees and
S = the number of training samples

The training complexity is:

O(M × S × log(S)). (10)

Ultimately, the proposed hybrid framework will sustain the computationally efficient levels necessary for use in IoMT environments where rapid detection and low latency are required.

(3) Autoencoder Model

For:
n input samples
d input dimension
E epochs
The training complexity is:

O(E×n×d) (11)

Since the feature dimension is reduced using GWO, the computational burden of the autoencoder is significantly minimized.

Overall, the proposed hybrid framework maintains computational efficiency suitable for IoMT environments, where real-time detection and low latency are critical requirements.

4. Feature Selection Using Grey Wolf Optimizer

Feature selection really matters in intrusion detection, especially in IoMT where efficiency and speed are crucial. This section explains why we need feature optimization, gives an overview of GWO, and describes how we use GWO for feature selection.

4.1 Motivation for Feature Optimization

IoMT network traffic datasets usually have lots of features from packet and flow data. While these features might represent network behavior, many are redundant or useless for detection. Processing all these features increases complexity, memory use, and training time, which is bad for resource-limited healthcare systems.

Moreover, redundant features can hurt detection by adding noise and raising overfitting risk. So feature optimization is essential to find a small set of useful features that keep accuracy while improving efficiency. By reducing dimensions, feature selection improves generalization, speeds up training and testing, and helps practical deployment in IoMT. These reasons led us to use efficient optimization-based feature selection.

4.2 Grey Wolf Optimizer Overview

Grey Wolf Optimizer is a bio-inspired algorithm that mimics grey wolf leadership and hunting [18]. GWO models social roles with four wolf types: alpha (α), beta (β), delta (δ), and omega (ω). Alpha is the best solution, followed by beta and delta, which guide the search. Omega wolves follow the leaders.

The hunting behavior has three steps: searching, encircling, and attacking prey [18], [19]. Wolf positions update based on alpha, beta, and delta positions. This balances exploration and exploitation, allowing good convergence with little tuning. GWO's simplicity, speed, and strength make it good for feature selection in IDS.

4.3 GWO-Based Feature Selection Process

In our framework, GWO selects an optimal feature subset from preprocessed IoMT data. Each wolf is a candidate feature subset as a binary vector, where 1 means include the feature and 0 means exclude. The goal is to maximize detection while minimizing features.

A fitness function evaluates each candidate by considering both accuracy and feature reduction. This guides selection of alpha, beta, and delta wolves each iteration, favoring subsets with high accuracy and few features. Through updates, GWO finds better feature subsets.

Tests on IoT healthcare datasets show GWO reduced binary dataset features from 10 to 6 while keeping high accuracy. For multi-class, it reduced from 10 to 4 without much

performance loss. This shows GWO removes redundant features and improves efficiency for IoMT security.

4.4 Selected Features After Optimization

The Grey Wolf Optimizer significantly reduced the dimensionality of the IoMT traffic dataset while preserving classification performance. The selected features for both binary and multi-class classification scenarios are listed below.

Binary Classification (10 → 6 Features)

The following six features were selected by the GWO algorithm for binary intrusion detection:

frame.time_delta
tcp.time_delta
tcp.flags.ack
mqtt.msgtype
mqtt.qos
mqtt.ver

These features demonstrated strong discriminatory capability between normal and malicious traffic patterns while reducing redundancy.

Multi-Class Classification (10 → 4 Features)

For the multi-class classification scenario, GWO selected four dominant features:

tcp.flags.ack
mqtt.msgtype
mqtt.qos
mqtt.ver

The reduction from ten to four features significantly decreases computational complexity while maintaining high classification accuracy.

The selected features primarily represent transport-layer behavior and MQTT protocol characteristics, indicating that protocol-level traffic attributes play a critical role in distinguishing IoMT attacks from legitimate communication.

4.5 Pseudocode of GWO-Based Feature Selection

To clearly describe the optimization procedure used for feature selection, the following pseudocode summarizes the steps of the Grey Wolf Optimizer applied in this work.

Algorithm 1: GWO-Based Feature Selection for IoMT Intrusion Detection

Input:

IoMT dataset with total feature set F_{Total}
Population size N
Maximum iterations T

Output:

Optimal feature subset $F_{Selected}$

1.Initialize grey wolf population randomly (binary feature vectors).
2.Evaluate fitness of each wolf using the defined fitness function.
3.Identify the three best wolves as α , β , and δ.
4.For each iteration t=1 to T:
Update coefficient vectors A and C.
Update positions of wolves based on α , β , and δ.
Apply binary transformation to updated positions.
Recalculate fitness for each wolf.
Update α , β , and δ.
5.End loop when maximum iterations are reached.
6.Return the feature subset corresponding to α.

This procedure enables efficient exploration of the feature search space while maintaining a balance between exploitation and diversification. The use of binary encoding ensures that the selected features are directly interpretable and suitable for machine learning classification.

5. Machine Learning–Based Intrusion Detection

The machine learning part of our framework detects known attacks in IoMT traffic. This section covers our chosen ML model, training approach, and performance on binary and multi-class tasks.

5.1 Selected Machine Learning Model

We picked Random Forest for known attack detection [4], [30]. RF is an ensemble method that builds many decision trees and combines their outputs. This ensemble approach improves robustness and reduces overfitting, making RF good for complex IoMT data.

RF also works well with reduced feature sets, which fits with our GWO selection. RF handles noisy data, class imbalance, and many features while staying stable. Plus, RF needs less tuning than complex models, making it useful for real-time IoMT security.

5.2 Training and Validation Strategy

We train the Random Forest model using optimized feature subsets from GWO. We split the dataset into training and testing sets to check generalization. We run separate tests for binary and multi-class cases to see performance in different settings.

During training, RF learns patterns between normal and malicious traffic using labeled data. We test model performance on the test set to make sure it finds known attacks without overfitting. This validation gives reliable assessment of ML-based detection in our hybrid framework.

5.3 Performance on Binary and Multi-Class Datasets

We measure Random Forest performance with **accuracy**, **precision**, **recall**, and **F1-score**. These metrics give a full picture of detection, especially in healthcare where false positives and false negatives really matter.

For **binary classification**, RF gets near 100% accuracy, showing it separates normal from known attacks well. Precision and recall confirm reliability, with very few wrong classifications.

For **multi-class classification**, RF stays above 99% accuracy across classes including normal and multiple attack types, even after GWO feature reduction. Class-wise precision and recall are strong. These results show RF with GWO gives good known attack detection in IoMT.

6. Deep Learning–Based Zero-Day Attack Detection

ML models detect known attacks but miss new or zero-day attacks. To handle this, our framework adds deep learning-based anomaly detection using an autoencoder. This finds unusual behavior without labeled attack data, making it good for zero-day detection.

6.1 Autoencoder Architecture

An autoencoder is an unsupervised neural network that learns compact data representations by trying to copy input to output [2], [14]. We use a fully connected autoencoder with encoder, bottleneck, and decoder. The encoder compresses input into lower dimension, and decoder rebuilds from that.

The bottleneck forces the model to learn key features of normal IoMT traffic, reducing noise. This lets the autoencoder rebuild normal samples well while giving higher errors for anomalies. The simple structure suits resource-limited IoMT.

6.2 Training on Normal Traffic

For zero-day detection, we train the autoencoder only on normal IoMT traffic [7], [8]. By learning only normal behavior, it creates a baseline of good communication patterns. During training, it minimizes reconstruction loss to reproduce normal samples well.

This avoids needing labeled attack data, which is often not available for new threats. So the autoencoder can spot deviations from normal, making it good for new attacks. Training only on normal data also improves generalization and reduces bias toward known attacks.

6.3 Threshold-Based Anomaly Detection

We find anomalies using reconstruction error. Normal samples give low error, while anomalies give higher error due to unfamiliar patterns..

We set a threshold based on error distribution from normal validation data, using mean and standard deviation. Samples with error above threshold are possible zero-day attacks.

Low false positives are crucial in healthcare, where false alarms can disrupt care. Our threshold method aims for reliability with few false alarms while detecting anomalies well. Tests show this autoencoder approach gives good zero-day detection with low false positives.

7. Experimental Setup

This section covers datasets, preprocessing, metrics, and implementation for testing our framework.

7.1 Datasets Description

We test our framework on public IoT healthcare datasets showing realistic IoMT traffic:

Binary Classification Dataset: Traffic labeled as normal or attack, to test distinguishing normal from known attacks.

Multi-Class Classification Dataset: Includes multiple categories like normal healthcare and different attack types, to test classifying several intrusion types.

Both have many samples and features from IoMT traffic, good for testing scalability and detection in healthcare IDS.

7.1.1 Dataset Source and Characteristics

Our dataset is the public IoT Healthcare Security Dataset from IoT-Flock traffic simulation [1]. It's at: https://www.kaggle.com/datasets/faisalmalik/iot-healthcare-security-dataset

This simulates an Intensive Care Unit with patient monitors, environmental sensors, and control units using MQTT and CoAP. It has normal traffic and several attacks.

The dataset has 56,609 total instances with 10 traffic features from packet and protocol data.

7.1.2 Attack Types Included

The dataset includes realistic IoMT attack patterns such as:

MQTT Distributed Denial of Service (DDoS)
MQTT Publish Flood Attack
Brute Force Attack
SlowITE Attack

These attacks simulate common threats targeting healthcare IoMT infrastructures, including service disruption, unauthorized access, and resource exhaustion.

7.1.3 Dataset Classification Structure

For evaluation purposes, two classification scenarios are considered:

Binary Classification:
Class 0: Normal IoMT Traffic
Class 1: Attack Traffic

Multi-Class Classification:
Class 0: Environment Monitoring Traffic
Class 1: Patient Monitoring Traffic
Class 2: Attack Traffic

The dataset exhibits moderate class imbalance [20], which justifies the use of evaluation metrics beyond simple accuracy.

7.1.4 Dataset Size and Feature Summary

Total Instances: 56,609
Original Features: 10
Selected Features (Binary Case): 6
Selected Features (Multi-Class Case): 4

The relatively small feature dimension makes the dataset suitable for metaheuristic optimization and hybrid intrusion detection modeling in IoMT environments.

7.1.5 Dataset Class Distribution Analysis

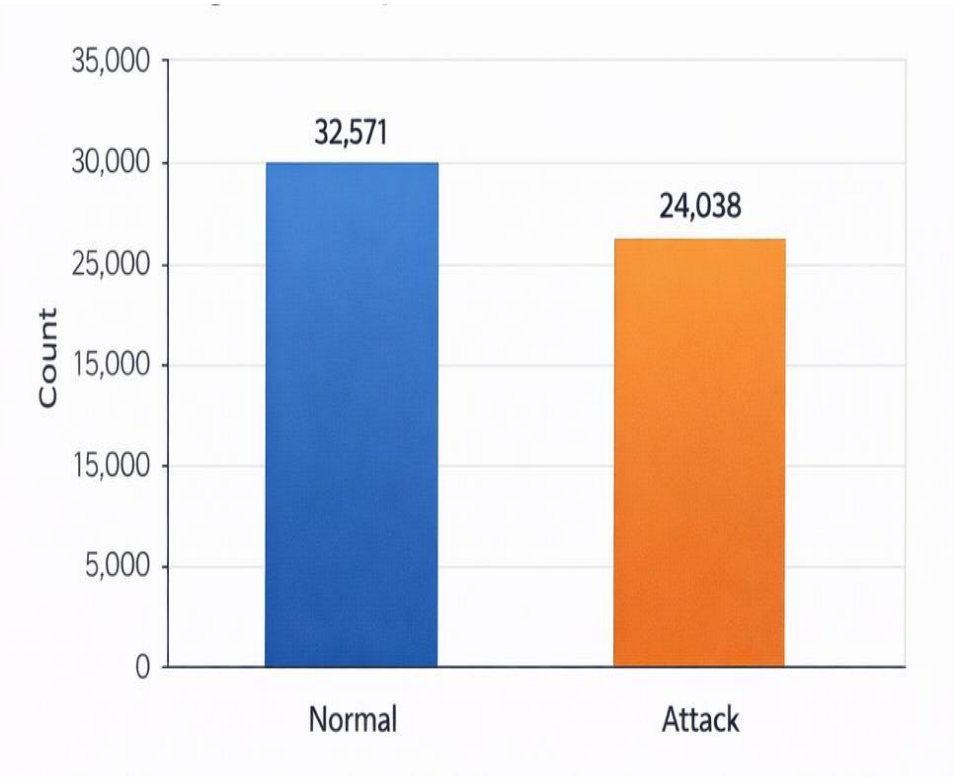

Figure 4.Binary Class Distribution of IoMT Dataset

The binary dataset consists of 32,571 normal traffic samples and 24,038 attack samples.

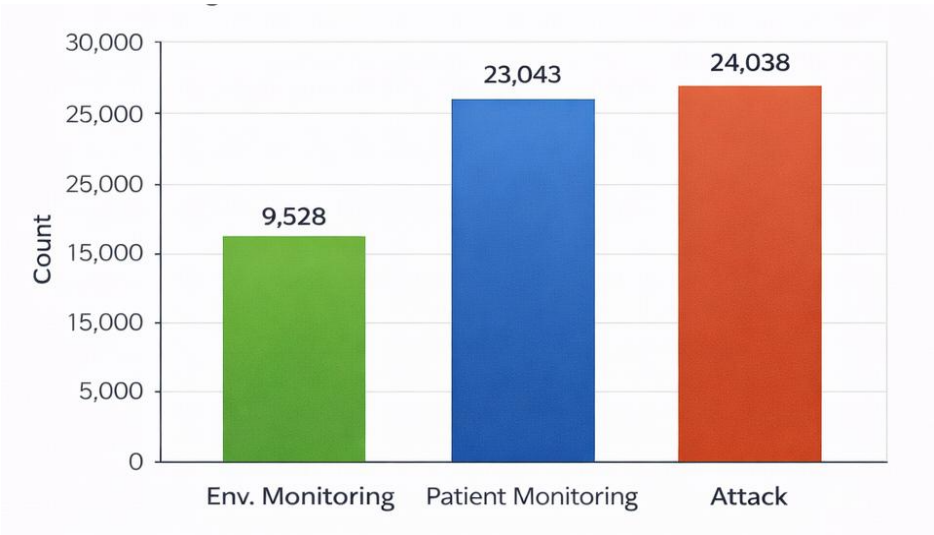

Figure 5. Multi-Class Distribution of IoMT Dataset

The multi-class dataset includes 9,528 environment monitoring samples, 23,043 patient monitoring samples, and 24,038 attack samples.

7.2 Preprocessing and Feature Engineering

Before training, we preprocess data: handle missing values, remove useless attributes, encode categorical features, and normalize numerical features.

Then GWO selects optimal feature subsets, cutting dimensions while keeping useful information. This optimized set is used for both ML and DL parts.

7.3 Evaluation Metrics

We measure performance with accuracy, precision, recall, and F1-score. These give a full view of detection.

Accuracy measures the overall correctness of the classification results, while precision and recall capture the reliability of attack detection and the ability to identify malicious samples, respectively. The F1-score provides a balanced

measure by combining precision and recall. These metrics are particularly important in healthcare IoMT environments, where both false positives and false.

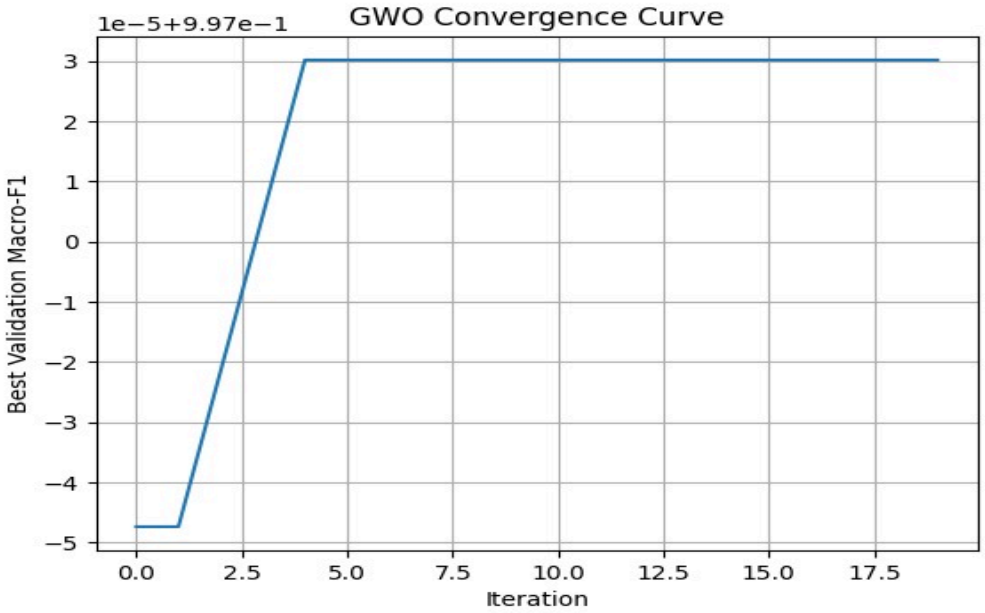

Figure 6. GWO convergence Curve

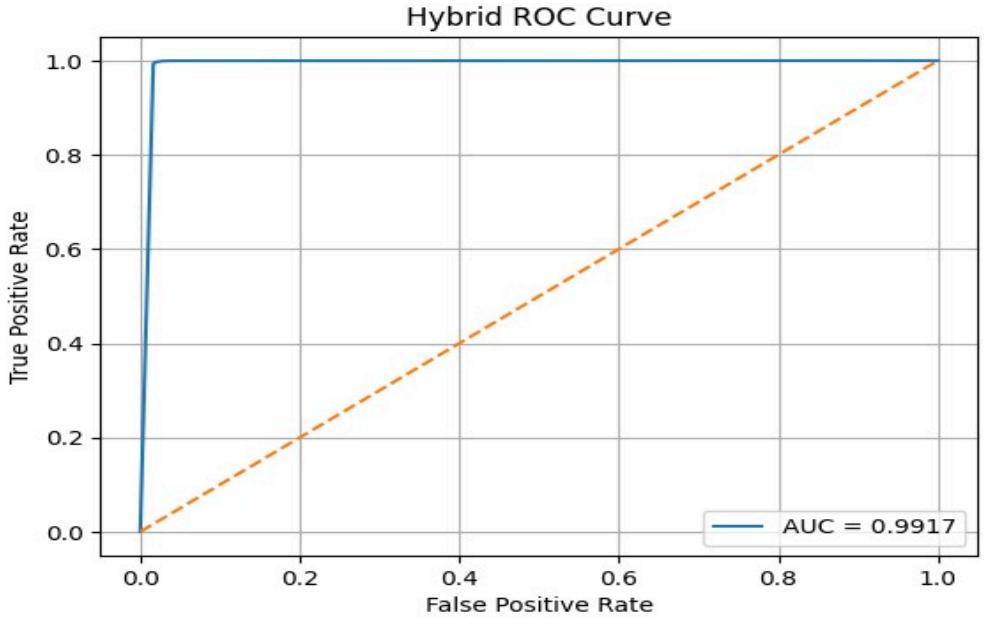

Figure 7. Hybrid ROC Curve

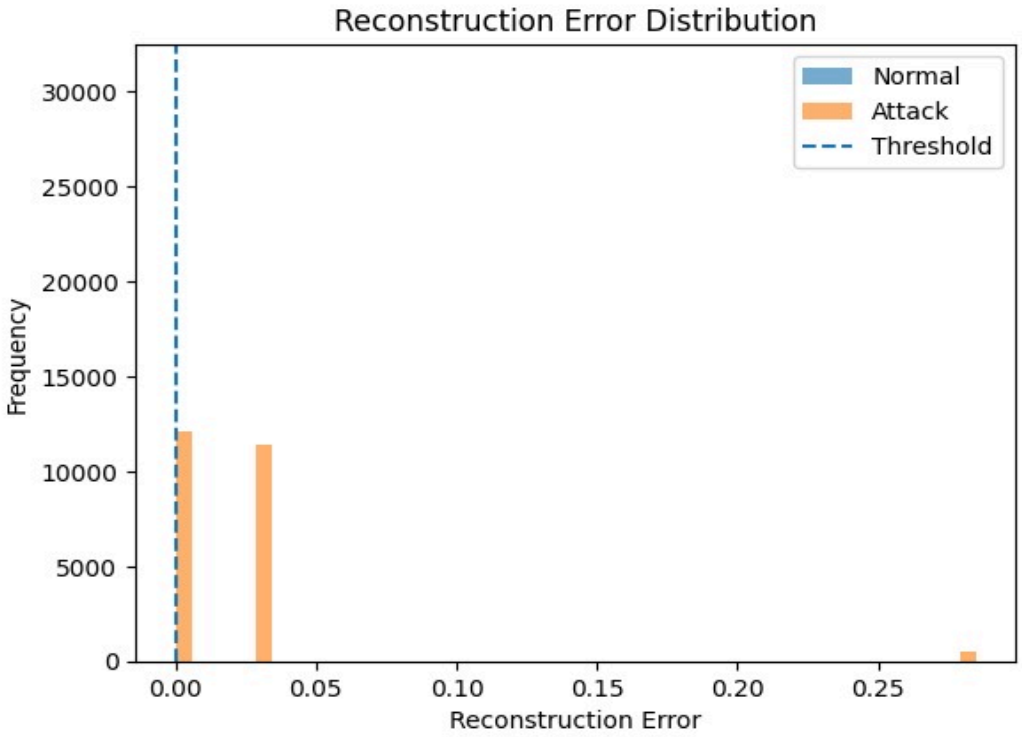

Figure 8. Reconstruction Error Distribution

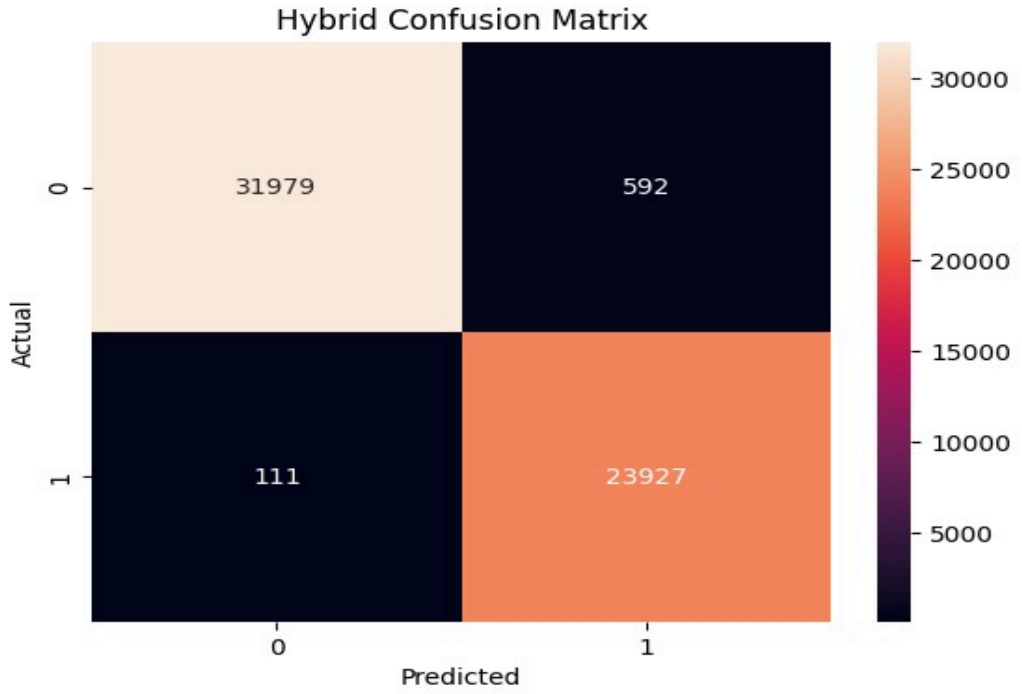

Figure 9. Hybrid Confusion Matrix

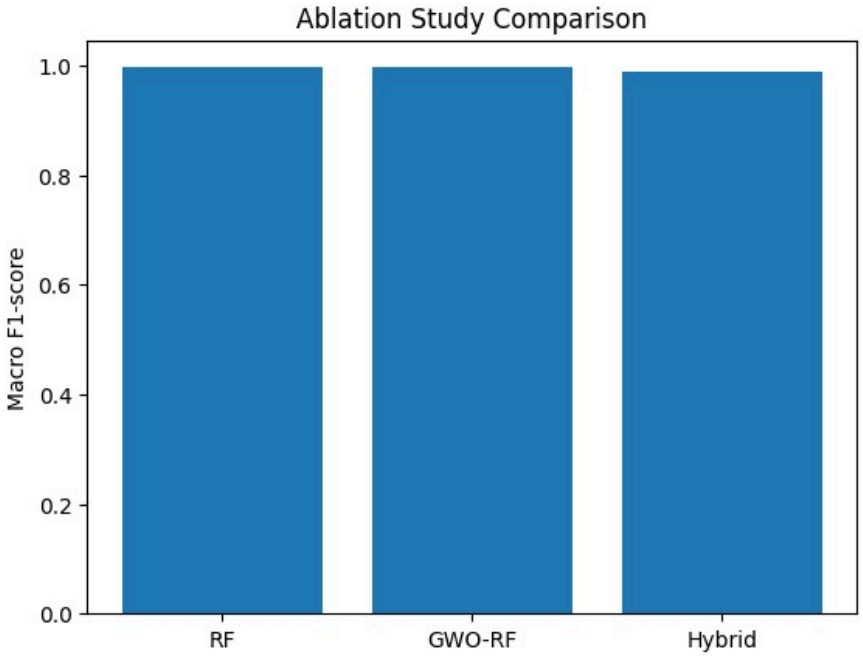

Figure 10. Ablation Study Comparision

7.3.1 Mathematical Definition of Evaluation Metrics

For the formal assessment of the proposed intrusion detection framework, the performance metrics can be defined through confusion matrix components. determine as follows:

- True Positives (TP)
- True Negatives (TN)
- False Positives (FP)
- False Negatives (FN)

Performance metrics employed in this study are presented in the sections that follow:

Accuracy

The Accuracy of an intrusion detection system (IDS) is the proportion of samples that were accurately classified, as computed by the following formula:

Accuracy=TP+TN / TP+TN+FP+FN

Precision

The Precision of an IDS is the reliability of the IDS's positive predictions based on the following formula:

Precision=TP / TP+FP

Recall (Detection Rate)

The Recall of an IDS is a measure of how successfully the IDS detects malicious traffic, as calculated by the following formula:

Recall=TP / TP+FN

F1-Score

The F1-Score measures the combination of an IDS's Precision and Recall.

F1=2×Precision×Recall / Precision+Recall

Cohen's Kappa Coefficient

The Cohen's Kappa Coefficient measures how well we predict the correct outcome compared to what we actually get by taking into account how much agreement would occurs by chance:

K=Pobs−Pexp / (1−Pexp)

where:

Pobs = Total number of true positives (TP) and true negatives (TN)/(The total number of predicted outcomes).

Pexp = Total number of TP+FP/Total number of predicted outcomes + Total number of FN+TN/ Total number of predicted outcomes

The kappa statistic lies between 0 and 1, meaning that closer to 1 represents great levels of agreement and vice versa.

False Positive Rate (FPR)

False Positives in healthcare environments need to be minimized. A False Positive Rate(FPR) is calculated by the following equation:

FPR=FP / FP+TN

Having a lower FPR is extremely important in order to maintain medical workflow.

7.4 Implementation Environment

We use Python on Google Colab with NumPy, Pandas, Scikit-learn for ML, and TensorFlow/Keras for autoencoder. This setup lets others reproduce our work easily.

This implementation environment enables efficient experimentation and ensures that the proposed intrusion detection framework can be easily reproduced and extended by other researchers.

8. Results and Discussion

This section presents results of our hybrid framework for binary, multi-class, and zero-day detection, with analysis and comparison.

8.1 Binary Classification Results

Binary tests check if our framework separates normal IoMT traffic from known attacks. Random Forest with GWO-selected features (10 to 6) gets about 99.7% accuracy.

Class	Precision	Recall	F1-Score	Support
Normal (0)	1.00	1.00	1.00	32,571
Attack (1)	1.00	1.00	1.00	24,028
Overall Accuracy			1.00	56,609

Table 2: Binary Classification Performance (GWO–RF)

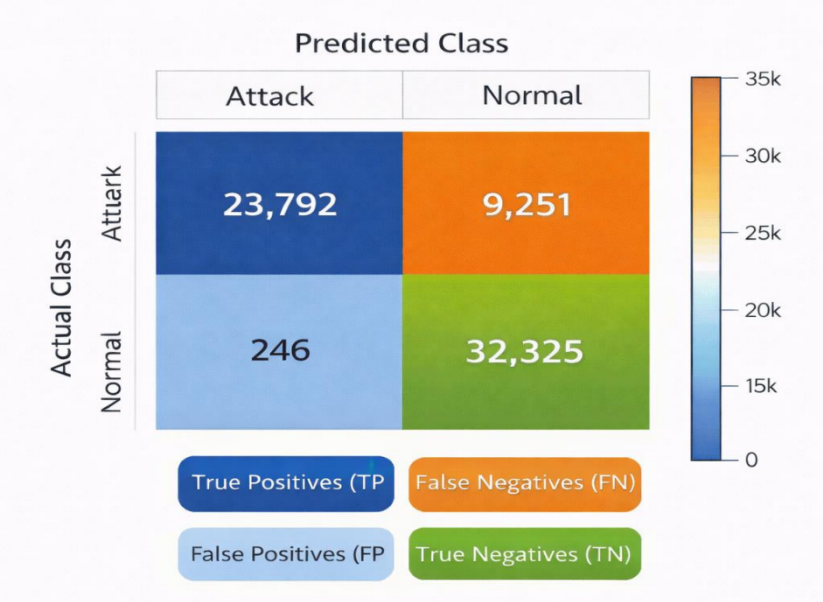

Figure 11. Confusion Matrix of IoMT Classification Model

The classification report indicates near-perfect precision, recall, and F1-score for both normal and attack classes. The confusion matrix shows that the majority of samples are correctly classified, with negligible misclassification. These results demonstrate that the proposed GWO-based feature selection effectively eliminates redundant features without degrading detection performance. The high accuracy achieved with a reduced feature set confirms the suitability of the proposed approach for known attack detection in IoMT environments.

Dataset Type	Original Features	Selected Features	Validation Accuracy
Binary IoMT Dataset	10	6	0.9971

Table 3: Feature Reduction Using GWO (Binary Dataset)

Actual \ Predicted	Normal	Attack
Normal	32,571	0
Attack	0	24,083

Confusion Matrix 1: Binary Classification (Known Attacks)

8.2 Multi-Class Classification Results

Multi-class tests check classifying several IoMT traffic types. Baseline RF gets about 99% accuracy.

Class	Precision	Recall	F1-Score	Support
Class 0 (Normal – Env Monitoring)	0.98	0.97	0.97	9,528
Class 1 (Normal – Patient Monitoring)	0.99	0.99	0.99	23,043
Class 2 (Attack)	1.00	1.00	1.00	24,083
Overall Accuracy			0.99	56,609

Table 4: Multi-Class Classification Performance (Baseline RF)

After applying GWO-based feature selection, the feature set is further reduced from **10 to 4 features** for the multi-class dataset. Despite this significant reduction, the classifier maintains consistent performance across all classes, including accurate detection of attack traffic. The corresponding confusion matrix shows minimal confusion between classes, indicating that the optimized feature subset retains sufficient discriminatory information.

Dataset Type	Original Features	Selected Features	Validation Accuracy
Multi-Class IoMT Dataset	10	4	0.9903

Table 5: Feature Reduction Using GWO (Multi-Class Dataset)

These results highlight the robustness of the proposed machine learning–based detection component and demonstrate that effective multi-class intrusion detection can be achieved with a compact feature representation. This is particularly important for real-time IoMT applications, where computational efficiency is critical.

Actual \ Predicted	Class 0	Class 1	Class 2
Class 0	9,251	277	0
Class 1	198	22,845	0
Class 2	0	0	24,083

Confusion Matrix 2: Multi-Class Classification (GWO–RF)

8.3 Zero-Day Attack Detection Analysis

To evaluate zero-day and anonymous attack detection capability, the autoencoder-based anomaly detection model is assessed using reconstruction error analysis. The autoencoder is trained exclusively on normal IoMT traffic, enabling it to learn baseline behavior patterns. During inference, samples with reconstruction errors exceeding a statistically defined threshold are classified as anomalous.

The experimental results show that the autoencoder achieves an overall detection accuracy of approximately **82%** for zero-day attack scenarios. The confusion matrix indicates a very low false-positive rate, with most normal samples correctly identified. While some attack samples are misclassified as normal, the conservative detection behavior helps prevent excessive false alarms.

Metric	Value
Detection Accuracy	0.82
Precision (Attack)	1.00
Recall (Attack)	0.57
F1-Score (Attack)	0.72

Table 6: Autoencoder Zero-Day Attack Detection Performance

In healthcare IoMT environments, low false-positive rates are particularly important, as frequent false alerts can disrupt medical operations and burden security personnel. The proposed anomaly detection model prioritizes reliability and operational safety, making it suitable for real-world healthcare deployments. These results confirm that the deep learning component effectively complements the machine learning classifier by detecting attack patterns that are not represented in labeled training data.

Actual \ Predicted	Normal	Anomaly
Normal	32,530	41
Attack (Zero-Day)	10,378	13,660

Confusion Matrix 3: Zero-Day Attack Detection (Autoencoder)

8.4 Comparison with Base Paper

A comparison between the proposed framework and the base paper highlights the key improvements introduced in this work. While the base paper focuses primarily on machine learning–based intrusion detection with metaheuristic optimization [1], the proposed approach extends this by integrating a hybrid ML–DL architecture and explicit zero-day attack detection.

Aspect	Base Paper	Proposed Work
Optimization Algorithm	Firefly Algorithm	Grey Wolf Optimizer
Feature Count	9–10	6 (Binary), 4 (Multi-Class)
ML Model	ML only	Hybrid ML + DL
Zero-Day Detection	Not addressed	Autoencoder-based
Dataset	IoMT Healthcare	Same dataset (fair comparison)
False Positive Control	Not emphasized	Low FP for healthcare safety

Table 7: Comparison with Base Paper

The proposed framework achieves comparable or improved detection accuracy while reducing the feature set more aggressively (**10 → 6** for binary classification and **10 → 4** for multi-class classification). In addition, the inclusion of an autoencoder-based anomaly detection model enables detection of unknown attacks, which is not addressed in the base paper These enhancements improve the robustness, scalability, and real-world applicability of the intrusion detection system for IoMT environments

8.5 Limitations and Future Research Directions

Despite good results with fewer features, we have limits. We used simulated IoMT traffic, not real hospital data. We need real-world testing. Autoencoder has low false positives but catches only 57% of unknown attacks, showing precision-recall trade-off. Future work could try adaptive thresholds, ensemble anomaly detection, or generative models to improve zero-day recall. Feature selection is offline now, so it can't adapt to changing traffic. Online optimization could help. We haven't tested much against advanced attacks like ransomware. We need more testing. Also, real-time deployment on edge devices and adding explainable AI are important for practical healthcare use.

9.Code snippets

Figure 12. GWO - RF Results

Figure 13. Selected Features

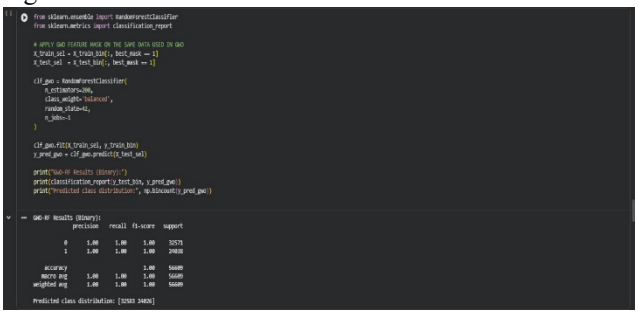

Figure 14. Hybrid GWO - RF

10.Comparison

Table

Used Algorithms,

1. Grey Wolf Optimizer
2. Particle Sworn Optimizer
3. Firefly Algorithm
4. Whale Optimizer Algorithm
5. Ant Colony Optimization
6. Random Forest
7. Decision Tree
8. XGBoost

S.no	Algorithms	Re-call	F1-score	Precision
1.	GWO / RF	1.00	1.00	1.00
2,	GWO / DT	0.99	0.99	0.99
3.	GWO / XGBoost	0.99	0.99	0.99
4.	PSO / RF	0.99	0.99	0.99

5.	**PSO / DT**	**0.99**	**0.99**	**0.99**
6.	**PSO / XGBoost**	**0.99**	**0.99**	**0.99**
7.	**FF / RF**	**0.99**	**0.99**	**0.99**
8.	**FF / DT**	**0.99**	**0.99**	**0.99**
9.	**FF / XGBoost**	**0.99**	**0.99**	**0.99**
10.	**WOA / RF**	**0.99**	**0.99**	**0.99**
11.	**WOA / DT**	**0.99**	**0.99**	**0.99**
12.	**WOA / XGBoost**	**0.99**	**0.99**	**0.99**
13.	**ACO / RF**	**0.99**	**0.99**	**0.99**
14.	**ACO / DT**	**0.99**	**0.99**	**0.99**
15.	**ACO / XGBoost**	**0.99**	**0.99**	**0.99**

Table 8. Comparison of Algorithms

CONCLUSION

This research presents a hybrid model for detecting intrusions in an IoMT (Internet of Medical Things) environment that uses both biocomputing-based optimization methods, in this case, Grey Wolf Optimization (GWO), and machine and deep learning (ML/DL). The solutions to some of the most significant security issues, including too many features, reliable detection of previously known attacks with a high degree of precision, as well as detection of unknown or zero-day attacks, are provided by the proposed method.

The empirical results show that using GWO-based feature selection reduces the number of features (binary classification from 10 to 6, and multi-classification from 10 to 4) without sacrificing the detection accuracy. The performance evaluation indicates that Random Forest allows for very accurate detection of known attacks, both with very high accuracy in the binary case, as well as almost perfect accuracy in the multi-class situation, based on both of the resulting IoMT data sets.

By adding a DL Autoencoder to the overall hybrid intrusion detection system, the proposed framework becomes much more capable of detecting new attacks and zero-day attacks. Learning what constitutes normal IoMT data traffic and finding anomalies from it through reconstruction error takes place in conjunction with the ML training. The hybrid ML/DL approach in this case is complementary, taking full advantage of both forms of computation for complete intrusions detection with low levels of false positives, which is critical in the healthcare environment. In conclusion, the proposed hybrid form of ML/DL based on GWO feature selection provides a well-organized and effective improvement in both the robustness of the intrusions detection for IoMT as well as in terms of the efficiency and scalability of the overall intrusions detection system, providing a new standard of reliability in the field of Healthcare 4.0

REFERENCE

[1] L. Shan, "(IoT) Network intrusion detection system using optimization algorithms," 2025.

[2] N. G. Nithyavani and N. R. G. Raja, "A comprehensive survey on security and privacy challenges in Internet of Medical Things applications: Deep learning and machine learning solutions, obstacles, and future directions," 2024.

[3] O. Aouedi, T.-H. Vu, A. Sacco, D. C. Nguyen, K. Piamrat, G. Marchetto, and Q.-V. Pham, "A survey on intelligent Internet of Things: Applications, security, privacy, and future directions," 2024

[4] I. Rakine, A. Oukaira, K. El Guemmat, I. Atouf, S. Ouahabi, M. Talea, and T. Bouragba, "Comprehensive review of intrusion detection system techniques: Machine learning and deep learning in different networks," 2025.

[5] A. A. Hady, A. Ghubaish, T. Salman, D. Unal, and R. Jain, "Intrusion detection system for healthcare systems using medical and network data: A comparison study," 2020.

[6] A. Si-Ahmedad, M. A. Al-Garadi, and N. Boustia, "Survey of machine learning-based intrusion detection methods for Internet of Medical Things," 2023

[7] N. Faruqui, M. A. Yousuf, and M. Whaiduzzaman, "SafetyMed: A novel IoMT intrusion detection system using CNN-LSTM hybridization," 2023.

[8] V. Ravi, T. D. Pham, and M. Alazab, "Deep learning-based network intrusion detection system for Internet of Medical Things," 2023.

[9]. A. Alzaqebah, I. Aljarah, O. Al-Kadi, and R. Damaševičius, "A modified Grey Wolf Optimization algorithm for an intrusion detection system," 2022.

[10]. Q. Al-Tashi, S. J. Abdulkadir, H. M. Rais, and S. Mirjalili, "Binary optimization using hybrid Grey Wolf Optimization for feature selection," 2019.

[11] C. Kouidri, M. Yahlali, M. A. Boudia, A. Amine, R. M. Hamou, and S. Kouidri, "Intrusion detection system with Grey Wolf Optimizer," 2021.

[12] Y. Hou, H. Gao, Z. Wang, and C. Du, "Improved Grey Wolf Optimization algorithm and its applications," 2024.

[13] R. Jablaoui, O. Cheikhrouhou, M. Hamdi, and N. Liouane, "Deep learning enabled intrusion detection system for IoT security," 2025.

[14] F. Ebrahimi, R. Javidan, R. Akbari, and Y. Hosseini, "Intrusion detection in the Internet of Things using convolutional neural networks: An explainable AI approach," 2025.

[15] M. Maazalahi and S. Hosseini, "A novel hybrid method using Grey Wolf algorithm and genetic algorithm for IoT botnet DDoS attacks detection," 2025

[16] A. Sezgin, M. Ulaş, and A. Boyacı, "Multi-objective

feature selection for intrusion detection systems: A comparative analysis of bio-inspired optimization algorithms," 2025.
[17] S. A. Elsaid, E. Shehab, A. M. Mattar, A. T. Azar, and I. A. Hameed, "Hybrid intrusion detection models based on Grey Wolf Optimizer optimized deep learning," 2024.
[18] Y. K. Saheed and M. O. Arowolo, "Efficient cyber attack detection on IoMT using deep recurrent neural networks and machine learning," 2021.
[19] G. Balhareth and M. Ilyas, "Optimized intrusion detection for IoMT networks with tree-based machine learning and filter-based feature selection," 2024.
[20] J. A. Shaikh, C. Wang, M. W. U. Sima, and M. Arshad, "A deep reinforcement learning-based robust intrusion detection system for securing IoMT healthcare networks," 2025.
[21] E. I. Elsedimy, H. Elhadidy, and S. M. M. Abohashish, "A novel intrusion detection system based on a hybrid quantum support vector machine and improved Grey Wolf optimizer," 2024
[22] Y. K. Saheed and S. Misra, "A voting grey wolf optimizer-based ensemble learning model for intrusion detection in the Internet of Things," 2024.
[23] G. Thamilarasu, A. Odesile, and A. Hoang, "An intrusion detection system for Internet of Medical Things," 2020.
[24] R. K. Malik, "Network intrusion detection by optimized feature engineering using hybridization of Grey Wolf Optimizer and nonlinear activation function," 2024.
[25] M. Alalhareth and S.-C. Hong, "An adaptive intrusion detection system in IoMT using fuzzy-based learning," 2023
[26] H. Goumidi, "Real-time anomaly detection in IoMT networks using stacking models and a healthcare-specific dataset," 2025.
[27] M. A. S. Arifin and A. T. Martadinata, "Securing the Internet of Medical Things: A machine learning approach for cyber threat detection," 2024.
[28] M. Benmalek, A. Seddiki, and K.-D. Haouam, "SNN-IoMT: A novel AI-driven model for intrusion detection in Internet of Medical Things," 2025.
[29] 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," 2025.
[30] F. M. Serhani, "Intrusion detection and real-time adaptive security in medical IoT using a cyber-physical systemdesign," 2025.
[31] Smith T.T. "Examining Data Privacy Breaches in Healthcare," 2020