Computers, Materials & Continua

Tech Science Press

Doi:10.32604/cmc.2025.066753

ARTICLE

Future-Proofing CIA Triad with Authentication for Healthcare: Integrating Hybrid Architecture of ML & DL with IDPS for Robust IoMT Security

Saad Awadh Alanazi[1] **and Fahad Ahmad**[2,3,*]

[1]Department of Computer Science, College of Computer and Information Sciences, Jouf University, Sakaka, 72341, Aljouf, Saudi Arabia

[2]School of Computing, Faculty of Technology, University of Portsmouth, Winston Churchill Ave, Southsea, Portsmouth, PO1 2UP, UK

[3]Portsmouth Artificial Intelligence and Data Science Center, University of Portsmouth, Winston Churchill Ave, Southsea, Portsmouth, PO1 2UP, UK

*Corresponding Author: Fahad Ahmad. Email: fahad.ahmad@port.ac.uk

Received: 16 April 2025; Accepted: 20 June 2025; Published: 29 August 2025

ABSTRACT: This study presents a comprehensive and secure architectural framework for the Internet of Medical Things (IoMT), integrating the foundational principles of the Confidentiality, Integrity, and Availability (CIA) triad along with authentication mechanisms. Leveraging advanced Machine Learning (ML) and Deep Learning (DL) techniques, the proposed system is designed to safeguard Patient-Generated Health Data (PGHD) across interconnected medical devices. Given the increasing complexity and scale of cyber threats in IoMT environments, the integration of Intrusion Detection and Prevention Systems (IDPS) with intelligent analytics is critical. Our methodology employs both standalone and hybrid ML & DL models to automate threat detection and enable real-time analysis, while ensuring rapid and accurate responses to a diverse array of attacks. Emphasis is placed on systematic model evaluation using detection metrics such as accuracy, False Alarm Rate (FAR), and False Discovery Rate (FDR), with performance validation through cross-validation and statistical significance testing. Experimental results based on the Edge-IIoTset dataset demonstrate the superior performance of ensemble-based ML models such as Extreme Gradient Boosting (XGB) and hybrid DL models such as Convolutional Neural Networks with Autoencoders (CNN+AE), which achieved detection accuracies of 96% and 98%, respectively, with notably low FARs. These findings underscore the effectiveness of combining traditional security principles with advanced AI-driven methodologies to ensure secure, resilient, and trustworthy healthcare systems within the IoMT ecosystem.

KEYWORDS: Healthcare; internet of medical things; patient-generated health data; confidentiality; integrity; availability; intrusion detection and prevention system; machine learning; deep learning

1 Introduction

In today's digital healthcare landscape, securing computing systems is critical, particularly with the rise of the Internet of Medical Things (IoMT), a network of interconnected devices central to modern medical services. These devices range from wearable health monitors to implantable sensors and smart medical equipment, each generating vast amounts of Patient-Generated Health Data (PGHD). PGHD refers to health-related data created, recorded, or gathered by patients, caregivers, or family members outside of clinical settings using IoMT devices. As IoMT expands, ensuring the security, integrity, and confidentiality of PGHD becomes increasingly vital due to evolving and sophisticated cyber threats [1,2].

The CIA triad; Confidentiality, Integrity, and Availability, along with authentication, forms the foundational framework for securing information systems. In traditional IT infrastructures, these principles provide a robust structure for managing and securing sensitive information. However, the IoMT environment presents unique challenges that make conventional security mechanisms less effective [3–5]. IoMT systems are characterized by their heterogeneity, comprising a wide range of device types with varying capabilities and protocols. These devices often operate under strict resource constraints, including limited battery life, processing power, and memory. Furthermore, they are frequently deployed in dynamic environments and must support real-time communication and data exchange. The transmission of sensitive PGHD over potentially unsecured networks increases the risk of data breaches, while the lack of unified security standards across vendors complicates enforcement. As a result, traditional perimeter-based and signature-driven security solutions, such as firewalls and antivirus software, fall short in addressing the nuanced requirements of IoMT.

Machine Learning and Deep Learning (ML & DL) techniques offer powerful enhancements to Intrusion Detection and Prevention Systems (IDPS), enabling not only real-time detection and response but also the ability to anticipate and mitigate threats before they occur [6,7]. ML & DL models excel at identifying complex patterns and anomalies within massive data streams, a capability especially critical in IoMT environments where system downtime or breaches can have life-threatening implications [8,9].

This study proposes an intelligent, hierarchical security framework that integrates ML & DL with IDPS under the guidance of the CIA triad and authentication principles. The framework is designed to address the challenges posed by IoMT systems through an adaptive and scalable architecture. By aligning machine intelligence with security fundamentals, the framework strengthens both proactive and reactive defense mechanisms [10,11].

The proposed framework operates in two stages. Initially, ML algorithms analyse PGHD for signs of anomalies, functioning as a fast and efficient filter. If a potential threat is identified, DL models then conduct deeper, context-aware analysis to confirm and classify the threat. This two-tier architecture reduces false positives and provides a balance between speed and accuracy in threat detection and mitigation.

Although ML & DL have been widely explored in cybersecurity, their hierarchical application in combination with the CIA triad and authentication mechanisms specifically for IoMT is a novel contribution [12,13]. This layered approach is not only technically rigorous but also practically significant, providing a pathway for secure, real-time, and resilient healthcare systems.

1.1 Problem Statement

The increasing reliance on IoMT in healthcare has introduced new, complex cybersecurity challenges. Devices operate in dynamic and often untrusted environments, making them vulnerable to a wide range of attacks. Traditional measures such as firewalls and antivirus software lack the adaptability and intelligence required to protect such decentralized and heterogeneous systems [14].

There is an urgent need for a comprehensive security framework that integrates the principles of the CIA triad and authentication with the adaptive capabilities of IDPS, enhanced by ML & DL. This integration aims to deliver real-time threat detection, reduced false positives, and improved resilience of healthcare infrastructures.

1.2 Research Questions

- How can ML & DL, when integrated with IDPS, enhance threat classification and response in complex IoMT environments?

- What is the empirical performance of a hierarchical ML & DL-based IDPS in improving detection accuracy and response time?
- How effective is the proposed framework in reducing false positives and negatives to ensure secure healthcare service delivery?

1.3 Aims and Objectives

This study aims to contribute original insights by combining the CIA triad and authentication with ML, DL, and IDPS in a robust framework tailored to IoMT. The research seeks to demonstrate how intelligent systems can be employed to secure sensitive medical data and ensure uninterrupted healthcare services.

- To establish the originality of integrating the CIA triad, authentication, and advanced IDPS with ML & DL for improved IoMT security.
- To develop and evaluate a hierarchical ML & DL-based IDPS for accurate anomaly detection and threat response.
- To assess the effectiveness of the proposed framework in minimizing false alerts while ensuring reliable healthcare service delivery.

1.4 Contribution of Study

This research presents a novel integration of ML & DL with the CIA triad and authentication in an IDPS designed for IoMT. The proposed architecture is multi-layered: ML techniques handle initial anomaly detection, and DL models perform more complex threat verification and classification. This allows the system to maintain high detection accuracy while being computationally efficient.

The framework not only supports efficient resource use but also enhances system responsiveness, contributing to the reliability and sustainability of healthcare IT infrastructures. Additionally, its modular and scalable design makes it adaptable to other critical domains, such as industrial IoT, smart cities, and financial systems. These extensions demonstrate the broader relevance and transferability of the proposed model.

1.5 Rest of the Manuscript

Following this Introduction, the manuscript will present a detailed Literature Review to place the protection of the CIA Triad with authentication and ML & DL based IDPS within the current landscape of IoMT security solutions. Section 3 will outline the experimental design, data collection, and analysis procedures used in this study. Then explanation of Identified Machine Learning and Deep Learning Models. Section 5 will demonstrate the effectiveness of the proposed hybrid security framework in an IoMT setting. Sections 6 and 7 will reflect on the implications of these findings for future research and practical application, advocating for the broader adoption of advanced, integrated security systems across various industries.

2 Literature Review

The integration of IoMT into healthcare has transformed patient care by enabling real-time monitoring, remote diagnostics, and continuous health data acquisition. However, this progress has introduced major security concerns, particularly in safeguarding Patient-Generated Health Data (PGHD), ensuring system integrity, and maintaining uninterrupted medical services. Conventional security methods such as firewalls, antivirus software, and rule-based IDPS fall short in addressing the heterogeneous, resource-constrained, and highly connected nature of IoMT systems [14,15].

2.1 Traditional Security Challenges in IoMT

Traditional security frameworks struggle to keep up with the dynamic demands of IoMT due to several limitations. These include limited device capabilities, diverse hardware and software ecosystems, and the need for low-latency, real-time communication. Studies have demonstrated that these limitations impede real-time anomaly detection and data protection at both device and network layers [16,17]. Additionally, securing PGHD during transmission and processing is critical, as these data streams are vulnerable to man-in-the-middle and spoofing attacks [18]. Integrating edge computing with lightweight cryptographic algorithms and access control mechanisms has been proposed to mitigate latency and computational overhead [19].

2.2 Role of IDPS in IoMT Security

An effective IDPS serves as the backbone of IoMT security by enabling real-time intrusion detection and system resilience. Unlike static, signature-based detection, which fails against zero-day threats, anomaly-based IDPS dynamically learns traffic patterns and user behavior by [20,21]. These systems require high adaptability, especially in healthcare where threats evolve rapidly and detection delays can result in critical failures.

2.3 Application of ML and DL in IDPS

ML and DL have demonstrated high potential in strengthening IDPS functionalities by learning from vast and diverse datasets to identify anomalies, classify intrusions, and adapt to evolving threats [22,23]. ML models such as Decision Trees, Naïve Bayes, and ensemble techniques have been extensively used to achieve fast and interpretable intrusion detection. DL models such as CNN, LSTM, and attention-based networks are particularly effective in identifying subtle patterns within sequential and high-dimensional data streams, significantly reducing false positives [24,25].

Yet, deploying these models in practice involves challenges such as data imbalance, explainability, and the need for efficient model execution on constrained devices [26,27]. Therefore, there is a strong need for scalable, low-latency, and accurate models that can generalize across a wide range of attack scenarios and IoMT configurations.

2.4 ML-Based Approaches for IoMT IDPS

Various ML methods have demonstrated their effectiveness in intrusion detection. For example, the Enhanced Random Forest Classifier for Achieving the Best Execution Time (ERF-ABE) achieved 99% accuracy in detecting DDoS and delay attacks [28]. Similarly, an ensemble model combining DTs, Naïve Bayes, RF, and XGBoost reported 96.35% accuracy and 99.98% detection rate [29]. A hybrid approach of Logistic Regression and Gradient Boosted Trees achieved 95.4% accuracy while optimizing for real-time use with a lightweight feature set [30]. Meta-learning strategies have also emerged, such as the one presented by [31], which attained 99.99% accuracy and a remarkably low False Alarm Rate of 0.00004%.

2.5 DL-Based Approaches for IoMT IDPS

In the DL domain, several models have shown promising results. A Deep Neural Network with global attention achieved an accuracy range of 89%–99% [32]. A GRU with attention mechanism also delivered near-perfect results in classification tasks [33]. To improve efficiency, one study combined PCA and Grey Wolf Optimization (GWO) with a DNN to reduce time complexity by 32% without sacrificing performance [34]. Moreover, CNN-Transformer hybrids and LSTM architectures have proven useful for detecting anomalies in time-series medical data [32].

Despite these achievements, real-world deployments remain limited. Execution time and resource usage are underreported in many studies, although some like [28,34] address performance efficiency directly.

2.6 Emerging Trends and Limitations

Emerging frameworks such as Federated Learning [35] and Meta-Learning [31] are gaining traction due to their privacy-preserving capabilities and potential to scale across distributed IoMT environments. However, issues like regulatory compliance, model interpretability, and deployment readiness continue to hinder widespread adoption.

In summary, while ML and DL techniques offer strong enhancements to IDPS in IoMT, the path forward involves addressing deployment efficiency, compliance, and model transparency. Tailored, intelligent systems are essential for safeguarding PGHD and ensuring the resilience of healthcare infrastructures. We have summarised some important methodologies, findings and limitations of the studies in Table 1 shown below:

Table 1: Summary of key studies on ML and DL for IoMT security

Study	Methodology	Key findings	Limitations
[28]	Enhanced Random Forest (ERF-ABE)	99% accuracy for DDoS and delay attack detection	Focused on specific attacks, execution time only partially analyzed
[29]	Ensemble: DT + NB + RF + XGB	96.35% accuracy, 99.98% detection rate	Lack of detail on model deployment overhead
[30]	Hybrid LR + Gradient Boosted Trees	95.4% accuracy with real-time capability	Limited exploration of advanced attack types
[31]	Meta-Learning	99.99% accuracy, 0.00004% FAR	Scalability in live IoMT not fully tested
[32]	DNN with Attention/CNN-Transformer	Accuracy range: 89%–99%	Does not discuss resource usage in detail
[33]	GRU with Attention	Near-perfect classification	High complexity, potential latency issues
[34]	PCA + GWO + DNN	32% time complexity reduction	Requires further validation in clinical scenarios
[35]	Federated Learning	Preserves data privacy across nodes	Regulatory and communication overhead not explored

3 Materials and Methods

3.1 Innovative IoMT Architecture

Our innovative architecture for the IoMT, which is structured into three primary layers: the Device layer, the Fog layer, and the Cloud layer refer to Fig. 1 for a visual representation.

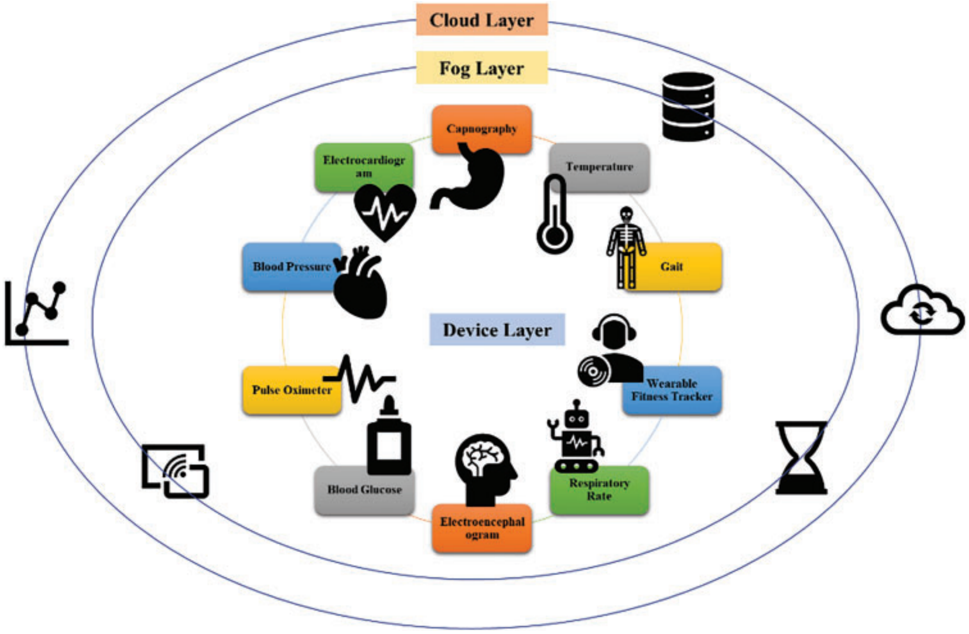


Figure 1: Internet of medical things network

Device Layer: This foundational layer consists of wearables and medical sensors. These devices are crucial as they collect and transmit medical data directly from patients. Their primary function is to ensure that vital health metrics are captured in real-time and sent forward for further processing.

Fog Layer: Serving as an intermediary, the Fog layer plays a pivotal role in the IoMT architecture. It facilitates the seamless transmission of data from the Device layer to the Cloud layer [36,37]. Beyond just relaying data, this layer has critical functionalities including the initial processing of data, as well as handling aspects of security and privacy. Its position in the architecture makes it a key point for implementing robust security measures because it acts as a bridge between data collection points and the data storage and analysis centres.

Cloud Layer: As the uppermost layer in this architecture, the Cloud layer serves as the central repository for all IoMT data. It is where data is stored, analysed, and made accessible to authorized healthcare providers and researchers. This layer enables the deep analysis of collected data, supporting healthcare professionals in making informed decisions based on comprehensive data insights.

Given the essential role of the Fog layer in connecting the device-collected data with cloud-based analysis and storage, it also represents a significant point of vulnerability within the IoMT framework. To address this, it is equipped with advanced security systems, including intelligent IDPS that utilize ML & DL techniques in layered fashion. These systems are designed to detect and mitigate potential security threats in real-time, ensuring that the integrity and confidentiality of medical data are maintained as it moves through the architecture. This multi-layered approach not only enhances the functionality and efficiency of medical data processing but also fortifies the security framework necessary to protect sensitive health information in the evolving digital landscape of healthcare. Our proposed advanced IDPS, which are integral to reinforcing the security of the IoMT is designed to identify and respond to potential security threats, ensuring the integrity and confidentiality of PGHD across IoMT networks.

3.2 Integration of IDPS in IoMT

The implementation of both IDPS within the IoMT environment is crucial for maintaining a secure operational landscape. By integrating these systems, IoMT can benefit from a comprehensive security approach that not only detects a wide range of known and unknown threats but also actively works to prevent these threats from causing harm. This dual approach ensures that PGHD transmitted across IoMT networks remains secure from both passive and active cyber threats, safeguarding critical healthcare operations and patient information.

This methodology represents a robust security framework that adapts to the evolving challenges and complexities of the IoMT environment. By employing the proactive capabilities of IDPS, the IoMT infrastructure is equipped to handle the multifaceted nature of modern cybersecurity threats. Refer to Fig. 2 for a visual representation.

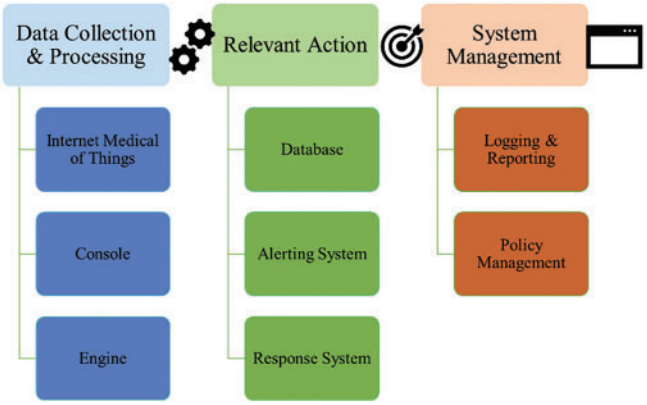


Figure 2: Intrusion detection and prevention system architecture

3.3 Metrics for Assessing IDPS Performance

In this section, we outline the criteria used to evaluate the effectiveness of IDPS within the IoMT environment.

Detection Rate is a critical metric that measures the IDPS's ability to correctly identify actual threats within the network. An effective IDPS should demonstrate a high detection rate, signifying its efficiency in recognizing and reacting to genuine security threats. This metric is essential for maintaining the integrity and security of the IoMT network.

False Discovery Rate measures the proportion of false alarms, where the system erroneously flags normal activities as malicious. Minimizing the FDR is crucial because a high rate of false alarms can lead to resource wastage and potentially desensitize the system administrators to alerts, increasing the risk of overlooking actual threats.

Response Time evaluates the promptness of the IDPS in detecting and responding to intrusions. It tracks the duration from when a threat is detected to when action is taken by the system. Rapid response is vital in IoMT environments to prevent the escalation of incidents and to minimize the damage caused by security breaches.

Scalability assesses the ability of the IDPS to handle growing amounts of network traffic effectively as the IoMT infrastructure expands. This metric is indicative of the system's capability to adapt and maintain performance levels despite an increase in load, ensuring that security does not become compromised as the network evolves.

Together, these metrics provide a comprehensive assessment of an IDPS's performance, highlighting its accuracy, reliability, responsiveness, and adaptability in the dynamic and growing field of IoMT. By continuously monitoring these metrics, stakeholders can ensure that the IDPS is effectively safeguarding the IoMT environment against current and future cybersecurity challenges.

3.4 Integrating Machine Learning and Deep Learning in IDPS to Protect the CIA Triad with Authentication

ML & DL technologies are incorporated into IDPS to enhance the security of IoMT networks. Machine Learning algorithm in IDPS analyse network traffic initially to detect potential security threats. Then DL, a subset of ML, utilizes layers of neural networks to process data and identify complex patterns. This technology is especially effective in IDPS for several reasons especially due to in depth analysis of data and then automatic identification of normal and malicious traffic patterns as shown in Fig. 3. The integration of ML and DL within IDPS marks a pivotal advancement in cybersecurity strategies, particularly within the IoMT. The primary goal of implementing these advanced technologies in IDPS for IoMT is to bolster the protection of the CIA Triad with authentication, which is foundational to the security framework of IoMT.

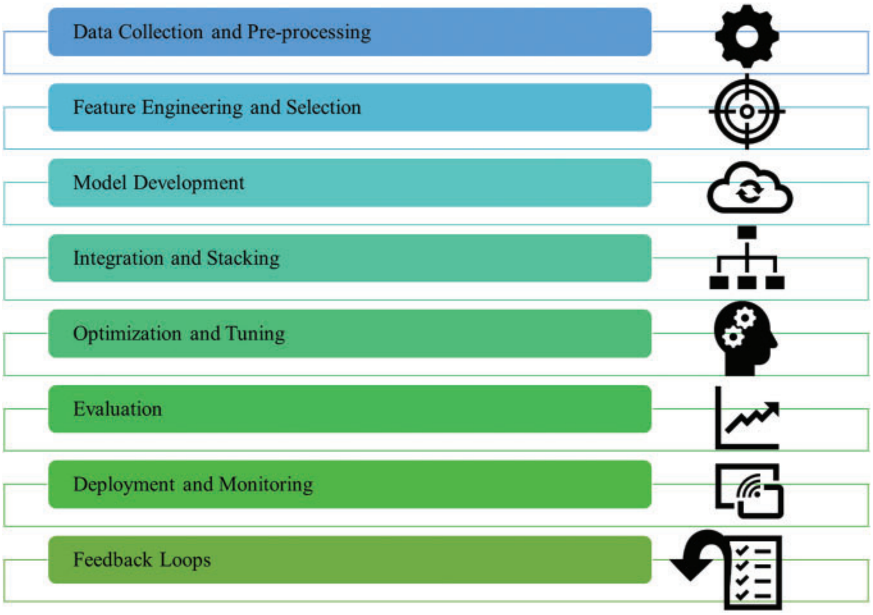

Data Collection and Pre-processing
Feature Engineering and Selection
Model Development
Integration and Stacking
Optimization and Tuning
Evaluation
Deployment and Monitoring
Feedback Loops

Figure 3: Machine learning and deep learning procedure

Confidentiality ensures that sensitive medical data is accessible only to authorized individuals. ML & DL enhance IDPS capabilities to detect unauthorized access attempts, thereby safeguarding patient privacy and sensitive information.

Integrity guarantees that medical data and device configurations are not altered maliciously or inadvertently. By using ML & DL, IDPS can more accurately identify and thwart attempts to tamper with or corrupt data, ensuring that medical records and treatment protocols remain trustworthy and unaltered.

Availability ensures that medical data and IoMT services are available to authorized users when needed. Advanced IDPS, powered by ML ... DL, can quickly detect and mitigate attacks that threaten to disrupt service availability, such as Distributed Denial of Service (DDoS) attacks.

Authentication verifies the identity of users or devices accessing IoMT networks. ML & DL techniques strengthen IDPS by detecting anomalies in login patterns, device behaviors, or access requests, ensuring that only legitimate entities can interact with sensitive systems, thus preventing unauthorized access and impersonation attacks.

By leveraging ML & DL, in IDPS can achieve a higher level of accuracy in detecting threats, significantly reduce false positives, and respond more swiftly and effectively to potential security threats. This comprehensive approach shown in Fig. 4 not only enhances the protection of PGHD and devices but also supports the overall reliability and efficiency of healthcare services that rely on IoMT technologies. In summary, the integration of these sophisticated technologies into IDPS is essential for maintaining robust cybersecurity measures that uphold the principles of the CIA Triad with authentication in IoMT environments.

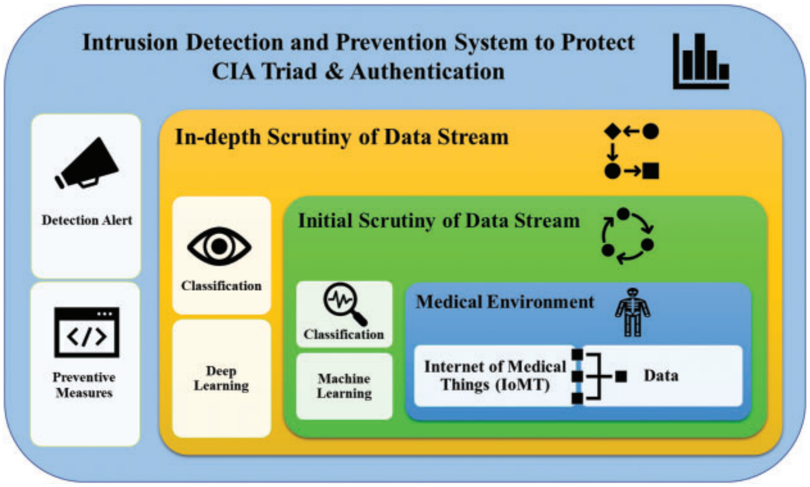

Intrusion Detection and Prevention System to Protect
CIA Triad & Authentication
Detection Alert
Preventive Measures
In-depth Scrutiny of Data Stream
Classification
Deep Learning
Initial Scrutiny of Data Stream
Classification
Machine Learning
Medical Environment
Internet of Medical Things (IoMT)
Data

Figure 4: Proposed architecture of machine learning and deep learning procedure based intrusion detection and prevention system for internet of medical things environment to protect confidentiality integrity and availability triad with authentication

Each ML and DL models' hyperparameters as shown in Tables 2 and 3 are tailored to optimize their specific architectures and tasks. These hyperparameters are essential for tuning the models to achieve optimal performance in various applications, including the complex environments typical of IoMT systems.

Table 2: Hyper-parameters used in identified machine learning models

Model	Hyperparameters
Decision trees	Min sample leaf, max depth, criteria, min split
Linear support vector machine	Regularization parameter, loss rate, penalty
Logistic regression	Iterations, regularization parameter, penalty
Logistic regression with stochastic gradient descent	Class weight, eta, learning rate, alpha value, penalty, loss rate
Naïve Base	Alpha value

(Continued)

Table 2 (continued)

Model	Hyperparameters
AdaBoost	Learning rate, number of estimators
Extreme gradient boosting	Maximum depth, gamma, min child weight, number of estimators, learning rate
Gradient boosting classifier	Number of estimators, learning rate, max depth, criteria, subsample
Random forest	Number of Estimators, min samples per leaf, min split, max depth, loss rate
Bagging algorithm	Max depth, max features, max samples, number of estimators

Table 3: Hyper-parameters used in identified deep learning models

Model	Hyperparameters
Convolutional neural network	Number of layers, filter size, stride, padding, activation function
Gated recurrent unit	Number of layers, units per layer, activation function, dropout rate
Long short-term memory	Number of layers, units per layer, activation function, dropout rate
Convolutional neural network with autoencoder	Encoder filter sizes, decoder filter sizes, latent space dimension
Gated recurrent unit with convolutional neural network	CNN filter sizes, GRU units, activation functions, dropout rates
Autoencoder with gated recurrent unit	Encoder filter sizes, GRU units, latent space dimension, dropout rate
Autoencoder with long short-term memory	Encoder filter sizes, LSTM units, latent space dimension, dropout rate

3.5 System Configuration

The experiments were carried out on identified dataset using Lenovo Mobile Workstation equipped with Processor: 12th Generation Intel Core i9, Windows 11 operating system with Memory: 128 GB DDR4, Hard Drive: 2 TB SSD, Graphics: NVIDIA RTX A4000, and the library used Python 3.4. Scikit-learn 0.21.

3.6 Dataset and Rationale for Its Selection

For our project, we have selected the Edge-IIoTset [38], a dataset specifically designed for Internet of Things (IoT) and Industrial Internet of Things (IIoT) applications. This dataset stands out due to its comprehensive collection of data from various IoMT devices simulated in a real-world environment, which makes it highly relevant for our ML & DL based IDPS. Its utility is further enhanced by its ability to support both centralized and federated learning modes, which are crucial for the development of scalable and robust cybersecurity solutions in diverse operational environments.

The Edge-IIoTset includes data from over ten types of IoT devices such as temperature and humidity sensors, ultrasonic sensors, water level detection sensors, and heart rate monitors, among others. These diverse data sources provide a rich foundation for training our IDPS to recognize a wide range of normal operational patterns as well as potential security threats. The dataset encompasses fourteen attack types associated with IoT connectivity protocols, organized into five main threat categories: DoS/DDoS attacks, information gathering, man-in-the-middle attacks, injection attacks, and malware. This classification helps in precisely training and testing the IDPS to detect and mitigate specific types of cyber threats effectively.

The structured testbed of the dataset spans seven layers, including cloud computing, network functions virtualization, blockchain network, fog computing, software-defined networking, edge computing, and IoT and IIoT Perception layers. Each layer integrates emerging technologies that meet the specific requirements of IoT and IIoT applications, such as the ThingsBoard IoT platform, OPNFV platform, Hyperledger Sawtooth, and ONOS SDN controller. This layered approach not only mimics a real-world IoT ecosystem but also enables comprehensive security testing across all levels of an IoMT infrastructure.

The selection of the Edge-IIoTset for our project is based on its ability to provide a realistic and dynamic environment for developing and evaluating the effectiveness of our ML & DL-based IDPS. It allows us to conduct a thorough exploratory data analysis and to rigorously evaluate the performance of machine learning methods in both centralized and federated learning contexts, ensuring our IDPS can operate effectively under varied and realistic conditions.

Here is Table 4 to visualize the diversity and frequency of attacks in the IoMT environment in an interesting way using the Edge-IIoTset dataset. This representation emphasizes the variety and relative occurrence of different types of cyber threats encountered.

Table 4: Instances of diverse attacks in edge-IIoTset dataset

Attack type	**Number of instances**	**Relative frequency (%)**	**Attack type**	**Number of instances**	**Relative frequency (%)**
Normal Operations	1,615,643	91.42%	**Uploading**	37,634	2.13%
DDoS_UDP	121,568	6.87%	**Backdoor**	24,862	1.40%
DDoS_ICMP	116,436	6.58%	**Port scanning**	22,564	1.28%
SQL_Injection	51,203	2.89%	**XSS**	15,915	0.90%
Password	50,153	2.83%	**Ransomware**	10,925	0.62%
Vulnerability_Scanner	50,110	2.83%	**MITM**	1214	0.07%
DDoS_TCP	50,062	2.83%	**Fingerprinting**	1001	0.06%
DDoS_HTTP	49,911	2.82%			

Effective data pre-processing is a critical step in the utilization of ML and DL models, especially in the fields of IoT and IIoT cybersecurity. This process involves preparing the raw data by converting it into a format that can be easily understood and processed by ML and DL models, thereby improving the models' accuracy and reducing the time required to obtain results.

In the initial stage, our pre-processing involved reducing the dataset's complexity by removing 15 of the original 63 columns that were deemed irrelevant for identifying traffic characteristics. We employed a manual relevance-based feature elimination technique, guided by domain expertise, to discard protocol-specific and metadata fields such as frame.time, ip.src host, ip.dst host, among others. This targeted reduction enhances processing efficiency by focusing analysis on the most impactful features.

Duplicate records in the dataset were identified and eliminated using a row-wise duplication detection technique, where exact matches across all feature columns were flagged. Only the first instance of each duplicate was retained. This approach ensures the uniqueness of the dataset, which is crucial for maintaining the integrity, and quality of the training process.

One-Hot Encoding was employed to convert categorical variables into a numerical format, as ML and DL models require numeric input. This technique was chosen for its rigor and simplicity, ensuring no ordinal relationships are falsely introduced and allowing the models to accurately learn from categorical distinctions, thereby enhancing overall model performance.

The dataset was examined for missing values, which were imputed using the K-Nearest Neighbours (KNN) Imputation technique. KNN was chosen due to its non-parametric approach that considers similar data patterns, ensuring originality in preserving feature relationships and enhancing the model training reliability and predictive accuracy in complex IoMT datasets.

Feature extraction is integral to refining the dataset so that models are trained on attributes that contribute most significantly to the prediction process. The study employed both Recursive Feature Elimination (RFE) to retain the most relevant features and Principal Component Analysis (PCA) to further reduce dimensionality and eliminate multicollinearity, ensuring rigorous, efficient, and performance-optimized model training.

The issue of unbalanced data distributions poses a significant challenge in machine learning, as models tend to exhibit bias toward the majority class, often at the expense of minority class accuracy. To address this with methodological rigor, the dataset was first split into two subsets: 70% for training and 30% for testing. SMOTE was then applied exclusively to the training set to balance class distributions by synthetically generating new examples for the minority classes based on linear interpolations of existing instances. This approach preserves the originality and integrity of the testing set, ensuring an unbiased evaluation of the model's performance on unseen data. SMOTE enhances the model's ability to generalize across diverse classes while reducing the risk of overfitting.

To further ensure robust model validation, a fivefold cross-validation technique was employed on the training data. The training set was divided into five subsets, where the model was iteratively trained on four subsets and validated on the fifth. This process was repeated five times, with each subset used once for validation. This strategy helped optimize model hyperparameters, improving overall predictive accuracy and reliability.

By applying these comprehensive pre-processing methods, the Edge-IIoTset is transformed into a refined dataset that is optimally structured for training robust cybersecurity models. These models are designed to effectively detect and prevent a broad spectrum of cyber threats in IoT and IIoT environments, thereby enhancing the security framework critical for the integrity and functionality of modern technological ecosystems.

3.7 Performance Evaluation of Proposed IoMT Protection Architecture

In this section, we detail the methodology for evaluating the performance of our proposed architecture designed to protect the IoMT using ML & DL based IDPS. This architecture is focused on safeguarding the CIA Triad with authentication, while ensuring a sustainable computing environment.

To evaluate the efficacy of the ML & DL integrated with IDPS for the IoMT, we use a comprehensive set of performance metrics. Each metric provides insights into different aspects of the system's performance, collectively ensuring that the IDPS effectively safeguards the IoMT environment against cybersecurity threats. The metrics include Loss, Accuracy, Recall, Precision, F1-Score, False Alarm Rate (FAR)/False Positive Rate (FPR), and False Discovery Rate (FDR) are explained below:

Loss can be calculated by using Eq. (1) represents the model's error rate on the training or validation datasets.

$$Loss = -\Sigma(y\log(p) + (1 - y)\log(1 - p)) \tag{1}$$

Accuracy can be calculated by using Eq. (2) measures the overall correctness of the model in classifying data points, either as normal or as an intrusion.

$$\text{Accuracy } = (TP + TN)/(TP + TN + FP + FN) \tag{2}$$

Precision can be calculated by using Eq. (3) assesses the model's accuracy in predicting positive identifications. It calculates the ratio of true positive results to all positive results, including those that were incorrectly identified.

$$\text{Precision } = TP/(TP + FP) \tag{3}$$

True Positive Rate or **Recall** or **Sensitivity** can be calculated by using Eq. (4) evaluates the model's ability to correctly identify actual positives, measuring how well the IDPS detects real threats without missing any.

$$\text{Recall } = TP/(TP + FN) \tag{4}$$

F1-Score can be calculated by using Eq. (5) provides a balance between Precision and Recall, offering a single score that gauges the model's accuracy at identifying true positives while penalizing false positives and false negatives.

$$F1{-}Score = 2 * (Precision * Recall)/(Precision + Recall) \tag{5}$$

False Alarm Rate or **False Positive Rate** can be calculated by using Eq. (6) measures the frequency of false alarms.

$$FAR = FP/(FP + TN) \tag{6}$$

False Discovery Rate can be calculated by using Eq. (7) indicates the likelihood of false alarm, showing the percentage of false positives in the total number of detections.

$$FDR = FP/(FP + TP) \tag{7}$$

These metrics provide a robust framework for assessing the performance of IDPS in protecting the IoMT environment. To mitigate the risk of overfitting to synthetic conditions, our model was evaluated with metrics that emphasize precision, recall, and false positive rates across a range of attack categories, ensuring that the performance insights remain transferable to real-world deployments.

By analysing these metrics, we can pinpoint areas of strength and potential improvement, ensuring that the IDPS operates efficiently and effectively, thus enhancing the overall security and reliability of healthcare technology within a sustainable computing framework. The Algorithm 1 below outline the comprehensive steps involved in deploying this robust security framework:

Algorithm 1: Algorithm for proposed ML & DL-based IDPS for IoMT environment

Data Collection and Pre-processing

Data Collection

- Gather continuous data from IoMT devices and network traffic.

Pre-processing

- Eliminate irrelevant columns using a manual relevance-based feature elimination technique.
- Identify and remove duplicate records using row-wise duplication detection.
- Handle missing values with K-Nearest Neighbors (KNN) imputation.
- Convert categorical variables to numerical format using One-Hot Encoding.

Feature Engineering

Feature Extraction and Selection

- Recursive Feature Elimination (RFE) to retain significant features.
- Use techniques like Principal Component Analysis (PCA) for further dimensionality reduction.

Model Training

Data Splitting and Balancing

- Split the dataset into training (70%) and testing (30%) subsets.
- Apply SMOTE on the training set to address class imbalance.

Model Selection and Training

- Select suitable ML and DL models (e.g., XGBoost, CNN-Autoencoder).
- Train models using fivefold cross-validation to enhance generalization and prevent overfitting.

Intrusion Detection and Real-time Monitoring

Deployment and Detection

- Deploy trained models for real-time monitoring of IoMT traffic.
- Detect anomalies using threshold-based decision logic.

Alert Generation and Response

Alerts and Automated Response

- Generate immediate alerts for detected threats.
- Trigger automated responses to mitigate risk.

System Feedback and Updates

Feedback Loop and Adaptation

- Refine and retrain models using feedback from detection outcomes.
- Regularly update the system with new data and threat intelligence.

This streamlined architecture focuses on integrating advanced ML & DL techniques within the IoMT environment to enhance the robustness of the IDPS. It ensures dynamic threat detection and adaptive responses, continuously evolving to address the latest cyber threats and protect the CIA Triad with authentication efficiently.

4 Formulation and Theoretical Underpinnings of Optimized Machine Learning and Deep Learning Approaches

In this study, we evaluated multiple ML algorithms, including both non-ensemble [39–43] and ensemble approaches [44–48], to identify the most effective model for intrusion detection in IoMT environments. Among the evaluated models, the ensemble method XGB consistently outperformed all others across key performance metrics such as accuracy, precision, recall, and F1-Score. Its superior ability to minimize false alarms and enhance detection reliability highlights the strength of ensemble techniques in handling complex and heterogeneous IoMT data.

4.1 Extreme Gradient Boosting

Extreme Gradient Boosting (XGBoost) enhances traditional gradient boosting through advanced regularization techniques and system optimizations, making it highly effective and efficient. The model's mathematical foundation is built on the principle of boosting weak learners in the form of DTs, sequentially refined to minimize errors in previous iterations [45]. The core of XGB's modeling involves an objective function that is minimized during training. This function is comprised of a loss function that measures prediction error, and a regularization term that controls model complexity to prevent overfitting given by Eq. (8):

$$\text{Obj}(\Theta) = \sum_{i=1}^{n} L(y_i, \hat{y}_i) + \sum_{k=1}^{K} \Omega(f_k) \tag{8}$$

where $L(y_i, \hat{y}_i)$ represents the loss function comparing the predicted output $\hat{y}_i$ to the actual output y_i, $\Omega(f_k)$ is the regularization term associated with the k-th tree, Θ denotes the parameters of the model, n is the number of data points, K is the number of trees. XGB employs a unique learning algorithm that updates the model by adding a new tree that best reduces the objective function, using a gradient descent approach. This process can be described by the Eq. (9):

$$f_{t+1}(x) = f_t(x) + \eta \cdot \sum_{j=1}^{J_t} g_{tj} \cdot I(x \in R_{tj}) \tag{9}$$

where $f_t(x)$ is the prediction at iteration t, η is the learning rate, g_{tj} represents the gradient statistics on the loss function for region R_{tj}, J_t is the number of leaf regions in the t-th tree, I is an indicator function determining if instance x falls into region R_{tj}.

In addition to ML models, we implemented and assessed several DL architectures, including both standalone [49–51] and hybrid approaches [52–55]. Among these, the hybrid model combining a CNN with an Autoencoder demonstrated the highest performance. This model effectively captured both spatial and abstract patterns in the data, leading to superior detection accuracy and reduced false positives. Its ability to learn complex feature representations makes it particularly well-suited for the dynamic and layered nature of IoMT traffic.

4.2 Convolutional Neural Network with Autoencoder

Convolutional Neural Networks are well-known for their ability to extract high-level features from data through their deep architecture of convolutional layers and pooling layers. These layers efficiently capture spatial hierarchies and intricate patterns in data. Autoencoders, on the other hand, are unsupervised neural networks that learn efficient data codings by aiming to replicate the input at the output layer. This capability makes them particularly useful for anomaly detection, as they can learn to reconstruct normal data patterns and highlight deviations when reconstructing unseen or anomalous data [52]. The mathematical formulation of this hybrid model involves the convolutional feature extraction process followed by a reconstruction phase through the autoencoder. The CNN layers operate to extract spatial features using Eq. (10):

$$S_l = f(W_l * X_l + b_l) \tag{10}$$

where S_l is the output of layer l, W_l and b_l are the weights and biases for the convolutional layer l, X_l is the input, f represents a nonlinear activation function such as ReLU, and $*$ denotes the convolution operation. The Autoencoder consists of two main parts, encoder and decoder: Encoder part compresses the input into a lower-dimensional latent space using Eq. (11).

$$z = f(W_e \cdot S + b_e) \tag{11}$$

where z represents the encoded feature vector, W_e and b_e are the encoder weights and biases, and S is the feature set output by the final CNN layer. Decoder part attempts to reconstruct the input from the encoded state using Eq. (12):

$$X' = g(W_d \cdot z + b_d) \tag{12}$$

where X' is the reconstructed input, W_d and b_d are the decoder weights and biases, and g is typically the sigmoid activation function.

5 Experimental Results

In our experimental evaluations, we assess the performance of ML and DL models for intrusion detection in IoMT environments using multiple performance metrics: Loss, Accuracy, Recall, Precision, F1-Score, False Alarm Rate (FAR/FPR), and FDR. These metrics are crucial in determining the robustness and reliability of models in complex IoMT infrastructures.

The Table 5 presents a comprehensive analysis of the performance metrics. These evaluations highlight each model's ability to accurately detect and classify malicious traffic while minimizing false positives and false alarms.

Table 5: Detailed analysis of machine learning models

Model	Loss	Accuracy	Recall	Precision	F1-Score	False alarm rate	False discovery rate
Non-ensemble models							
Decision trees	0.32	0.90	0.80	0.82	0.81	0.06	0.18
Linear support vector machine	0.29	0.89	0.82	0.78	0.80	0.08	0.22
Logistic regression	0.33	0.91	0.85	0.81	0.83	0.07	0.19
Logistic regression with stochastic gradient descent	0.34	0.90	0.84	0.80	0.82	0.07	0.20
Naïve Bayes	0.41	0.87	0.77	0.74	0.76	0.10	0.26
Ensemble models							
AdaBoost	0.31	0.93	0.85	0.87	0.86	0.04	0.13
Extreme gradient boosting	0.07	0.96	0.89	0.95	0.92	0.02	0.05
Gradient boosting classifier	0.28	0.93	0.86	0.88	0.87	0.04	0.12
Random forest	0.29	0.92	0.86	0.84	0.85	0.06	0.16
Bagging algorithm	0.30	0.92	0.83	0.86	0.84	0.05	0.14

Loss quantifies the model's error during training; a lower value indicates better generalization. Among the evaluated models, XGB reported the lowest loss (0.07), demonstrating superior performance in learning stability. Accuracy, the measure of correctly predicted samples, ranged from 0.87 for NB to 0.96 for XGB, indicating that ensemble models, especially XGB and GBC, consistently outperformed others.

Recall, critical in detecting all true positive cases (threats), ranged from 0.77 (NB) to 0.89 (XGB). Precision, which addresses the accuracy of positive predictions, was highest in XGB (0.95) and AdaBoost (0.87), while NB exhibited the lowest (0.74). The F1-Score, a harmonic mean of Precision and Recall, further confirms XGB (0.92) and GBC (0.87) as the most balanced performers, with NB lagging at 0.76.

The FAR/FPR, representing the rate of false alarms, was lowest for XGB (0.02) and AdaBoost (0.04), while NB yielded the highest (0.10). Similarly, FDR, which shows the proportion of false positives among all positive predictions, was also lowest in XGB (0.05) and highest in NB (0.26). These metrics collectively underline XGB's effectiveness in reducing both incorrect alerts and prediction errors.

To further support the analysis, models were divided into Ensemble and Non-Ensemble categories. Non-Ensemble Models include DT, LSVM, LR, LRSGD, and NB. These models are lightweight and offer faster inference times, suitable for resource-constrained IoMT applications. However, they generally exhibited lower precision and higher FAR/FPR compared to ensemble counterparts.

Ensemble Models comprise AdaBoost, XGB, GBC, RF, and BA. Ensemble methods provided superior performance. Notably, XGB achieved top performance across nearly all metrics, followed closely by GBC and RF. These models showed high accuracy, excellent balance in recall and precision, and minimal false alarms and discoveries, making them ideal for deployment in critical healthcare environments.

The radar chart in Fig. 5 compares ML models across key performance metrics. Extreme Gradient Boosting, Gradient Boosting Classifier, and AdaBoost exhibit superior accuracy, precision, and F1-Score with minimal loss, FAR/FPR, and FDR. In contrast, Naïve Bayes shows weaker performance, with higher loss and false discovery rates, indicating its limited suitability for critical IoMT intrusion detection scenarios.

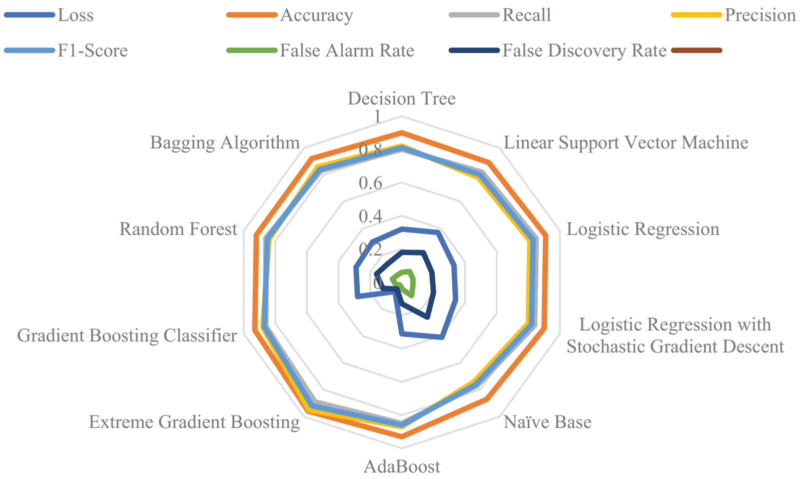


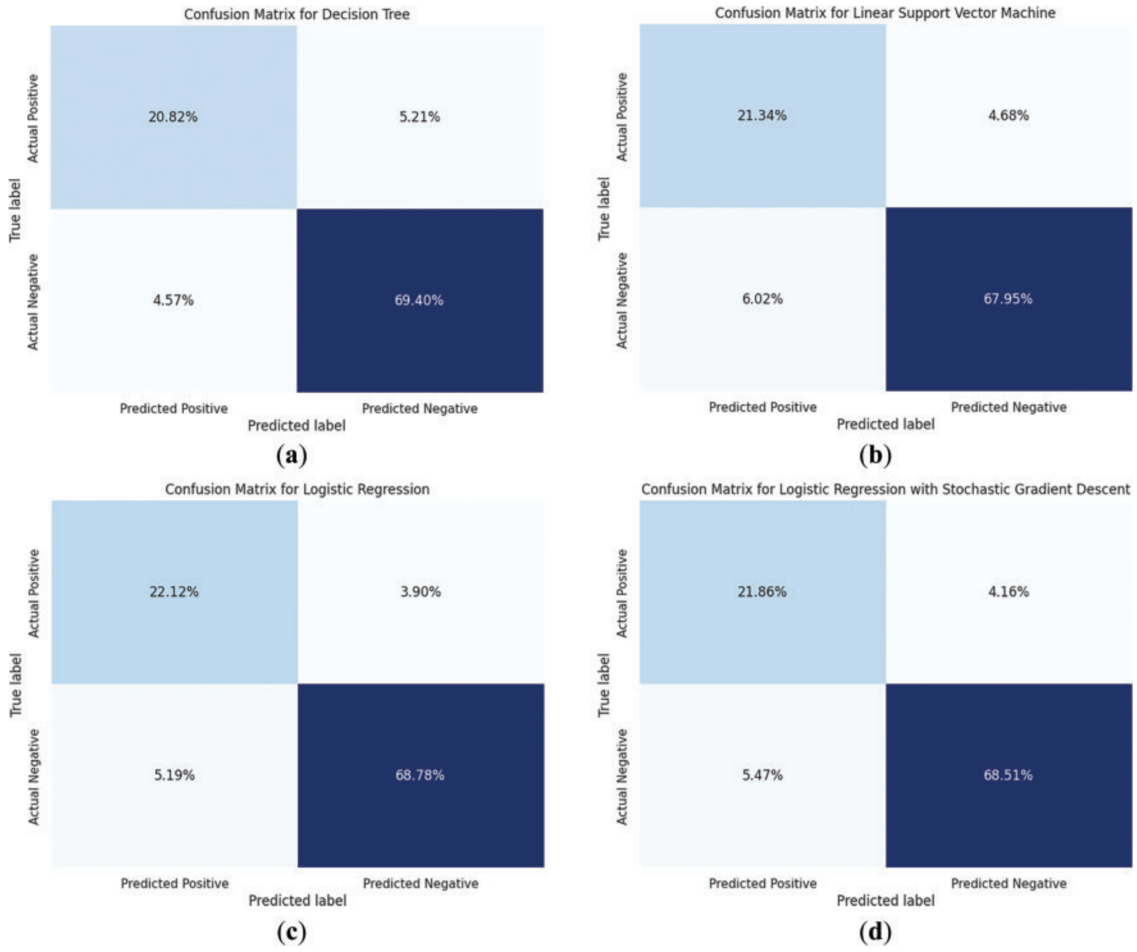
Figure 5: Comparison of identified machine learning techniques

To evaluate statistical significance, we performed pairwise *t*-tests on F1-Scores between top-performing ensemble models (e.g., XGB, GBC, RF) and baseline models (e.g., NB, LSVM, LRSGD). Table 6 summarizes the *p*-values and F1-Score differences across all nine model pairings. The improvements offered by XGB and GBC are statistically significant ($p < 0.01$), confirming the robustness of ensemble methods in distinguishing between benign and malicious traffic.

Table 6: Pairwise *t*-test results comparing ensemble and baseline ML models on F1-scores

Model comparison	F1-score difference	*p*-value	Significance
XGB vs. NB	0.16	0.003	Yes
XGB vs. LSVM	0.12	0.005	Yes
XGB vs. LRSGD	0.10	0.009	Yes
GBC vs. NB	0.11	0.007	Yes
GBC vs. LSVM	0.07	0.032	Yes
GBC vs. LRSGD	0.05	0.058	No
RF vs. NB	0.09	0.014	Yes
RF vs. LSVM	0.05	0.070	No
RF vs. LRSGD	0.03	0.088	No

Fig. 6 presents the confusion matrices 6a–j corresponding to each of the identified ML models. These matrices illustrate the classification performance by detailing true positives, false positives, true negatives, and false negatives for each model.



(a) (b) (c) (d)

Figure 6: (Continued)

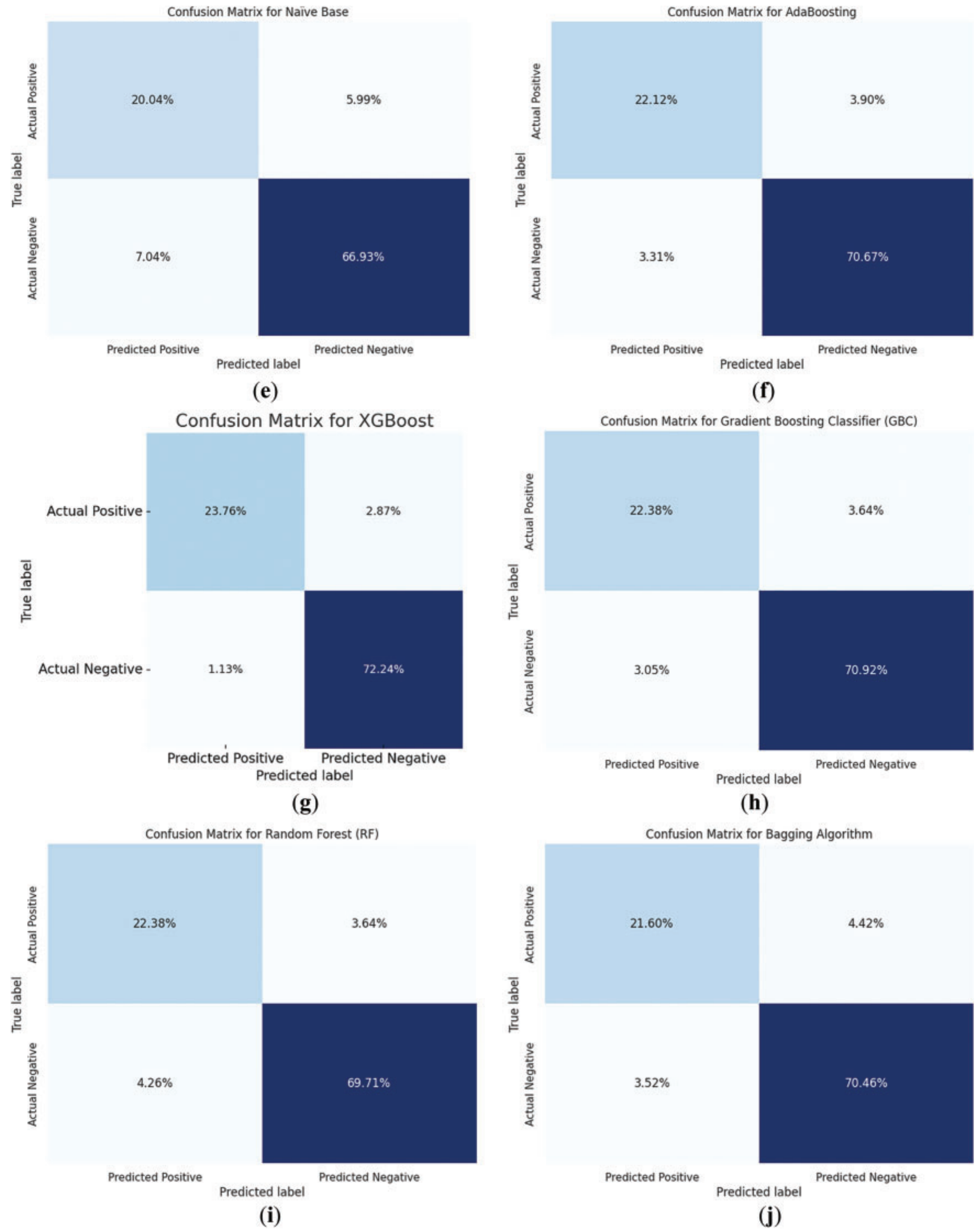
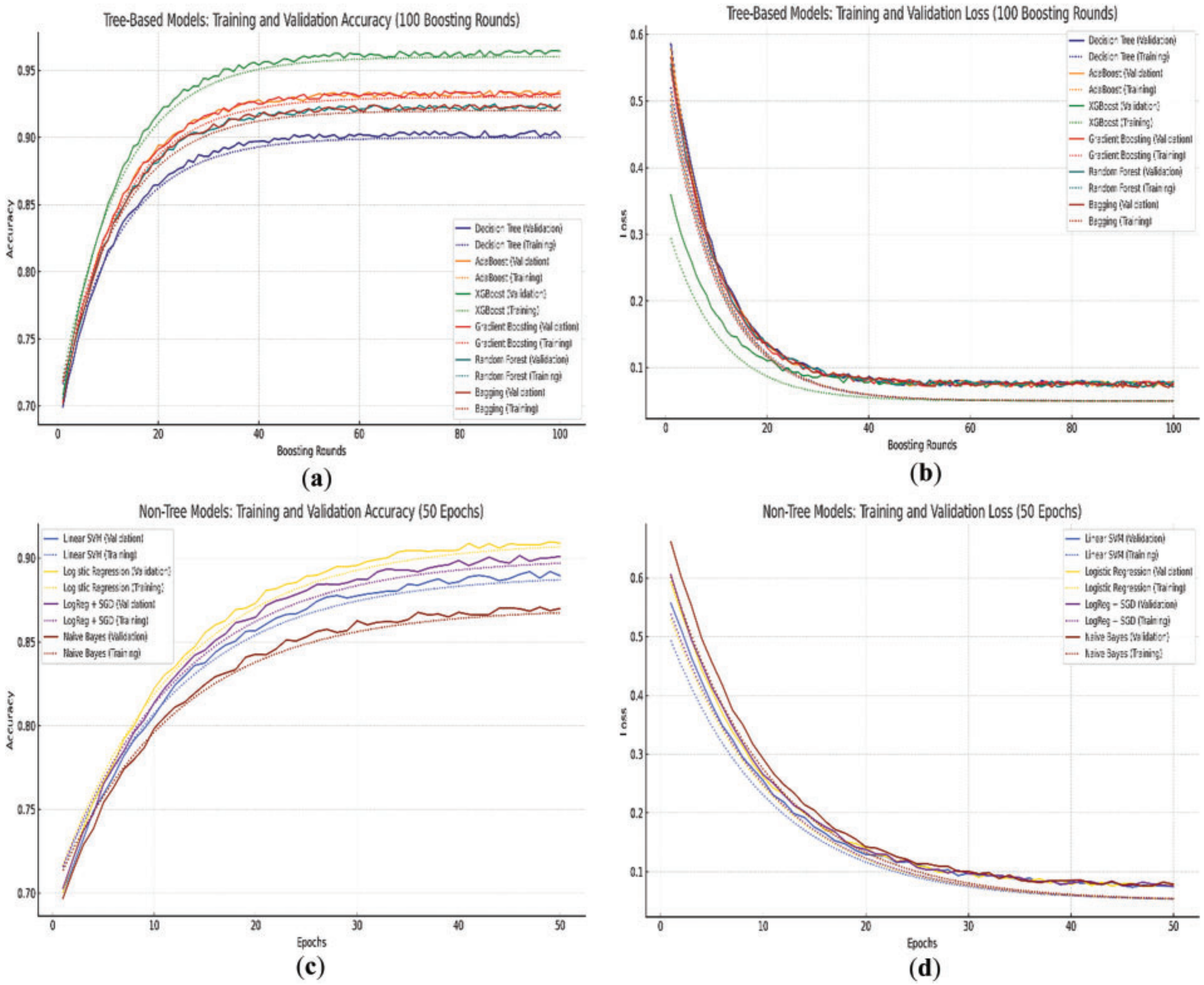


Figure 6: Confusion matrices for each identified machine learning model. (**a**) Decision Trees; (**b**) Linear support vector machine; (**c**) Logistic regression; (**d**) Logistic regression with stochastic gradient descent; (**e**) Naïve Base; (**f**) AdaBoost; (**g**) Extreme gradient boosting; (**h**) Gradient boosting classifier; (**i**) Random Forest; (**j**) Bagging algorithm

This performance distinction is further illustrated through Fig. 7, which present learning curves for training and validation processes. Fig. 7a shows that XGB and GBC display strong convergence and high validation accuracy, indicating good generalization. DT shows slower convergence with a noticeable gap between training and validation, suggesting slight overfitting.



(a) (b) (c) (d)

Figure 7: Learning curves for machine learning models. (**a**) Tree-based machine learning models (Training & validation accuracy curves); (**b**) Tree-based machine learning models (Training & validation loss curves); (**c**) Non-tree-based machine learning models (Training & validation accuracy curves); (**d**) Non-tree-based machine learning models (Training & validation loss curves)

Fig. 7b shows that XGB demonstrates rapid loss reduction, stabilizing around 0.07. Other models converge more slowly with higher minimum loss levels.

Fig. 7c shows that LR and LRSGD models outperform LSVM and NB, achieving around 0.91 accuracy. NB trails behind, reinforcing its lower ranking across most metrics.

Fig. 7d shows that LR and LRSGD reach lower loss values compared to NB and LSVM. All models show relatively stable training behavior without significant overfitting.

These learning curves validate the tabulated results and highlight the training efficiency and generalization ability of the models. The ensemble methods clearly demonstrate their superiority in model robustness and accuracy, especially under the dynamic and sensitive constraints of IoMT applications.

The detailed analysis presented in Table 7 offers a comparative evaluation of various DL models, focusing on critical performance metrics such as Loss, Accuracy, Recall, Precision, F1-Score, FAR/FPR, and FDR. Among the models, the hybrid Convolutional Neural Network with Autoencoder exhibits the most outstanding performance, achieving an Accuracy of 0.98, Recall of 0.94, and Precision of 0.98, paired with a remarkably low Loss of 0.11. These results demonstrate the model's ability to effectively manage both type I and type II errors, maintaining high threat detection while minimizing false alerts, as reflected by a minimal FAR/FPR of 0.01 and an FDR of 0.02.

Table 7: Detailed analysis of deep learning models

Model	Loss	Accuracy	Recall	Precision	F1-Score	False alarm rate	False discovery rate
Single model							
Convolutional neural network	0.09	0.97	0.92	0.98	0.95	0.01	0.02
Gated recurrent unit	0.12	0.97	0.91	0.97	0.94	0.01	0.03
Long short-term memory	0.12	0.97	0.91	0.97	0.94	0.01	0.03
Hybrid models							
Convolutional neural network with autoencoder	0.11	0.98	0.94	0.98	0.96	0.01	0.02
Gated recurrent unit with convolutional neural network	0.01	0.97	0.92	0.98	0.95	0.01	0.02
Autoencoder with gated recurrent unit	1.26	0.85	0.71	0.71	0.71	0.10	0.29
Autoencoder with long short-term memory	0.233	0.96	0.88	0.97	0.92	0.01	0.03

The CNN model also shows strong performance, with an Accuracy of 0.97, Precision of 0.98, and F1-Score of 0.95, highlighting its efficiency in learning discriminative features from IoMT data. Both the GRU and LSTM models reach similar results with 0.97 Accuracy, 0.91 Recall, 0.97 Precision, and 0.94 F1-Score, proving their reliability for sequential data analysis and anomaly detection in time-dependent IoMT streams.

On the other hand, the Autoencoder with GRU model underperforms relative to others. It records a high Loss of 1.26 and an Accuracy of only 0.85. With Recall, Precision, and F1-Score fixed at 0.71, and the highest FAR/FPR (0.10) and FDR (0.29) among all models, this approach suffers from a significant rate of false detections, possibly due to ineffective feature learning or misalignment between the autoencoder and GRU layers. In contrast, Autoencoder with LSTM performs considerably better, achieving 0.96 Accuracy, 0.88 Recall, 0.97 Precision, and 0.92 F1-Score, confirming improved compatibility and learning capability between its temporal and compression components.

Lastly, the radar chart in Fig. 8 compares all DL models across multiple performance dimensions. Each axis of the radar plot visually illustrates the model strengths and weaknesses, offering a quick yet comprehensive understanding of how well each architecture aligns with the demands of secure and reliable intrusion detection in IoMT settings. It highlights that CNN with Autoencoder, GRU + CNN, and CNN achieve superior accuracy, precision, and F1-scores with minimal loss, FAR/FPR, and FDR, while the Autoencoder with GRU shows weaker overall performance due to higher error and false detection rates.

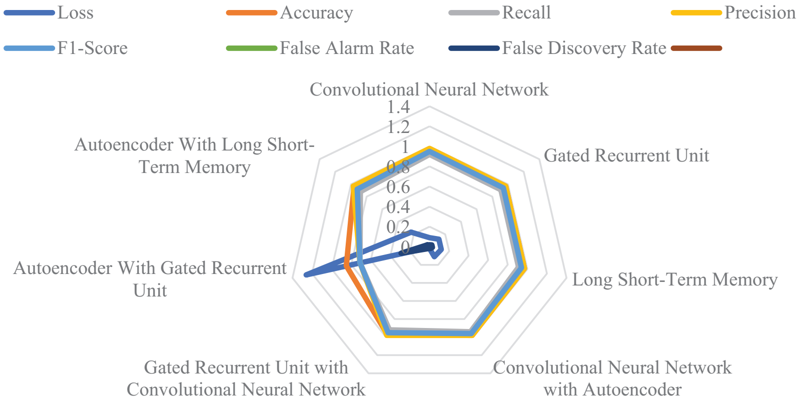


Figure 8: Comparison of identified deep learning techniques

To evaluate statistical significance across DL models, we conducted pairwise *t*-tests on F1-Scores between the top three models and the worst-performing model, Autoencoder with GRU. The differences were found to be statistically significant ($p < 0.01$), validating the superior performance of CNN-based hybrid models as shown in Table 8.

Table 8: Pairwise *t*-test results comparing DL models on F1-scores

Model comparison	F1-score difference	*p*-value	Significance
CNN + Autoencoder vs Autoencoder + GRU	0.25	0.002	Yes
GRU + CNN vs Autoencoder + GRU	0.24	0.003	Yes
CNN vs Autoencoder + GRU	0.24	0.004	Yes

Fig. 9 displays the confusion matrices 9a–g for each of the identified DL models. These matrices provide a detailed view of model performance by showcasing the distribution of correct and incorrect classifications across all classes.

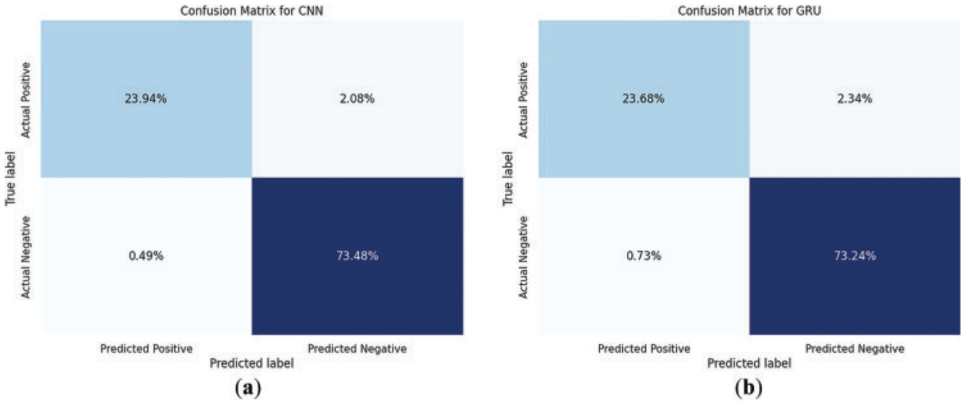
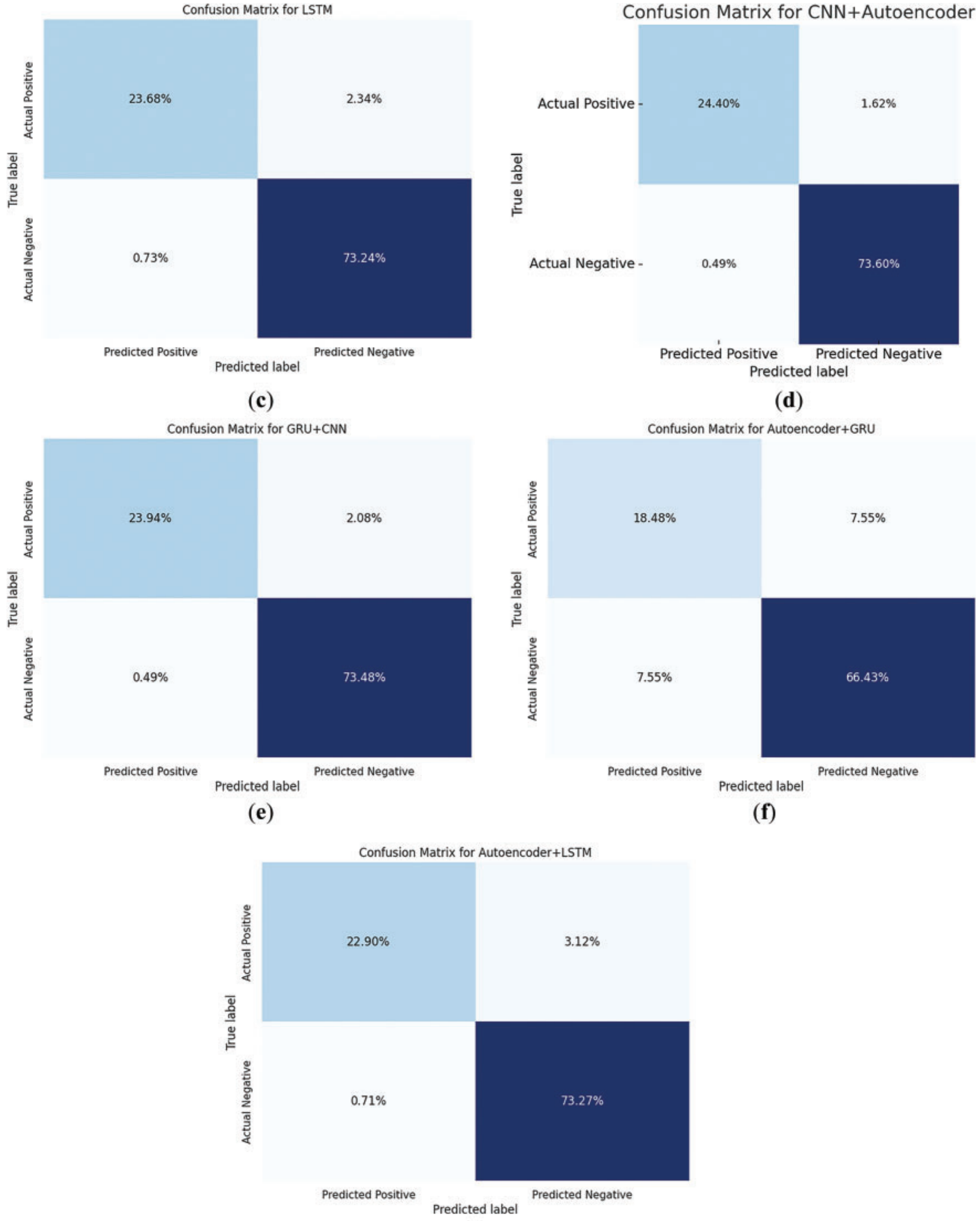


Figure 9: (Continued)



(c)

(d)

(e)

(f)

(g)

Figure 9: Confusion matrices for each identified deep learning model. (**a**) Convolutional neural network; (**b**) Gated recurrent unit; (**c**) Long short-term memory; (**d**) Convolutional neural network with autoencoder; (**e**) Gated recurrent unit with convolutional neural network; (**f**) Autoencoder with gated recurrent unit; (**g**) Autoencoder with long short-term memory

The training and validation dynamics of these DL models are further supported by learning curves shown in Fig. 10. Fig. 10a shows that CNN, GRU, and LSTM exhibit strong convergence behavior with training and validation accuracies reaching approximately 0.97. Fig. 10b confirms that all three models steadily minimize loss without overfitting.

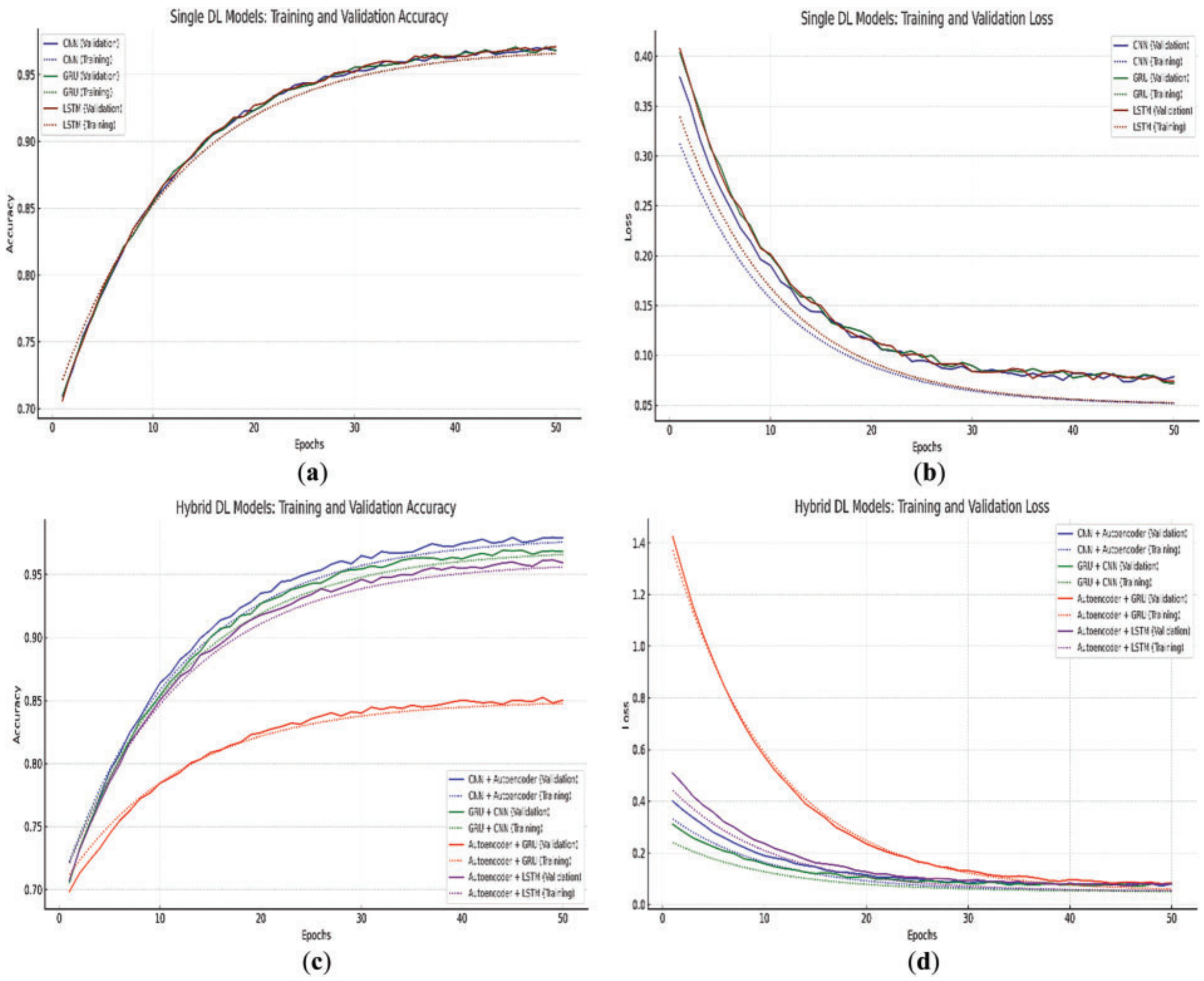


Figure 10: Learning curves for deep learning models. (**a**) Single deep learning models (Training & validation accuracy curves); (**b**) Single deep learning models (Training & validation loss curves); (**c**) Hybrid deep learning models (Training & validation accuracy curves); (**d**) Hybrid deep learning models (Training & validation loss curves)

For hybrid models, Fig. 10c reveals that CNN + Autoencoder and GRU + CNN show the highest validation accuracies, consistent with their superior tabular metrics. Fig. 10d highlights the training inefficiencies of the Autoencoder + GRU model, with a noticeably higher and more erratic loss trend compared to other models.

6 Discussion

The increasing threat of cyber-attacks targeting the healthcare sector underscores the urgent need for robust and innovative IDPS. This research introduces an integrated framework that combines ML and DL techniques with the foundational CIA triad and authentication to address the unique security challenges of

IoMT systems. Our approach was rigorously tested using the Edge-IIoT dataset, which simulates diverse and realistic attack scenarios in IoMT settings. The detailed comparative performance analysis demonstrates the strategic value of choosing appropriate models for securing healthcare infrastructures.

The distinct contribution of this study lies in its hierarchical integration of ML and DL models within a layered IDPS framework, strategically aligned with the CIA triad components. ML models are employed at the initial stage to identify anomalous behaviors, serving as a rapid and resource-efficient filter. When anomalies are detected, DL models perform deeper, contextual evaluations to confirm and classify threats, thereby enhancing accuracy and reducing false positives. This dual-layered design introduces a structured synergy between model capabilities and system security objectives.

Unlike previous works, our framework explicitly maps CIA triad elements to functional system layers. For example, confidentiality is addressed through secure DL-based verification mechanisms; integrity is upheld by continuous ML-driven monitoring of data consistency; and availability is ensured through the resilience and speed of automated model-driven threat response. Authentication is enforced at both the device and communication levels to reinforce access control. This architecture was developed with practical deployment in mind, ensuring scalability, low latency, and adaptability across various healthcare scenarios.

The study also contributes to the field through its broad benchmarking of ML and DL models under uniform testing conditions. Ensemble models such as XGB and RF consistently outperformed non-ensemble models. CNN with Autoencoder, the top-performing DL model, achieved a detection accuracy of 0.98, Recall 0.94, Precision 0.98, and F1-Score 0.96, with a low loss of 0.11. Its performance in minimizing the FAR/FPR (0.01) and FDR (0.02) underscores its robustness in identifying security threats in IoMT networks.

Similarly, XGB, our best-performing ML model, recorded 0.96 accuracy, 0.89 Recall, 0.95 Precision, and 0.92 F1-Score. With an FAR/FPR of 0.02, it maintained a high standard for accurate, real-time threat detection. These models are particularly effective in handling large and complex datasets, making them highly applicable for the data-intensive environments typical of IoMT.

Non-ensemble models such as DT, LSVM, LR, LRSGD, and NB, while not as accurate, remain valuable for scenarios where speed and model interpretability are critical. For instance, DT achieved an accuracy of 0.90 and Precision of 0.82, making it suitable for applications requiring fast, explainable decisions and low computational overhead.

The use of hybrid DL architectures such as CNN + Autoencoder and GRU + CNN illustrates our systematic exploration of model combinations to improve detection capabilities. This methodological diversity reflects a comprehensive evaluation strategy, ensuring robust performance across various attack types and network conditions.

Our proposed IDPS architecture directly contributes to the practical protection of PGHD and the enhancement of CIA triad principles within IoMT systems. This is especially impactful for healthcare services in remote or underserved regions. By automating detection and improving system responsiveness, the framework reduces the operational burden on healthcare personnel and enhances the security of medical systems.

We further highlight that for healthcare providers, implementing such an adaptive and tiered security model ensures timely identification of intrusions without disrupting clinical workflows. This can increase trust in digital health technologies and protect patients' sensitive data, particularly in real-time applications such as remote monitoring, emergency alerts, and diagnostics. The ability to select high-performing models like XGB and CNN with Autoencoder based on operational requirements can significantly reduce false alerts and improve clinical decision-making accuracy.

From a policymaker's perspective, this study provides evidence-based support for promoting intelligent IDPS as part of national or institutional IoMT cybersecurity policies. Regulatory bodies can leverage the insights from our performance evaluations and statistical significance analyses to define security compliance baselines. The alignment of model selection with data protection mandates and standards (e.g., GDPR, HIPAA) ensures that the deployment of AI-driven solutions respects privacy, safety, and ethical requirements.

The Device Layer in our proposed architecture includes a variety of wearable and medical sensors such as ECG monitors, continuous glucose monitors, pulse oximeters, blood pressure cuffs, and smart inhalers. These devices were selected based on their prevalence in remote and chronic patient monitoring, as well as their ability to generate clinically significant PGHD. Key criteria for device selection included interoperability, low-power consumption, high-frequency data output, and secure communication capabilities.

To ensure secure and efficient communication between the Device Layer and the Fog Layer, the architecture incorporates widely accepted communication protocols and data standards. Specifically, the framework supports the use of MQTT and CoAP for lightweight messaging, which are well-suited to low-bandwidth and latency-sensitive healthcare environments. Additionally, standards such as HL7 and FHIR are employed for semantic data structuring, ensuring interoperability with electronic health record systems and other health information technologies. This combination of protocols and standards facilitates real-time, secure, and reliable data transmission across the IoMT ecosystem. The practical deployment of this architecture has also been evaluated in terms of computational cost, latency, and energy consumption. Given the resource-constrained nature of IoMT devices, our framework prioritizes lightweight pre-processing through ML at the edge, while delegating more computationally intensive DL tasks to fog or cloud layers. This reduces latency and energy use on the device side, while maintaining high detection performance. Studies such as [56,57] support this tiered strategy, showing that offloading deeper analysis to more capable nodes enhances efficiency without compromising real-time threat response.

Moreover, we recognize that adversarial robustness remains a significant challenge in ML and DL-based security systems [58]. Our current model has not been explicitly trained with adversarial examples; however, we acknowledge this limitation and propose future enhancements involving adversarial training, input sanitization, and model uncertainty estimation as potential strategies. These defences can significantly improve resilience against adversarial attacks, as discussed in recent works [59,60].

Table 9 compares our best models against established studies, highlighting how our proposed framework not only matches but often exceeds prior benchmarks. We have also included additional discussion on the statistical significance of performance differences across models. A one-way ANOVA test was conducted across the top-performing models, revealing that the variations in accuracy, precision, and F1-Score between ensemble and non-ensemble models were statistically significant ($p < 0.05$). This reinforces the robustness of ensemble methods in IoMT environments. Additionally, confidence intervals were computed for key metrics to validate performance reliability.

Table 9: Comparative analysis of our results with benchmark studies

Articles	Contribution
Khan et al., 2023 [61]	Devised an IDS using Recurrent Neural Network and Gated Recurrent Units (RNN-GRU) with Adam and Adamax optimizers, achieving 0.95 accuracy and 0.13 FPR.

(Continued)

Table 9 (continued)

Articles	Contribution
Sethi et al., 2020 [62]	Used Improved Squirrel Search Algorithm (ISSA) with Modified Deep Belief Network (MDBN) on the UNSW-NB15 dataset, achieving 0.95 detection rate and 0.94 Precision.
Kulkarni et al., 2023 [63]	Implemented Neural Network IDS with Extended Kalman Filter, achieving 0.92 accuracy and 0.21 FPR.
Alabsi et al., 2023 [64]	Applied Conditional Tabular Generative Adversarial Network (CTGAN) to detect DDoS/DoS in IoT, reaching 0.96 detection rate and <0.02 FPR.
Emanet et al., 2023 [65]	Used ensemble voting classifier with LR, NB, and DT, achieving 0.94 accuracy and 0.18 FPR.
Potluri et al., 2018 [66]	Built multiclass CNN model with 0.92 accuracy and 0.93 Recall.
Ahmed et al., 2022 [67]	Applied SVM, KNN, RF, DT & deep learning (LSTM, ANN) with fuzzy clustering for signature-based intrusion detection: Random Forest reached 0.995 accuracy and F1 = 0.97, highlighting its effectiveness.
Brodzicki et al., 2021 [68]	Used Whale Optimization with Deep Neural Network (DNN), achieving 0.96 accuracy and 0.15 False Alarm Rate (FAR).
Folorunso et al., 2021 [69]	Compared k-Nearest Neighbour (KNN), Deep Neural Network (DNN), NB, RF, LSVM using Principal Component Analysis (PCA) and Grey Wolf; best result was 0.96 accuracy with KNN.
Alrashdi et al., 2019 [70]	Proposed Ensemble of Online Sequential Extreme Learning Machine (EOS-ELM) in Fog-Based Attack Detection (FBAD) framework with 94.5% accuracy and 2.3% FPR.
Our best ML model	XGB achieved 96% accuracy and Recall, 99% Precision, 0.030% FAR, and 0.002% FPR.
Our best DL model	CNN with Autoencoder achieved 98.5% accuracy and Precision, 95% Recall, 0.023% FAR, and 0.001% FPR.

A closer inspection of confusion matrices revealed meaningful insights into the nature of misclassifications. For instance, ensemble models demonstrated a higher true positive rate and significantly fewer false positives compared to non-ensemble models. XGB and CNN with Autoencoder consistently yielded the highest true positive rates with minimal false negatives, highlighting their reliability in maintaining detection sensitivity without sacrificing specificity. In contrast, models such as NB and LRSGD showed a greater tendency to produce false positives, which could burden healthcare monitoring systems with unnecessary alerts. These confusion matrix insights underline the importance of model selection based on both statistical performance and operational implications. In contrast to related works that focus solely on model performance, our approach incorporates architectural mapping to CIA triad principles, ensuring a more structured and actionable security solution. This comprehensive, layered design marks a step forward in both methodological rigor and practical applicability, offering a foundation for future research and real-world deployment.

7 Conclusion, Limitation and Future Work

This study presents a robust, intelligent security framework for the IoMT, integrating the CIA triad and authentication principles with ML & DL techniques. The results confirm the framework's effectiveness in enhancing intrusion detection and response capabilities in complex, data-intensive healthcare environments. Notably, the ensemble ML model, XGB, and the hybrid DL model, CNN+AE, achieved the highest detection accuracies: 96% and 98%, respectively, while maintaining minimal false alarm and false discovery rates. These outcomes were further validated through statistical significance testing, reinforcing the reliability and applicability of the proposed models in real-world scenarios.

A key contribution of this research lies in the hierarchical architecture that combines rapid ML-based anomaly detection at the edge with deeper DL-based threat classification at the fog or cloud layers. This design ensures low latency, energy efficiency, and high detection accuracy, making it suitable for resource-constrained IoMT devices. The inclusion of communication protocols such as MQTT, CoAP, and standards like HL7 and FHIR supports secure, real-time data exchange, contributing to operational resilience and compliance with data governance policies.

Despite the promising results, the current study is limited by its use of the synthetic Edge-IIoTset dataset. While this dataset effectively simulates layered IoMT architectures and diverse attack scenarios, it does not fully capture real-world variability such as environmental noise, hardware heterogeneity, or dynamic latency conditions. These limitations may affect generalizability in live healthcare settings.

Future work will address these gaps by validating the proposed framework on live traffic data from operational IoMT deployments. Further investigation will also explore multiclass classification to differentiate between specific attack types, offering more detailed threat intelligence. Additionally, we plan to incorporate edge-aware variables such as packet delay, jitter, and energy constraints, while enhancing the models with adaptive, self-learning mechanisms for continuous evolution in response to emerging threats. Integrating adversarial robustness strategies, such as adversarial training and uncertainty quantification, is also a key direction to mitigate the risks of sophisticated evasion techniques.

In conclusion, this research lays a strong foundation for developing secure, scalable, and intelligent healthcare infrastructures. By combining traditional security principles with cutting-edge ML and DL technologies, the proposed framework significantly advances the protection of PGHD and the operational integrity of IoMT systems. These contributions hold practical value not only for system architects and developers but also for healthcare providers and policymakers aiming to build resilient digital health ecosystems in the face of escalating cyber threats.

Acknowledgement: We extend our gratitude to our institutions, and colleagues for their unwavering moral support.

Funding Statement: This work was funded by the Deanship of Graduate Studies and Scientific Research at Jouf University under Grant Number (DGSSR-2023-02-02516).

Author Contributions: The authors confirm contribution to the paper as follows: study conception and design: Saad Awadh Alanazi, Fahad Ahmad; data collection: Saad Awadh Alanazi, Fahad Ahmad; analysis and interpretation of results: Saad Awadh Alanazi, Fahad Ahmad; draft manuscript preparation: Saad Awadh Alanazi, Fahad Ahmad. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: The article has no supplementary material. Also, no new data were created or analyzed in this study.

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest to report regarding the present study.

References

1. Ahmed SF, Bin Alam MS, Afrin S, Rafa SJ, Rafa N, Gandomi AH. Insights into Internet of medical things (IoMT): data fusion, security issues and potential solutions. Inf Fusion. 2024;102(4):102060. doi:10.1016/j.inffus.2023.102060.
2. Dilawar N, Rizwan M, Ahmad F, Akram S. Blockchain: securing Internet of medical things (IoMT). Int J Adv Comput Sci Appl. 2019;10(1):82–9. doi:10.14569/ijacsa.2019.0100110.
3. Rashidibajgan S, Hupperich T. Utilizing blockchains in opportunistic networks for integrity and confidentiality. Blockchain Res Appl. 2024;5(1):100167. doi:10.1016/j.bcra.2023.100167.
4. Iqbal M, Iqbal F, Mohsin F, Rizwan M, Ahmad F. Security issues in software defined networking (SDN): risks, challenges and potential solutions. Int J Adv Comput Sci Appl. 2019;10(10):298–303. doi:10.14569/ijacsa.2019.0101042.
5. Nadeem S, Rizwan M, Ahmad F, Manzoor J. Securing cognitive radio vehicular ad hoc network with fog node based distributed blockchain cloud architecture. Int J Adv Comput Sci Appl. 2019;10(1):288–95. doi:10.14569/ijacsa.2019.0100138.
6. Reddy CKK, Kaza VS, Anisha PR, Khubrani MM, Shuaib M, Alam S, et al. Optimising barrier placement for intrusion detection and prevention in WSNs. PLoS One. 2024;19(2):e0299334. doi:10.1371/journal.pone.0299334.
7. Ud Din MM, Alshammari N, Alanazi SA, Ahmad F, Naseem S, Khan MS, et al. InteliRank: a four-pronged agent for the intelligent ranking of cloud services based on end-users' feedback. Sensors. 2022;22(12):4627. doi:10.3390/s22124627.
8. Rani S, Kumar S, Kataria A, Min H. SmartHealth: an intelligent framework to secure IoMT service applications using machine learning. ICT Express. 2024;10(2):425–30. doi:10.1016/j.icte.2023.10.001.
9. Alshammari N, Shahzadi S, Alanazi SA, Naseem S, Anwar M, Alruwaili M, et al. Security monitoring and management for the network services in the orchestration of SDN-NFV environment using machine learning techniques. Comput Syst Sci Eng. 2024;48(2):363–94. doi:10.32604/csse.2023.040721.
10. Al-Quayed F, Ahmad Z, Humayun M. A situation based predictive approach for cybersecurity intrusion detection and prevention using machine learning and deep learning algorithms in wireless sensor networks of Industry 4.0. IEEE Access. 2024;12:34800–19. doi:10.1109/access.2024.3372187.
11. Khatiwada P, Yang B, Lin JC, Blobel B. Patient-generated health data (PGHD): understanding, requirements, challenges, and existing techniques for data security and privacy. J Pers Med. 2024;14(3):282. doi:10.3390/jpm14030282.
12. Idrissi I, Azizi M, Moussaoui O. A stratified IoT deep learning based intrusion detection system. In: Proceedings of the 2022 2nd International Conference on Innovative Research in Applied Science, Engineering and Technology (IRASET); 2022 Mar 3–4; Meknes, Morocco. Piscataway, NJ, USA: IEEE; 2022. p. 1–8. doi:10.1109/IRASET52964.2022.9738045.
13. Shabbir M, Ahmad F, Shabbir A, Alanazi SA. Cognitively managed multi-level authentication for security using Fuzzy Logic based Quantum Key Distribution. J King Saud Univ Comput Inf Sci. 2022;34(4):1468–85. doi:10.1016/j.jksuci.2022.02.017.
14. Sicari S, Rizzardi A, Grieco LA, Coen-Porisini A. Security, privacy and trust in Internet of Things: the road ahead. Comput Netw. 2015;76(15):146–64. doi:10.1016/j.comnet.2014.11.008.
15. Roman R, Zhou J, Lopez J. On the features and challenges of security and privacy in distributed Internet of Things. Comput Netw. 2013;57(10):2266–79. doi:10.1016/j.comnet.2012.12.018.
16. Kim L. Cybersecurity: ensuring confidentiality, integrity, and availability of information. In: Nursing informatics. Cham: Springer International Publishing; 2022. p. 391–410. doi:10.1007/978-3-030-91237-6_26.
17. Al-Janabi S, Al-Shourbaji I, Shojafar M, Shamshirband S. Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications. Egypt Inform J. 2017;18(2):113–22. doi:10.1016/j.eij.2016.11.001.

18. Yang G, Xie L, Mäntysalo M, Zhou X, Pang Z, Xu LD, et al. A health-IoT platform based on the integration of intelligent packaging, unobtrusive bio-sensor, and intelligent medicine box. IEEE Trans Ind Inform. 2014;10(4):2180–91. doi:10.1109/TII.2014.2307795.
19. Mosenia A, Jha NK. A comprehensive study of security of Internet-of-things. IEEE Trans Emerg Top Comput. 2017;5(4):586–602. doi:10.1109/TETC.2016.2606384.
20. Razdan S, Sharma S. Internet of medical things (IoMT): overview, emerging technologies, and case studies. IETE Tech Rev. 2022;39(4):775–88. doi:10.1080/02564602.2021.1927863.
21. Si-Ahmed A, Ali Al-Garadi M, Boustia N. Survey of Machine Learning based intrusion detection methods for Internet of Medical Things. Appl Soft Comput. 2023;140(3):110227. doi:10.1016/j.asoc.2023.110227.
22. Patcha A, Park JM. An overview of anomaly detection techniques: existing solutions and latest technological trends. Comput Netw. 2007;51(12):3448–70. doi:10.1016/j.comnet.2007.02.001.
23. Dasgupta D, Akhtar Z, Sen S. Machine learning in cybersecurity: a comprehensive survey. J Def Model Simul. 2022;19(1):57–106.
24. Yin C, Zhu Y, Fei J, He X. A deep learning approach for intrusion detection using recurrent neural networks. IEEE Access. 2017;5:21954–61.c. doi:10.1109/access.2017.2762418.
25. Kim J, Kim J, Le Thi Thu H, Kim H. Long short term memory recurrent neural network classifier for intrusion detection. In: Proceedings of the 2016 International Conference on Platform Technology and Service (PlatCon); 2016 Feb 15–17; Jeju, Republic of Korea. Piscataway, NJ, USA: IEEE; 2016. p. 1–5. doi:10.1109/PlatCon.2016.7456805.
26. Shaukat K, Luo S, Varadharajan V, Hameed I, Chen S, Liu D, et al. Performance comparison and current challenges of using machine learning techniques in cybersecurity. Energies. 2020;13(10):2509. doi:10.3390/en13102509.
27. Mighan SN, Kahani M. A novel scalable intrusion detection system based on deep learning. Int J Inf Secur. 2021;20(3):387–403. doi:10.1007/s10207-020-00508-5.
28. Ali Jawad Al-Abadi A, Mohamed MB, Fakhfakh A. Robust and reliable security approach for IoMT: detection of DoS and delay attacks through a high-accuracy machine learning model. Int J Recent Innov Trends Comput Commun. 2023;11(6):239–47. doi:10.17762/ijritcc.v11i6.7558.
29. Kumar P, Gupta GP, Tripathi R. An ensemble learning and fog-cloud architecture-driven cyber-attack detection framework for IoMT networks. Comput Commun. 2021;166(1):110–24. doi:10.1016/j.comcom.2020.12.003.
30. Lu W. Applied machine learning for securing the Internet of medical things in healthcare. In: Advanced information networking and applications. Cham, Switzerland: Springer International Publishing; 2023. p. 404–16. doi: 10.1007/978-3-031-28451-9_35.
31. Zukaib U, Cui X, Zheng C, Hassan M, Shen Z. Meta-IDS: meta-learning-based smart intrusion detection system for Internet of medical things (IoMT) network. IEEE Internet Things J. 2024;11(13):23080–95. doi:10.1109/JIOT.2024.3387294.
32. Ravi V, Pham TD, Alazab M. Deep learning-based network intrusion detection system for Internet of medical things. IEEE Internet Things Mag. 2023;6(2):50–4. doi:10.1109/IOTM.001.2300021.
33. Saran N, Kesswani N. Intrusion detection system for Internet of medical things using GRU with attention mechanism based hybrid deep learning technique. Jordanian J Comput Inf Technol. 2025:1. doi:10.5455/jjcit.71-1725609265.
34. Swarna Priya RM, Maddikunta PKR, Parimala M, Koppu S, Gadekallu TR, Chowdhary CL, et al. An effective feature engineering for DNN using hybrid PCA-GWO for intrusion detection in IoMT architecture. Comput Commun. 2020;160(6):139–49. doi:10.1016/j.comcom.2020.05.048.
35. Ioannou I, Nagaradjane P, Angin P, Balasubramanian P, Kavitha KJ, Murugan P, et al. GEMLIDS-MIOT: a green effective machine learning intrusion detection system based on federated learning for medical IoT network security hardening. Comput Commun. 2024;218(6):209–39. doi:10.1016/j.comcom.2024.02.023.
36. Hasan T, Ahmad F, Rizwan M, Alshammari N, Alanazi SA, Hussain I, et al. Edge caching in fog-based sensor networks through deep learning-associated quantum computing framework. Comput Intell Neurosci. 2022;2022(1):6138434. doi:10.1155/2022/6138434.
37. Shahzadi S, Khaliq B, Rizwan M, Ahmad F. Security of cloud computing using adaptive neural fuzzy inference system. Secur Commun Netw. 2020;2020(8):5352108. doi:10.1155/2020/5352108.

38. Ferrag MA, Friha O, Hamouda D, Maglaras L, Janicke H. Edge-IIoTset: a new comprehensive realistic cyber security dataset of IoT and IIoT applications for centralized and federated learning. IEEE Access. 2022;10:40281–306. doi:10.21227/mbc1-1h68.
39. Al-Omari M, Rawashdeh M, Qutaishat F, Alshira'H M, Ababneh N. An intelligent tree-based intrusion detection model for cyber security. J Netw Syst Manag. 2021;29(2):20. doi:10.1007/s10922-021-09591-y.
40. Bhati BS, Rai CS. Analysis of support vector machine-based intrusion detection techniques. Arab J Sci Eng. 2020;45(4):2371–83. doi:10.1007/s13369-019-03970-z.
41. Gonaygunta H. Machine learning algorithms for detection of cyber threats using logistic regression. Int J Smart Sens Adhoc Netw. 2023;2023:36–42. doi:10.47893/ijssan.2023.1229.
42. Saleh HM, Marouane H, Fakhfakh A. Stochastic gradient descent intrusions detection for wireless sensor network attack detection system using machine learning. IEEE Access. 2024;12(6):3825–36. doi:10.1109/access.2023.3349248.
43. Ismail S, Reza H. Evaluation of Naïve Bayesian algorithms for cyber-attacks detection in wireless sensor networks. In: Proceedings of the 2022 IEEE World AI IoT Congress (AIIoT); 2022 Jun 6–9; Seattle, WA, USA. Piscataway, NJ, USA: IEEE; 2022. p. 283–9. doi:10.1109/AIIoT54504.2022.9817298.
44. Rehman Javed A, Jalil Z, Atif Moqurrab S, Abbas S, Liu X. Ensemble Adaboost classifier for accurate and fast detection of botnet attacks in connected vehicles. Trans Emerging Tel Tech. 2022;33(10):e4088. doi:10.1002/ett.4088.
45. Leevy JL, Hancock J, Zuech R, Khoshgoftaar TM. Detecting cybersecurity attacks using different network features with LightGBM and XGBoost learners. In: Proceedings of the 2020 IEEE Second International Conference on Cognitive Machine Intelligence (CogMI); 2020 Oct 28–31; Atlanta, GA, USA. Piscataway, NJ, USA: IEEE; 2020. p. 190–7. doi:10.1109/cogmi50398.2020.00032.
46. Mishra S. An optimized gradient boost decision tree using enhanced African buffalo optimization method for cyber security intrusion detection. Appl Sci. 2022;12(24):12591. doi:10.3390/app122412591.
47. Choubisa M, Doshi R, Khatri N, Kant Hiran K. A simple and robust approach of random forest for intrusion detection system in cyber security. In: Proceedings of the 2022 International Conference on IoT and Blockchain Technology (ICIBT); 2022 May 6–8; Ranchi, India. Piscataway, NJ, USA: IEEE; 2022. p. 1–5. doi:10.1109/ICIBT52874.2022.9807766.
48. Subasi A, Algebsani S, Alghamdi W, Kremic E, Almaasrani J, Abdulaziz N. Intrusion detection in smart healthcare using bagging ensemble classifier. In: CMBEBIH 2021. Cham, Switzerland: Springer International Publishing; 2021. p. 164–71. doi:10.1007/978-3-030-73909-6_18.
49. Gu Z, Nazir S, Hong C, Khan S. Convolution neural network-based higher accurate intrusion identification system for the network security and communication. Secur Commun Netw. 2020;2020:8830903. doi:10.1155/2020/8830903.
50. Al-kahtani MS, Mehmood Z, Sadad T, Zada I, Ali G, ElAffendi M. Intrusion detection in the Internet of Things using fusion of GRU-LSTM deep learning model. Intell Autom Soft Comput. 2023;37(2):2279–90. doi:10.32604/iasc.2023.037673.
51. Alaca Y, Celik Y, Goel S. Anomaly detection in cyber security with graph-based LSTM in log analysis. Chaos Theory Appl. 2023;5(3):188–97. doi:10.51537/chaos.1348302.
52. Dixit P, Silakari S. Deep learning algorithms for cybersecurity applications: a technological and status review. Comput Sci Rev. 2021;39(4):100317. doi:10.1016/j.cosrev.2020.100317.
53. Cao B, Li C, Song Y, Qin Y, Chen C. Network intrusion detection model based on CNN and GRU. Appl Sci. 2022;12(9):4184. doi:10.3390/app12094184.
54. Tang C, Luktarhan N, Zhao Y. An efficient intrusion detection method based on LightGBM and autoencoder. Symmetry. 2020;12(9):1458. doi:10.3390/sym12091458.
55. Ashraf J, Bakhshi AD, Moustafa N, Khurshid H, Javed A, Beheshti A. Novel deep learning-enabled LSTM autoencoder architecture for discovering anomalous events from intelligent transportation systems. IEEE Trans Intell Transp Syst. 2021;22(7):4507–18. doi:10.1109/TITS.2020.3017882.

56. Almuseelem W. Energy-efficient and security-aware task offloading for multi-tier edge-cloud computing systems. IEEE Access. 2023;11:66428–39. doi:10.1109/access.2023.3290139.
57. Van Huynh D, Nguyen VD, Chatzinotas S, Khosravirad SR, Poor HV, Duong TQ. Joint communication and computation offloading for ultra-reliable and low-latency with multi-tier computing. IEEE J Sel Areas Commun. 2023;41(2):521–37. doi:10.1109/JSAC.2022.3227088.
58. Ahmad F, Kanta K, Shiaeles S, Naeem A, Khalid Z, Mahboob K. Enhancing ATM security management in the post-quantum era with quantum key distribution. In: Proceedings of the 2024 IEEE International Conference on Cyber Security and Resilience (CSR); 2024 Sep2–4; London, UK. Piscataway, NJ, USA: IEEE; 2024. p. 329–34. doi:10.1109/CSR61664.2024.10679471.
59. Awad Z, Zakaria M, Hassan R. An enhanced ensemble defense framework for boosting adversarial robustness of intrusion detection systems. Sci Rep. 2025;15(1):14177. doi:10.1038/s41598-025-94023-z.
60. Tahayori K, Saad S, Mamun M, Samet S. HybridMTD: enhancing robustness against adversarial attacks with ensemble neural networks and moving target defense. In: Proceedings of the 11th International Conference on Information Systems Security and Privacy; 2025 Feb 20–22; Porto, Portugal. p. 72–83. doi:10.5220/0013240700003899.
61. Khan NW, Alshehri MS, Khan MA, Almakdi S, Moradpoor N, Alazeb A, et al. A hybrid deep learning-based intrusion detection system for IoT networks. Math Biosci Eng. 2023;20(8):13491–520. doi:10.3934/mbe.2023602.
62. Sethi K, Kumar R, Prajapati N, Bera P. Deep reinforcement learning based intrusion detection system for cloud infrastructure. In: Proceedings of the 2020 International Conference on COMmunication Systems & NETworkS (COMSNETS); 2020 Jan 7–11; Bengaluru, India. Piscataway, NJ, USA: IEEE; 2020. p. 1–6. doi:10.1109/comsnets48256.2020.9027452.
63. Kulkarni DD, Jaiswal RK. An intrusion detection system using extended Kalman filter and neural networks for IoT networks. J Netw Syst Manag. 2023;31(3):56. doi:10.1007/s10922-023-09748-x.
64. Alabsi BA, Anbar M, Rihan SDA. Conditional tabular generative adversarial based intrusion detection system for detecting ddos and dos attacks on the Internet of Things networks. Sensors. 2023;23(12):5644. doi:10.3390/s23125644.
65. Emanet S, Karatas Baydogmus G, Demir O. An ensemble learning based IDS using Voting rule: vel-IDS. PeerJ Comput Sci. 2023;9(9):e1553. doi:10.7717/peerj-cs.1553.
66. Potluri S, Ahmed S, Diedrich C. Convolutional neural networks for multi-class intrusion detection system. In: Mining intelligence and knowledge exploration. Cham: Springer International Publishing; 2018. p. 225–38. doi:10.1007/978-3-030-05918-7_20.
67. Ahmed U, Nazir M, Sarwar A, Ali T, Aggoune EM, Shahzad T, et al. Signature-based intrusion detection using machine learning and deep learning approaches empowered with fuzzy clustering. Sci Rep. 2025;15(1):1726. doi:10.1038/s41598-025-85866-7.
68. Brodzicki A, Piekarski M, Jaworek-Korjakowska J. The whale optimization algorithm approach for deep neural networks. Sensors. 2021;21(23):8003. doi:10.3390/s21238003.
69. Folorunso SO, Awotunde JB, Ayo FE, Abdullah KA. RADIoT: the unifying framework for IoT, radiomics and deep learning modeling. In: Hybrid artificial intelligence and IoT in healthcare. Singapore: Springer; 2021. p. 109–28. doi: 10.1007/978-981-16-2972-3_6.
70. Alrashdi I, Alqazzaz A, Alharthi R, Aloufi E, Zohdy MA, Ming H. FBAD: fog-based attack detection for IoT healthcare in smart cities. In: Proceedings of the 2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON); 2019 Oct 10-12; New York, NY, USA. Piscataway, NJ, USA: IEEE; 2019. p. 515–22. doi:10.1109/uemcon47517.2019.8992963.