Article

MVIIC: A Lightweight Modified GRU Framework for Multi-Vector DDoS Detection in IoMT Healthcare Systems

Ahwar Khan * and Faisal Anwer

Posted Date: 16 October 2025

doi: 10.20944/preprints202509.0650.v2

Keywords: genetic algorithm feature selection; healthcare cybersecurity; internet of medical things; lightweight intrusion detection; modified GRU; multi-vector DDoS detection

 doi:10.20944/preprints202509.0650.v2

Article

MVIIC: A Lightweight Modified GRU Framework for Multi-Vector DDoS Detection in IoMT Healthcare Systems

Ahwar Khan * and Faisal Anwer

Department of Computer Science, Aligarh Muslim University, Aligarh, India

* Correspondence: khanahwar4@gmail.com

Abstract

The rapid growth of Internet of Medical Things (IoMT) devices has improved healthcare delivery but also created new cybersecurity risks, especially from advanced multi-vector DDoS attacks that target devices with limited resources. Many existing intrusion detection systems either consume excessive computing power or cannot keep pace with evolving attack methods, making them impractical for real-time healthcare applications. In this study, we present the Multi-Vector IoT Intrusion Classifier (MVIIC), a lightweight framework that leverages Modified Gated Recurrent Units (MGRUs) and a genetic algorithm-based feature selection approach to efficiently detect multi-vector DDoS attacks. MVIIC includes two classifiers: a Binary Label Classifier (BLC) that gives simple threat alerts for non-technical healthcare staff, and a Multi-Label Classifier (MLC) that provides detailed attack information for cybersecurity experts. The MGRU design reduces computational complexity by 33% compared to a standard GRU while maintaining high detection accuracy by removing the reset gate. Tests on the CICIoT2023 and CICIoMT2024 datasets show strong results: the MLC reaches 99.92% accuracy, precision, recall, and F1-score on CICIoMT2024, which is 0.42% better than leading methods. The BLC achieves 99.96% accuracy with a 0.04% false-positive rate, making it well-suited for urgent healthcare settings. Using genetic algorithms to select features cuts feature size by 46-52% without losing detection quality. The lightweight design of the MGRU layers makes the architecture efficient and suitable for real-time deployment in resource-limited IoMT environments.

Keywords: genetic algorithm feature selection; healthcare cybersecurity; internet of medical things; lightweight intrusion detection; modified GRU; multi-vector DDoS detection

1. Introduction

The Internet of Things (IoT) represents a significant shift where smart devices communicate over internet protocols, creating a vast network of intelligent systems. IoT has driven significant advancements across various areas, such as smart agriculture, industrial automation, and medical applications, significantly improving human life [1]. Among these applications, smart health systems have become essential infrastructure, especially during the global COVID-19 pandemic, when telemedicine services were vital for maintaining public health [2].

The Internet of Medical Things (IoMT) is a part of IoT that focuses on meeting medical needs with networked medical devices, sensors, and monitoring systems [3][4]. These systems provide continuous patient monitoring via wearable, implantable, and mobile health sensors and applications. This approach enables early medical intervention, which helps reduce healthcare costs and the need for hospital stays [2]. Various stakeholders, including healthcare professionals, patients, caregivers, hospital administrators, and emergency responders, depend on safe and reliable IoMT systems to deliver adequate healthcare.

As IoMT devices have increased, so have numerous cybersecurity threats that endanger healthcare systems and patient safety. Many of these connected devices have weak security features,

 doi:10.20944/preprints202509.0650.v2

including the lack of encryption, inconsistent firmware updates, and unprotected data channels [3]. These vulnerabilities make them prime targets for cybercriminals who might steal sensitive patient data and disrupt important healthcare services.

Distributed Denial of Service (DDoS) attacks have become one of the most common and complex threats to Internet of Medical Things (IoMT) infrastructure [5]. Unlike single-vector attacks, multi-vector DDoS attacks use multiple methods simultaneously. They target weaknesses across different network layers to cause more damage and avoid detection. Recent statistics show a surprising 417% rise in multi-vector DDoS attacks. Healthcare systems in countries like India face about 1.9 million of these attacks each year.

Multi-vector DDoS attacks generally unfold in six phases [6] as shown in Figure 1:

1) Malware infects compromised IoT devices.
2) The malware spreads through device-to-device infection to create botnets.
3) Synchronised attacks use different methods (Layer 7 application-based, IP-based, TCP-based, UDP-based, and Service Discovery Protocol-based).
4) Resources are exhausted through bandwidth and processing overload.
5) Legitimate service requests are blocked.
6) Finally, this results in denial-of-service for all legitimate users, regardless of their authenticity.

The evolving nature of these attacks adds to their complexity, with various attack vectors entering and exiting at different strengths throughout the attack [6]. Traditional security solutions struggle to detect and address these threats because they cannot handle the varied nature of attacks.

Current intrusion detection systems (IDSs) fail to effectively address multi-vector attacks in IoMT environments. Traditional signature-based detection methods rely on predefined attack patterns, making them ineffective against new or evolving attack methods. Anomaly-based IDSs can better detect unknown threats by establishing baseline behaviour patterns, but they often produce high false-positive rates and require significant computational power.

Recent research has looked into various machine learning methods for DDoS detection. These include Random Forests, Naïve Bayes, Support Vector Machines, and deep learning techniques such as Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTMs) [7][8]. However, high computational complexity, inadequate real-time processing, and insufficient adaptation to the specific needs of IoMT networks limit the majority of current solutions [9][10].

The limited resources of many IoMT devices further complicate the challenge and hinder the implementation of resource-intensive security measures [11]. Additionally, the urgent nature of healthcare applications necessitates rapid detection and response to attacks, preventing potential harm to patients [1].

 doi:10.20944/preprints202509.0650.v2

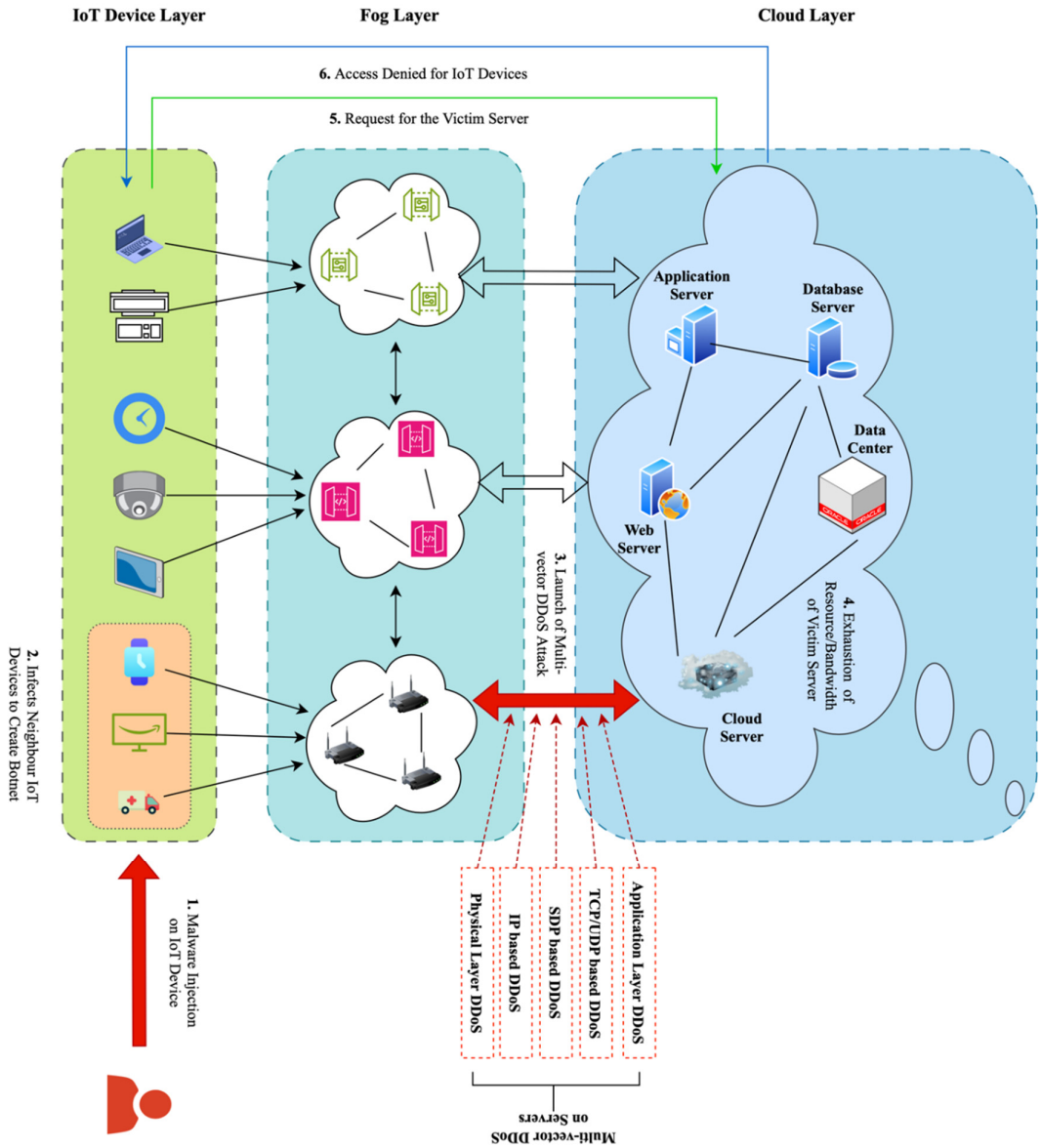


Figure 1. A Visualisation of Multi-vector DDoS Attacks in an Internet of Things Environment.

The urgent need for IoMT security in healthcare underscores the need to develop advanced threat-detection capabilities. Healthcare organisations face a unique risk; a security breach can lead to severe consequences beyond typical data loss or service outages. Recent reports indicate that 99% of healthcare networks have known exploited vulnerabilities, and 53% of connected devices are at risk of multi-vector DDoS attacks.

The need for user-specific detection systems arises from varying skills among healthcare stakeholders. For example, technical users, such as medical staff, require simple binary alerts to indicate the presence of security threats. In contrast, more experienced users need detailed information about specific attack vectors and exploited systems [9]. This situation necessitates the creation of flexible detection frameworks that can provide appropriate information to different user groups.

Moreover, the growing use of mobile healthcare informatics systems adds complexity. These systems must ensure security while allowing for patient mobility and remote monitoring [2]. The integration of Electronic Health Records (EHR) and medical database servers into mobile systems expands the attack surface and requires robust protection measures [12].

 doi:10.20944/preprints202509.0650.v2

This study addresses the gaps in multi-vector intrusion detection for IoMT systems and makes several important contributions.

a. We created an efficient anomaly-based intrusion detection framework using Modified Gated Recurrent Units (MGRU). This framework is designed specifically for multi-vector intrusion detection in resource-limited IoMT environments [9]. The MGRU model outperforms traditional LSTM networks by reducing computational demands while maintaining effective sequence modelling for network traffic monitoring [13].
b. We developed two detection classifiers to meet different user needs. The Binary Label Classifier (BLC) serves non-technical healthcare staff by providing basic notifications of attack presence, while the Multi-Label Classifier (MLC) provides technical users with detailed information on attack vectors and categorisation. This dual-classifier approach ensures that the correct information reaches various groups within healthcare facilities.
c. We conducted thorough testing using current datasets, specifically the CICIoT2023 and CICIoMT2024 datasets, and applied a genetic algorithm-based feature selection to optimise detection performance [14][15]. The testing assesses various performance metrics, including accuracy, precision, recall, F1-score, sensitivity, specificity, false alarm rate (FAR), false positive rate (FPR), Matthews Correlation Coefficient (MCC), model size, training time, and attack detection time [16][17].
d. We evaluate MGRU's performance against previous intrusion detection models, highlighting the benefits of a genetic algorithm-based feature selection approach.

These results suggest that combining genetic algorithms with stacked MGRU networks can significantly enhance intrusion detection efficiency in IoT healthcare settings.

The remainder of the study is structured to provide a detailed discussion of the proposed research methods and findings. Section 2 reviews current literature on intrusion detection systems for IoT-enabled healthcare networks, covering existing methods and identifying research gaps. Section 3 describes the theoretical basis of the improved Gated Recurrent Unit architecture and the enhancements that boost performance for cybersecurity tasks. Section 4 outlines the careful selection and preprocessing of datasets, explaining why we chose the datasets and how we employed a genetic algorithm-based feature selection method. Section 5 explains the overall design of the proposed intrusion detection framework. It covers the architecture, implementation, and integration of the two detection engines. Section 6 presents experimental evaluation results. It compares the proposed system's performance with that of other methods using various metrics and datasets. Section 7 discusses the complexity and computational costs of the proposed framework. It includes scalability challenges and implementation issues. Finally, Section 8 summarises the research findings, addresses limitations, and suggests future research directions to improve IoMT security.

This framework enables a detailed examination of all aspects of the research. It covers theoretical concepts and real-world implementation. Through this, readers gain a complete understanding of the proposed multi-vector intrusion detection framework for IoMT systems.

2. Literature Review

Recent research has focused on attack classification methods, specifically investigating binary versus multi-label classification for healthcare-specific threat detection. Researchers believe that mitigation strategies should not only detect malicious activities but also accurately identify the nature of attack vectors.

Previous efforts in this research area include the creation of realistic healthcare datasets by leading researchers. Experimental setups explicitly tailored for capturing smart healthcare data by Hady et al. [21] and Ahmed et al. [25] yielded two large-scale datasets: WUSTL-EHMS-2020 and ECU-IoHT. These datasets have now emerged as reference tools for all future research, offering realistic healthcare IoT traffic patterns integrated with a range of attack models. Table 1 shows a detailed overview of the related literature.

 doi:10.20944/preprints202509.0650.v2

2.1. Deep Learning Approaches in Healthcare IDS

The ImmuneNet framework, which was introduced by Kumaar et al. [18], is a novel deep learning-based hybrid IDS developed explicitly for smart health systems. The framework uses network traffic capture with CICFlowMeter and Wireshark to detect attacks in Electronic Health Records (EHRs) via binary classification. The system shows promise in integrating various detection methods to enhance the overall security posture in healthcare settings.

Table 1. A Comprehensive Overview of Intrusion Detection Techniques in Smart Healthcare Systems.

Reference	Mechanism	Dataset/Database	Detection Strategy	Attack Classification	Lightweight IDS	User Specific Results
Ariffin et al. [28]	Hybrid feature selection with XGBoost and MaxPoolingID	MQTT attacks dataset	Lightweight IDS for MQTT-enabled IoT	Binary classification	Yes—specifically designed	90% accuracy for both uni/bidirectional flows
Alani [29]	Machine learning-based IDS (IoTProtect)	TON_IoT dataset	ML-based attack detection	Binary classification	Yes—optimised for IoT devices	99.999% accuracy, 0.001% FPR, 0% FNR
Ramaiah and Rahamathulla [30]	LSTM and ML models for Industrial IoT	EdgeIIoT-2021 dataset	Network traffic irregularity detection	Multi-class classification	Designed for IIoT networks	ERT: 99.93%, LSTM: 99.85% accuracy
Adebayo et al. [31]	AI-based IPS/IDS with Light Gradient Boosting Machine	N-BaIoT dataset	Ensemble features complexity reduction	Real-time attack prediction	Yes—gateway-based processing	99.9% accuracy with LightGBM
Guo et al. [32]	ML-based IDS with stacking-ensemble	TON_IoT attack dataset	Ten learning methods evaluation	Binary and multi-class classification	Not specified	Stacking-ensemble: 0.9971 MCC (binary), 0.9909 (multi-class)
Ma et al. [33]	Random Forest with feature selection on edge computing	CIC-DdoS2019 dataset	Edge computing deployment with RF	DDoS attack classification	Yes—edge computing focused	99.99% accuracy, 0.4s prediction time
Ahmed et al. [34]	Multilayer Perceptron (MLP) deep learning	Application-layer DDoS dataset	Packet characteristics inspection	Application-layer DDoS detection	Not specified	98.99% efficiency, 2.11% FPR
Li et al. [35]	Federated Learning with	Industrial IoT distributed datasets	FL-based global model training	Industrial IoT attack detection	Yes—distributed edge approach	98% accuracy, 72% response time reduction

 doi:10.20944/preprints202509.0650.v2

	fog/edge computing					
Vishwakarma and Jain [36]	Honeypot-based ML for malware detection	IoT honeypots data	Dynamic ML model training from honeypots	Zero-day DDoS attacks	Honeypot-based approach	Zero-day attack detection capability
Zeeshan et al. [37]	Protocol-Based Deep Intrusion Detection (PB-DID)	UNSWNB15 and Bot-IoT merged datasets	Deep learning with class imbalance handling	Normal, DoS, and DDoS classification	Protocol-based optimisation	96.3% attack recognition accuracy
Roopak et al. [38]	CNN-LSTM with multi-objective optimisation	CISIDS2017 dataset	DL with Jumping Gene-adapted NSGA-II	DDoS attack classification	Dimensionality reduction applied	99.03% accuracy, reduced training time
Jia et al. [39]	FlowGuard with LSTM and CNN models	CICDDoS2019 and DDoS simulators data	Traffic variation-based detection	DDoS attack identification and classification	Edge server deployment	LSTM: 98.9% identification, CNN: 99.9% classification
Sangodoyin et al. [40]	CART, k-NN, QDA, and GNB algorithms	SDN experimental data (throughput, jitter, response time)	ML techniques for SDN DDoS detection,	DDoS flooding attacks classification	SDN-specific optimisation	CART: 98% accuracy, 5.3x10^6 obs/sec, 12.4ms training
McDermott et al. [41]	Bidirectional LSTM-RNN (BLSTM-RNN)	Home automation botnet data	Word embedding with bidirectional LSTM	Mirai botnet multi-vector attacks	Botnet-specific detection	Superior long-term performance vs standard LSTM

As a complement to this study, Patel et al. [20] proposed a neural network-based intrusion detection system for cloud-based ECG healthcare data. Their method combines a hybrid Tempest algorithm with the Tempest-NN architecture, extending beyond mere intrusion detection to incorporate arrhythmia classification. This two-in-one system demonstrates the potential for healthcare IDS to provide both security and clinical decision-support capabilities.

Recent advances in deep learning for healthcare security have focused on advanced neural architectures. Dina et al. [26] conducted extensive comparisons between Feed-forward Neural Networks (FNN) and Convolutional Neural Networks (CNN) in the context of IoT-based healthcare intrusion detection. Empirical analysis confirmed that FNN architectures outperformed CNNs in specific healthcare attack-detection scenarios, achieving accuracy rates exceeding 97%.

The use of Recurrent Neural Networks (RNNs) has proven especially promising for recognising sequential patterns in healthcare IoT networks. Almutairi and Alshargabi [27] developed RNN-based detection mechanisms trained using the NSL-KDD dataset and demonstrated 87% accuracy in multi-class attack classification. Their study identified the need for further optimisation to enhance detection capabilities.

 doi:10.20944/preprints202509.0650.v2

2.2. Lightweight IDS Solutions for Resource-Constrained Environments

The difficulty of implementing IDS solutions on resource-limited IoMT devices has driven extensive research into lightweight detection mechanisms. Ariffin et al. [28] proposed a hybrid feature selection mechanism using XGBoost and MaxPoolingID techniques specifically for MQTT-based IoT systems. Their lightweight IDS measured 90% accuracy in both unidirectional and bidirectional traffic flow scenarios, with bidirectional analysis performing best in all evaluation metrics.

Iwendi et al. [22] tackled feature optimisation issues using a genetic algorithm, this time applied to the KSL-KDD dataset for multi-label attack vector classification. Their method demonstrated significantly improved feature selection efficiency, reducing computation overhead without compromising detection accuracy. This paper laid the groundwork for follow-up research on evolutionary optimisation methods for healthcare IDS.

Cross-validation frameworks and statistical significance testing have become the standard for ensuring robust performance comparisons. Recent research [42] has highlighted the need to address class imbalance and avoid overfitting through sophisticated preprocessing methods, such as the Synthetic Minority Over-sampling Technique (SMOTE) and Quantile Transformer standardisation.

The deployment of IDS in conjunction with edge computing paradigms has become a crucial area of research. Ma et al. [33] deployed Random Forest classifiers with feature selection functions on edge computing devices in Software Defined Networking (SDN) settings. The performance of their system was excellent, achieving 99.99% accuracy and 0.4-second prediction times, proving the practicability of real-time threat detection at network edges.

Li et al. [35] proposed FLEAM, a federated learning-enhanced architecture to mitigate DDoS attacks in Industrial IoT networks. Their distributed system achieved a detection accuracy of 98% by reducing mitigation response time by 72% and increasing the cost of attack by 2.7 times. This study shows that organisations can implement collaborative defence methods across dispersed healthcare networks.

2.3. Multi-Vector Attack Detection and Classification

Modern healthcare networks are increasingly vulnerable to advanced multi-vector DDoS attacks that exploit weaknesses across multiple network layers simultaneously. Ahmed et al. [34] developed a multilayer perceptron (MLP) deep learning model for detecting application-layer DDoS attacks, emphasising analysis of packet attributes, such as HTTP frame lengths, IP address distributions, and port mapping patterns. Their method achieved a 98.99% detection efficiency with a false-positive rate of 2.11%.

The FlowGuard system proposed by Jia et al. [39] is a milestone in traffic variation-based DDoS detection. It is an intelligent edge defensive mechanism that utilises two machine learning models: LSTM networks for attack detection (with 98.9% accuracy) and CNN architectures for attack classification (with 99.9% accuracy). The system adequately meets IoT delay requirements when implemented on edge servers with upgraded computational power.

Protocol-Based Deep Intrusion Detection (PB-DID), proposed by Zeeshan et al. [37], addresses the complexity of combining multiple datasets to build robust training environments. They blend the UNSWNB15 and Bot-IoT datasets, applying methods to handle class imbalance and prevent overfitting. The system achieved 96.3% attack-detection accuracy across the normal, DoS, and DDoS traffic classes.

Sangodoyin et al. [40] conducted a comprehensive analysis of machine learning algorithms for DDoS flooding attacks in SDN frameworks, comparing Classification and Regression Tree (CART), k-Nearest Neighbors (k-NN), Quadratic Discriminant Analysis (QDA), and Gaussian Naïve Bayes (GNB). An empirical analysis using real-time experimental data, including throughput, jitter, and response time metrics, showed that CART was the best, achieving 98% prediction accuracy, a processing rate of 5.3 ×10 observations per second, and a training time of 12.4 ms.

 doi:10.20944/preprints202509.0650.v2

2.4. Ensemble and Hybrid Learning Approaches

Ensemble learning techniques enhance detection effectiveness by combining algorithms. Basharat et al. [23] applied ensemble machine learning techniques to intelligent healthcare systems, achieving the highest attack-detection rates with AdaBoost classifiers across multiple models. Their extended evaluation framework established standards for ensemble performance in healthcare application-based attack scenarios.

Guo et al. [32] conducted comprehensive testing of 10 learning techniques on the TON_IoT attack dataset, with stacking-ensemble models performing best. Their method yielded Matthews Correlation Coefficient scores of 0.9971 for binary classification and 0.9909 for multi-class classification, demonstrating the strong efficacy of ensemble methods in recognising intricate attack patterns.

The integration of multiple detection paradigms into a single framework has proven efficient for handling diverse threat profiles. Alani [29] designed IoTProtect, an IDS based on machine learning, achieving remarkable performance metrics, including a 99.999% attack detection rate, a 0.001% false-positive rate, and a 0% false-negative rate. The system's success is due to comprehensive ensemble feature-complexity reduction schemes, coupled with real-time processing at the IoT gateway level.

Roopak et al. [38] proposed an intrusion detection system that integrated CNN and LSTM architectures with multi-objective optimisation methods. Their system utilised Jumping Gene-adapted NSGA-II algorithms for dimension reduction, achieving an accuracy of 99.03%. Additionally, five-fold cross-validation strategies enabled a drastic reduction in training time.

2.5. Specialised Detection for Healthcare Applications

Healthcare IDS studies have increasingly emphasised the integration of medical and biometric data sources to improve threat detection performance. Hady et al. [21] established robust testbeds for Enhanced Healthcare Monitoring Systems (EHMS) that capture both network traffic and patient biometric data. Their validation against the WUSTL-EHMS-2020 MITM dataset demonstrated the viability of multimodal data fusion for realistic healthcare threat detection scenarios.

Tuteja et al. [24] investigated logistic regression-based methods for healthcare intrusion detection, integrating LSTM networks for recognising attack patterns. Their research provided building blocks for integrating clinical data patterns with network security monitoring, demonstrating the potential for healthcare-specific threat intelligence.

The migration of healthcare systems to cloud-based environments has created the need for specialised security methods. Saif et al. [19] applied hybrid IDS solutions to IoT-based smart healthcare on AI-based cloud medical servers. Their analysis of six hybrid machine learning methods revealed that Decision Tree methods are optimal for cloud-based healthcare threat detection, setting standards for cloud security in medical settings.

Sophisticated cloud security studies have investigated automated threat response mechanisms. Adebayo et al. [31] proposed AI-driven intrusion prevention systems using Light Gradient Boosting Machine (LightGBM) classifiers for real-time IoT network defence. Their system achieved 99.9% accuracy through ensemble feature complexity reduction, demonstrating the potential of autonomous threat mitigation in healthcare cloud environments.

2.6. Emerging Threats and Advanced Detection Techniques

The healthcare industry is under growing pressure from zero-day attacks and changing threat environments. Vishwakarma and Jain [36] proposed honeypot-based machine learning models for defence against IoT botnet DDoS attacks. It supports dynamic model updates based on honeypot-collected data, enabling detection and neutralisation of unknown attack patterns.

McDermott et al. [41] designed Bidirectional Long Short-Term Memory Recurrent Neural Networks (BLSTM-RNN) for detecting botnets in home automation systems. Their framework used

 doi:10.20944/preprints202509.0650.v2

word embeddings to tokenise attack packets, achieving better long-term performance than regular LSTM methods for detecting multi-vector attacks associated with Mirai botnets.

Healthcare networks are increasingly coexisting in Industrial IoT (IIoT) environments, requiring targeted security methods. Ramaiah and Rahamathulla [30] proposed robust network intrusion detection systems for IIoT networks and attained 99.93% detection with Extremely Randomised Trees (ERT) and 99.85% detection with LSTM-based methods using the EdgeIIoT-2021 dataset.

The integration of blockchain and advanced AI is a promising approach to enhancing the security of key healthcare infrastructure. Current studies have investigated the fusion of federated learning with fog/edge computing frameworks, resulting in substantial improvements in detection accuracy, reduced response times, and increased attack costs for attackers.

The literature review identifies a thorough transformation in healthcare IDS research, from basic signature-based detection to advanced machine learning and deep learning techniques. Recent studies have shown impressive results in detection rates, with various methods achieving more than 99% accuracy across different test scenarios. Nevertheless, the complexity of current healthcare IoT environments and the development of sophisticated multi-vector attacks justify further research in lightweight, adaptive, and user-oriented detection methodologies.

The creation of realistic datasets and standardised testing techniques has dramatically improved the quality and comparability of educational assessments. The availability of complete datasets, such as CICIoT2023 and CICIoMT2024, enables the realistic testing of IDS performance in various healthcare scenarios.

3. Preliminaries

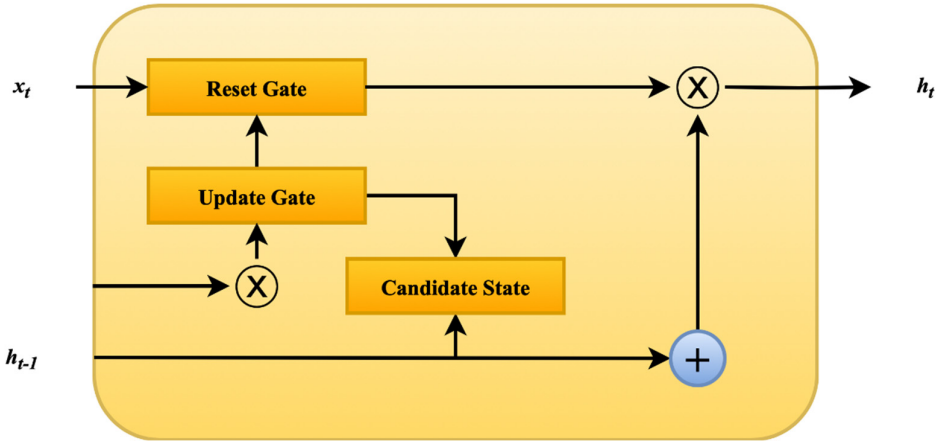
In designing anomaly-based intrusion detection systems (IDSs) for multi-vector intrusion detection in IoT-enabled healthcare facilities, selecting an appropriate deep learning architecture is crucial. While there are several recurrent neural network (RNN) models, LSTM, Transformers, and Autoencoders have each shown superiority in different domains. These models exhibit significant disadvantages in healthcare facilities with time-sensitive operations. Although powerful at capturing long-range dependencies, LSTM networks consume significant computational resources and require longer training times, making them not ideal for quick deployment in healthcare applications where real-time response and resource conservation are priorities. Transformers require substantial computational power due to their self-attention mechanism. Their complexity and susceptibility to catastrophic forgetting can interfere with sustained accuracy and stability in streaming, real-time scenarios common in IoT healthcare data. Although autoencoders have the potential to perform unsupervised anomaly detection, they are prone to overfitting and data loss, which can compromise reliability in critical and sensitive areas, such as medical informatics.

Consequently, the above-mentioned architectures are challenging to manage in resource-limited, latency-critical, and adaptive healthcare networks.

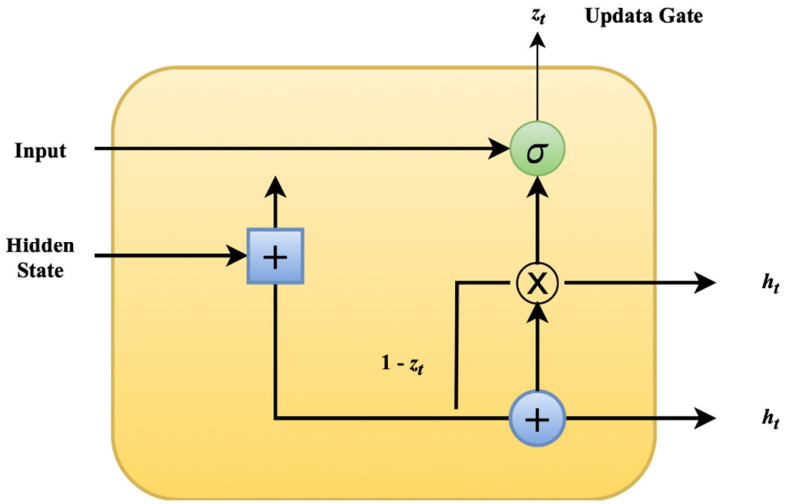
3.1. Gated Recurrent Unit (GRU)

GRU is a better alternative because it is simpler to implement, converges faster, and requires less memory than the LSTM and Transformer models. GRU effectively captures sequential dependencies in time-series data, addressing the vanishing gradient problem and reducing computational overhead. These properties position GRU as an ideal choice for real-time anomaly detection in the healthcare environment, where both speed and accuracy are critical. Figure 2 (a) shows the architecture of a standard GRU cell containing a reset gate, an update gate, and a candidate state. Figure 2 (b) illustrates the design of an MGRU cell with an abandoned reset gate.

 doi:10.20944/preprints202509.0650.v2



(a) Standard GRU Cell



(b) Modified GRU Cell

Figure 2. Standard GRU and Modified GRU Architecture.

The baseline GRU cell uses two gating mechanisms—the reset gate and the update gate—that control information flow and retain practical context over time.

Standard GRU Cell Mathematical Formulation

Let x_t be the input vector for the current time step t, and h_{t-1} be the previous hidden state:

- **Update Gate (z_t):** This gate determines the amount of the past hidden state to retain for the current hidden state. It is calculated by:

$$z_t = \sigma(W_z x_t + U_z h_{t-1} + b_z) \quad (1)$$

- **Reset Gate (r_t):** This gate controls how much of the past hidden state to forget when calculating the candidate hidden state. It is calculated by:

$$r_t = \sigma(W_r x_t + U_r h_{t-1} + b_r) \quad (2)$$

- **Candidate Activation ($\tilde{h}_t$):** The reset gate will add this new information.:

$$\tilde{h}_t = \tanh(W_h x_t + U_h(r_t \odot h_{t-1}) + b_h) \quad (3)$$

- **Hidden State Update (h_t):** The new hidden state is a weighted sum of the old hidden state and the candidate hidden state, governed by the update gate:

 doi:10.20944/preprints202509.0650.v2

$$h_t = (1 - z_t) \odot h_{t-1} + z_t \odot \tilde{h}_t \quad (4)$$

where σ is the sigmoid activation function, $\odot$ denotes element-wise multiplication, and W, U, and b are the learnable parameters for each gate.

3.2. Modified GRU Architecture

To further reduce network complexity in IoT-based healthcare settings, the GRU is simplified by removing the reset gate. This design modification reduces the number of parameters and calculations, making the network even lighter and faster, and is widely known as the Modified GRU (MGRU).

MGRU Cell Mathematical Formulation

The MGRU works as follows:

- **Update Gate (z_t):** Similar to the regular GRU, it regulates the proportion of keeping the past hidden state and integrating new information:

$$z_t = \sigma(W_z x_t + U_z h_{t-1} + b_z) \quad (5)$$

- **Candidate Activation ($\tilde{h}_t$):** Without a reset gate, the candidate hidden state is calculated directly from the last hidden state:

$$\tilde{h}_t = \tanh(W_h x_t + U_h h_{t-1} + b_h) \quad (6)$$

- **Hidden State Update (h_t):** Calculate the latest hidden state as:

$$h_t = (1 - z_t) \odot h_{t-1} + z_t \odot \tilde{h}_t \quad (7)$$

Eliminating the reset gate simplifies the gating structure of the MGRU, resulting in faster training, reduced computational requirements, and on-device deployability in healthcare IoT applications.

4. Dataset Selection and Preparation

The process of building efficient intrusion detection systems for IoT-enabled healthcare infrastructure requires a systematic inspection and the selection of suitable benchmark datasets that accurately reflect modern threat scenarios. This section provides an in-depth assessment of current attack datasets to evaluate their suitability for multi-vector intrusion detection in healthcare IoT networks. The choice factors prioritise datasets with heterogeneous attack vectors, realistic traffic patterns, and complete labelling schemes that support both binary and multi-class classification.

Modern cybersecurity research has yielded numerous benchmark datasets for testing intrusion detection systems across various network settings. Nonetheless, the distinct nature of healthcare IoT networks, including resource constraints, communication protocols, and time-criticality, requires custom datasets that accurately reflect the intricacies of medical device communication and potential attack behaviour. This review categorises existing datasets into healthcare-specific and general IoT datasets and discusses their suitability for training effective multi-vector intrusion detection models.

4.1. Healthcare-Specific Dataset Analysis

The healthcare field presents specific security needs that require specialised datasets to capture network traffic and communication patterns among medical devices. Researchers have created various large-scale healthcare datasets to meet these needs, each with different properties and restrictions for multi-vector DDoS detection.

Initially developed for intensive care unit monitoring, the HiRID dataset is primarily centred on patient physiological data rather than network security-related data. Although applicable to research in medical informatics, HiRID does not encompass the network traffic patterns and attack scenarios necessary to train robust intrusion detection models [43]. Ahmed et al. [25] created this dataset, which is a valuable addition to healthcare IoT security research. The ECU-IoHT dataset comprises realistic

 doi:10.20944/preprints202509.0650.v2

traffic patterns from health devices, including both benign communications and various types of attacks. However, its drawback is that the diversity of DDoS attack vectors is limited, making it inadequate for extensive multi-vector DDoS detection training.

Designed by Hady et al. [21], the WUSTL-EHMS-2020 dataset encompasses both network traffic and biometric patient data, providing a comprehensive view of healthcare system communications. It contains scenarios involving Man-in-the-Middle (MITM) attacks and some healthcare-related threat patterns. Although it has a realistic strategy for collecting healthcare data, WUSTL-EHMS-2020 lacks the same range of DDoS attack vectors to train a robust multi-vector detection system. Researchers dedicate the MIT-BIH Arrhythmia Database to cardiac rhythm analysis and arrhythmia detection. Although useful for medical device security studies, it lacks network traffic or DDoS attack patterns, making it less suitable for network-based intrusion detection systems [44].

The CICIoMT2024 dataset [15] is a significant contribution towards healthcare IoT security research, tailored to overcome the shortcomings of existing healthcare datasets. The Canadian Institute for Cybersecurity has designed a comprehensive dataset to emulate real IoMT network traffic, utilising a wide range of communication protocols in healthcare settings. CICIoMT2024 consists of 18 unique attack types targeting a testbed comprising 40 IoMT devices, 25 physical and 15 simulated. This holistic strategy ensures the realistic simulation of modern healthcare IoT settings while providing sufficient attack diversity to train robust models.

The data collects traffic from multiple healthcare communication protocols, including Wi-Fi, MQTT (Message Queuing Telemetry Transport), and Bluetooth Low Energy (BLE). This multi-protocol data collection reflects the heterogeneous nature of contemporary healthcare IoT networks, in which devices use different communication standards tailored to their specific needs. The CICIoMT2024 dataset classifies the attacks into five main categories: Distributed Denial of Service (DDoS), Denial of Service (DoS), Reconnaissance (Recon), MQTT-specific attacks, and spoofing attacks. The robust classification framework supports both binary classification (benign vs. malicious) and fine-grained multi-class attack identification.

4.2. General IoT Dataset Evaluation

Emphasising Industrial IoT settings, the WUSTL-IIOT-2021 dataset has multiple attack scenarios attacking industrial control systems. Although useful for industrial security analysis, the dataset's focus on industrial protocols and attack patterns restricts its direct application to healthcare IoT settings [45]. As one of the first intrusion detection datasets, the DARPA 1999 dataset set significant research benchmarks for security. Due to its age and focus on traditional network environments, it is inadequate for today's IoT security needs, especially regarding healthcare-specific threats and current communication protocols [46].

Cybersecurity studies have extensively used this dataset, which contains various attack types. Although it comprises DDoS attack traffic, UNSW-NB15 does not provide the detailed categorisation of various DDoS attack vectors required for training a multi-vector detection system [48]. CICIDS2017 and CSE-CIC-IDS2018 are modern intrusion detection datasets that provide comprehensive network attack scenarios with accurate labelling. Although they include DDoS traffic, the datasets target general network environments instead of IoT-specific communication patterns and limitations [51][52].

Formulated explicitly to attack research, the CICDDoS2019 dataset includes attack vectors such as Portmap, LDAP, NetBIOS, and volumetric attacks. The rich labelling and diversity of attacks make CICDDoS2019 particularly suitable for multi-vector DDoS attack detection training, but it lacks a healthcare-related context [53]. As a landmark in IoT security research, the CICIoT2023 dataset comprises traffic from 105 IoT devices across 33 distinct attack types, categorised into seven major classes: DDoS, DoS, Reconnaissance, Web-based, Brute Force, Spoofing, and Mirai attacks. The dataset's comprehensive coverage of attacks and simulation of a realistic IoT environment makes it eminently suitable for training robust intrusion detection systems [14].

 doi:10.20944/preprints202509.0650.v2

The BoT-IoT, NSL-KDD, and N-BaIoT datasets are exemplary contributions to IoT security research, but they have shortcomings in multi-vector attack detection. BoT-IoT focuses solely on botnet behaviours. In contrast, NSL-KDD is an enhanced version of the original KDD dataset, but it lacks modern attack patterns. Additionally, N-BaIoT targets specific IoT device weaknesses rather than overall multi-vector attacks [47][49][50].

4.3. Dataset Selection Methodology

Healthcare IoT settings require considering appropriate datasets for multi-vector intrusion detection. Key conditions include diversity of attack vectors, protocol coverage, labelling quality, dataset size, and relevance to healthcare IoT contexts, as outlined in Table 2.

Effective multi-vector intrusion detection requires training datasets that encompass a range of attack types, which can occur concurrently or in sequence. The chosen datasets should include representations of Layer 3 (network layer) attacks, such as ICMP floods; Layer 4 (transport layer) attacks, including SYN floods and UDP floods; and Layer 7 (application layer) attacks, such as HTTP-based DDoS. IoT networks in healthcare use various communication protocols, depending on device type and application. Sampled datasets should reflect traffic across protocols commonly used in healthcare settings, such as regular IP-based communications, MQTT for low-bandwidth device messaging, and Bluetooth for personal health devices.

Strong model training requires high-quality labels that support both binary classification (attack/benign) and fine-grained multi-class classification, enabling the detection of specific attack types. The labelling scheme must be consistent, precise, and exhaustive for all attack scenarios.

Focused on **CICIoT2023** and **CICIoMT2024** as the main datasets for the development of multi-vector intrusion detection systems based on extensive analysis of accessible datasets against selection criteria, this study:

CICIoT2023: The dataset provides comprehensive IoT attack coverage, including 33 attack types across seven classes, including a wide variety of DDoS attack variants, as shown in Figure 3(a). The dataset's size (105 devices) and the diversity of attacks make it suitable for training effective detection models that can handle diverse IoT environments.

CICIoMT2024: Tailored for research in healthcare IoT security, this dataset meets the distinct needs of medical device networks. Its emphasis on healthcare-relevant protocols and attack scenarios provides valuable context for developing healthcare-specific intrusion detection systems. The dataset provides comprehensive IoT attack coverage, encompassing 20 distinct attack types across six classes, including a diverse range of DDoS attack variants, as illustrated in Figure 3(b).

Table 2. Analysis of the Benchmark Dataset on IoT Networks.

Dataset	Data Source	Number of Features	Labels	Suitability for Multi-vector Intrusion Detection
HiRID [43]	Healthcare data	18	Contains demographic information of 34,000 patents, but no attack data is included	Not Suitable
ECU-IoHT [25]	Healthcare data	6	ARP Spoofing, No Attack, Nmap Port Scan, Smurf Attack, DoS Attack	Not Suitable
WUSTL EHMS 2020 [21]	Healthcare data	44	Normal, Attack	Not Suitable
MIT-BIH Arrhythmia database [44]	Healthcare data	47	Benign, Malicious	Not Suitable

 doi:10.20944/preprints202509.0650.v2

CICIoMT2024 [15]	Healthcare data	46	ARP_Spoofing, ICMP, UDP, SYN TCP, MQTT, Recon, Benign	**Fully Suitable**
WUSTL-IIOT-2021 [45]	IoT data	41	Command Injection, DoS, Reconnaissance, Backdoor, Normal	Not Suitable
DARPA 1999 [46]	IoT data	41	Probe, DoS, R2L, U2R	Not Suitable
BoT-IoT [47]	IoT data	29	DoS-HTTP, DoS-TCP, DoS-UDP, Benign	Partially Suitable
UNSW-NB15 [48]	IoT data	49	Normal, Attack	Not Suitable
NSL-KDD [49]	IoT data	41	TCP, UDP, ICMP	Partially Suitable
N-BaIoT [50]	IoT data	115	Scan, Ack, Syn, UDP, UDPplain	
CICIDS2017 [51]	IoT data	80	Brute Force FTP, Brute Force SSH, DoS, Heartbleed, Web Attack, Infiltration, Botnet, and DDoS	Not Suitable
CSE-CIC-IDS2018 [52]	IoT data	78	Benign, DDoS, DoS, Brute Force, Botnet, Infiltration, Web attack	Not Suitable
CICDDoS2019 [53]	IoT data	88	BENIGN, UDP-Lag, TFTP, Portmap, DNS, MSSQL, LDAP, NetBIOS, NTP, SSDP, SNMP, Syn and UDP	**Fully Suitable**
CICIoT2023 [14]	IoT data	47	PSHACKFlood, ICMP, UDP, Benign, ICMPFragmentation, SYN, SlowLoris, HTTP, SynonymousIPFlood, RSTFINFlood, TCP, ACKFragmentation, UDPFragmentation	**Fully Suitable**

4.4. Attack Label Selection and Categorisation

This study examines the most common DDoS attack vectors found in CICIoT2023, considering the comprehensive set of attack types:

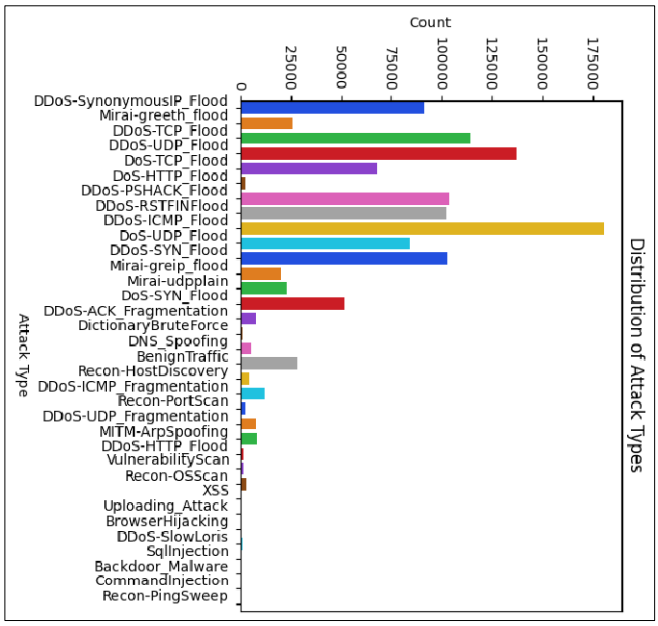
Portmap: Exploiting Network File System (NFS) portmapper services for amplification attacks
LDAP: Lightweight Directory Access Protocol amplification attacks
NetBIOS: Network Basic Input/Output System-based DDoS attacks
SlowLoris: Application-layer DDoS attacks targeting web servers
SYN: TCP SYN flood attacks overwhelm connection establishment processes
UDP: User Datagram Protocol flood attacks consume bandwidth and processing resources
ICMP: Internet Control Message Protocol flood attacks
TCP: General TCP-based flooding attacks
HTTP: Hypertext Transfer Protocol-based application layer attacks

The CICIoMT2024 dataset offers healthcare-related attack instances with the following chosen labels used for training of multi-vector intrusion detection:

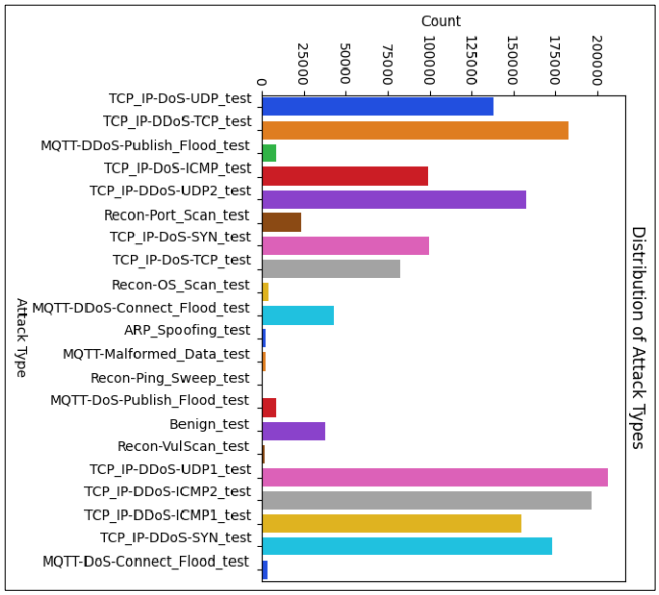
ICMP: Healthcare device-targeted ICMP flooding attacks
UDP: UDP-based attacks against medical device communications
SYN: SYN flood attacks targeting healthcare service availability
TCP: TCP-based attacks disrupting medical data transmission
MQTT: Message Queuing Telemetry Transport protocol-specific attacks
Recon: Reconnaissance attacks gather intelligence for subsequent attacks
Benign: Normal healthcare IoT traffic patterns

 doi:10.20944/preprints202509.0650.v2

Both datasets contain multiple common attack categories (Benign, SYN, TCP, UDP, ICMP), facilitating cross-dataset validation and robust model assessment across various IoT settings. The overlap offers prospects of transfer learning and overall performance evaluation.



(a)



(b)

Figure 3. Different Attack Types in (a) CICIoT2023, and (b) CICIoMT2024.

4.5. Data Preprocessing and Preparation Pipeline

Efficient machine learning model construction requires thorough data preprocessing to achieve optimal training performance and model accuracy. The preprocessing pipeline for CICIoT2023 and CICIoMT2024 datasets involves several phases aimed at addressing data quality issues, optimising

 doi:10.20944/preprints202509.0650.v2

features, and preparing the classification scheme. Figure 4 shows the preprocessing steps for the CICIoT2023 and CICIoMT2024 datasets.

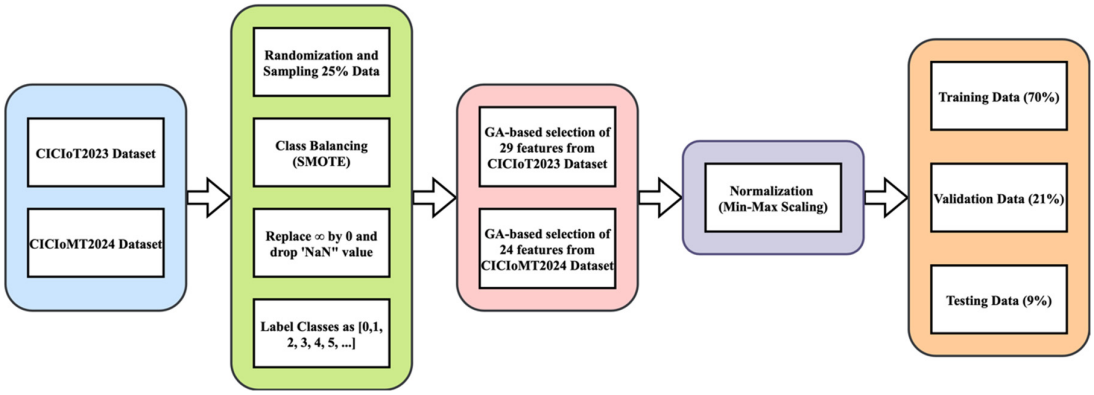


Figure 4. A Visualisation of Preprocessing Steps of CICIoT2023 and CICIoMT2024 Datasets.

Network traffic data often contains missing values due to measurement failures, hardware faults, or communication failures. The preprocessing pipeline detects features with 'NaN' (Not a Number) values and applies the appropriate handling techniques. We impute missing values in categorical features using the mean, preserving the most frequent category. Numerical features having missing values are subject to mean imputation to reduce the effect of outliers on the replaced values. The preprocessing pipeline conducts rigorous data validation checks to detect and resolve inconsistencies in feature values, timestamp ordering, and labels. We use manual verification or automatic repair to mark inconsistent records.

4.5.1. Feature Engineering and Selection

Randomisation and Sampling: To prevent bias in model training, the preprocessing pipeline uses randomisation methods while sampling the data. Researchers intentionally omitted specific rows to ensure randomisation while maintaining a representative sample of all attack types and typical traffic patterns.

Feature Categorisation: The attack types in the datasets are classified into distinct attack categories, as shown in Figure 6, based on their operational similarities and effects on IoT healthcare systems. The classes represent shared characteristics, such as resource exhaustion, information gathering, protocol exploitation, and identity deception, to enable more effective analysis and detection. The classification matches the design of the datasets to support both binary (benign vs. attack) and multi-class (specific attack types) intrusion detection.

Genetic Algorithm-Based Feature Selection: Building on conventional feature selection techniques, this study utilises genetic algorithm (GA) optimisation to select a subset of features. The GA method systematically explores the feature space to find the best feature combination that yields the highest classification performance while minimising computational cost, as shown in Algorithm 1. Figure 5 illustrates the features selected by GA for binary classification and multi-label classification from the CICIoT2023 and CICIoMT2024 datasets.

The genetic algorithm implementation employs the following parameters:

Population Size: 10 individuals representing different feature subsets

Selection Method: Tournament selection with a tournament size of 3

Crossover Rate: 0.5 for generating new feature combinations

Mutation Rate: 0.2 for introducing feature variation

Fitness Function: LightGBM model across validation sets

Termination Criteria: 5 generations or convergence threshold achievement

 doi:10.20944/preprints202509.0650.v2

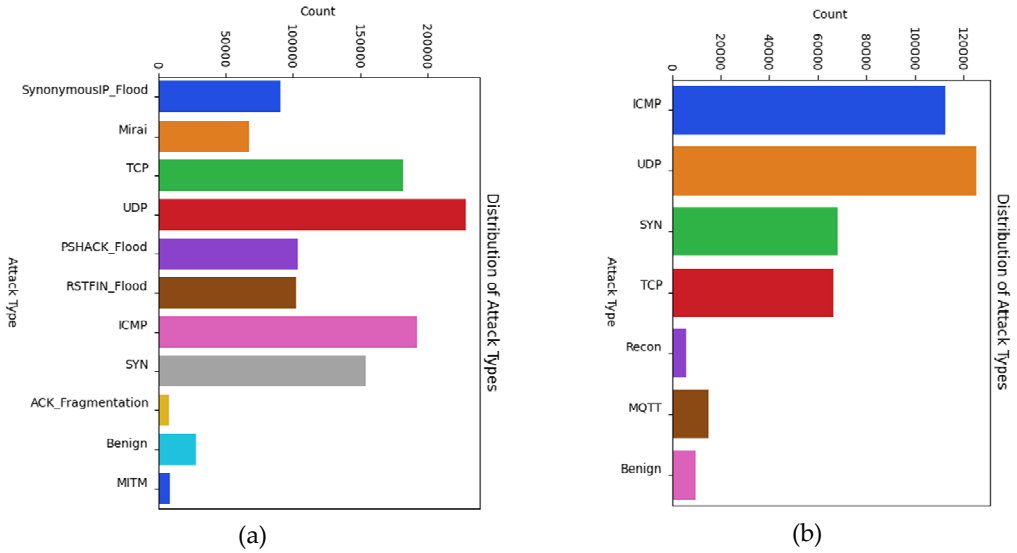
flow_duration	Header_Length	Protocol Type	Duration	Srate	Drate
fin_flag_number	syn_flag_number	rst_flag_number	psh_flag_number	ack_flag_number	ece_flag_number
cwr_flag_number	ack_count	syn_count	fin_count	urg_count	HTTPS
DNS	UDP	ARP	IPv	Tot sum	Min
Max	AVG	Tot size	IAT	Number	

(a) Selected Features from CICIoT2023

Header_Length	Rate	Srate	psh_flag_number	ack_flag_number	cwr_flag_number
syn_count	rst_count	HTTP	HTTPS	Telnet	SMTP
IRC	TCP	ICMP	IGMP	LLC	Tot sum
AVG	Std	Tot size	IAT	Radius	Variance

(b) Selected Features from CICIoMT2024

Figure 5. Features Selected from CICIoT2023 and CICIoMT2024 datasets using GA.



(a) (b)

Figure 6. Different Attack Categories with Majority and Minority classes for (a) CICIoT2023, and (b) CICIoMT2024 Datasets.

 doi:10.20944/preprints202509.0650.v2

4.5.2. Dataset Balancing and Augmentation

Class Imbalance Assessment: Real-world network traffic datasets are generally highly class-imbalanced, with benign traffic far outnumbering attack occurrences. The preprocessing pipeline performs a thorough class distribution analysis to measure the severity of imbalance and determine suitable balancing measures.

Algorithm 1 Genetic Algorithm for Feature Selection

Ensure: Training data matrix $\boldsymbol{X} \in \mathbb{R}^{\boldsymbol{N}\times\boldsymbol{D}}$, labels $\boldsymbol{Y} \in \{\boldsymbol{0}, \ldots, \boldsymbol{K}-\boldsymbol{1}\}^{\boldsymbol{N}}$

Require: Population size P, number of generations G, crossover probability p_c, mutation probability p_m, tournament size T

1. Initialize Population

1.1. For each individual $i = 1$ to P, generate a random bitmask

$$\boldsymbol{s}^{(\boldsymbol{i})} \in \{\boldsymbol{0}, \boldsymbol{1}\}^{\boldsymbol{D}}$$

where $s_j^{(i)} = 1$ indicates feature j is selected.

2. Evaluate Initial Fitness

2.1. For each individual $s^{(i)}$:

Form reduced dataset $\boldsymbol{X}' = \boldsymbol{X}\left[:, \left\{\boldsymbol{j} \mid \boldsymbol{s}_{\boldsymbol{j}}^{(\boldsymbol{i})} = \boldsymbol{1}\right\}\right]$

Train a lightweight classifier on (X', Y).

Compute validation accuracy $F(s^{(i)})$.

3. Evolutionary Loop

For generation $g = 1$ to G:

3.1. Selection (Tournament)

For each of P offspring:

Randomly pick T individuals from the current population.

Parent p := individual with the highest fitness among those T.

3.2. Crossover

Pair up selected parents at random.

For each pair (p_a, p_b):

With probability p_c, choose two crossover points $c_1 < c_2$.

Swap bits between c_1 and c_2 to form two children.

Otherwise, children = exact copies of parents.

3.3. Mutation

For each bit in each child, flip the bit with probability p_m.

3.4. Fitness Evaluation

For each new child s:

Compute $F(s)$ as in step 2.

3.5. Elitism & Replacement

 doi:10.20944/preprints202509.0650.v2

Combine the current population and offspring.

Sort all $2P$ individuals by fitness F.

Keep the top P individuals for the next generation.

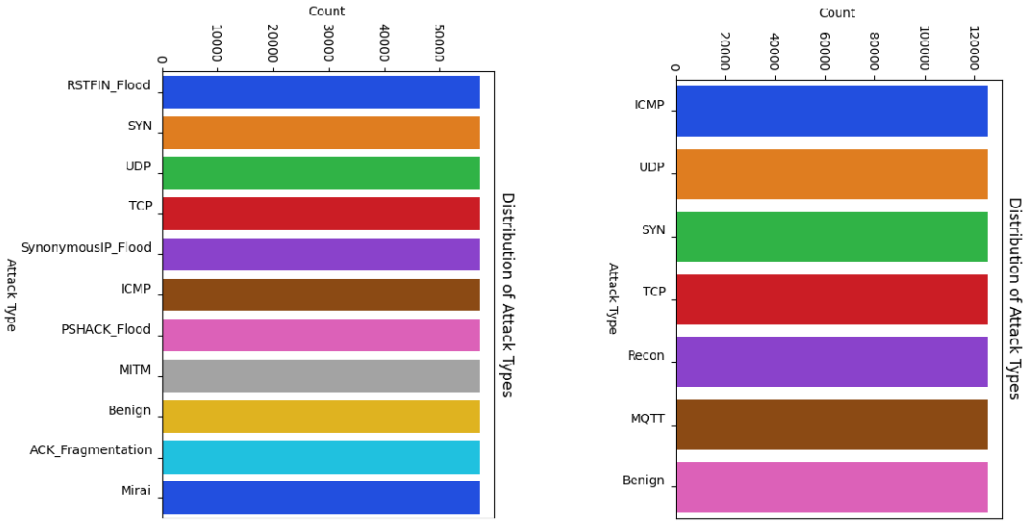
4. Return Best Mask

Let $s^* = \arg max_i F(s^{(i)})$

Output the feature index set

$$S = \{j \mid s_j^* = 1\}$$

Synthetic Minority Oversampling Technique (SMOTE): The pipeline uses SMOTE to introduce synthetic minority-class samples to address class imbalance, effectively increasing their representation, as depicted in Figure 7. It creates new attack samples by interpolating between existing attack instances to enhance the model's training on rare attack modes.



(a) CICIoT2023 (b) CICIoMT2024

Figure 7. Different Attack Categories with Oversampling Minority Classes.

5. Proposed Framework

The rapid exponential growth of Internet of Medical Things (IoMT) devices in modern healthcare settings has revolutionised the delivery of medical services while simultaneously introducing unprecedented cybersecurity risks. Interconnected medical devices spanning implantable biosensors, wearable health monitors, and more form extensive attack surfaces that malicious actors can target to launch sophisticated multi-vector intrusion attacks on critical healthcare infrastructure.

The proposed framework addresses the unique security challenges of IoMT environments with a robust, dual-type intrusion detection system designed explicitly for healthcare. This novel solution integrates the computational power of Modified Gated Recurrent Units (MGRU) with a GA-based feature selection approach.

Modern healthcare networks are becoming increasingly vulnerable to advanced attack vectors that exploit the inherent weaknesses in resource-limited medical devices. The high availability and accessibility features of IoMT devices significantly increase the likelihood and potential severity of multi-vector attacks on smart healthcare systems. Such attacks can disrupt critical patient care services, expose sensitive medical information, and even endanger patients' safety.

 doi:10.20944/preprints202509.0650.v2

The Internet of Medical Things ecosystem is a highly interconnected system of medical devices, communication infrastructure, and data-processing systems that work together to enable sophisticated healthcare service delivery. To develop effective security mechanisms that safeguard patient data and maintain service continuity, it is crucial to understand the flow of data and communication patterns within this ecosystem.

The IoMT architecture comprises several layers of interconnected components with specific functions within the healthcare data-gathering and processing pipeline. Designers create these devices, gateways, servers, and interfaces to fulfil the varied needs of healthcare stakeholders, as illustrated in Figure 8.

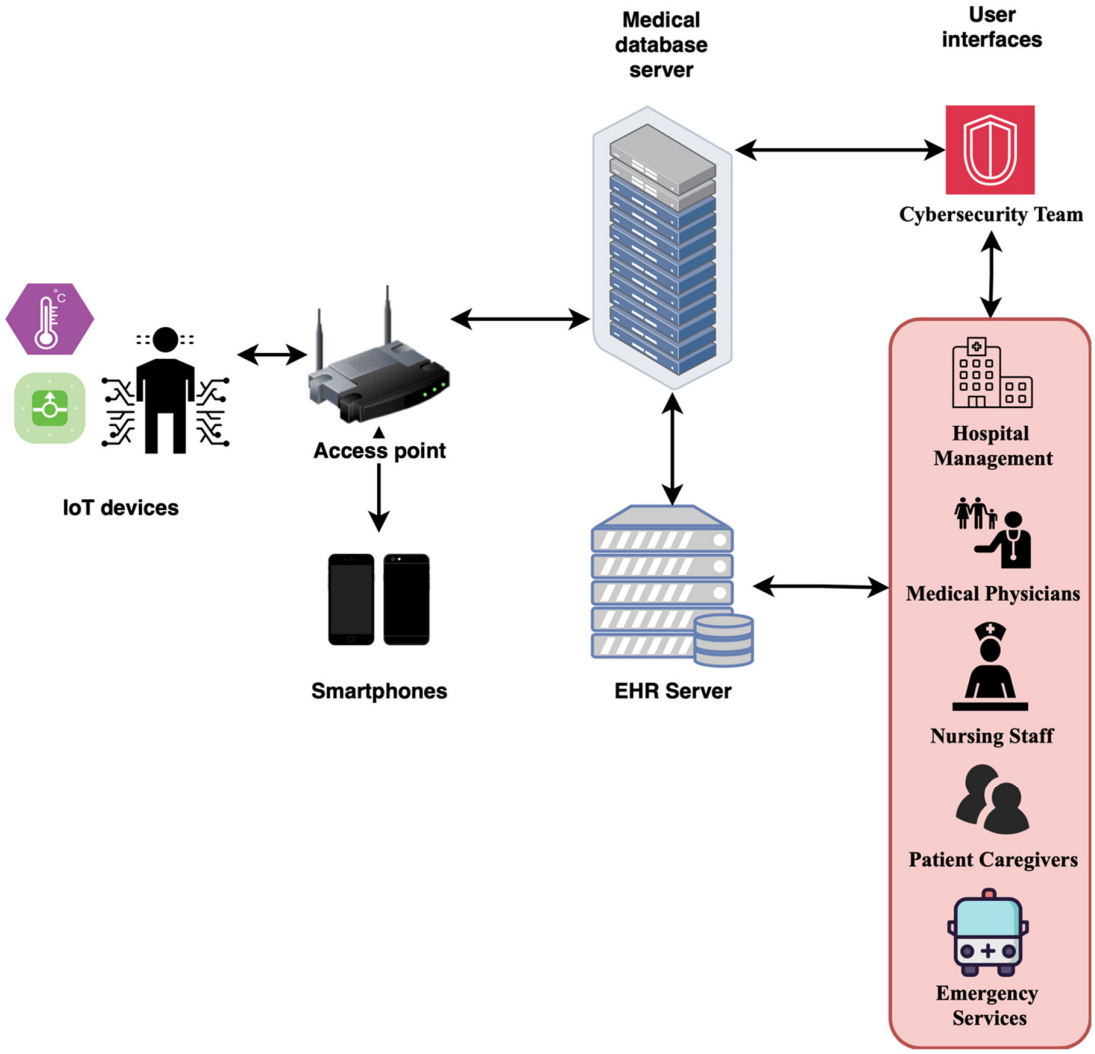


Figure 8. Comprehensive IoMT system architecture showing data flow from devices to servers.

The IoMT framework integrates advanced implantable devices that continuously track patients' physiological parameters and administer therapeutic interventions. These include:

- **Cardiac Pacemakers:** High-end cardiac rhythm management devices that track heart function and offer electrical stimulation to ensure optimal cardiac performance.
- **Cochlear Implants:** Advanced auditory prosthetic devices that translate sound signals into electrical impulses for individuals with profound hearing loss.
- **Gastric Stimulators:** Medical devices that modulate digestive system function by controlled electrical stimulation.

 doi:10.20944/preprints202509.0650.v2

- **Implantable Biosensors:** Real-time monitoring devices that monitor multiple physiological parameters such as glucose, blood pressure, and tissue oxygenation.

Advanced wearable technology provides comprehensive health monitoring capabilities by integrating non-invasive sensors. Primary categories of wearable devices are:

- **Smart ECG Monitors:** Handheld electrocardiogram units that continuously record cardiac electrical activity and identify arrhythmias or other cardiac abnormalities.
- **Depression Level Monitors:** An advanced way to track psychological health-related behavioural patterns, along with physiological markers involved.
- **Smart Insulin Monitors:** Continuous glucose monitoring systems combined with the provision of automatic implantable mechanisms for insulin delivery in patients who have diabetes.
- **Smart Blood Pressure Monitors:** Blood pressure measurement units with automatic capabilities and remote monitoring via wireless connectivity.

Medical devices generate sensor data and forward it to mobile devices, which serve as communication hubs. Smartphones act as intelligent sink devices, collecting information from multiple IoMT sources and securely transmitting it to the healthcare network infrastructure.

The data path for transmission from mobile devices to healthcare servers utilises standardised network access points that facilitate secure connections, ensure data integrity, and maintain patient confidentiality. The layer employs authentication methods and encryption techniques to safeguard personal medical data in transit.

Data from aggregated IoMT is processed on specialised medical database servers equipped with advanced data analysis capabilities. These servers apply machine learning methods for pattern analysis, anomaly detection, and knowledge extraction to facilitate clinical decision-making.

Analysed medical data and analytical findings are systematically consolidated into Electronic Health Record (EHR) systems, developing comprehensive patient profiles that incorporate diagnostic data, treatment histories, laboratory results, imaging data, and demographic information. Such integration enables healthcare professionals to have complete patient details, allowing them to make informed clinical decisions.

5.1. Stakeholder Classification and Alert Mechanisms

Technical users of the IoMT framework are primarily cybersecurity experts responsible for detection, analysis, and threat mitigation. Cybersecurity experts require precise information on attack vectors to implement effective countermeasures and maintain a robust system security posture.

Technical users benefit from fine-grained threat intelligence that includes detailed attack classifications, source detection, attack vector breakdowns, and suggested mitigation steps. The designed framework delivers holistic, multi-class classification outputs that facilitate technical teams' comprehension of attack properties and the deployment of specialised defence strategies.

Non-technical stakeholders include various healthcare professionals whose primary concern is patient care rather than cybersecurity. These stakeholders include:

- **Hospital Management:** Management staff are responsible for operational management and resource allocation decisions.
- **Medical Physicians:** Clinicians who need continued access to patient data and medical systems.
- **Nursing Staff:** Frontline medical caregivers who rely on stable IoMT systems for patient monitoring and care provision.
- **Patient Caregivers:** Support staff involved in patient care activities and in monitoring health status.
- **Emergency Services:** Emergency response teams need immediate access to patient information during emergency responses.

Non-technical users receive straightforward binary classification alerts indicating whether security threats exist, without requiring exhaustive technical analysis. This method enables

 doi:10.20944/preprints202509.0650.v2

healthcare professionals to quickly grasp the security status without being distracted from patient care tasks.

5.2. Proposed Intrusion Detection Framework Architecture

The proposed intrusion detection system employs a two-instance architecture that addresses the diverse information needs of healthcare stakeholders without compromising computational efficiency in resource-limited IoMT contexts. This solution integrates two classification instances: a Binary Label Classifier (BLC) to serve non-technical users and a Multi-Label Classifier (MLC) for technical users. The design approach acknowledges that adequate security in healthcare settings requires customised information-delivery mechanisms that account for users' levels of expertise and operational roles.

5.2.1. Binary Label Classifier (BLC) Design

The Binary Label Classifier focuses on quick threat detection through simplified binary classification, identifying benign network traffic and malicious attack patterns. The method is suited for non-technical healthcare practitioners who need instant threat awareness without technical complexity.

The BLC utilises optimised Modified Gated Recurrent Units, specifically designed for binary classification tasks in healthcare IoT networks. Figure 9 depicts the architecture of the proposed BLC. The MGRU architecture processes sequential network traffic data to detect attack patterns while maintaining low computational overhead suitable for real-time healthcare use cases.

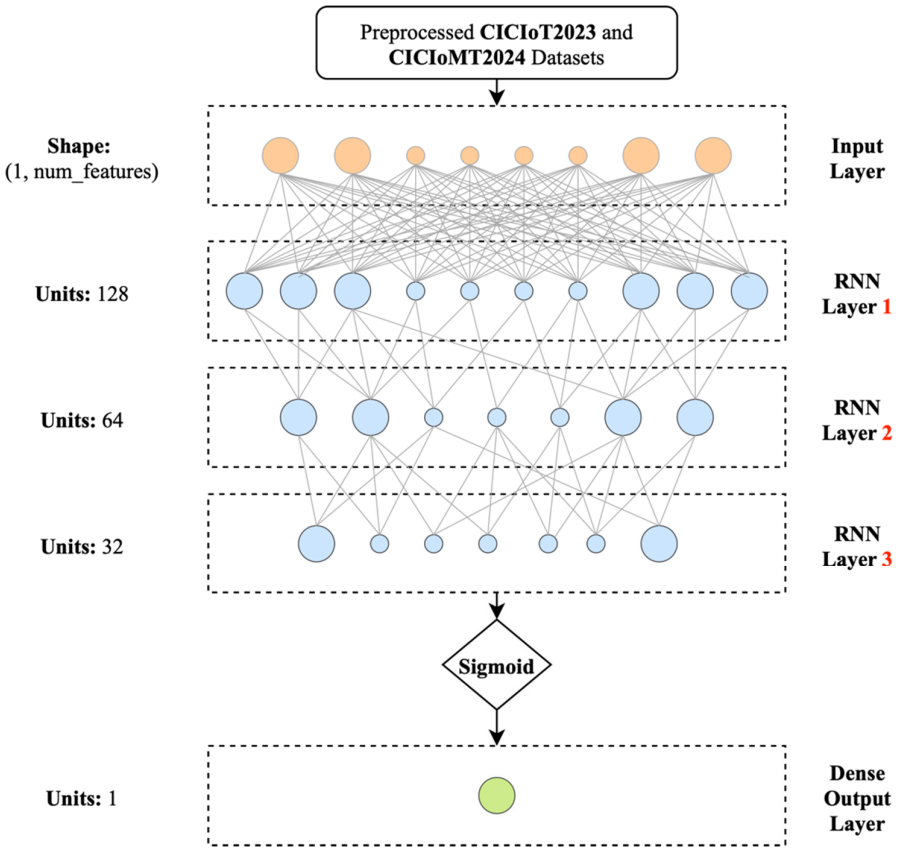


Figure 9. Architecture of BLC.

 doi:10.20944/preprints202509.0650.v2

5.2.2. Multi-Label Classifier (MLC) Design

The Multi-Label Classifier provides in-depth identification and classification of attack vectors for cybersecurity experts. The method conducts granular threat analysis of identified threats, classifying attacks by targeted vector types, attack patterns, and threat patterns.

The MLC utilises advanced MGRU settings tailored for multi-class classification across multiple attack categories. Figure 10 depicts the architecture of the proposed MLC. The improved architecture handles complex network traffic patterns to differentiate among numerous attack categories, including DDoS attack variants, reconnaissance activities, and protocol-specific attacks.

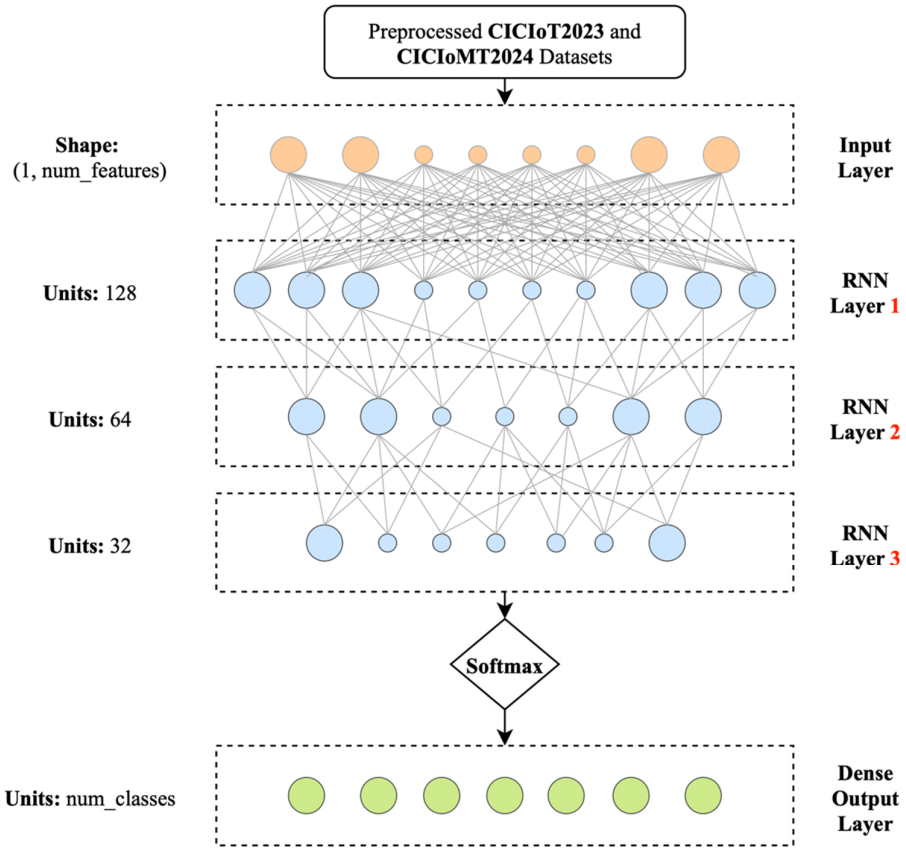


Figure 10. Architecture of MLC.

5.3. MGRU-Based Deep Learning Implementation

5.3.1. Modified GRU Architecture Optimisation

We selected Modified Gated Recurrent Units based on the distinct needs of IoMT environments, where limited computational budgets require real-time processing. MGRU architecture eliminates unnecessary computational complexity while maintaining efficient sequence modelling capabilities for network traffic analysis.

Network traffic in IoMT settings exhibits sequential features, necessitating dedicated processing strategies that can identify temporal relationships and detect patterns of attack development. The MGRU architecture is particularly efficient at handling sequential data streams with low memory usage and high-speed inference.

The framework architecture supports networks at varying scales —from small practices to large healthcare systems —through modular MGRU implementations. This scalability enables effective threat detection across a wide range of healthcare environments while maintaining consistent performance.

 doi:10.20944/preprints202509.0650.v2

5.3.2. Training and Optimisation Methodology

The MGRU models undergo thorough training using the CICIoT2023 and CICIoMT2024 datasets, which contain real-world attack scenarios and threat models specific to the healthcare sector. This training method ensures the framework can effectively identify today's multi-vector attacks on healthcare infrastructure. The comprehensive training and evaluation of BLC and MLC are shown in Algorithms 2 and 3, respectively.

The system employs a GA-based feature selection method to improve MGRU performance based on healthcare-specific network traffic profiles. Ongoing optimisation procedures enable MGRU models to maintain high detection efficiency and meet the real-time performance requirements necessary for medical care applications. Optimisation involves hyperparameter tuning, model compression, and inference acceleration.

6. Experimental Results and Performance Analysis

This section presents the results and performance of the suggested intrusion detection system. The system consists of two independent Intrusion Detection Systems (IDS) instances, which we refer to as BLC and MLC. Both instances were created in Python using the Keras library in Google Colab, an environment that offers a neural network framework based on TensorFlow.

Algorithm 2 Training and Evaluation of BLC

Inputs: Datasets, Batch size B, Number of epochs E, Learning rate Lr

```
Split Dataset into training set X_train, validation set X_val, and test set X_test
Preprocess features:
    for each X in X_train, X_val, X_test do
        X_norm ← normalize(X)
    end for

Define model:
    Input → mGRU(128, return_sequences=True)
          → mGRU(64,  return_sequences=True)
          → mGRU(32,  return_sequences=False)
          → Dense(1, activation='sigmoid')

Compile model with:
    optimizer = Adam(learning_rate=Lr)
    loss      = BinaryCrossentropy()
    metrics   = [Accuracy()]

Train model:
    history ← model.fit(
        x = X_train.features,
        y = X_train.labels,
        batch_size = B,
```

 doi:10.20944/preprints202509.0650.v2


```
            epochs = E,
            validation_data = (X_val.features, X_val.labels)
            )

Evaluate model on X_test:
    results ← model.evaluate(X_test.features, X_test.labels)
    Print test loss and metrics from results
```

Algorithm 3 Training and Evaluation of MLC

Inputs: Datasets, Batch size B, Number of epochs E, Learning rate Lr

```
Split Dataset into training set X_train, validation set X_val, and test set X_test
Preprocess features:
    for each X in X_train, X_val, X_test do
        X_norm ← normalize(X)
    end for

Define model:
    Input → mGRU(128, return_sequences=True)
          → mGRU(64,  return_sequences=True)
          → mGRU(32,  return_sequences=False)
          → Dense(C, activation='softmax')

Compile model with:
    optimizer = Adam(learning_rate=Lr)
    loss      = SparseCategoricalCrossentropy()
    metrics   = [Accuracy()]

Train model:
    history ← model.fit(
        x = X_train.features,
        y = X_train.labels,
        batch_size = B,
        epochs = E,
        validation_data = (X_val.features, X_val.labels)
        )

Evaluate model on X_test:
```

 doi:10.20944/preprints202509.0650.v2

28:	results ← model.evaluate(X_test.features, X_test.labels)
29:	Print test loss and metrics from results

The centre of both BLC and MLC models is a latent layer comprising three stacked MGRU layers, which detect dependencies in the input data. Specific hyperparameters regulate learning and are broad settings that affect how the model learns. Optimal values for these parameters, under which the model performed best, are recorded in Table 3.

For both data sets, the data was divided into training, validation, and testing sets to train, validate, and test the models. In particular, 70% of the data was applied for training, 20% for validation, and the remaining 10% was for testing the ultimate performance of the BLC and MLC models. The subsequent sections explain how the models performed on this 10% test dataset, demonstrating their effectiveness and efficiency in detecting attacks, and provide more specific results. We provide an analysis of several key performance metrics, including accuracy, precision, recall, F1-score, Sensitivity, Specificity, etc.

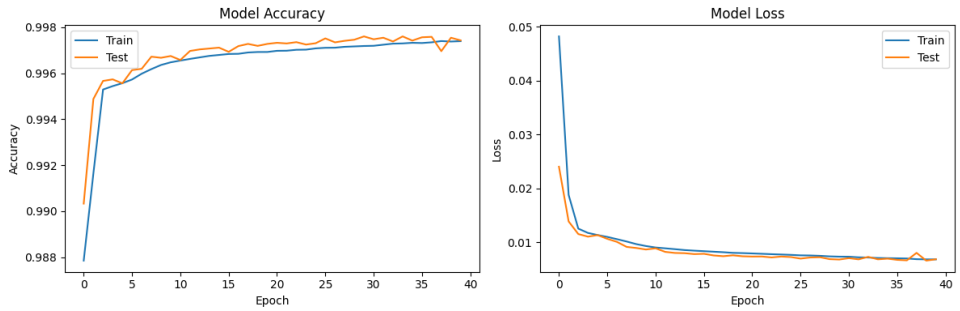
Table 3. Model Parameter of IDS Instances.

Model Parameters	**Selected Choices**
Loss Function	Binary Crossentropy (Binary Classification) & Categorical Crossentropy (Multi-label Classification)
Optimizer	Adam
Activation Function	Relu, Sigmoid, Softmax
No. of Epochs, Batch Size, Learning Rate	40, 1000, 0.001
No. of Hidden Layers	3

6.1. Results of BLC

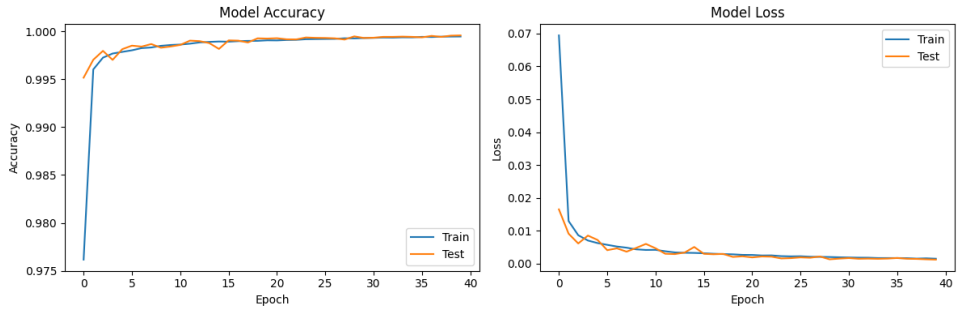
This subsection compares the performance of the BLC model on the CICIoT2023 and CICIoMT2024 datasets. We provide an analysis of some important measures on both the CICIoT2023 and CICIoMT2024 datasets.

Figure 11(a) shows the BLC model's training and test accuracy and loss curves on the CICIoT2023 dataset. Figure 11 (b) shows the corresponding accuracy and loss curves for the CICIoMT2024 dataset.



(a) Accuracy and Loss Plots of CICIoT2023 Dataset for Binary Classification by the BLC

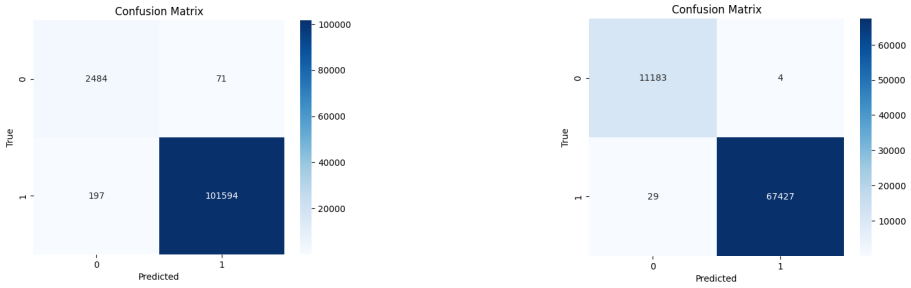
 doi:10.20944/preprints202509.0650.v2



(b) Accuracy and Loss Plots of CICIoMT2024 Dataset for Binary Classification by the BLC

Figure 11. Accuracy and Loss Plot of BLC.

Figure 12 (a) is the confusion matrix of BLC's performance on the CICIoT2023 dataset, and Figure 12 (b) is that of the CICIoMT2024 dataset. We tabulated the performance measures extracted from these matrices in Table 4.



(a) Confusion Matrix of BLC on CICIoT2023 Dataset

(b) Confusion Matrix of BLC on CICIoMT2024 Dataset

Figure 12. Confusion Matrices of BLC.

Table 4. Performance metrics of the proposed BLC on CICIoT2023 and CICIoMT2024 Datasets.

Metric	CICIoT2023	CICIoMT2024
Accuracy	0.9974	0.9996
Precision	0.9993	0.9999
Recall	0.9981	0.9996
F1-score	0.9987	0.9998
FAR	0.0278	0.0004
FPR	0.0278	0.0004
Sensitivity	0.9981	0.9996
Specificity	0.9722	0.9996
MCC	0.9478	0.9983

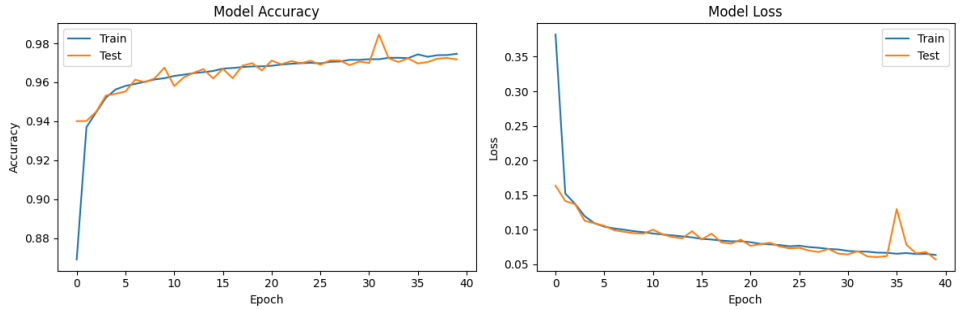
6.2. Results of MLC

This subsection presents corresponding performance metrics for the MLC model on both the CICIoT2023 and CICIoMT2024 datasets, with an emphasis on accuracy, loss, and confusion matrices.

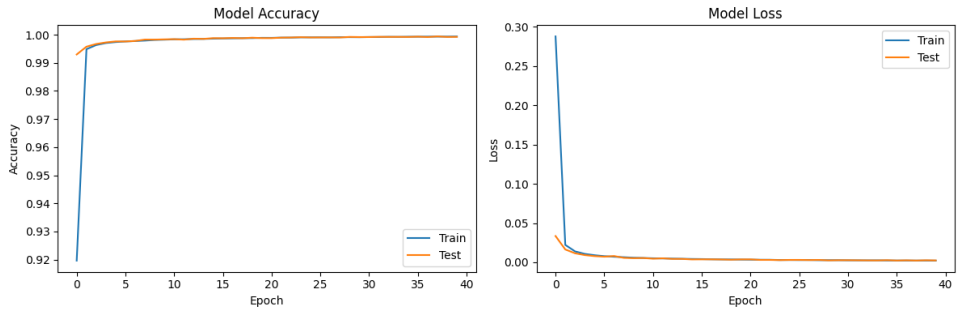
Figure 13(a) illustrates the MLC model's training and test accuracy and loss curves on the CICIoT2023 dataset. Figure 13 (b) illustrates the accuracy and loss plots for the CICIoMT2024 dataset.

 doi:10.20944/preprints202509.0650.v2

Figure 14(a) depicts the confusion matrix for the MLC model on the CICIoT2023 dataset, and Figure 14(b) similarly illustrates the confusion matrix for the CICIoMT2024 dataset, with the resulting performance metrics tabulated in Table 5.



(a) Accuracy and Loss Plots of CICIoT2023 Dataset for Multi-label Classification by the MLC



(b) Accuracy and Loss Plots of CICIoMT2024 Dataset for Multi-label Classification by the MLC

Figure 13. Accuracy and Loss Plot of MLC.

(a) Confusion Matrix of MLC on CICIoT2023 Dataset (b) Confusion Matrix of MLC on CICIoMT2024 Dataset

Figure 14. Confusion Matrices of MLC.

Table 5. Performance Metrics of the Proposed MLC on CICIoT2023 and CICIoMT2024 Datasets.

Metric	CICIoT2023	CICIoMT2024
Accuracy	0.9718	0.9992
Precision	0.9746	0.9992
Recall	0.9718	0.9992

 doi:10.20944/preprints202509.0650.v2

F1-score	0.9706	0.9992
FAR	0.0029	0.0001
FPR	0.0029	0.0001
Sensitivity	0.9396	0.9991
Specificity	0.9969	0.9998
MCC	0.9679	0.9991

7. Discussion

Implications: This study presents a novel, lightweight, and user-specific approach to detecting multi-vector DDoS attacks in IoT-enabled healthcare systems. The methodology employs two independent deep-learning-based intrusion detection systems (IDS), each with hidden layers constructed using a modified GRU (Gated Recurrent Unit) architecture.

Evaluations: We compared the performance of suggested IDS instances (BLC and MLC) to the CICIoT2023 and CICIoMT2024 datasets. After training, the BLC model categorises incoming IoMT traffic as 'Attack' or 'Benign.' The MLC model can categorise traffic as 'Benign' or a specific type of attack, such as 'ICMP,' 'UDP,' 'SYN,' 'TCP,' 'MQTT,' and flood and fragmentation attacks.

To highlight the efficiency and creativity of our models, we compared their performance with that of existing intrusion detection methods. As shown in Table 6, our proposed IDS instance (MLC) outperformed state-of-the-art mechanisms across four key metrics — accuracy, precision, recall, and F1 score — for multi-class classification and multi-vector attack detection. Figure 15 depicts the behaviour of the BLC model on the two datasets, which perform similarly on key measures. Figure 16 displays the behaviour of the MLC model, which, despite varied performance across the two datasets, performed better when trained on the CICIoMT2024 dataset than on the CICIoT2023 dataset.

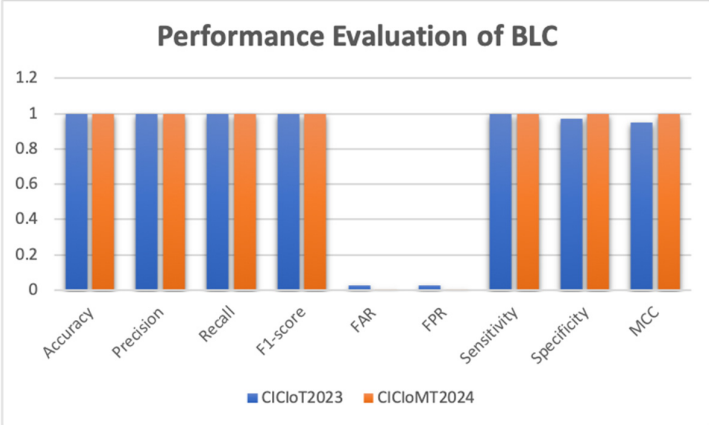


Figure 15. Performance Metrics of BLC.

Table 6. MVIID Framework Performance Metrics Comparison with State-of-the-Art Techniques.

Method	Accuracy	Precision	Recall	F1-score
MVIID	**0.9992**	**0.9992**	**0.9992**	**0.9992**
DDoSViT [42]	0.9950	0.9953	0.9950	0.9950
RestNet18 [54]	08706	0.8700	0.8600	0.8600
LEDEM [55]	0.9628	0.9700	0.9800	0.9700
DeepGFL [56]	0.9300	0.7567	0.3024	0.4321
MLP [57]	0.8634	0.8847	0.8625	08735

 doi:10.20944/preprints202509.0650.v2

ID-CNN [57]	0.9514	0.9017	0.9017	0.9399
LSTM [57]	0.9624	0.9814	0.8989	0.8959
ID-CNN-LSTM [57]	0.9716	0.9741	0.9910	0.9825

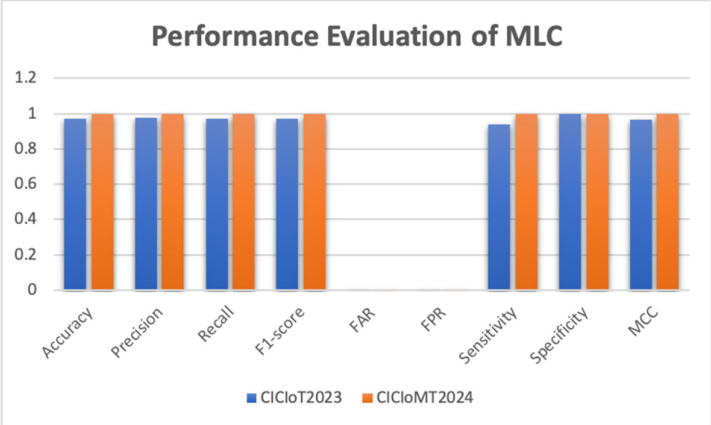


Figure 16. Performance Metrics of MLC.

Complexity Analysis

Here, we analyse the complexity of our IDS instance on our stacked MGRU layers. We compare them based on several measures: model size, training and testing time, accuracy, loss, and detection time.

Table 7 compares these models on the CICIoT2023 and CICIoMT2024 datasets. This research found that IDS instances trained with our stacked MGRU layers consistently achieved better performance metrics.

Table 7. Comparative Analysis of BLC and MLC on CICIoT2023 and CICIoMT2024 Datasets.

Dataset	BLC					MLC				
	Model Size (KB)	Training Time (Sec.)	Accuracy	Loss	Detection Time per Sample (Sec.)	Model Size (KB)	Training Time (Sec.)	Accuracy	Loss	Detection Time per Sample (Sec.)
CICIoT2023	379.61	715.06	0.9974	0.0068	0.000099	383.05	707.86	0.9718	0.0571	0.000099
CICIoMT2024	364.26	625.46	0.9996	0.0012	0.000131	366.51	363.55	0.9992	0.0024	0.000131

However, applying deep learning models in real-time healthcare systems presents several challenges, including latency, hardware and software requirements, the need for frequent updates, and the difficulty in collating detection outcomes from different IoT devices to detect multi-vector DDoS attacks. Since our models utilise lightweight mGRU layers, they are easier to deploy in real time, enabling fast attack detection with reasonable computational complexity. In the future, we plan to implement a lightweight blockchain framework that will process collaborative detection outcomes across multiple mobile devices, enabling even quicker responses for healthcare application users.

Limitations: Although our framework exhibits unique and efficient performance, we found a few primary limitations:

- **Real-Time Data:** In the future, we will construct a testbed to monitor real-time IoT healthcare traffic through multiple medical sensors and wearable devices.
- **Authentication:** This study assumes that all IoMT devices in an IoT environment are authenticated. Hence, it does not cover authentication and identification schemes. We aim to develop a lightweight authentication protocol for IoT-based healthcare devices based on Authenticated Encryption with Associated Data (AEAD).

 doi:10.20944/preprints202509.0650.v2

8. Conclusions and Future Work

The study successfully designed and tested a lightweight multi-vector DDoS detection framework directly tailored for IoMT-based healthcare systems. We have demonstrated that we can achieve high-performance intrusion detection without the heavy computational cost of traditional deep learning models by utilising a new MGRU architecture and a genetic algorithm-based feature selection approach. The dual-classifier technique (BLC and MLC) satisfies the key requirement of user-centric threat intelligence, supporting both healthcare professionals with simplified detection and cybersecurity teams with deep insights. Our experimental results, which include a detailed analysis of the CICIoT2023 and CICIoMT2024 datasets, validate that our proposed mechanism outperforms current mechanisms and is deployable in real-time scenarios. The analysis of complexity also highlights the effectiveness and cost-effectiveness of the framework, opening the door for its implementation in practical time-sensitive healthcare environments.

Although this study has made notable contributions, some limitations provide the path for future research. One key area for improvement is the development of a dedicated testbed to collect and process real-time IoT healthcare traffic from diverse medical sensors and wearable devices. It would enable more realistic validation and testing. Moreover, the current research assumes that the IoT environment has authenticated IoMT devices; hence, future research will aim to develop a lightweight authentication scheme on top of Authenticated Encryption with Associated Data (AEAD) to strengthen the overall security level of the framework. Lastly, to address the challenge of cooperative attack detection across multiple devices, we plan to develop a lightweight blockchain framework. It would enable the secure and efficient processing of collaborative detection outcomes, ultimately providing faster response times and greater resilience against advanced multi-vector attacks in healthcare applications.

Author Contributions: Author 1 has conducted the experiments and written the complete manuscript. Author 2 has reviewed the manuscript and suggested additional modifications.

Funding: Not Applicable

Acknowledgments: Not Applicable

Conflicts of Interest: The authors declare that they have no competing financial or non-financial interests that could have influenced the work reported in this paper.

References

1. [1] I. ul, M. Bin, M. Asif, and R. Ullah, "DoS/DDoS Detection for E-Healthcare in Internet of Things," *International Journal of Advanced Computer Science and Applications*, vol. 9, no. 1, 2018, doi: 10.14569/ijacsa.2018.090140.
2. [2] S. Sharma et al., "Mobile technology," *Journal of Family Medicine and Primary Care*, vol. 11, no. 1, pp. 37–43, Jan. 2022, doi: 10.4103/jfmpc.jfmpc_1114_21.
3. [3] L. Dzamesi and N. Elsayed, "A Review on the Security Vulnerabilities of the IoMT against Malware Attacks and DDoS," arXiv.org. [Online]. Available: https://arxiv.org/abs/2501.07703
4. [4] N. Elsayed, L. Dzamesi, Z. ElSayed, and M. Ozer, "Extreme Learning Machine-Based System for DDoS Attacks Detections on IoMT Devices," arXiv.org. [Online]. Available: https://arxiv.org/abs/2507.05132
5. [5] A. Pakmehr, A. Aßmuth, N. Taheri, and A. Ghaffari, "DDoS attack detection techniques in IoT networks: a survey," *Cluster Computing*, vol. 27, no. 10, pp. 14637–14668, Jul. 2024, doi: 10.1007/s10586-024-04662-6.
6. [6] A. Aguru and S. Erukala, "OTI-IoT: A Blockchain-based Operational Threat Intelligence Framework for Multi-vector DDoS Attacks," *ACM Transactions on Internet Technology*, vol. 24, no. 3, pp. 1–31, Jul. 2024, doi: 10.1145/3664287.
7. [7] S. Abiramasundari and V. Ramaswamy, "Distributed denial-of-service (DDOS) attack detection using supervised machine learning algorithms," *Scientific Reports*, vol. 15, no. 1, Apr. 2025, doi: 10.1038/s41598-024-84879-y.

 doi:10.20944/preprints202509.0650.v2

8. [8] A. I. Hassan, E. A. El Reheem, and S. K. Guirguis, "An entropy and machine learning based approach for DDoS attacks detection in software defined networks," *Scientific Reports*, vol. 14, no. 1, Aug. 2024, doi: 10.1038/s41598-024-67984-w.
9. [9] P. N. K., "Intrusion Detection System Using Gated Recurrent Neural Network," *618*, vol. 10, no. 01, pp. 1–8, May 2024.
10. [10] D. Kumar, R. K. Pateriya, R. K. Gupta, V. Dehalwar, and A. Sharma, "DDoS Detection using Deep Learning," *Procedia Computer Science*, vol. 218, pp. 2420–2429, 2023, doi: 10.1016/j.procs.2023.01.217.
11. [11] S. M. Kasongo and Y. Sun, "A Deep Gated Recurrent Unit based model for wireless intrusion detection system," *ICT Express*, vol. 7, no. 1, pp. 81–87, Mar. 2021, doi: 10.1016/j.icte.2020.03.002.
12. [12] D. Neal, "Choosing an electronic health records system: professional liability considerations," *Innovations in clinical neuroscience*, vol. 8, no. 6, pp. 43–5, Jun. 2011.
13. [13] A. F. M. Agarap, "A Neural Network Architecture Combining Gated Recurrent Unit (GRU) and Support Vector Machine (SVM) for Intrusion Detection in Network Traffic Data," in *Proceedings of the 2018 10th International Conference on Machine Learning and Computing*, New York, NY, USA: ACM, Feb. 2018, pp. 26–30. Accessed: Aug. 04, 2025. [Online]. Available: https://doi.org/10.1145/3195106.3195117
14. [14] E. C. P. Neto, S. Dadkhah, R. Ferreira, A. Zohourian, R. Lu, and A. A. Ghorbani, "CICIoT2023: A Real-Time Dataset and Benchmark for Large-Scale Attacks in IoT Environment," *Sensors*, vol. 23, no. 13, p. 5941, Jun. 2023, doi: 10.3390/s23135941.
15. [15] S. Dadkhah, E. Carlos Pinto Neto, R. Ferreira, R. Chukwuka Molokwu, S. Sadeghi, and A. Ghorbani, "CiCIoMT2024: Attack Vectors in Healthcare Devices-A Multi-Protocol Dataset for Assessing IoMT Device Security," Elsevier BV, 2024. Accessed: Aug. 04, 2025. [Online]. Available: https://doi.org/10.2139/ssrn.4725150
16. [16] E. M. Maseno and Z. Wang, "Hybrid wrapper feature selection method based on genetic algorithm and extreme learning machine for intrusion detection," *Journal of Big Data*, vol. 11, no. 1, Feb. 2024, doi: 10.1186/s40537-024-00887-9.
17. [17] E. S. Alghoson and O. Abbass, "Detecting Distributed Denial of Service Attacks using Machine Learning Models," *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 12, 2021, doi: 10.14569/ijacsa.2021.0121277.
18. [18] M. Akshay Kumaar, D. Samiayya, P. M. D. R. Vincent, K. Srinivasan, C.-Y. Chang, and H. Ganesh, "A Hybrid Framework for Intrusion Detection in Healthcare Systems Using Deep Learning," *Frontiers in Public Health*, vol. 9, Jan. 2022, doi: 10.3389/fpubh.2021.824898.
19. [19] S. Saif, P. Das, S. Biswas, M. Khari, and V. Shanmuganathan, "HIIDS: Hybrid intelligent intrusion detection system empowered with machine learning and metaheuristic algorithms for application in IoT based healthcare," *Microprocessors and Microsystems*, p. 104622, Aug. 2022, doi: 10.1016/j.micpro.2022.104622.
20. [20] S. K. Patel, "Improving intrusion detection in cloud-based healthcare using neural network," *Biomedical Signal Processing and Control*, vol. 83, p. 104680, May 2023, doi: 10.1016/j.bspc.2023.104680.
21. [21] 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," *IEEE Access*, vol. 8, pp. 106576–106584, 2020, doi: 10.1109/access.2020.3000421.
22. [22] C. Iwendi, J. H. Anajemba, C. Biamba, and D. Ngabo, "Security of Things Intrusion Detection System for Smart Healthcare," *Electronics*, vol. 10, no. 12, p. 1375, Jun. 2021, doi: 10.3390/electronics10121375.
23. [23] A. Basharat, Mohd. M. B. Mohamad and A. Khan, "Machine Learning Techniques for Intrusion Detection in Smart Healthcare Systems: A Comparative Analysis," in *2022 4th International Conference on Smart Sensors and Application (ICSSA)*, IEEE, Jul. 2022, pp. 29–33. Accessed: Aug. 04, 2025. [Online]. Available: https://doi.org/10.1109/icssa54161.2022.9870973
24. [24] A. Tuteja, P. Matta, S. Sharma, K. Nandan, and P. Gautam, "Intrusion Detection in Health Care System: A logistic Regression Approach," in *2022 5th International Conference on Contemporary Computing and Informatics (IC3I)*, IEEE, Dec. 2022, pp. 1794–1799. Accessed: Aug. 04, 2025. [Online]. Available: https://doi.org/10.1109/ic3i56241.2022.10072882

 doi:10.20944/preprints202509.0650.v2

25. [25] M. Ahmed, S. Byreddy, A. Nutakki, L. F. Sikos, and P. Haskell-Dowland, "ECU-IoHT: A dataset for analysing cyberattacks in Internet of Health Things," Ad Hoc *Networks*, vol. 122, p. 102621, Nov. 2021, doi: 10.1016/j.adhoc.2021.102621.
26. [26] A. S. Dina, A. B. Siddique, and D. Manivannan, "A deep learning approach for intrusion detection in Internet of Things using focal loss function," *Internet of Things*, vol. 22, p. 100699, Jul. 2023, doi: 10.1016/j.iot.2023.100699.
27. [27] A. F. Almutairi and A. Abdulghani Alshargabi, "Using Deep Learning Technique to Protect Internet Network from Intrusion in IoT Environment," in *2022 2nd International Conference on Emerging Smart Technologies and Applications (eSmarTA)*, IEEE, Oct. 2022, pp. 1–6. Accessed: Aug. 04, 2025. [Online]. Available: https://doi.org/10.1109/esmarta56775.2022.9935467
28. [28] S. H. S. Ariffin, N. H. Mustaffa, F. Dewanta, I. W. Hamzah, M. A. Baharudin, and N. H. Abdul Wahab, "Hybrid Feature Selection Based Lightweight Network Intrusion Detection System for MQTT Protocol," in *2023 15th International Conference on Software, Knowledge, Information Management and Applications (SKIMA)*, IEEE, Dec. 2023, pp. 226–230. Accessed: Aug. 04, 2025. [Online]. Available: https://doi.org/10.1109/skima59232.2023.10387337
29. [29] M. M. Alani, "IoTProtect: A Machine-Learning Based IoT Intrusion Detection System," in *2022 6th International Conference on Cryptography, Security and Privacy (CSP)*, IEEE, Jan. 2022. Accessed: Aug. 04, 2025. [Online]. Available: https://doi.org/10.1109/csp55486.2022.00020
30. [30] M. Ramaiah and M. Y. Rahamathulla, "Securing the Industrial IoT: A Novel Network Intrusion Detection Models," in *2024 3rd International Conference on Artificial Intelligence For Internet of Things (AIIoT)*, IEEE, May 2024, pp. 1–6. Accessed: Aug. 04, 2025. [Online]. Available: https://doi.org/10.1109/aiiot58432.2024.10574728
31. [31] P. O. Adebayo, M. Jubrin Abdulahi, O. M. Lawrence, Y. A. Ibrahim, S. A. Faki, and B. A. Hassan, "An Artificial Intelligence-based Ensemble Technique for Intrusion Detection and Prevention in IoT Systems," in *2024 International Conference on Science, Engineering and Business for Driving Sustainable Development Goals (SEB4SDG)*, IEEE, Apr. 2024, pp. 1–6. Accessed: Aug. 04, 2025. [Online]. Available: https://doi.org/10.1109/seb4sdg60871.2024.10629681
32. [32] G. Guo, X. Pan, H. Liu, F. Li, L. Pei, and K. Hu, "An IoT Intrusion Detection System Based on TON IoT Network Dataset," in *2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC)*, IEEE, Mar. 2023. Accessed: Aug. 04, 2025. [Online]. Available: https://doi.org/10.1109/ccwc57344.2023.10099144
33. [33] R. Ma, Q. Wang, X. Bu, and X. Chen, "Real-Time Detection of DDoS Attacks Based on Random Forest in SDN," *Applied Sciences*, vol. 13, no. 13, p. 7872, Jul. 2023, doi: 10.3390/app13137872.
34. [34] S. Ahmed et al., "Effective and Efficient DDoS Attack Detection Using Deep Learning Algorithm, Multi-Layer Perceptron," *Future Internet*, vol. 15, no. 2, p. 76, Feb. 2023, doi: 10.3390/fi15020076.
35. [35] J. Li, L. Lyu, X. Liu, X. Zhang, and X. Lyu, "FLEAM: A Federated Learning Empowered Architecture to Mitigate DDoS in Industrial IoT," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 6, pp. 4059–4068, Jun. 2022, doi: 10.1109/tii.2021.3088938.
36. [36] R. Vishwakarma and A. K. Jain, "A Honeypot with Machine Learning based Detection Framework for defending IoT based Botnet DDoS Attacks," in *2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI)*, IEEE, Apr. 2019, pp. 1019–1024. Accessed: Aug. 04, 2025. [Online]. Available: https://doi.org/10.1109/icoei.2019.8862720
37. [37] M. Zeeshan et al., "Protocol-Based Deep Intrusion Detection for DoS and DDoS Attacks Using UNSW-NB15 and Bot-IoT Datasets," *IEEE Access*, vol. 10, pp. 2269–2283, 2022, doi: 10.1109/access.2021.3137201.
38. [38] M. Roopak, G. Y. Tian, and J. Chambers, "An Intrusion Detection System Against DDoS Attacks in IoT Networks," in *2020 10th Annual Computing and Communication Workshop and Conference (CCWC)*, IEEE, Jan. 2020, pp. 0562–0567. Accessed: Aug. 04, 2025. [Online]. Available: https://doi.org/10.1109/ccwc47524.2020.9031206
39. [39] Y. Jia, F. Zhong, A. Alrawais, B. Gong, and X. Cheng, "FlowGuard: An Intelligent Edge Defense Mechanism Against IoT DDoS Attacks," *IEEE Internet of Things Journal*, vol. 7, no. 10, pp. 9552–9562, Oct. 2020, doi: 10.1109/jiot.2020.2993782.

 doi:10.20944/preprints202509.0650.v2

40. [40] A. O. Sangodoyin, M. O. Akinsolu, P. Pillai, and V. Grout, "Detection and Classification of DDoS Flooding Attacks on Software-Defined Networks: A Case Study for the Application of Machine Learning," *IEEE Access*, vol. 9, pp. 122495–122508, 2021, doi: 10.1109/access.2021.3109490.
41. [41] C. D. McDermott, F. Majdani, and A. V. Petrovski, "Botnet Detection in the Internet of Things using Deep Learning Approaches," in *2018 International Joint Conference on Neural Networks (IJCNN)*, IEEE, Jul. 2018, pp. 1–8. Accessed: Aug. 04, 2025. [Online]. Available: https://doi.org/10.1109/ijcnn.2018.8489489
42. [42] M. Ali, Y. Saleem, S. Hina, and G. A. Shah, "DDoSViT: IoT DDoS attack detection for fortifying firmware Over-The-Air (OTA) updates using vision transformer," *Internet of Things*, vol. 30, p. 101527, Mar. 2025, doi: 10.1016/j.iot.2025.101527.
43. [43] M. Faltys et al., "HiRID, a high time-resolution ICU dataset." [Online]. Available: https://physionet.org/content/hirid/1.1.1/
44. [44] A. L. Goldberger et al., "PhysioBank, PhysioToolkit, and PhysioNet," *Circulation*, vol. 101, no. 23, Jun. 2000, doi: 10.1161/01.cir.101.23.e215.
45. [45] "WUSTL-IIOT-2021 Dataset for IIoT Cybersecurity Research." [Online]. Available: http://www.cse.wustl.edu/~jain/iiot2/index.html
46. [46] C. Thomas, V. Sharma, and N. Balakrishnan, "Usefulness of DARPA dataset for intrusion detection system evaluation," in *SPIE Proceedings*, SPIE, Mar. 2008. Accessed: Aug. 05, 2025. [Online]. Available: https://doi.org/10.1117/12.777341
47. [47] N. Koroniotis, N. Moustafa, E. Sitnikova, and B. Turnbull, "Towards the development of realistic botnet dataset in the Internet of Things for network forensic analytics: Bot-IoT dataset," *Future Generation Computer Systems*, vol. 100, pp. 779–796, Nov. 2019, doi: 10.1016/j.future.2019.05.041.
48. [48] N. Moustafa and J. Slay, "UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)," in *2015 Military Communications and Information Systems Conference (MilCIS)*, IEEE, Nov. 2015, pp. 1–6. Accessed: Aug. 05, 2025. [Online]. Available: https://doi.org/10.1109/milcis.2015.7348942
49. [49] R. Bala, "A REVIEW ON KDD CUP99 AND NSL-KDD DATASET," *International Journal of Advanced Research in Computer Science*, vol. 10, no. 2, pp. 64–67, Apr. 2019, doi: 10.26483/ijarcs.v10i2.6395.
50. [50] Y. Meidan et al., "N-BaIoT: Network-based Detection of IoT Botnet Attacks Using Deep Autoencoders," arXiv.org. [Online]. Available: https://arxiv.org/abs/1805.03409
51. [51] Kurniabudi, D. Stiawan, Darmawijoyo, M. Y. Bin Idris, A. M. Bamhdi, and R. Budiarto, "CICIDS-2017 Dataset Feature Analysis With Information Gain for Anomaly Detection," *IEEE Access*, vol. 8, pp. 132911–132921, 2020, doi: 10.1109/access.2020.3009843.
52. [52] J. L. Leevy, J. Hancock, R. Zuech, and T. M. Khoshgoftaar, "Detecting cybersecurity attacks across different network features and learners," *Journal of Big Data*, vol. 8, no. 1, Feb. 2021, doi: 10.1186/s40537-021-00426-w.
53. [53] I. Sharafaldin, A. H. Lashkari, S. Hakak, and A. A. Ghorbani, "Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy," in *2019 International Carnahan Conference on Security Technology (ICCST)*, IEEE, Oct. 2019, pp. 1–8. Accessed: Aug. 05, 2025. [Online]. Available: https://doi.org/10.1109/ccst.2019.8888419
54. [54] F. Hussain, S. G. Abbas, M. Husnain, U. U. Fayyaz, F. Shahzad, and G. A. Shah, "IoT DoS and DDoS Attack Detection using ResNet," in *2020 IEEE 23rd International Multitopic Conference (INMIC)*, IEEE, Nov. 2020. Accessed: Aug. 08, 2025. [Online]. Available: https://doi.org/10.1109/inmic50486.2020.9318216
55. [55] N. Ravi and S. M. Shalinie, "Learning-Driven Detection and Mitigation of DDoS Attack in IoT via SDN-Cloud Architecture," *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 3559–3570, Apr. 2020, doi: 10.1109/jiot.2020.2973176.

 doi:10.20944/preprints202509.0650.v2

56. [56] Y. Yao, L. Su, and Z. Lu, "DeepGFL: Deep Feature Learning via Graph for Attack Detection on Flow-Based Network Traffic," in *MILCOM 2018—2018 IEEE Military Communications Conference (MILCOM)*, IEEE, Oct. 2018, pp. 579–584. Accessed: Aug. 08, 2025. [Online]. Available: https://doi.org/10.1109/milcom.2018.8599821
57. [57] M. Roopak, G. Yun Tian, and J. Chambers, "Deep Learning Models for Cyber Security in IoT Networks," in *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*, IEEE, Jan. 2019. Accessed: Aug. 08, 2025. [Online]. Available: https://doi.org/10.1109/ccwc.2019.8666588