Adaptive Graph-Based Intrusion Detection for Internet of Medical Things (IoMT) Networks

G. S. Chethan
Department of Information Science and Engineering, Jawaharlal Nehru New College of Engineering, Shivamogga, Karnataka, India
chethangs999@gmail.com (corresponding author)

N. S. Patil
Department of Information Science and Engineering, Bapuji Institute of Engineering and Technology, Davangere, Karnataka, India
patilbathi@gmail.com

GL Prakash
Department of Computer Science and Engineering, BMS Institute of Technology and Management, Bengaluru, Karnataka, India
glprakash@bmsit.in

M. S. Muneshwara
Department of Computer Science and Engineering, BMS Institute of Technology and Management, Bengaluru, Karnataka, India
muneshwarams@bmsit.in

Received: 16 January 2026 | Revised: 31 March 2026 | Accepted: 17 April 2026

 DOI: https://doi.org/10.48084/etasr.17590

ABSTRACT

The widespread adoption of the Internet of Medical Things (IoMT) has significantly enhanced healthcare services but has also introduced increased vulnerability to sophisticated cyberattacks, highlighting the need for robust Intrusion Detection Systems (IDS). Traditional Machine Learning (ML) and Deep Learning (DL) methods often struggle with class imbalance and fail to effectively capture inter-device relationships and contextual dependencies, which limits their performance, particularly for fine-grained attack detection. To overcome these challenges, we propose the Adaptive Graph-based Hybrid Graph Convolutional Network Intrusion Detection System (AGH-GCN IDS). The system models IoMT devices and network flows as a graph, extracts attention-aware features using Graph Attention Networks (GAT), and employs a hybrid graph convolutional classifier enhanced with Attention-Weighted Graph Synthetic Oversampling (AWGSO) to address class imbalance. Extensive experiments on the CICIoMT2024 dataset demonstrate that AGH-GCN IDS achieves an accuracy of 99.98% for binary-class, 98.45% for 6-class, and 96.87% for 19-class classification, outperforming conventional ML and DL approaches. These results establish AGH-GCN IDS as a robust and high-performance solution for IoMT security, with future extensions targeting edge-cloud architectures for distributed and privacy-preserving detection.

Keywords-IoMT security; Intrusion Detection System (IDS); Graph Convolutional Network (GCN); class imbalance; Graph Attention Network (GAT); CICIoMT2024

I. INTRODUCTION

The rapid adoption of the Internet of Medical Things (IoMT) has significantly transformed healthcare delivery by enabling real-time monitoring, remote diagnosis, and automated patient care [1]. However, the interconnected nature of IoMT devices also introduces critical cybersecurity vulnerabilities, as these networks are increasingly targeted by sophisticated attacks such as Denial of Service (DoS), Distributed DoS (DDoS), spoofing, and reconnaissance [2, 3]. Ensuring the security and reliability of IoMT networks is thus a pressing concern, necessitating the development of robust Intrusion Detection Systems (IDS) designed for these environments. Recent research has leveraged Machine Learning (ML) and Deep Learning (DL) techniques for IoMT security. ML approaches, including Random Forest (RF) [4], Decision Trees (DTs) [5], eXtreme Gradient Boosting (XGB)

[6], and AdaBoost (AB) [7], have been employed for anomaly detection and attack classification, often combined with feature selection and ensemble strategies to enhance performance. DL-based methods, such as Long Short-Term Memory (LSTM) [8] and Convolutional Neural Network (CNN) [9], have been explored to capture temporal and spatial patterns in network traffic, achieving high detection accuracy. For instance, in [10], the CICIoMT2024 dataset was presented to improve IoMT cybersecurity. In this work, an IoMT testbed was constructed comprising 40 devices (25 real and 15 simulated) executing 18 diverse cyberattacks. Network traffic was captured using specialized tools within a Faraday Cage to ensure accuracy. ML approaches, including Logistic Regression (LR), AB, RF, and Deep Neural Network (DNN), were applied for 2-class, 6-class, and 19-class evaluations, achieving an accuracy ranging from 73.3% to 99.6%. In [11], a deep learning (DL) framework combining LSTM with UNet++ was employed to extract and analyze traffic features. The hybrid UNet++-LSTM model was trained on CICIoMT data for anomaly and attack classification, achieving 99.92% accuracy for attack detection and 87.96% for attack classification. In [12], an RF-based Explainable AI approach (RF-XAI) combined with feature selection was utilized to reduce redundancy and improve performance. SHapley Additive exPlanations (SHAP) were used to identify key features for enhanced predictions, yielding 99% multi-class accuracy on CICIoMT2024. In [13], fine-tuned XGBoost (XGB) was integrated with a late-fusion Max-Voting scheme using LR, with SHAP-based feature importance analysis, achieving 97% binary-class accuracy on CICIoMT2024. In [14], multiple ML methods were trained on CICIoT2023 and tested on CICIoMT2024, applying dataset balancing, temporal adjustments, train-test-validation splits, and uniform windowing, with RF and XGB reaching ~99.85% accuracy. In [15], ensemble and traditional ML models with feature selection based on importance scores were evaluated on CICIoMT and CICIoT datasets, showing that stacked ensembles achieved 99% accuracy on CICIoT2023 and 97.58% on CICIoMT2024. In [16], Artificial Neural Network (ANN), Support Vector Machine (SVM), and RF models were trained on simulated IoMT network traffic with extensive feature engineering; RF performed best for complex attacks, whereas SVM handled ambiguous cases effectively. In [17], SecureMed combined Federated Learning (FL), secure multi-party computation, and blockchain for decentralized, privacy-preserving model training, achieving improved outcomes on CICIoMT2024 while ensuring fairness and secure collaboration.

Despite these advances, existing approaches often struggle with class imbalance, as attack types are disproportionately represented compared to benign traffic, leading to reduced detection performance for minority classes. Moreover, many methods fail to effectively model the inter-device relationships and contextual dependencies inherent in IoMT networks. To address these challenges, this work proposes an Adaptive Graph-based Hybrid Graph Convolutional Network IDS (AGH-GCN IDS). By constructing a graph representation of IoMT devices and flows, the model captures structural and contextual dependencies, while a Graph Attention Network (GAT) dynamically weighs the importance of device interactions. The hybrid GCN classifier integrates spectral convolution with attention-enhanced aggregation, enabling robust classification even under severe class imbalance. Additionally, a novel Attention-Weighted Graph Synthetic Oversampling (AWGSO) technique mitigates data imbalance, ensuring accurate detection of rare attacks. The contributions of AGH-GCN IDS are as follows.

- Proposes a novel approach to represent IoMT devices and flows as a graph, capturing inter-device communication and contextual dependencies.
- Introduces GAT to dynamically weigh node relationships, enhancing the relevance of extracted features for classification.
- Develops a hybrid GCN that combines spectral graph convolution with attention-enhanced aggregation for robust detection across diverse attack types.
- Introduces AWGSO to generate synthetic samples for minority classes, improving detection of rare attacks.
- Demonstrates superior performance on the CICIoMT2024 dataset, highlighting accuracy and resilience to class imbalance, outperforming traditional ML and DL methods.

II. METHODOLOGY

This section presents the AGH-GCN IDS methodology for detecting and classifying cyberattacks in IoMT environments. It first discusses the AGH-GCN IDS architecture and then provides a detailed explanation of the dataset used for training and testing. Further, it discusses the feature extraction process (adaptive graph-based approach) and classifier (hybrid GCN approach) in detail. The main objective of AGH-GCN IDS is to model inter-device relationships using graph-based learning, leveraging attention for contextual relevance, and employing hybrid graph convolution for classification even under class imbalance.

A. Architecture

The architecture of AGH-GCN IDS is presented in Figure 1. In this architecture, first, the dataset used is the CICIoMT2024 dataset [10]. The CICIoMT2024 dataset underwent Exploratory Data Analysis (EDA), where it was found that the dataset did not contain any missing values; hence, preprocessing was not considered. Further, the dataset was divided into an 80:20 ratio, where 80% of the data were utilized for training, and 20% of the data were utilized for testing. The training data underwent the feature extraction process using the adaptive graph-based approach, which is discussed in detail in Section C. Further, after feature extraction, the extracted features were fed into the classifier, which is a hybrid graph-convolution network developed for IDS, as discussed in detail in Section D. The classifier undergoes a cross-validation process, and if satisfactory performance is achieved, the model performance is evaluated. Otherwise, the framework proceeds to a class-handling process, where class imbalance is addressed using the proposed approach discussed in Section D. The classifier is then retrained, and the process is repeated until satisfactory

performance is achieved, after which the final performance is evaluated.

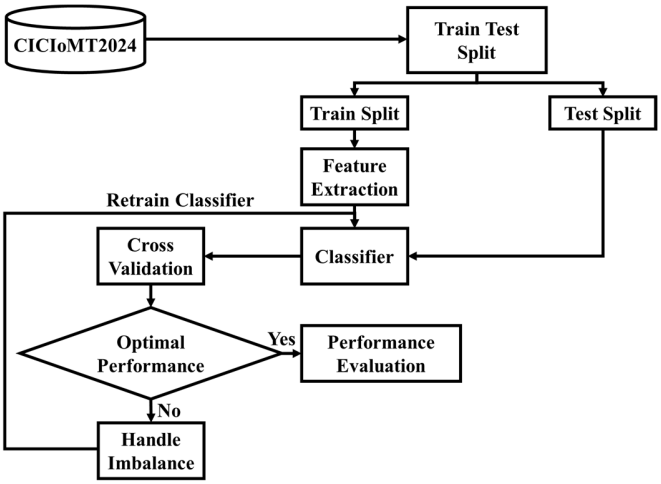

Fig. 1. AGH-GCN IDS architecture.

Moreover, the AGH-GCN IDS integrates several existing techniques, i.e., GAT, hybrid GCN classifiers, and graph-based oversampling, into a framework for IoMT intrusion detection. While each component builds upon prior work in graph learning and imbalance handling, the novelty of our approach lies in its practical integration and domain-specific adaptation, enabling effective detection of diverse and imbalanced attack types in IoMT networks. Hence, this work emphasizes that the contribution is primarily methodological and application-driven, rather than being based on a new theoretical graph-learning model.

B. Dataset

The AGH-GCN IDS was developed and evaluated using the CICIoMT2024 dataset, available at [18] and further discussed in [11]. The CICIoMT2024 dataset provides a realistic and comprehensive benchmark for IDS in IoMT environments. It captures network traffic from 40 IoMT devices (25 physical and 15 simulated) across three communication protocols. The dataset includes 18 distinct cyberattacks and one benign class, representing a total of 19 classes for classification. Moreover, the attacks in the dataset are grouped into five major categories, i.e., spoofing, MQTT, Reconnaissance (Recon), DoS, and DDoS. Each record in the dataset is represented by a multi-dimensional feature vector consisting of protocol-based, temporal, and statistical attributes. The training and test splits for binary and multi-class classification considered in this study are presented in Tables I, II, and III.

TABLE I. CICIOMT2024 BINARY-CLASS CLASSIFICATION DATASET

Class	Count	Training	Testing
Benign	230,339	184,271	46,068
Attack	8,544,674	6,835,739	1,708,935
Total samples	8,775,013	7,020,010	1,755,003

TABLE II. CICIOMT2024 6-CLASS CLASSIFICATION DATASET

Class	Count	Training	Testing
DoS	2,222,205	1,777,764	444,441
DDoS	5,846,623	4,677,298	1,169,325
MQTT	326,653	261,322	65,331
Recon	131,402	105,122	26,280
Spoofing	17,791	14,233	3,558
Benign	230,339	184,271	46,068
Total samples	8,775,013	7,020,010	1,755,003

TABLE III. CICIOMT2024 19-CLASS CLASSIFICATION DATASET

Class	Count	Training	Testing
DoS UDP	704,503	563,602	140,901
DoS SYN	540,498	432,398	108,100
DoS ICMP	514,724	411,779	102,945
DoS TCP	462,480	369,984	92,496
DDoS UDP	1,998,026	1,598,421	399,605
DDoS SYN	974,359	779,487	194,872
DDoS ICMP	1,887,175	1,509,740	377,435
DDoS TCP	987,063	789,650	197,413
DoS Connect Flood	15,904	12,723	3,181
DoS Publish Flood	52,881	42,305	10,576
DDoS Connect Flood	214,952	171,962	42,990
DDoS Public Flood	36,039	28,831	7,208
Malformed data	6,877	5,502	1,375
Ping sweep	926	741	185
Port scan	106,603	85,282	21,321
Recon VulScan	3,207	2,566	641
OS scan	20,666	16,533	4,133
ARP spoofing	17,791	14,233	3,558
Benign	230,339	184,271	46,068
Total samples	8,775,013	7,020,010	1,755,003

C. Feature Extraction

For capturing structural dependencies among IoMT devices and flows, this work presents an adaptive-graph-based approach in AGH-GCN IDS, which constructs a graph representation of the dataset and extracts contextual graph features using GAT. The approach allows AGH-GCN IDS to learn the significance of each device connection in determining attack behavior. Let the IoMT network be represented as a graph $G = (V, E, X)$, where $V = \{v_1, v_2, \dots, v_n\}$ denotes the set of nodes (IoMT devices/flows), $E \subseteq V \times V$ denotes the set of edges representing similarity relationships and communications, and $X \in \mathbb{R}^{n \times d}$ denotes the feature matrix. Each node v_i is represented by the associated feature vector $x_i \in \mathbb{R}^d$. An edge (i, j) is established if devices i and j share a communication protocol or common broker, topic, or MAC address, or have high feature similarity defined using (1):

$$s(i,j) = \frac{x_i}{\|x_i\|\|x_j\|} \geq \tau_s \quad (1)$$

In (1), τ_s denotes the similarity threshold, which was set to 0.6. Further, the GAT assigns learnable attention weights for each neighboring node to determine the importance of representing node i. The unnormalized attention coefficient among nodes i and j was evaluated using (2):

$$e_{ij} = LeakyReLU(a^{\mathrm{T}}[Wh_i || Wh_j]) \quad (2)$$

In (2), h_i denotes the input feature for node i, W denotes a learnable weight matrix, a denotes a learnable attention vector, $||$ denotes concatenation, and $LeakyReLU$ denotes the activation function introducing non-linearity. Further, the normalized attention coefficient is obtained using the softmax function defined using (3):

$$\alpha_{ij} = \frac{\exp(e_{ij})}{\sum_{k\in\mathcal{N}(i)}\exp(e_{ik})} \quad (3)$$

In (3), $\mathcal{N}(i)$ denotes the set of neighbors of node i. The new representation of node i after attention aggregation is denoted by (4):

$$h_i' = \sigma\left(\sum_{j\in\mathcal{N}(i)}\alpha_{ij}Wh_j\right) \quad (4)$$

In (4), $\sigma(\cdot)$ denotes a non-linear activation function (Rectified Linear Unit (ReLU)). Further, for improving stability and expressiveness, K parallel attention-heads are utilized as presented in (5):

$$h_i' = ||_{k=1}^{K}\sigma\left(\sum_{j\in\mathcal{N}(i)}\alpha_{ij}^{(k)}W^{(k)}h_j\right) \quad (5)$$

In (5), $||$ indicates concatenation. The resulting embedding matrix $Z = [h_1', h_2', \ldots, h_n']^T$ provides input to the classifier.

D. Classifier

This work presents a hybrid GCN classifier that integrates spectral convolution from traditional GCNs with attention-enhanced aggregation derived using GAT embeddings. This fusion allows the classifier to effectively model both global structure and local contextual relevance. The spectral graph convolution layer transforms node embeddings by aggregating information from neighboring nodes using (6):

$$H^{(l+1)} = \sigma\left(\tilde{D}^{-\frac{1}{2}}\tilde{A}\tilde{D}^{-\frac{1}{2}}H^{(l)}W^{(l)}\right) \quad (6)$$

In (6), $H^{(l)}$ denotes the input feature matrix of layer l, $\tilde{A} = A + I$ denotes the adjacency matrix with added self-connections, $\tilde{D}$ denotes the corresponding degree matrix, and $W^{(l)}$ denotes the trainable weight matrix. Further, for integrating attention, an attention-weighted transformation is introduced as presented in (7):

$$H^{(l+1)} = \sigma\left(\tilde{D}^{-\frac{1}{2}}\tilde{A}\tilde{D}^{-\frac{1}{2}}H^{(l)}W^{(l)} + \beta\mathcal{A}\left(H^{(l)}\right)\right) \quad (7)$$

In (7), β denotes a tunable coefficient that balances the influence between spectral convolution and attention aggregation. The function $\mathcal{A}\left(H^{(l)}\right)$ computes attention-weighted neighbor contributions based on previously learned coefficients α_{ij}. The final output logits for node i are denoted using (8):

$$\ell_i = W_o H_i^{(L)} + b_o \quad (8)$$

Further, the corresponding class probabilities are evaluated using the softmax function using (9):

$$\hat{p}_{ic} = \frac{\exp(\ell_{ic})}{\sum_{k=1}^{C}\exp(\ell_{ik})} \quad (9)$$

In (9), C denotes the number of classes. For handling class imbalance, a class-weighted cross-entropy loss function is utilized as presented in (10):

$$\mathcal{L} = -\frac{1}{N_{train}}\sum_{i=1}^{N_{train}} w_{y_i}\sum_{c=1}^{C}1\{y_i = c\}\log(\hat{p}_{ic}) + \lambda\left|\left|\theta\right|\right|_2^2 \quad (10)$$

In (10), $w_{y_i} = \frac{N_{train}}{C\times N_{y_i}}$ balances class frequencies, λ denotes the regularization coefficient, and θ denotes model parameters. If validation performance is below the threshold, AWGSO is invoked, i.e., for the minority class node i, synthetic samples are generated using (11):

$$\tilde{h} = h_i + \gamma_{ij}(h_j - h_i) \quad (11)$$

In (11), $\gamma_{ij}\sim Uniform(0, \alpha_{ij})$ and j is a neighbor of i within the same class. In this work, Bayesian optimization was utilized for hyperparameter tuning by minimizing the expected validation loss using (12):

$$\theta^* = \arg\min_{\theta\in\Theta}\mathbb{E}_{k-fold}[\mathcal{L}_{val}(\theta)] \quad (12)$$

Further, the overall workflow of AGH-GCN IDS is given in Algorithm 1.

```
Algorithm 1. AGH-GCN IDS for IoMT environments
Input   CICIoMT dataset D with N samples, features X ∈ ℝ^{n×d}, labels Y ∈ {1,…,C}, τ_s similarity threshold for graph construction, K number of attention heads, L number of GCN layers, λ regularization coefficient, θ_init initial model parameters, and perf_threshold minimum acceptable validation performance
Output  ŷ_test, accuracy, precision, recall, and F1-score
Step 1  Start
Step 2  Normalize features in X and split dataset D into training (X_train, Y_train) and testing (X_test, Y_test) subsets
Step 3  Initialize graph G = (V, E, X_train)
Step 4  For each node i in V
          For each node j in V
            Compute similarity using (1)
            If s(i,j) ≥ τ_s
              Add edge (i,j) to E
            End if
          End for
        End for
Step 5  For each node i in V
          For each neighbor j in N(i)
            Compute unnormalized attention using (2)
          Normalize attention using (3)
```

```
        End for
      End for
Step 6 Initialize H^θ = X_train
      For layer l = θ to L − 1
        Evaluate (7)
      End for
Step 7 k_fol_dsplit(X_train, Y_train, k)
      While True
        For each fold f = 1 to k
          Train hybrid GCN on training
          folds
          Validate on fold f
        Compute validation performance
        Perf
        If Perf ≥ Perf_threshold
          break
        Else
          Execute AWGSO
          For each minority class node i
            Select neighbor j of the
            same class
            Generate a synthetic node
            using (11)
          End for
          Add synthetic samples to the
          training set
          Perform Bayesian optimization
          on θ to minimize validation
          loss
        End for
      End while
Step 8 Compute H_test embeddings for X_test
      using the trained GCN
Step 9 Predict class probabilities using
      (9)
Step 10 Obtain predicted labels ŷ_test =
      argmax_c p̂_ic
Step 11 Initialize TP = sum(ŷ_test == 1)&(Y_test =
      = 1), FP = sum(ŷ_test == 1)&(Y_test! = 1),
      FN = sum(ŷ_test! = 1)&(Y_test == 1), TN =
      sum(ŷ_test! = 1)&(Y_test! = 1)
      Compute Accuracy = (TP+TN)/N_test, Precision =
      TP/(TP+FP), Recall = TP/(TP+FN), and F1 =
      (2×Precision×Recall)/(Precision+Recall)
Step 12 Return ŷ_test, accuracy, precision,
      recall, and F1-scores
```

The AGH-GCN IDS integrates a graph-based approach that fuses attention-aware feature learning and hybrid graph convolutional classification. While AGH-GCN IDS is evaluated on IoMT traffic datasets, it primarily focuses on modeling inter-device relationships and class imbalance in network flows. Explicit consideration of medical device criticality, asymmetric misclassification costs, and latency or availability constraints in real-world healthcare systems is not currently implemented. These factors are important for real-time and mission-critical IoMT deployments and will be addressed in future extensions. By dynamically weighting communication relationships and addressing data imbalance through the proposed AWGSO technique, AGH-IDS achieves superior detection of diverse IoMT attack types, ensuring reliable intrusion detection within healthcare IoT infrastructures, as discussed in detail in the results and discussion section.

III. RESULTS AND DISCUSSION

The evaluation of AGH-GCN IDS was conducted on a computing environment equipped with Windows 11, an AMD Ryzen 9 processor, an NVIDIA GTX 5090 GPU, and 64 GB of RAM. The AGH-GCN IDS evaluation was performed on a high-end GPU, and large-scale graph construction for millions of flows was computationally demanding. While offline graph construction and precomputed attention embeddings mitigated online overhead, deployment in hospital networks may face memory and latency constraints. Moreover, the near-real-time detection could be achieved through incremental graph updates or edge-cloud integration. Addressing these practical deployment challenges is part of future work, aiming to make AGH-GCN IDS feasible for resource-constrained IoMT environments. Further, AGH-GCN IDS was implemented using Python and executed within a Python programming environment, ensuring efficient computation for both graph-based feature extraction and hybrid graph-convolutional network training.

For the evaluation of AGH-GCN IDS, the CICIoMT2024 dataset was utilized [10], which is discussed in detail in the methodology section. Further, as discussed in the architecture section, the evaluation in this study is conducted exclusively on the CICIoMT2024 dataset, using an 80:20 train–test split. Devices appeared in both training and test sets, which introduced some dependency between samples. While the dataset is comprehensive and allows for thorough benchmarking, this work acknowledges that generalization to unseen devices or different IoMT deployments may vary.

A. AGH-GCN IDS Performance Evaluation of CICIoMT2024 Binary-Class Classification

Figure 2 shows that AGH-GCN IDS achieves an accuracy of 99.98% for binary-class detection. The attention-based graph embeddings contribute to improved recall for rare attack classes, while AWGSO mitigates class imbalance, explaining the higher F1-scores compared to baseline ML methods. Moreover, the AGH-GCN IDS leverages graph-based feature extraction and attention-driven hybrid graph convolution, enabling it to capture both inter-device relationships and contextual dependencies effectively. This structural understanding, combined with AWGSO to address class imbalance, ensures robust detection of even rare attacks.

B. AGH-GCN IDS Performance Evaluation of CICIoMT2024 Multi-Class Classification

The multi-class evaluation of AGH-GCN IDS demonstrates its effectiveness in detecting and classifying diverse attack types in IoMT networks, as presented in Figure 3. For 6-class

classification, which includes major attack categories and benign traffic, the AGH-GCN IDS achieved 98.45% accuracy, indicating highly reliable performance across all classes.

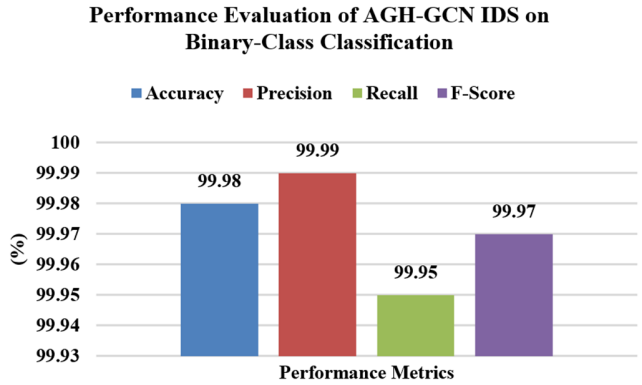

Fig. 2. AGH-GCN IDS performance evaluation of CICIoMT2024 dataset for binary-class classification (2 classes).

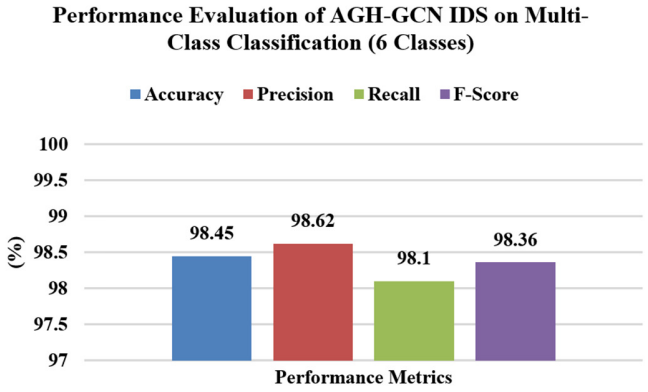

Fig. 3. AGH-GCN IDS performance evaluation of CICIoMT2024 dataset for multi-class classification (6 classes).

Figure 4 presents the performance of AGH-GCN IDS on the 19-class classification task. The AGH-GCN IDS demonstrates high overall accuracy, although lower performance was observed for certain classes, such as DDoS TCP flows, due to class imbalance. The AWGSO method contributes to mitigating this imbalance by generating synthetic samples for minority classes, improving their representation during training. The graph-based feature extraction captures structural relationships between devices, while the hybrid GCN classifier, combining spectral convolution with attention-enhanced aggregation, enables AGH-GCN IDS to leverage both global graph structure and local contextual dependencies. The attention mechanism assigns higher weights to nodes associated with more frequent or influential flows, allowing AGH-GCN IDS to adaptively emphasize important connections. Collectively, these methodological components contribute to the detection of diverse attack types, including rare and fine-grained categories, showing AGH-GCN IDS effectively models inter-device interactions and maintains strong predictive performance across all classes.

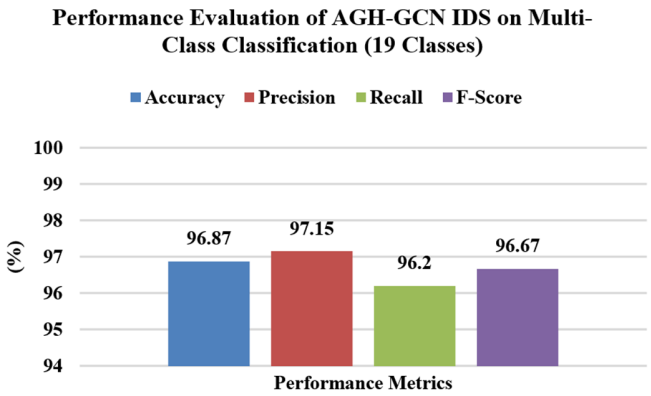

Fig. 4. AGH-GCN IDS performance evaluation of CICIoMT2024 dataset for multi-class classification (19 classes).

C. Ablation Study

To address the risk of overfitting and to provide a clearer insight into the contribution of each component of AGH-GCN IDS, an ablation study has been conducted on the 19-class CICIoMT2024 dataset, where results are presented in Table IV. The study evaluates the model performance by systematically removing or modifying key components: (i) graph-based feature extraction, (ii) hybrid GCN layers, and (iii) AWGSO oversampling. Results are averaged over 5-fold cross-validation, and standard deviations are reported to reflect variability.

TABLE IV. ABLATION STUDY

Component configuration	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)
Full AGH-GCN IDS	96.87±0.12	97.15±0.14	96.20±0.13	96.67±0.12
Without AWGSO	95.32±0.18	95.60±0.20	94.85±0.21	95.22±0.19
Without a hybrid GCN	94.78±0.21	95.02±0.23	94.11±0.22	94.56±0.21
Without graph-based attention features	93.45±0.25	93.80±0.27	92.90±0.26	93.35±0.24

D. Comparative Study

Table V presents a comparative analysis of AGH-GCN IDS against existing ML and DL approaches for binary, 6-class, and 19-class IDS in IoMT networks. In a binary-class scenario, traditional methods like LR, AB, RF, and DNN achieved accuracies between 99.5% and 99.6%, with F1-scores ranging from 94.6% to 96.1%. While these models perform well for binary classification, the proposed AGH-GCN IDS surpasses them, achieving an accuracy of 99.98%, precision of 99.99%, recall of 99.95%, F1-score of 99.97%, and Area Under the Receiver Operating Characteristic (AUC-ROC) curve of 99.98%, demonstrating superior reliability in distinguishing benign and attack traffic.

For 6-class classification, conventional ML approaches exhibited significantly lower performance, with accuracies around 72–74% and F1-scores below 68%, reflecting challenges in handling multiple attack categories. AGH-GCN IDS significantly improves performance, attaining 98.45% accuracy and 98.36% F1-score, highlighting its ability to

capture inter-device relationships and contextual dependencies effectively.

In the 19-class classification, the challenge of fine-grained and imbalanced attack types reduces the performance of existing models, with DNN and RF achieving F1-scores around 55–57%. AGH-GCN IDS outperforms these methods, reaching 96.87% accuracy and 96.67% F1-score, thanks to its graph-based feature extraction, hybrid GCN classification, and AWGSO oversampling.

Overall, the results clearly demonstrate that AGH-GCN IDS provides robust, precise, and reliable intrusion detection across all classification tasks.

TABLE V. COMPARATIVE STUDY

Ref.	Model	Classes	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)	AUC-ROC (%)
[10]	LR	2	99.5	95.2	94	94.6	-
	AB		99.6	95.9	96.1	95.9	-
	DNN		99.6	95.6	94.8	95.2	-
	RF		99.6	97.1	95.1	96.1	-
	LR	6	72.9	74.8	71.2	69.4	-
	AB		43.7	58.7	50.6	50.1	-
	DNN		73.4	72.5	69.3	66.5	-
	RF		73.5	73.5	71.3	67.6	-
	LR	19	72.7	54.7	47.1	43.2	-
	AB		42.2	14.4	23.8	14.1	-
	DNN		72.9	64.9	55.3	52.2	-
	RF		73.3	69.1	57.7	55.1	-
[11]	Unet++LSTM	2	99.92	99.99	99.84	99.92	99.92
		19	87.96	94.55	93.31	96.47	93.64
[13]	XGB	2	97	96	100	98	93
	LR		95	95	89	92	89
	Late Fusion		96	98	91	94	-
Proposed	AGH-GCN IDS	2	99.98	99.99	99.95	99.97	99.98
		6	98.45	98.62	98.1	98.36	98.5
		19	96.87	97.15	96.2	96.67	97.05

IV. CONCLUSION

The proliferation of Internet of Medical Things (IoMT) devices in healthcare has significantly improved patient care but has simultaneously increased the risk of cyberattacks, creating a critical need for robust Intrusion Detection Systems (IDS). Existing approaches based on traditional Machine Learning (ML) and Deep Learning (DL) often struggle to handle class imbalance, model inter-device relationships, and capture contextual dependencies, particularly for fine-grained attack classification.

To address these challenges, this work proposed an Adaptive Graph-based Hybrid Graph Convolutional Network IDS (AGH-GCN IDS), designed to detect and classify cyberattacks in IoMT environments. The model constructs a graph representation of IoMT devices and flows, leverages Graph Attention Networks (GAT) for adaptive feature extraction, and employs a hybrid GCN classifier that integrates spectral convolution with attention-enhanced aggregation. A novel Attention-Weighted Graph Synthetic Oversampling (AWGSO) technique was introduced to mitigate class imbalance.

Extensive experiments on the CICIoMT2024 dataset demonstrate the efficacy of AGH-GCN IDS. The model achieved binary-class accuracy of 99.98%, 6-class accuracy of 98.45%, and 19-class accuracy of 96.87%, outperforming existing ML and DL approaches. These results highlight the ability of AGH-GCN IDS to provide robust and high-performance intrusion detection across diverse attack types.

For future work, AGH-GCN IDS will be extended to an edge-cloud architecture, enabling distributed detection and enhanced security in large-scale IoMT deployments while preserving data privacy and reducing latency. Additionally, future work will explore cross-dataset evaluation, temporal validation, and edge-cloud deployment to further assess the robustness and generalizability of the proposed framework.

DECLARATION OF COMPETING INTERESTS

The authors declare that they have no known competing financial interests, personal relationships, or affiliations that could have appeared to influence the work reported in this paper.

ACKNOWLEDGMENT

The authors acknowledge the creators and maintainers of the CICIoMT2024 dataset for making the dataset publicly available for cybersecurity research in IoMT environments. No external funding was received for this research work.

DATA AVAILABILITY

The data used in this study are publicly available from the CICIoMT2024 dataset, introduced in [10]. The dataset can be accessed from the official repository/publication associated with the dataset [18].

AI USE AND DECLARATION OF GENERATIVE AI USE

During the preparation of this work, the authors used Grammarly AI for English language correction, grammar refinement, and improving the readability of the manuscript. After using this tool, the authors reviewed and edited the content as needed and take full responsibility for the content of the publication.

REFERENCES

[1] D. Alshehri, N. Noman, R. Chiong, S. J. Miah, A. L. Sverdlov, and D. TM. Ngo, "Factors influencing the adoption of Internet of Medical Things for remote patient monitoring: A systematic literature review," *Computers in Biology and Medicine*, vol. 192, June 2025, Art. no. 110142, https://doi.org/10.1016/j.compbiomed.2025.110142.

[2] K. G *et al.*, "Enhancing IoT Resilience at the Edge: A Resource-Efficient Framework for Real-Time Anomaly Detection in Streaming Data," *Computer Modeling in Engineering & Sciences*, vol. 143, no. 3, pp. 3005–3031, June 2025, https://doi.org/10.32604/cmes.2025.065698.

[3] M. F. Ali *et al.*, "HCAP: Hybrid cyber attack prediction model for securing healthcare applications," *Plos One*, vol. 20, no. 5, May 2025, Art. no. e0321941, https://doi.org/10.1371/journal.pone.0321941.

[4] M. Lucia Hernandez-Jaimes, A. Martínez-Cruz, K. Alejandra Ramírez-Gutiérrez, and E. Guevara-Martínez, "Enhancing Machine Learning Approach Based on Nilsimsa Fingerprinting for Ransomware Detection in IoMT," *IEEE Access*, vol. 12, pp. 153886–153897, 2024, https://doi.org/10.1109/ACCESS.2024.3480889.

[5] G. Balhareth and M. Ilyas, "Optimized Intrusion Detection for IoMT Networks with Tree-Based Machine Learning and Filter-Based Feature

Selection," *Sensors*, vol. 24, no. 17, Sept. 2024, Art. no. 5712, https://doi.org/10.3390/s24175712.

[6] S. W. Nourildean, W. Mefteh, and A. M. Frihida, "DTXG-RF-based Intrusion Detection System for Artificial IoT Cyber Attacks," *Engineering, Technology & Applied Science Research*, vol. 15, no. 1, pp. 19610–19614, Feb. 2025, https://doi.org/10.48084/etasr.9464.

[7] A. Salehpour, M. Norouzi, M. A. Balafar, and K. SamadZamini, "A cloud-based hybrid intrusion detection framework using XGBoost and ADASYN-Augmented random forest for IoMT," *IET Communications*, vol. 18, no. 19, pp. 1371–1390, Dec. 2024, https://doi.org/10.1049/cmu2.12833.

[8] R. H. Altaie and H. K. Hoomod, "An Intrusion Detection System using a Hybrid Lightweight Deep Learning Algorithm," *Engineering, Technology & Applied Science Research*, vol. 14, no. 5, pp. 16740–16743, Oct. 2024, https://doi.org/10.48084/etasr.7657.

[9] N. Faruqui *et al.*, "SafetyMed: A Novel IoMT Intrusion Detection System Using CNN-LSTM Hybridization," *Electronics*, vol. 12, no. 17, Sept. 2023, Art. no. 3541, https://doi.org/10.3390/electronics12173541.

[10] S. Dadkhah, E. C. P. Neto, R. Ferreira, R. C. Molokwu, S. Sadeghi, and A. A. Ghorbani, "CICIoMT2024: A benchmark dataset for multi-protocol security assessment in IoMT," *Internet of Things*, vol. 28, Dec. 2024, Art. no. 101351, https://doi.org/10.1016/j.iot.2024.101351.

[11] A. Mezina, J. Nurmi, and A. Ometov, "Novel Hybrid UNet++ and LSTM Model for Enhanced Attack Detection and Classification in IoMT Traffic," *IEEE Access*, vol. 13, pp. 57589–57603, 2025, https://doi.org/10.1109/ACCESS.2025.3553966.

[12] S. Lipsa, R. K. Dash, and N. Ivković, "An interpretable dimensional reduction technique with an explainable model for detecting attacks in Internet of Medical Things devices," *Scientific Reports*, vol. 15, no. 1, Mar. 2025, Art. no. 8718, https://doi.org/10.1038/s41598-025-93404-8.

[13] A. Hafid, M. Rahouti, and M. Aledhari, "Optimizing Intrusion Detection in IoMT Networks Through Interpretable and Cost-Aware Machine Learning," *Mathematics*, vol. 13, no. 10, May 2025, Art. no. 1574, https://doi.org/10.3390/math13101574.

[14] J. Doménech, O. León, M. S. Siddiqui, and J. Pegueroles, "Evaluating and enhancing intrusion detection systems in IoMT: The importance of domain-specific datasets," *Internet of Things*, vol. 32, July 2025, Art. no. 101631, https://doi.org/10.1016/j.iot.2025.101631.

[15] R. Sharma, N. Sharma, and S. Nandan Mohanty, "Attack Detection in Internet of Medical Things Through Ensemble Machine Learning Models," *Security and Privacy*, vol. 8, no. 3, May 2025, Art. no. e70042, https://doi.org/10.1002/spy2.70042.

[16] L. Alsbatin, B. M. Alrifai, F. Zawaideh, and T. A. Alawneh, "Advancing IoMT Security: Machine Learning-Based Detection and Classification of Multi-Protocol Cyberattacks," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, vol. 16, no. 2, pp. 228–247, June 2025, https://doi.org/10.58346/JOWUA.2025.I2.015.

[17] H. Moudoud, Z. Abou El Houda, and B. Brik, "Advancing Privacy and Fairness in Healthcare Using Federated Edge Learning and Blockchain," *IEEE Internet of Things Journal*, vol. 12, no. 22, pp. 46129–46137, Nov. 2025, https://doi.org/10.1109/JIOT.2025.3589179.

[18] "CIC IoMT dataset 2024." Canadian Institute for Cybersecurity, University of New Brunswick. [Online]. Available: https://www.unb.ca/cic/datasets/iomt-dataset-2024.html.