International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(18s) 2026 pp. 424-437
https://doi.org/10.70917/ijcisim-2026-4880
Article

Deep learning-based Attack Detection in Internet of Medical Things Network using Deep Convolutional Neural Network and Long Short-Term Memory

Rajashree Bhokare[1], Urmila Patil[2]

[1]Department of Electrical Engineering, Dr. D. Y. Patil Institute of Technology, Pimpri, Pune, Maharashtra 411018, India
[2]Department of Electronics and Telecommunication Engineering, Dr. D. Y. Patil Institute of Technology, Pimpri, Pune, Maharashtra 411018, India
[1]rajashree.bhokare2020@gmail.com, 2urmilaapatil76@gmail.com

Abstract: The rapid growth of Industry 4.0 has led to the use of artificial intelligence and the Internet of Medical Things (IoMT) in many healthcare applications, facilitating remote diagnosis, data collection, data analysis, and healthcare management. The IOMT provides a healthcare framework that collects biomedical data from patients via sensors or devices, stores it in the cloud, analyzes it, and provides clinical diagnoses. However, the privacy, security, reliability, and integrity of the healthcare data is challenging due to different cyber attacks on the IoMT framework. Therefore, this paper presents a deep learning-based network attack detection method, IoMT attack detection (IADNet), based on a 1-D deep convolutional neural network to capture multilevel correlations and a long short-term memory (LSTM) to capture long-term dependencies in network attributes. Further, it provides the dynamic synthetic minority oversampling technique (DSMOTE) for data augmentation, mitigating data scarcity by generating synthetic samples for training. The IADNet provides the overall accuracy of 99.12%, precision of 99.12%, recall of 95.50%, and F1-score of 97.24% for the original dataset, whereas it resulted in improved accuracy of 99.80%, recall of 98.80%, precision of 98.80%, and F1-score of 98.80% for the DSMOTE augmented dataset.
Keywords: IoMT, Wireless Sensor Network, SMOTE, DCNN, LSTM, Attack Detection, Cyber Security

1. Introduction

The Internet of Medical Things (IoMT) framework consists of wearable sensors, smart medical devices, and remote patient monitoring systems [1]. The IoMT enables real-time diagnosis, data sharing, and treatment. IoMT devices operate in real-world critical environments 24/7 and are highly susceptible to single points of failure, which can compromise privacy and safety. Security in IoMT is critical due to the high sensitivity of healthcare data and the associated security threats [2]. The major security attacks include data breaches, device hijacking, malware, malicious node attacks, sybil attacks, evasdroping, sinkhole attacks, ransomware, man-in-the-middle attacks, replay attacks, and false data injection [3-5]. Various security attacks on healthcare networks lead to incorrect diagnoses, identity theft, treatment manipulation, hospital service disruptions, and legal and financial losses. Therefore, it is necessary to ensure integrity, availability, confidentiality, access control, and authentication [6-10].

Various attack-detection frameworks have been proposed to enhance IoT and WSN security. Muhammad et al. [11] suggested the histogram of gradient boosting (HGB) for malicious node detection for the WSN-DS dataset. It enhances data storage security using a blockchain-based distributed storage mechanism. Osma et al. [12] presented a malicious node detection framework for WSNs using a random forest (RF) classifier. The RF classifier captures patterns in network attributes under normal and malicious conditions and achieves 99.5% accuracy on the

SensorNetGuard dataset. However, the dataset's class imbalance reduces the system's reliability for real-time analysis. Further, Osam et al. [13] proposed CNN framework for malicious node detection along with adaptive synthetic sampling (ADASYN) for data augmentation. The CNN and CNN-ADASYN achieve overall accuracies of 96.5% and 99% on the SensorNetGuard dataset, indicating that data augmentation improves the system's accuracy. However, ADASYN introduces less realistic, noisier samples due to the generation of borderline synthetic samples.

Almakayeel and Lydia [14] proposed a sand cat swarm optimization algorithm for feature selection and a deep ensemble classifier that combines LSTM, extreme learning machine (ELM), and deep neural networks (DNNs) for malicious node detection. It achieved 98.97% accuracy on the ISCX 2012 IDX dataset. However, the ensemble classifier's complexity is higher, reducing the algorithm's deployment flexibility. Bilal et al. [15] presented a hybrid DL framework based on CNN and gated recurrent unit (GRU) for predicting malicious traffic in industrial Internet of Things (IoT) networks. It suggests that the performance of the DL algorithms is highly sensitive to hyperparameter tuning. Proper hyperparameter tuning helps to improve the effectiveness of the DL model. Furthermore, Sathishkumar et al. [16] explored a fuzzy temporal LSTM for Denial-of-Service (DoS) attack detection in WSNs. It utilized temporal modeling and a fuzzy system for LSTM weight fitting to improve the temporal representation and distinctiveness of the features. It provided an overall accuracy of 99.58% for the KDDCup99 and NSL-KDD datasets. Gunjal et al. [17] suggested a DCNN-LSTM framework based on score-level fusion for malicious node detection in WSN. The DCNN-LSTM achieved an overall accuracy of 99.80% on the SMOTE-augmented dataset. The score level fusion needs independent training for the DCNN and LSTM, which increases the computational intricacy and fails to capture the correlation in DCNN and LSTM attributes. However, the algorithm's effectiveness is limited by extensive hyperparameter tuning of the DCNN-LSTM framework and reduced variability in the augmented dataset. From the literature survey, various research gaps have been identified that need to be addressed to improve the service quality of the IoMT framework. Ileri et al. [18] proposed an LSTM-based intrusion detection framework for the IoMT that uses chi-square feature selection. The feature selection helps minimize the computational complexity of intrusion detection systems and achieves 99.27% accuracy with 20 features from the MedSec-25 dataset. Although the LSTM achieved superior accuracy, its generalization capability is limited on the other dataset, and no statistical results were presented to assess the model's stability on an imbalanced dataset.

Based on an extensive survey of intrusion detection systems in IoMT frameworks, the following research gaps have been identified.

- Lower long-term dependency in sequential categorical data, which fails to provide correlation in features.
- Class imbalance problem due to limited training samples for the attack classes.
- Poor generalization capability for the intrusion detection system.
- High computational intricacy due to complicated models of attack detection.
- Lower accuracy due to noisy, outlier, and missing attributes in the dataset.
- Limited explainability and interpretability of the intrusion detection system that limits the trust in the system.

Thus, this paper presents a cyberattack detection framework to improve the integrity and security of healthcare data in the IoMT ecosystem. The main contributions of the paper are summarized as follows:

- Development of the cybewer attack detection framework for the IoMT, based on IADNet, that combines parallel DCNN and BILSTM to capture high-level distinguishing correlations and long-term dependencies in network attributes.
- Development of the dynamic SMOTE for the data augmentation based on dynamic neighbor selection for generating a synthetic dataset to minimize the class overlapping issue, lower feature correlation, and borderline sample generation issue.

- The results of the attack detection framework is evaluated on the MedSec-25 dataset for detecting Benign, exfiltration, initial access, lateral movement, and reconnaissance attacks.

The remaining article is structured as follows: Section 2 presents the methodology of the attack-detection framework for the IoMT. Section 3 provides a detailed discussion of the simulation results for the attack detection system. Lastly, section 4 offers the conclusions of the attack detection system and its potential future scopes.

2. Methodology

The flow of the IADNet-based intrusion detection system for the IoMT framework is shown in Fig. 1 and comprises data preprocessing, feature extraction, and classification.

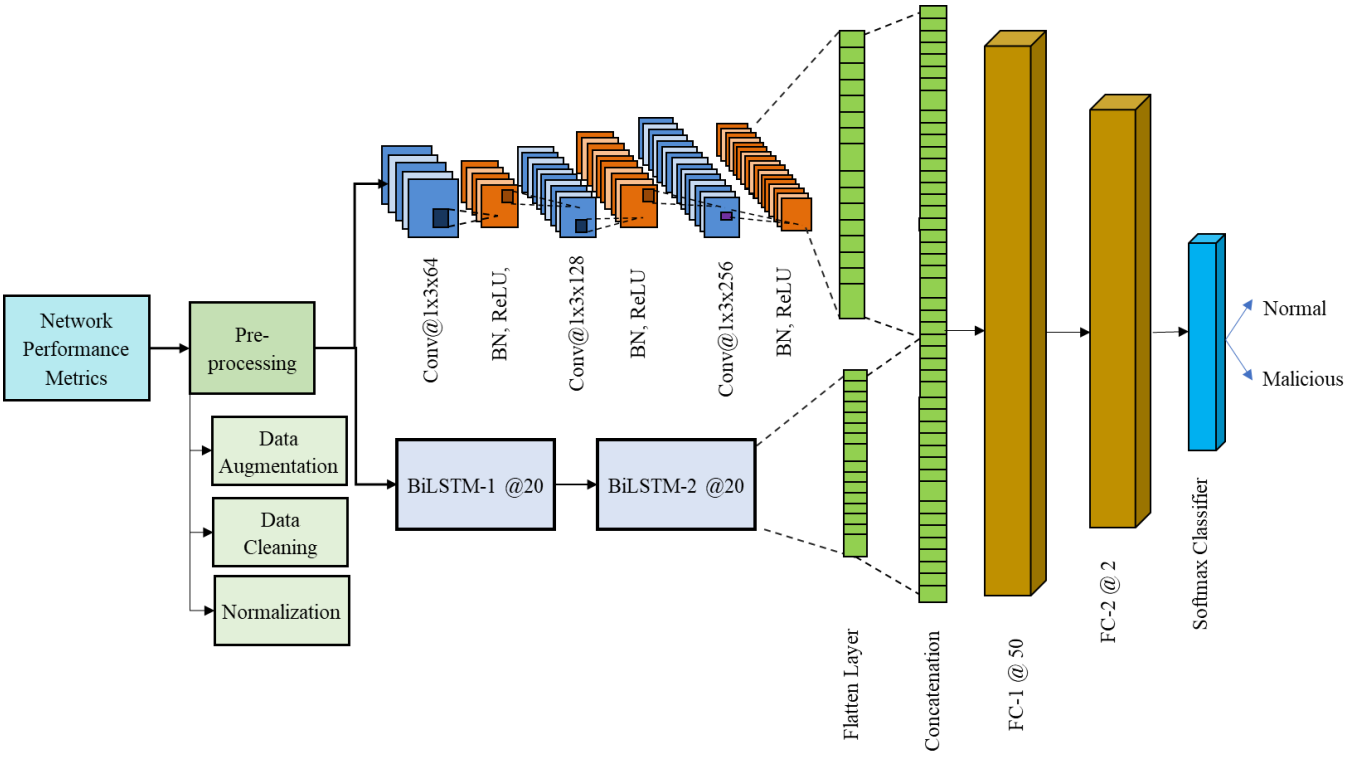


Fig. 1 Flow diagram of the proposed IoMT attack detection system

Fig. 1 presents the flow diagram of the proposed IoT network security mechanism, comprising data preprocessing, attack detection, and performance evaluation. The preprocessing included data normalization, cleaning, and data augmentation. The raw data is normalized using z-score normalization, and data cleaning is performed to remove outliers and missing values in the network attributes. The proposed network attack detection network consists of a 1-D DCNN and a BiLSTM in parallel to provide deep, high-level, complex feature representations. The DCNN captures correlations and complex patterns in network attributes, whereas the BiLSTM models temporal dependencies and long-term correlations. The three-layer DCNN with 64, 128, and 256 filters at three consecutive layers is used for feature depiction. Every convolution layer is followed by a rectified linear unit layer (ReLU) and a batch normalization (BN) layer. The ReLU layer enhances the non-linear characteristics of the features, improving the system's accuracy. The BN layer standardizes the deep features to minimize the outliers in deep features for enhancing the speed of training. The output of the last BN layer in DCNN and the second BiLSTM-2 are flattened and concatenated together. Further, a fully connected layer with 50 hidden neurons is used to improve feature connectivity by connecting each input neuron to all other neurons, thereby capturing correlations between DCNN and BiLSTM features. Finally, a softmax classifier is utilized to predict the normal and attack conditions in the network.

2.1 Dynamic SMOTE-based Data Augmentation

SMOTE is a simple technique for sequential data augmentation that has shown noteworthy improvements in mitigating class imbalance in many applications by creating synthetic data. However, the effectiveness of the SMOTE is limited due to poor intra-class and inter-class disparity, prone to noise, distortion in decision boundaries, and less feature representation due to ignorance of data distribution [20-21]. The improved SMOTE accounts for overlap when selecting neighbors to dynamically generate synthetic samples. The flow of the DSMOTE is provided in Fig. 2.

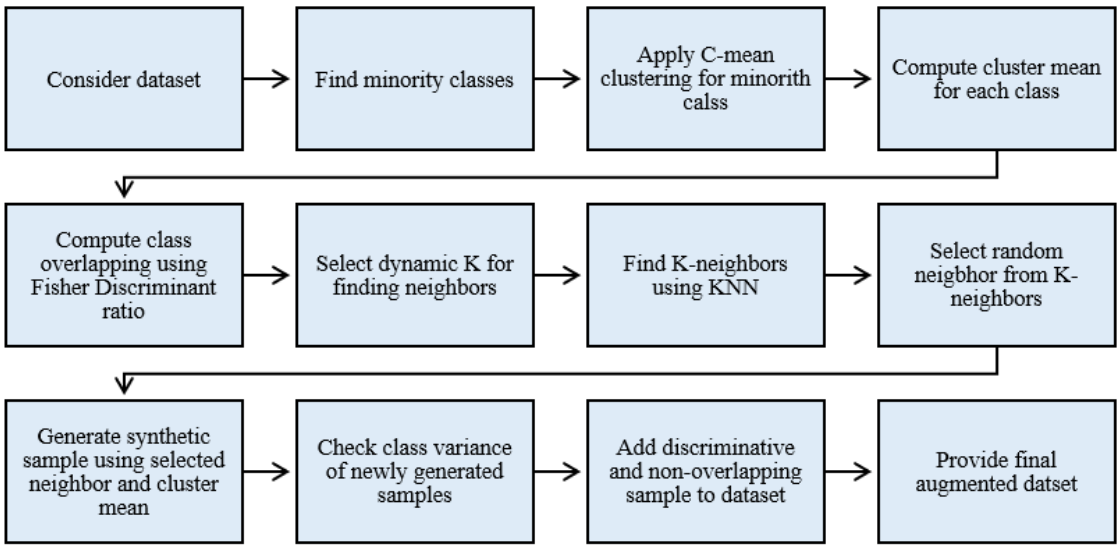


Fig. 2 Flow of DSMOTE-based data augmentation

The stages of the improved SMOTE are provides as follows:

Step 1: Consider the input data and class labels as $\{x_i, C_i\}$.

Step 2: Find the class with minority samples

Step 3: Apply C-mean clustering for the minority class and compute the cluster means as xc_{mean}.

Step 4: Compute class overlap: Fisher's discriminant ratio (FDR) is used to measure class overlap for the network attributes. If the FDR value is higher, it indicates better class separation; if it is lower, it indicates greater overlap in the class attributes. The FDR is computed using the equation 1 where C denotes the number of classes, n_i signifies the number of samples in class i, μ_i stands for the mean of the class i, μ symbolizes the overall mean of all classes and σ_i^2 denotes the variance of the class i.

$$FDR = \left(\sum_{i=1}^{C} n_i(\mu_i - \mu)^2\right) / \left(\sum_{i=1}^{C} n_i\sigma_i^2\right) \quad (1)$$

Step 5: Select a higher value of K (K=5) for lower overlapping EDR<0.5 and a lower value of K for higher overlapping (K=1) to avoid class overlapping.

Step 6: Apply the K-Nearest Neighbors algorithm to find the nearest neighbor of the chosen sample.

Step 7: Generate the synthetic samples for selected sample x_{old} using Equation 2, where r1 is an arbitrary number lying in 0 and 1, x_{nn} is randomly selected neighbor from the K neighbors and X_{new} denotes newly generated sample.

$$X_{new} = x_{old} + r1 * \left(x_{old} - \frac{xc_{mean} + x_{nn}}{2}\right) \quad (2)$$

Step 8: Compute the distance of the newly generated sample and old sample with the cluster mean of x_{old} using Euclidean distance as given in equation 3 and 4 respectively.

$$d1 = \sqrt{X_{new}{}^2 - xc_{mean}} \quad (3)$$

$$d2 = \sqrt{X_{old}{}^2 - xc_{mean}} \quad (4)$$

Step 9: If the distance between the newly generated sample and cluster mean is greater than the distance between the old sample and cluster mean, then the sample is added to the synthetic dataset; otherwise, the sample is discarded.

Step 10: Repeat step 2-9 till considered class samples count reaches to majority class samples count.

3. Results and Discussions

The proposed system is simulated in MATLAB R2025b on a personal computer with a Core i7 processor, 20 GB of RAM, and 4 GB of graphics memory. The hyperparameters used in the IADNet implementation are listed in Table 1.

Table 1: Parameters of the IADNet

Parameter	**Specification**
Loss function	Cross-Entropy
Learning rate	0.001
Optimization Method	Adam
Epoch	100
Dropout	0.5
Momentum	0.8

3.1 Dataset

The MedSec-25 [19] dataset contains 84 features generated by CICFlowMeter, designed to capture various characteristics of network traffic in a clear and structured manner. MedSec-25 is a comprehensive, tagged network traffic dataset designed specifically for the Internet of Medical Things (IoMT) in hospital environments. It addresses the limitations of existing generic IoT datasets by capturing real traffic from a purpose-built healthcare IoT lab that mimics real hospital operations. The collection includes both malicious and benign (normal) traffic from multi-stage attack campaigns based on MITRE ATT&CK techniques. The details of various features is provided in Table 2.

Table 2: Details about the features of the MedSec-25 dataset

Category	**Description**	**Example Features**	**No. of Features**
Identifiers	Basic information that uniquely defines each network flow/session	Flow ID, Src IP, Src Port, Dst IP, Dst Port, Protocol, Timestamp	7

Time-Series Metrics	Describe timing behavior of packets within flows	Flow Duration, Flow IAT Mean/Std/Max/Min, Fwd/Bwd IAT Tot/Mean/Std/Max/Min	15
Size & Count Stats	Capture volume and statistical distribution of packets and bytes	Tot Fwd/Bwd Pkts, TotLen Fwd/Bwd Pkts, Pkt Len Mean/Std/Min/Max	18
Flag Counts	Represent TCP control flags indicating connection states	SYN, ACK, FIN, RST, PSH, URG, CWE, ECE Flag Counts	8
Rates & Ratios	Measure traffic speed and directional relationships	Flow Byts/s, Flow Pkts/s, Fwd/Bwd Pkts/s, Down/Up Ratio	10
Activity Metrics	Describe active and idle periods of network flows	Active Mean/Std/Max/Min, Idle Mean/Std/Max/Min	8
Segmentation Features	Provide details about flow structure and segmentation	Fwd/Bwd Seg Size Avg/Min, Subflow Fwd/Bwd Pkts/Byts	10
Advanced Metrics	Additional flow-level characteristics for deeper analysis	Init Win Bytes, Fwd Act Data Pkts, Block Rate Avg	8

The dataset consists of 12348 samples for benign (normal), 25915 for exfiltration, 102090 for initial access, 12498 for lateral movement, and 401683 for reconnaissance. We have augmented the samples to 401,683 per class to mitigate data scarcity. The details of the original and augmented datasets are provided in Table 3, where the original dataset consists of 554534 samples, and the augmented dataset includes 2008415 samples across the five classes.

Table 3: Details of original and augmented samples of MedSec-25 dataset

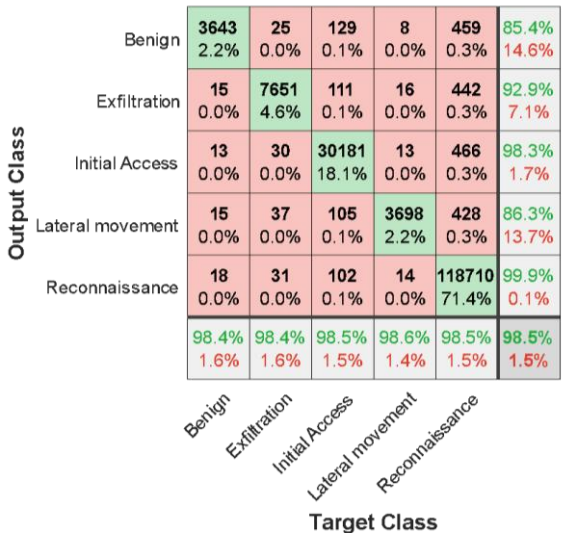
Class	**Original Samples**	**Augmented Samples**
Benign	12348	401683
Exfiltration	25915	401683
Initial Access	102090	401683
Lateral movement	12498	401683
Reconnaissance	401683	401683
Total Samples	554,534	2,008,415

3.2 Discussions on Results

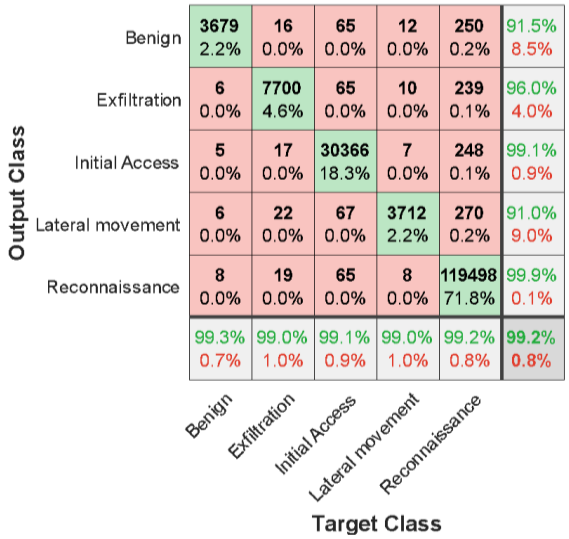
The confusion matrices for the DCNN, BiLSTM, and IADNet for the five-class attack detection on the MedSec-25 dataset are provided in Fig. 3.


Output Class
Benign
Exfiltration
Initial Access
Lateral movement
Reconnaissance
3628 2.2%
40 0.0%
148 0.1%
15 0.0%
612 0.4%
81.7% 18.3%
18 0.0%
7601 4.6%
152 0.1%
23 0.0%
661 0.4%
89.9% 10.1%
16 0.0%
42 0.0%
29983 18.0%
14 0.0%
638 0.4%
97.7% 2.3%
23 0.0%
44 0.0%
189 0.1%
3681 2.2%
676 0.4%
79.8% 20.2%
19 0.0%
47 0.0%
156 0.1%
16 0.0%
117918 70.9%
99.8% 0.2%
97.9% 2.1%
97.8% 2.2%
97.9% 2.1%
98.2% 1.8%
97.9% 2.1%
97.9% 2.1%
Benign
Exfiltration
Initial Access
Lateral movement
Reconnaissance
Target Class

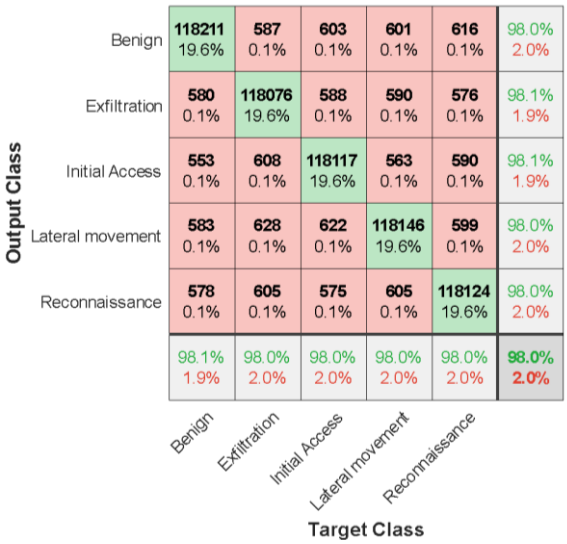
a)


Output Class
Benign
Exfiltration
Initial Access
Lateral movement
Reconnaissance
3643 2.2%
25 0.0%
129 0.1%
8 0.0%
459 0.3%
85.4% 14.6%
15 0.0%
7651 4.6%
111 0.1%
16 0.0%
442 0.3%
92.9% 7.1%
13 0.0%
30 0.0%
30181 18.1%
13 0.0%
466 0.3%
98.3% 1.7%
15 0.0%
37 0.0%
105 0.1%
3698 2.2%
428 0.3%
86.3% 13.7%
18 0.0%
31 0.0%
102 0.1%
14 0.0%
118710 71.4%
99.9% 0.1%
98.4% 1.6%
98.4% 1.6%
98.5% 1.5%
98.6% 1.4%
98.5% 1.5%
98.5% 1.5%
Benign
Exfiltration
Initial Access
Lateral movement
Reconnaissance
Target Class

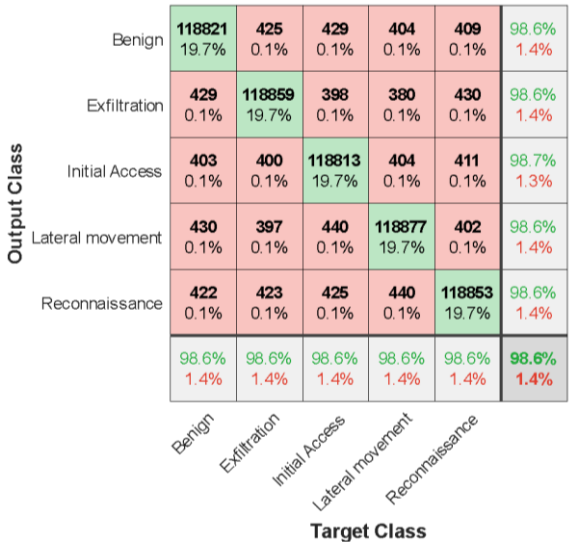
b)

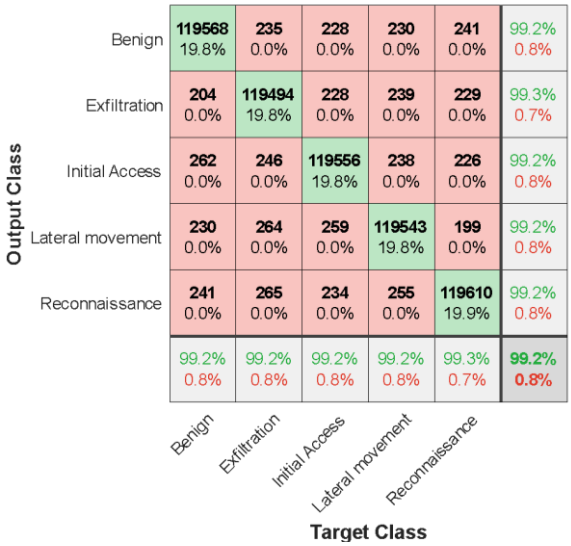

Output Class
Benign
Exfiltration
Initial Access
Lateral movement
Reconnaissance
3679 2.2%
16 0.0%
65 0.0%
12 0.0%
250 0.2%
91.5% 8.5%
6 0.0%
7700 4.6%
65 0.0%
10 0.0%
239 0.1%
96.0% 4.0%
5 0.0%
17 0.0%
30366 18.3%
7 0.0%
248 0.1%
99.1% 0.9%
6 0.0%
22 0.0%
67 0.0%
3712 2.2%
270 0.2%
91.0% 9.0%
8 0.0%
19 0.0%
65 0.0%
8 0.0%
119498 71.8%
99.9% 0.1%
99.3% 0.7%
99.0% 1.0%
99.1% 0.9%
99.0% 1.0%
99.2% 0.8%
99.2% 0.8%
Benign
Exfiltration
Initial Access
Lateral movement
Reconnaissance
Target Class

c)


Output Class
Benign
Exfiltration
Initial Access
Lateral movement
Reconnaissance
118211 19.6%
587 0.1%
603 0.1%
601 0.1%
616 0.1%
98.0% 2.0%
580 0.1%
118076 19.6%
588 0.1%
590 0.1%
576 0.1%
98.1% 1.9%
553 0.1%
608 0.1%
118117 19.6%
563 0.1%
590 0.1%
98.1% 1.9%
583 0.1%
628 0.1%
622 0.1%
118146 19.6%
599 0.1%
98.0% 2.0%
578 0.1%
605 0.1%
575 0.1%
605 0.1%
118124 19.6%
98.0% 2.0%
98.1% 1.9%
98.0% 2.0%
98.0% 2.0%
98.0% 2.0%
98.0% 2.0%
98.0% 2.0%
Benign
Exfiltration
Initial Access
Lateral movement
Reconnaissance
Target Class

d)


Output Class
Benign
Exfiltration
Initial Access
Lateral movement
Reconnaissance
118821 19.7%
425 0.1%
429 0.1%
404 0.1%
409 0.1%
98.6% 1.4%
429 0.1%
118859 19.7%
398 0.1%
380 0.1%
430 0.1%
98.6% 1.4%
403 0.1%
400 0.1%
118813 19.7%
404 0.1%
411 0.1%
98.7% 1.3%
430 0.1%
397 0.1%
440 0.1%
118877 19.7%
402 0.1%
98.6% 1.4%
422 0.1%
423 0.1%
425 0.1%
440 0.1%
118853 19.7%
98.6% 1.4%
98.6% 1.4%
98.6% 1.4%
98.6% 1.4%
98.6% 1.4%
98.6% 1.4%
98.6% 1.4%
Benign
Exfiltration
Initial Access
Lateral movement
Reconnaissance
Target Class


Output Class
Benign
Exfiltration
Initial Access
Lateral movement
Reconnaissance
119568 19.8%
235 0.0%
228 0.0%
230 0.0%
241 0.0%
99.2% 0.8%
204 0.0%
119494 19.8%
228 0.0%
239 0.0%
229 0.0%
99.3% 0.7%
262 0.0%
246 0.0%
119556 19.8%
238 0.0%
226 0.0%
99.2% 0.8%
230 0.0%
264 0.0%
259 0.0%
119543 19.8%
199 0.0%
99.2% 0.8%
241 0.0%
265 0.0%
234 0.0%
255 0.0%
119610 19.9%
99.2% 0.8%
99.2% 0.8%
99.2% 0.8%
99.2% 0.8%
99.2% 0.8%
99.3% 0.7%
99.2% 0.8%
Benign
Exfiltration
Initial Access
Lateral movement
Reconnaissance
Target Class

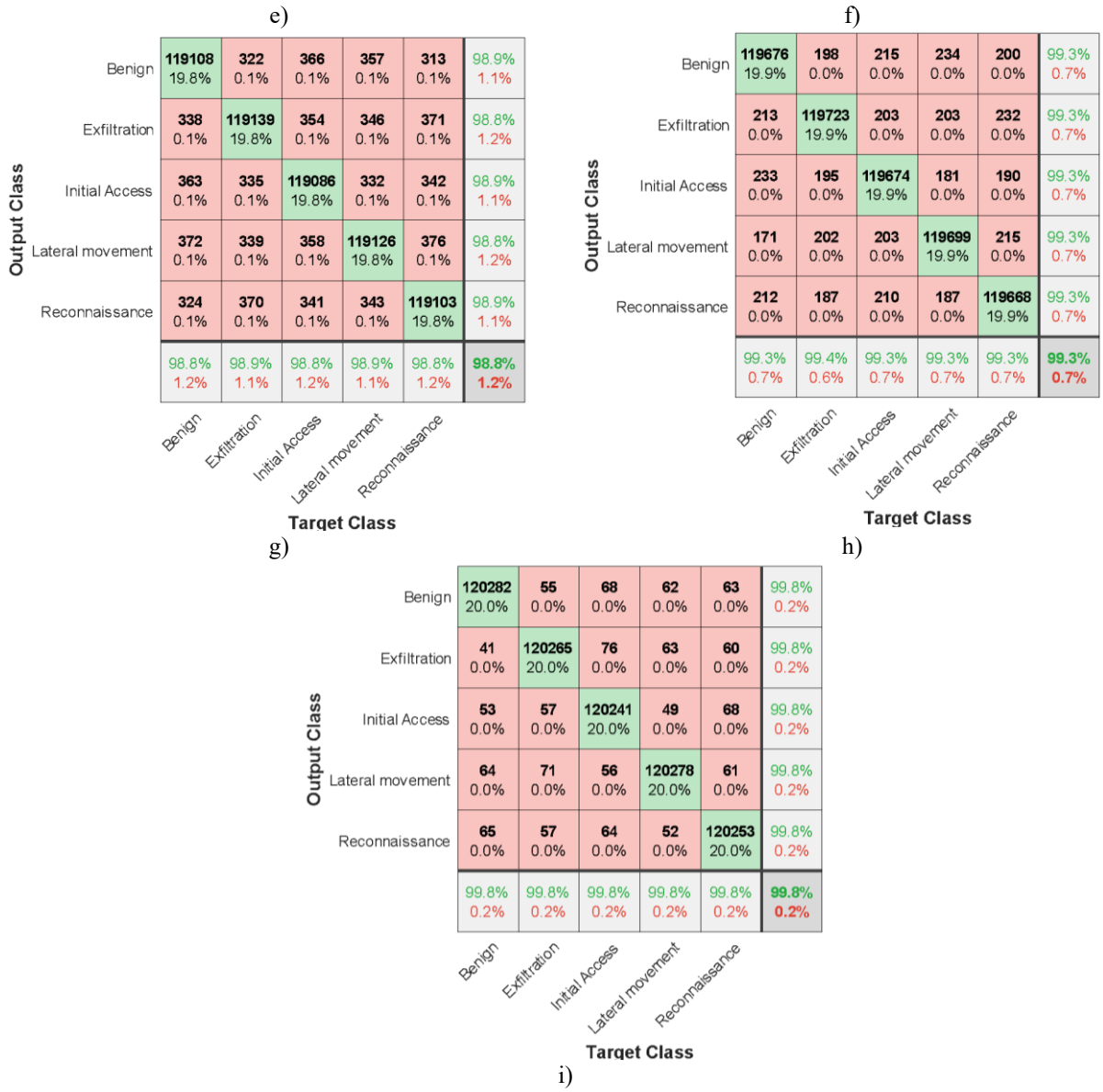


Fig. 4 Confusion matrx for attack detection in IoMT for MedSec-25 dataset for a-c) DCNN, BiLSTM, and IADNet for original dataset; d-f) DCNN, BiLSTM, and IADNet for SMOTE augmented dataset; g-i) DCNN, BiLSTM, and IADNet for DSMOTE augmented dataset;

Table 4 shows the results of attack detection in IoMT using DCNN, BiLSTM, and IADNet on the original, SMOTE-augmented, and DSMOTE-augmented datasets. The DCNN-BiLSTM achieves an overall accuracy of 99.12%, a recall of 99.12%, a precision of 95.50%, and an F1-score of 97.24% on the original dataset, indicating a notable disparity between recall and precision. The lower number of training samples results in poor precision of 91% and 91.50% and for the reconnaissance and benign class which decreases the F1-score of the system. This class imbalance problem limits the deployment flexibility for the real-time attack detection system, where quality of service is very important. The DCNN resulted in an average accuracy of 97.94%, recall of 97.94%, precision of 89.98%, and F1-score of 93.59%, whereas BilSTM shows better temporal modeling and long-term depiction that provides an average accuracy of 98.48%, recall of 98.48%, precision of 92.56% and F1-score of 95.33% for 5-class attack detection. The SMOTE-based data augmentation provides a very minor improvement in the system's accuracy and recall but shows significant improvements in the system's F1-score and precision. The IADNet shows balanced recall and precision, achieving an overall accuracy, recall, precision, and F1-score of 99.22% for the SMOTE-augmented

dataset. The DSMOTE offers improved results compared to SMOTE, helping minimize data clustering, borderline sample creation, and interclass and intraclass disparities in augmented samples. The IADNet achieves an accuracy of 99.80%, a recall of 99.80%, a precision of 99.870%, and an F1-score of 99.80% on the DSMOTE-augmented dataset. The IADNEt achieves an improved F1-score of 98.8% across all attack types, representing a significant boost over the F1-Scores of the SMOTE-augmented and original datasets. The results are visualized in Fig. 4-7 respectively.

Table 4: Results comparison of attack detection methods for the original, SMOTE augmented and ISMOTE augmented datasets

Method	Attack Type	DCNN				BiLSTM				IADNet (DCNN-BiLSTM)			
		Accuracy	Recall	Precision	F1-score	Accuracy	Recall	Precision	F1-score	Accuracy	Recall	Precision	F1-score
Original Dataset	Benign	97.90	97.90	81.70	89.07	98.40	98.40	85.40	91.44	99.30	99.30	91.50	95.24
	Exfiltration	97.80	97.80	89.90	93.68	98.40	98.40	92.90	95.57	99.00	99.00	96.00	97.48
	Initial Access	97.90	97.90	98.70	98.30	98.50	98.50	98.30	98.40	99.10	99.10	99.10	99.10
	Lateral Movement	98.20	98.20	79.80	88.05	98.60	98.60	86.30	92.04	99.00	99.00	91.00	94.83
	Reconnaissance	97.90	97.90	99.80	98.84	98.50	98.50	99.90	99.20	99.20	99.20	99.90	99.55
	Average	**97.94**	**97.94**	**89.98**	**93.59**	**98.48**	**98.48**	**92.56**	**95.33**	**99.12**	**99.12**	**95.50**	**97.24**
SMOTE Augmented Dataset	Benign	98.10	98.10	98.00	98.05	98.60	98.60	98.60	98.60	99.20	99.20	99.20	99.20
	Exfiltration	98.00	98.00	98.10	98.05	98.60	98.60	98.60	98.60	99.20	99.20	99.30	99.25
	Initial Access	98.00	98.00	98.10	98.05	98.60	98.60	98.70	98.65	99.20	99.20	99.20	99.20
	Lateral Movement	98.00	98.00	98.00	98.00	98.60	98.60	98.60	98.60	99.20	99.20	99.20	99.20
	Reconnaissance	98.00	98.00	98.00	98.00	98.60	98.60	98.60	98.60	99.30	99.30	99.20	99.25
	Average	**98.02**	**98.02**	**98.04**	**98.03**	**98.60**	**98.60**	**98.62**	**98.61**	**99.22**	**99.22**	**99.22**	**99.22**
DSMOTE Augmented Dataset	Benign	98.80	98.80	98.90	98.85	99.30	99.30	99.30	99.30	99.80	99.80	99.80	99.80
	Exfiltration	98.90	98.90	98.90	98.90	99.40	99.40	99.30	99.35	99.80	99.80	99.80	99.80
	Initial Access	98.80	98.80	98.90	98.85	99.30	99.30	99.30	99.30	99.80	99.80	99.80	99.80
	Lateral Movement	98.90	98.90	98.80	98.85	99.30	99.30	99.30	99.30	99.80	99.80	99.80	99.80
	Reconnaissance	98.80	98.80	98.90	98.85	99.30	99.30	99.30	99.30	99.80	99.80	99.80	99.80
	Average	**98.84**	**98.84**	**98.88**	**98.86**	**99.32**	**99.32**	**99.30**	**99.31**	**99.80**	**99.80**	**99.80**	**99.80**

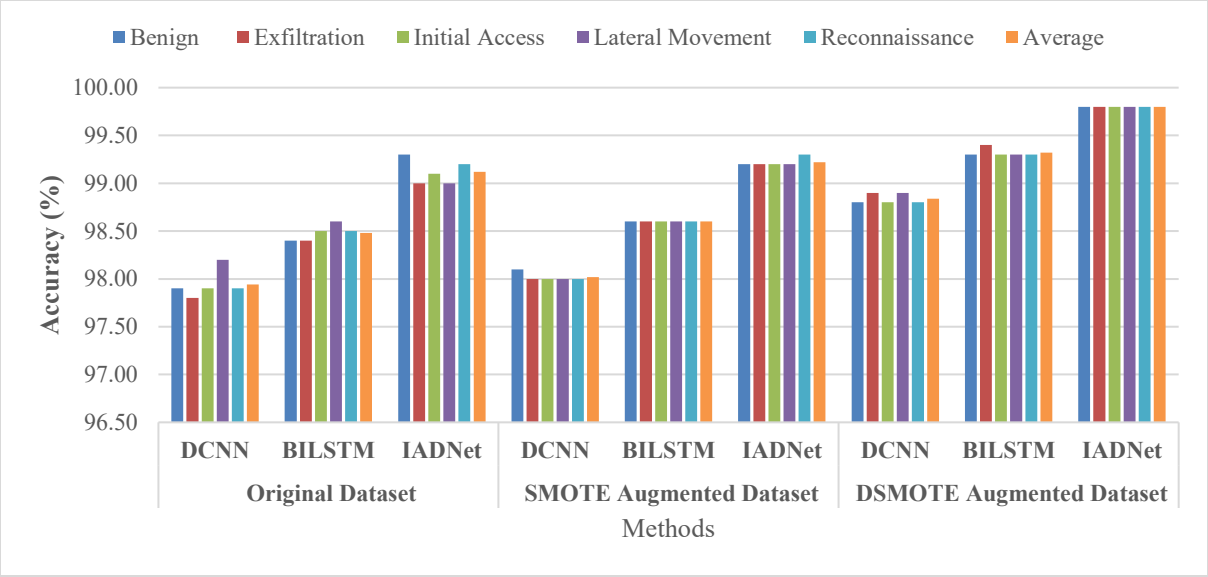


Fig. 4 Accuracy comparison for various methods for original and augmented datasets for different attacks

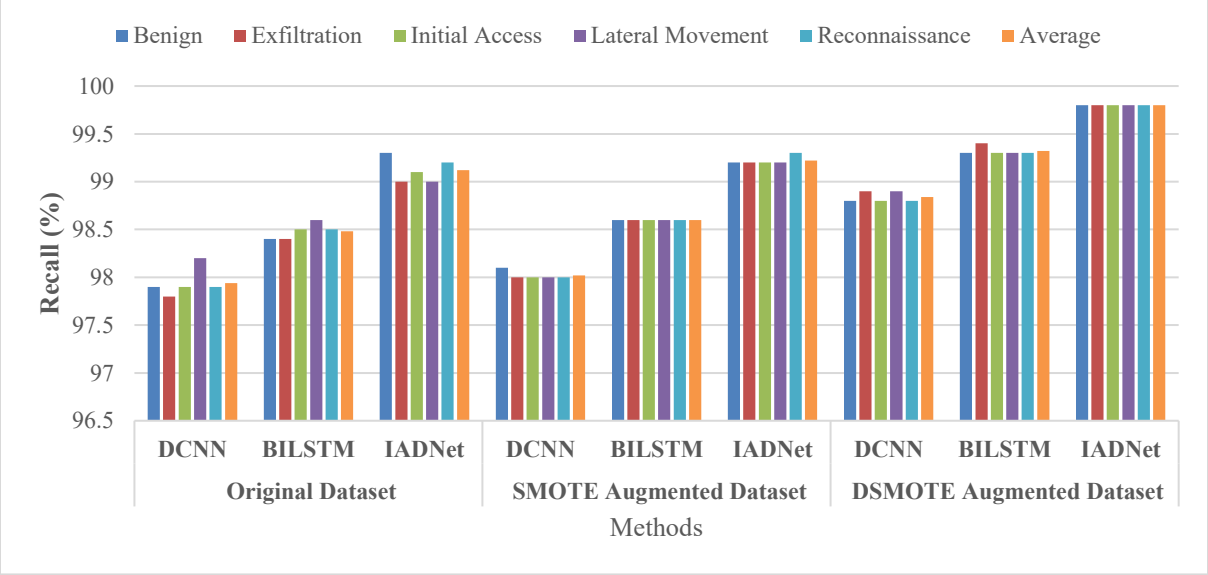


Fig. 5 Recall comparison for various methods for original and augmented datasets for different attacks

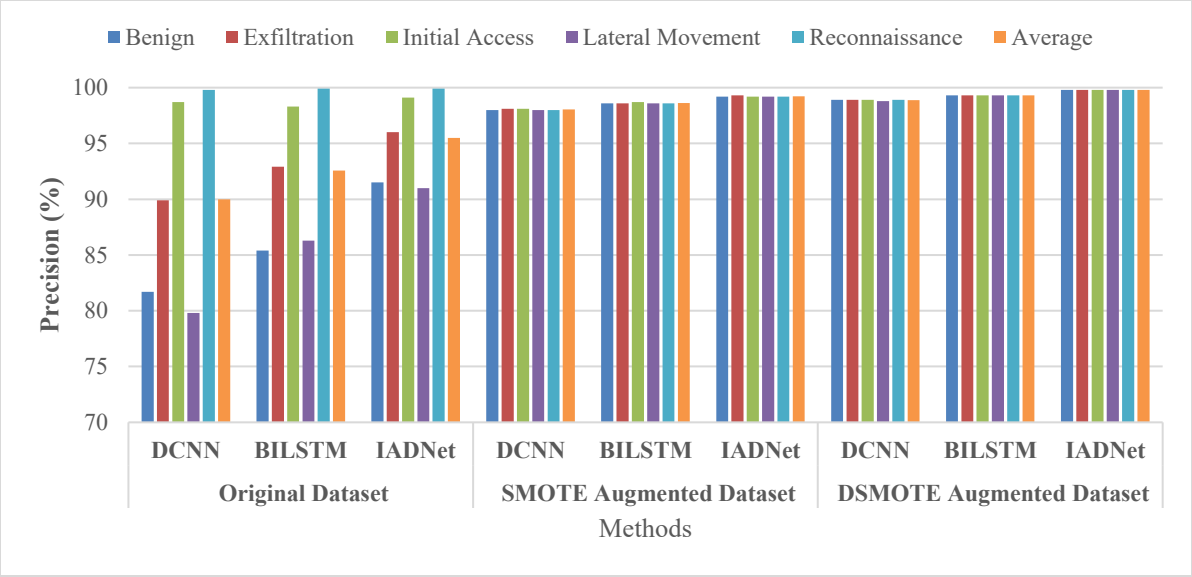


Fig. 6 Precision comparison for various methods for original and augmented datasets for different attacks

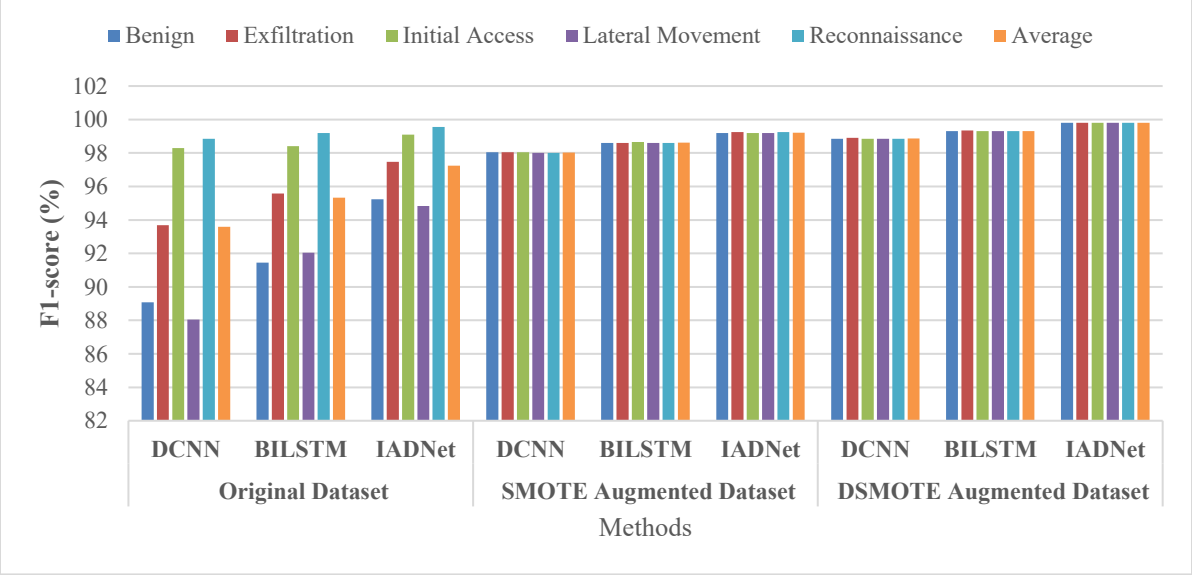


Fig. 7 F1-score comparison for various methods for original and augmented datasets for different attacks

The results of the attack detection system are compared with various ML algorithms, such as KNN, CT, and SVM-Linear, on the original and DSMOTE-augmented datasets as given in Table 5 and Fig. 8-11 respectively. The IADNet achieves 99.80% accuracy, improving over BiLSTM (99.32%), DCNN (98.84%), RF (98.37%), SVM-linear (97.89%), CT (97.41%), and CT (96.93%) on the augmented dataset using DSMOTE. For the original dataset, IADNet achieves an accuracy of 99.12%, higher than BiLSTM (98.48%), DCNn (97.94%), RF (97.87%), SVM (97.22%), CT (96.58%), and KNN (95.93%). The ML models achieve precision ranging from 82.69% to 89.77% on the original dataset and from 96.93% to 98.37% on the augmented dataset. However, IADNet achieves improved recall, precision, and F1-score of 98.80% each on the DSMOTE-augmented dataset.

Table 5: Results comparison of IADNet with traditional ML techniques

Method	Original Dataset	DSMOTE Augmented Dataset

	Accuracy	Precision	Recall	F1-score	Accuracy	Precision	Recall	F1-score
KNN	95.93	82.69	95.91	88.24	96.93	96.93	96.93	96.93
CT	96.58	84.99	96.47	89.96	97.41	97.41	97.41	97.41
SVM-Linear	97.22	87.30	97.16	91.68	97.89	97.89	97.89	97.89
RF	97.87	89.77	97.93	93.48	98.37	98.37	98.37	98.37
DCNN	97.94	97.94	89.98	93.59	98.84	98.84	98.88	98.86
BiLSTM	98.48	98.48	92.56	95.33	99.32	99.32	99.30	99.31
IADNet	99.12	99.12	95.50	97.24	99.80	99.80	99.80	99.80

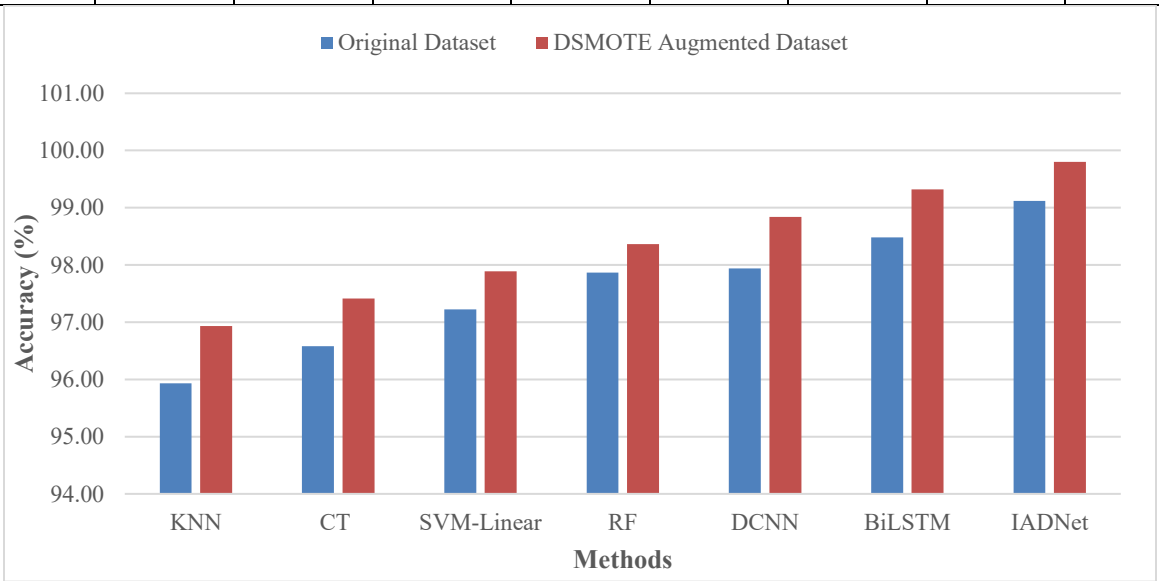


Fig. 8 Accuracy comparison for various methods for attack detection for MedSec-25 dataset

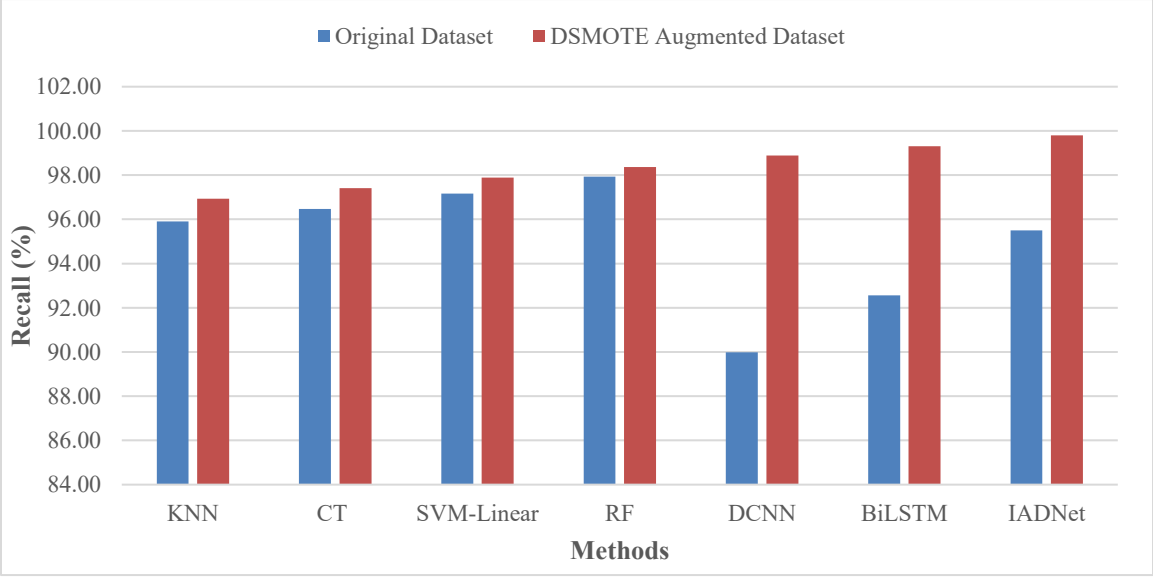


Fig. 9 Recall comparison for various methods for attack detection for MedSec-25 dataset

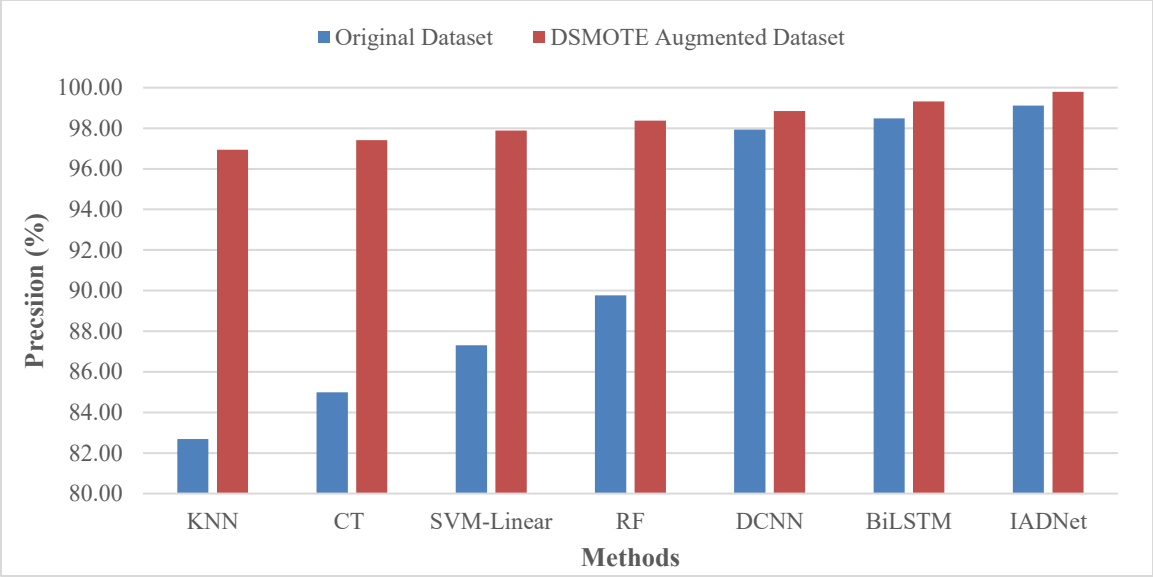


Fig. 10 Precision comparison for various methods for attack detection for MedSec-25 dataset

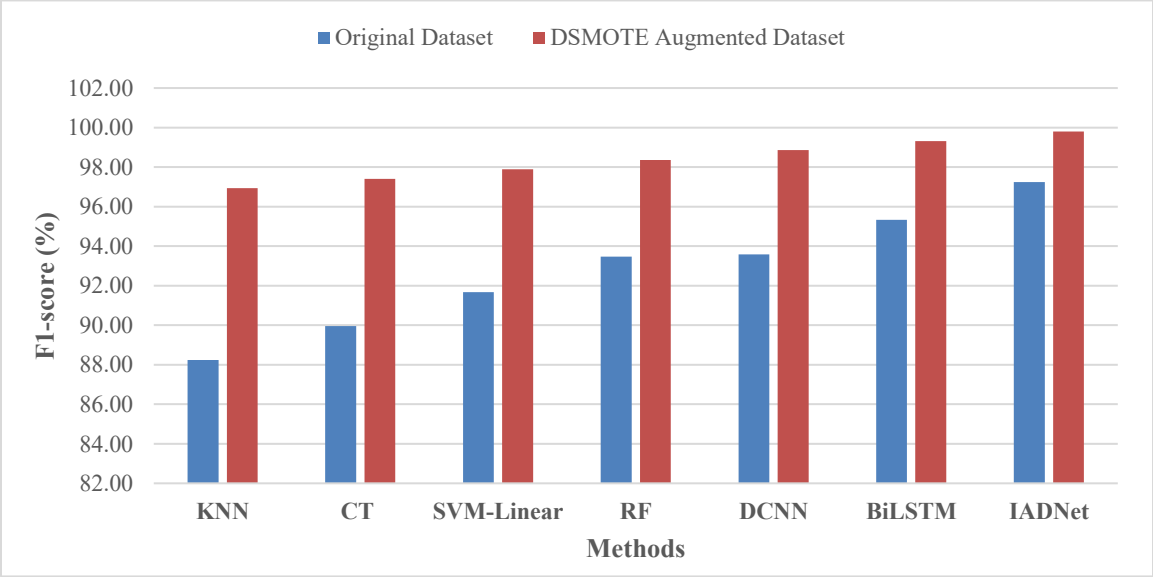


Fig. 11 F1-score comparison for various methods for attack detection for the MedSec-25 dataset

4. Conclusions and Future Scopes

Thus, this paper presents an attack-detection framework for the IoMT that uses IADNet to ensure the privacy, security, and integrity of healthcare data. The IADNet combines the advantages of DCNN and BiLSTM to improve local correlation and long-term representations of network attributes. The dynamic SMOTE significantly improves the precision and F1-score of the attack detection system by generating synthetic samples to mitigate data scarcity. The IADNet model achieves an overall accuracy of 99.12%, with precision at 99.12%, recall at 95.50%, and an F1-score of 97.24% on the original dataset. After applying SMOTE and DSMOTE augmentations, performance further improves, reaching an accuracy of 99.80%, with recall, precision, and F1-score increasing to 99.22%, 98.80%, and 98.80%, respectively. In the future, the outcomes of the attack detection framework can be improved by selecting features that minimize its computational complexity in IoMT. The system's effectiveness can be enhanced by optimizing IADNet's hyperparameters.

REFERENCES

1. El-Saleh, Ayman A., Abdul Manan Sheikh, Mahmoud AM Albreem, and Mohamed Shaik Honnurvali. "The internet of medical things (IoMT): opportunities and challenges." *Wireless networks* 31, no. 1 (2025): 327-344.
2. Naghib, Arezou, Farhad Soleimanian Gharehchopogh, and Azadeh Zamanifar. "A comprehensive and systematic literature review on intrusion detection systems in the internet of medical things: current status, challenges, and opportunities." *Artificial Intelligence Review* 58, no. 4 (2025): 114.
3. El-deep, Shorouk E., Amr A. Abohany, Karam M. Sallam, and Amr A. Abd El-Mageed. "A comprehensive survey on impact of applying various technologies on the internet of medical things." *Artificial Intelligence Review* 58, no. 3 (2025): 86.
4. Matthew, Peter, Sarah Mchale, Xutao Deng, Ghada Nakhla, Marcello Trovati, Nonso Nnamoko, Ella Pereira, Huaizhong Zhang, and Mohsin Raza. "A review of the state of the art for the internet of medical things." *Sci* 7, no. 2 (2025): 36.
5. Ramya, M., Pradeep Sudhakaran, Yuvaraj Sivagnanam, and C. Santhana Krishnan. "Advanced intrusion detection technique (AIDT) for secure communication among devices in internet of medical things (IoMT)." *EURASIP Journal on Wireless Communications and Networking* 2025, no. 1 (2025): 34.
6. Thomas, Tony, Ravi Prakash, and Soumya Pal. "Intrusion Detection in Internet of Medical Things Using Digital Twins—A Review." *Computers, Materials & Continua* 84, no. 3 (2025).
7. Alqahtani, Aljorey, and Monir Abdullah. "A Review on Intrusion Detection Models in Internet of Medical Things (IoMT)." *International Journal of Advanced Computer Science & Applications* 17, no. 1 (2026).
8. Berguiga, Abdelwahed, Ahlem Harchay, and Ayman Massaoudi. "HIDS-IoMT: A deep Learning-Based intelligent intrusion detection system for the internet of medical things." *IEEE Access* (2025).
9. Hosain, Yousif, and Muhammet Çakmak. "XAI-XGBoost: an innovative explainable intrusion detection approach for securing internet of medical things systems." *Scientific Reports* 15, no. 1 (2025): 22278.
10. Georgiades, Michael, and Faisal Hussain. "An explainable ai approach for interpretable cross-layer intrusion detection in internet of medical things." *Electronics* 14, no. 16 (2025): 3218.
11. Nouman, Muhammad, et al. "Malicious node detection using machine learning and distributed data storage using blockchain in WSNs." IEEE Access 11 (2023): 6106-6121.
12. Khashan, Osama A. "Dual-stage machine learning approach for advanced malicious node detection in WSNs." Ad Hoc Networks 166 (2025): 103672.
13. Khashan, Osama A. "Blockchain-machine learning fusion for enhanced malicious node detection in wireless sensor networks." Knowledge-Based Systems 304 (2024): 112557.
14. Almakayeel, Naif, and E. Laxmi Lydia. "Improved sand cat swarm optimization with deep learning based enhanced malicious activity recognition for cybersecurity." *Alexandria Engineering Journal* 98 (2024): 187-198.
15. Babayigit, Bilal, and Mohammed Abubaker. "Towards a generalized hybrid deep learning model with optimized hyperparameters for malicious traffic detection in the Industrial Internet of Things." Engineering Applications of Artificial Intelligence 128 (2024): 107515.
16. Sathishkumar, P., et al. "Dos attack detection using fuzzy temporal deep long Short-Term memory algorithm in wireless sensor network." Ain Shams Engineering Journal 15.12 (2024): 103052.
17. Gunjal, Monica, and Pramodkumar Kulkarni. "Adaptive Deep Learning-Driven Framework for Malicious Node Detection in Wireless Sensor Networks." In *2025 Global Conference in Emerging Technology (GINOTECH)*, pp. 1-7. IEEE, 2025.
18. K. Ileri, "LSTM-Driven Multi-Class Intrusion Detection in IoMT Networks with Chi-Square Feature Selection," 2026 International Conference on Artificial Intelligence in Information and Communication (ICAIIC), Tokyo, Japan, 2026, pp. 1-6, doi: 10.1109/ICAIIC68212.2026.11454251.
19. W. Almobaideen, M. Abdullah, U. Alam, S. B. Hussain and A. Bouharrat, "MedSec-25: Creating an IoMT Dataset for a Healthcare IoT Environment," 2025 7th International Conference on Blockchain Computing and Applications (BCCA), Durbovnic, Croatia, 2025, pp. 628-634, doi: 10.1109/BCCA66705.2025.11229535.
20. Liaw, Lawrence Chuin Ming, Shing Chiang Tan, Pey Yun Goh, and Chee Peng Lim. "A histogram SMOTE-based sampling algorithm with incremental learning for imbalanced data classification." *Information sciences* 686 (2025): 121193.
21. Suguna, R., J. Suriya Prakash, H. Aditya Pai, T. R. Mahesh, Venkatesan Vinoth Kumar, and Temesgen Engida Yimer. "Mitigating class imbalance in churn prediction with ensemble methods and SMOTE." *Scientific Reports* 15, no. 1 (2025): 16256.