A Stacked Ensemble Method with Adaptive Attribute Selection to Detect DDoS Attack in Cloud-Assisted WBAN

Priyanka Verma[1(✉)], John G. Breslin[1], Donna O'Shea[2], and R. K. Pateriya[3]

[1] Data Science Institute, NUI Galway, Galway, Ireland
priyanka.verma@nuigalway.ie
[2] Department of Computer Science, MTU Cork, Cork, Ireland
[3] Department of Computer Science and Engineering, MANIT, Bhopal, India

Abstract. The present era of technology improves the health care services and Wireless Body Area Network (WBAN) is one of them. It is a technology which uses wireless sensors to gather the vital signs from human body for monitoring. The WBAN is often connected with cloud to overcome processing and storage limitations. However, using cloud with WBAN opens up the door for various attacks. DDoS is one of the major threat which directly affects the availability of patient data, and harness the adoption of cloud-assisted WBAN technology. Therefore, in this work we propose a approach to detect DDoS attack in cloud-assisted WBAN and ensures the availability of patients data. The proposed approach is based on Adaptive and Supreme Attribute Selection with Stacked Ensemble Classification (ASAS-SEC). All the requests intended to use the patient data stored on cloud must have to pass through ASAS-SEC mechanism. The request classified as benign are only allowed to access the patient data and DDoS requests are passed to Intensive Care Unit (ICU), where the source of the attack is identified and blocked. Publically available NSL-KDD dataset is utilized to evaluate the proposed ASAS-SEC approach and results shows that proposed approach outperforms other state-of-the-art approaches and achieves classification accuracy of 98.86%, F1-Score of 98.3%, and false alarm of 0.017.

Keywords: Wireless Body Area Network (WBAN) · Cloud network · DDoS · Availability · Healthcare system · Classification

1 Introduction

WBAN have emerged out as a promising technology that improves the human healthcare system [1, 2] and widens their wings to a broad range of medical applications. WBAN majorly benefitted patients with older age and having chronic diseases. In WBAN, the patient's data are collected through sensors in the form of bio-signals. Further, these signals need to be stored and processed for future reference by the healthcare workers such as doctors and physicians. The applications of WBAN may include health monitoring to an emergency medical response system. Autonomous nodes such as sensors and actuators positioned in the body, clothes, or under the patient's skin are connected to WBAN

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2022
N. Khare et al. (Eds.): MIND 2022, CCIS 1763, pp. 329–344, 2022.
https://doi.org/10.1007/978-3-031-24367-7_32

through a wireless communication channel. In the medical field, for continuous monitoring of particular biological functions like electrocardiogram (ECG), Blood Pressure (BP), heartbeat rate, body temperature, etc., a patient might be equipped with WBAN. The benefit of using such a system is that the patient is not restricted to a fixed location (bed). Moreover, it allows more accurate results and sometimes even faster diagnosis since the data is collected in the patient's natural environment and over a longer period of time, thus offers more helpful information.

However, the inadequate resources of WBAN sensors [3] cannot deal with such an enormous quantity of information for storage and processing. Therefore, for the colossal data collected from WBAN sensor nodes, there is a need for secure storage and processing for such data. Consequently, to deal with such a huge amount of information produced by WBAN nodes, an innovative solution to meet this growing challenge is highly desirable. On that account, to provide a robust, hybrid, and viable platform to deal with such an enormous quantity of information collected from various nodes, the integration of cloud computing and WBANs is performed and also known as cloud-assisted WBAN [4].

Cloud computing is considered as a promising innovation to achieve the objectives mentioned above in healthcare management [5]. With the help of cloud-assisted WBAN, physicians and doctors can access the infrastructure storage and processing of health data on a pay-per-usage model [6]. Figure 1 shows the general cloud-assisted architecture for the E-healthcare WBAN system.

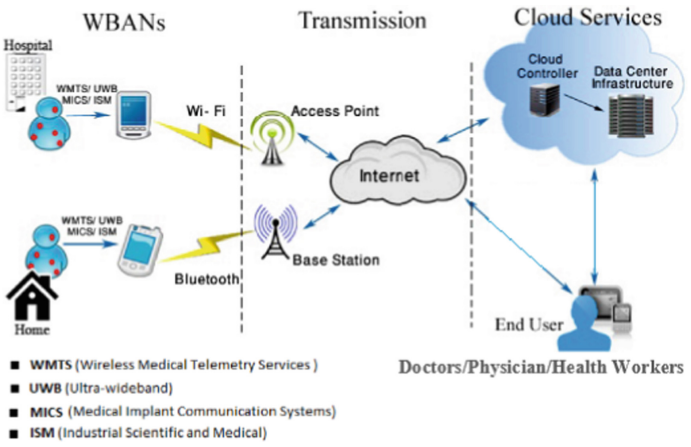


Fig. 1. WBAN architecture for E-health monitoring [1]

Nonetheless, the advent of the cloud-aided WBAN system is still in its growing stage. Recent research in this domain focuses on the framework for cloud-aided WBAN to acknowledge e-healthcare benefits. However, they do not consider the security issues. The availability of patient health data is of significant concern in such networks. A DDoS attack is the most severe threat to data availability that can directly harness the everlasting accessibility of a patient's information. Unavailability of patient's data degrades the overarching performance and credibility of the healthcare administration. The solutions currently used for traditional WBANs against DDoS attacks are not appropriate for

cloud-assisted WBAN technology. There is a need for a defensive approach to detect the DDoS attacks in cloud-based WBAN that understands the varying network traffic conditions during the attack.

Therefore, an adaptive and supreme attribute selection with a stacked ensemble classification (ASAS-SEC) approach is proposed to overcome such issues. The proposed method considers various adaptive thresholding approaches to select the intermediate attribute list under the individual thresholding technique. Further, the attributes under each technique are refined using the supreme behavior approach. After selecting the most supreme attributes, a stacked ensemble classifier is used to classify the DDoS and legitimate request. In stacked ensemble classifier at level-0 Gradient Boost (GB), Random Forest (RF) classifier are used. Further, the output of these two classifiers is given as input to the level-1 classifier. At level-1, the eXtreme Gradient Boost (XGBoost) classifier is used to predict the final output. Using the adaptive approach makes the detection mechanism more robust and efficient against varying network traffic conditions during DDoS attacks. The major contributions of this work are listed as:

1. Proposed an efficient ASAS-SEC approach that can classify the incoming requests towards cloud-assisted WBAN to access patient healthcare data and detect DDoS attacks.
2. Attributes are selected based on the incoming traffic stream; hence adaptive and dynamic behavior can handle different DDoS attack intensities.
3. Also proposes a stacked ensemble classifier that integrates the advantages of different ML classifier such as RF and GB at one level and combines the output and select the dominating result at the next level as final output using XGBoost classifier.
4. ASAS-SEC achieves classification accuracy of 98.86%, F1-Score of 98.3%, and false alarm of 0.017.

The remainder section of the paper is organized as: the state of art approaches for DDoS defense in literature is presented in Sect. 2 and proposed used in this work is discussed in Sect. 3. Section 4 shows the result evaluation and observation of the proposed approach, and finally, Sect. 5 concludes the work and gives the future direction.

2 Related Work

This section presents work done in this domain against DDoS attacks. Many researchers have contributed towards the detection, prevention, and mitigation schemes against such attacks. Several attack avoidance strategies use a challenge-response approach for avoiding the DDoS attack at the entrance of the network [7]. On the other side, attack detection is performed using network traffic analysis. Further anomaly detection methods are also used for the attack detection [8]. Besides the detection and avoidance of DDoS, a great deal of work has been done regarding the mitigation methods of DDoS in the cloud domain [9].

Idhammad et al. [10] evaluated incoming network's information entropy using time-based sliding window method for handling DDoS attack. CIDDS-001 dataset was used to verify the presented approach. Verma et al. [11] offers an adaptive threshold technique

that uses Mean Absolute Deviation (MAD) to select the attributes responsible for the DDoS attack. Then random forest is used for the classification, which provides the best results with the MAD threshold technique.

Sreeram et al. [30] presents a bioinspired bat algorithm that uses the bats records population-based evolution process to detect the HTTP based DDoS attacks quickly. The experiments were carried out on the CAIDA dataset to assess the model. Another bio-inspired algorithm based on the cuckoo search is proposed by Verma et al. [12] to classify the attack and benign requests. In this work, bi-variate flight instead of levy flight provides direction in the cuckoo search space to assign a label for the incoming request. Results prove the dominance proposed approach against the present bio-inspired techniques used to identify the DDoS attack.

Homogeneous ensemble classifier contains similar types of classifiers in the ensemble. A combination of homogeneous and heterogeneous classifiers called the hybrid model was used to study its performance as discussed by Aburomman et al. [13]. Identification of the source of the DDoS attack is as much important as detecting the attack. Attack detection was done using the various filter methods available to select attributes, which conglomerates the top feature in different selection techniques. The features are selected based on its occurrence in the individual filter method. If the frequency count crosses the threshold value, then the feature is selected. The requests identified as attack are sent to a special unit where the attack source is identified and blocked for future reference [14].

A deep learning based technique is presented by Shone et al. [15] called Non-symmetric Deep Auto Encoder (NDAE). The proposed method selects attributes using unsupervised learning, and stacked NDAE is used for the classification. Results shows a noteworthy progress in accuracy and deterioration in computational time. Choi et al. [16] also proposed a approach autoencoder based IDS system for unsupervised data. The proposed approach helps in detecting the anomalies in such data. It results in 91.7% accuracy for classifying the attack and benign requests when tested on NSL-KDD dataset.

The above-discussed security solutions towards DDoS attack are not directly applicable to cloud-assisted WBAN environments. The major cause for this lack of applicability are as cloud-assisted WBAN persists the shortcoming of both WBAN and cloud technology. Therefore for detecting security attacks in these networks, there is a need to develop defensive attack approach that understand and analyze the variable network traffic conditions and overcomes the limitations of both the technologies.

3 Proposed Method

This work proposes a security mechanism to ensure data availability and save the network from such attacks [17]. Figure 2 shows the detection node's placement in the cloud-assisted WBAN, and Fig. 3 shows the flowchart of the proposed approach.

The proposed approach consists of 4 sections as: (i) Preprocessing, (ii) Adaptive and Supreme Attribute Selection (ASAS), (iii) Stacked Ensemble Classifier (SEC), and (iii) Attack request processing unit (ICRPU). In the proposed approach, whenever the request to access the patient healthcare data stored in the cloud network arrives, then before passing the request, the defense mechanism is initiated.

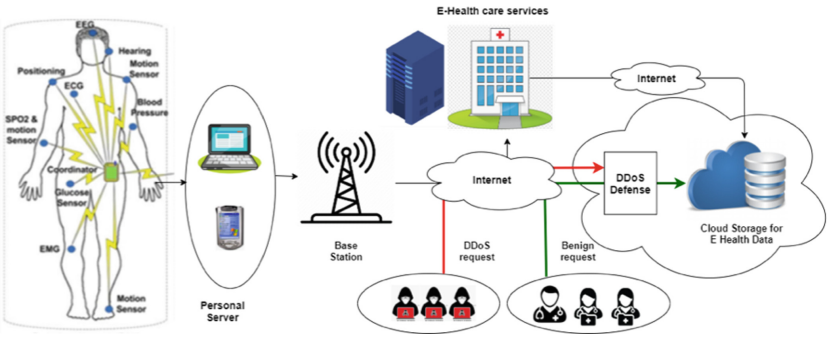


Fig. 2. Placement of defense mechanism for the detection of DDoS attack in cloud-assisted WBAN

3.1 Pre-processing

The incoming request contains multiple statistics, which helps in determining the attributes to detect the attack. These attributes need to be extracted from the incoming request for further processing. However, in this work a standard dataset NSL-KDD is used which requires the data normalization due to presence diversified attribute values. If the attributes in the dataset are spread in dynamic ranges then it does not helps proper fitting of the model and it may get bias toward a particular attributes. Thus to handle this issue, scaling of attributes is performed using Min-Max normalization before model fitting. The formula used for Min-Max normalization is:

$$X_{new} = \frac{X_i - X_{min}}{X_{max} - X_{min}} * (Y_{max} - Y_{min}) + Y_{min} \tag{1}$$

Here X is the feature that needs to be scaled, X_{min} and X_{max} are the lowest and highest values of attribute X. X_i is the current value being processed and X_{new} will be the new value. Whereas Y_{min} and Y_{max} are the minimum and maximum value in the new range. Algorithm 1 show the preprocessing steps of the data.

***

Algorithm 1: Preprocessing		
Input	:	D(x) = NSL-KDD dataset, where x ϵ{A1 , A2 …….A41}
Output	:	Preprocessed train and test datasets as D'_{train}(x) and D'_{test}(x)
Step1	:	Select attribute x_i from D(x)
Step2	:	Normalize x_i with Min-Max normalization using Eq. (1)
Step3	:	Partition normalized data $D'(x)$ into train and test sets as D'_{train}(x) and D'_{test}(x)

3.2 Adaptive and Supreme Attribute Selection (ASAS)

Algorithm 2 shows the method for adaptive and supreme attribute selection process. Here firstly the entropy of each feature is determined. Entropy is a measure of randomness

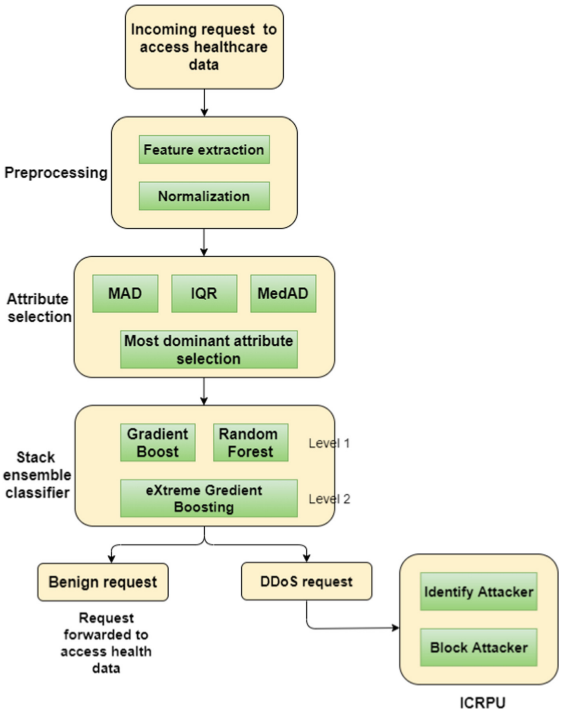


Fig. 3. Flowchart of the proposed approach

or uncertainty in the data. As the randomness increases, the value of the entropy also increases [18]. The incoming traffic activities at the time of attack can be analyzed with the help of entropy [19]. The entropy against each attribute in the incoming traffic is evaluated as:

$$Entropy(A_i) = -\sum P(A_i/x)\log(P(A_i/x)) \tag{2}$$

Algorithm 2: Adaptive and Supreme Attribute Selection (ASAS)

Input : Preprocessed train dataset D'_{train}(x)
Output : Final selected attribute set f(x)

Step1 : Calculate entropy E(x) for each attribute in D'_{train}(x) using Eq. (2)
Step2 : Calculate threshold value (THR) using MAD, IQR, MedAD
Step3 : Select attribute under each thresholding technique
For each attribute x_i in D'_{train}(x)
If $E(x_i) \geq MAD\ (THR)$
Then x_i is added to MAD (x)
If $E(x_i) \geq IQR\ (THR)$
Then x_i is added to IQR (x)
If $E(x_i) \geq MedAD\ (THR)$
Then x_i is added to MedAD (x)
Step4 : Partition MAD (x), IQR (x), MedAD (x)
If $MAD(x_i) \geq T_h$
Then x_i is added to AMAD-1
Else x_i is added to AMAD-2
If $IQR(x_i) \geq T_h$
Then x_i is added to AIQR-1
Else x_i is added to AIQR-2
If $MedAD(x_i) \geq T_h$
Then x_i is added to AMedAD-1
Else x_i is added to AMedAD-2
Step5 : Calculate $f'(x)$ = AMAD-1 ∪ AIQR-1 ∪ MedAD-1
Step6 : Calculate $f''(x)$ = AMAD-2 ∪ AIQR-2 ∪ MedAD-2
Step7 : Calculate final attribute set f(x)
$f(x) = f'(x) \cup f''(x)$

Now, three threshold-based attribute selection techniques, namely Interquartile Range (IQR), Mean Absolute Deviation (MAD), and Median Absolute Deviation (MedAD), are applied to the data individually. On using MAD threshold technique on the dataset, we get a threshold value MAD (THR). Based on MAD (THR) the attributes having the entropy value greater than or equal to MAD (THR) are selected under MAD threshold-based attribute selection technique. Thereafter, attributes selected under the MAD technique are further divided into two subsets, namely AMAD-1, AMAD-2. The attributes chosen under MAD having a value greater than T_h (fixed threshold) are selected under AMAD-1 else selected in AMAD-2. Similarly, IQR and MedAD are also used to create the sets AIQR-1, AIQR-2, and AMedAD-1, AMedAD-2, respectively.

The attributes selected under AMAD-1, AIQR-1, and AMedAD-1 subsets, possess a higher score than the attributes selected under AMAD-2, AIQR-2, and AMedAD-2. Thus, the original attribute set under each threshold technique is split into two subsets. Where one subset shows more supreme attribute subsets and the other shows less supreme

attribute subsets. Further, the union of more supreme attribute subsets and the intersection of less supreme attribute subsets is performed. The union of AMAD-1, AIQR-1 and AMedAD-1 gives a More Supreme Attribute Subset (MSAS) and the intersection of AMAD-2, AIQR-2 and AMedAD-2 gives a Less Supreme Attribute Subset (LSAS). Finally, the union of MSAS and LSAS gives a new subset called Final Attribute Subset (FAS).

3.3 Stacked Ensemble Classification (SEC)

A stacked ensemble model classifies unknown data by building new training data using a set of classifiers as base classifiers. The classifiers of this category are also known as multiple classifier systems. The stacked ensemble learning model creates multiple learners L1, L2,…Ln from the training process by selecting different base classifiers (or Level-0), say B1, B2,…Bn, train them using the training part of the dataset. These learners' output is merged and fed as input to the next level (Level-1) classifier.

The learners selected at the base level can be homogeneous or heterogeneous ensembles. The learners are called homogeneous learners if they are under the same type otherwise, they are called as heterogeneous learners. At level-1, the selected classifier takes the base classifier's output as input and gives the final output. At level-1, the base learner's errors are identified and then adjusted to achieve an optimal solution. A generalized model for any input data is obtained by repeating this process on level classifiers. In traditional methods, the elected classifier may not achieve good results on new and unseen data even though it has good training data performance. This problem can be eliminated by using the stacked ensemble approach.

Since the method performs averaging of all classifiers, even though one of the selected classifiers is unfit for the approach, the menace of relying on one technique can be reduced. Therefore, the ensemble approach reduces the risk of inappropriate selection of classifier. Algorithm 3 shows the steps for stacked ensemble classification.

In this work, Gradient Boost (GB) [20] and Random Forest (RF) [21] classifiers are used as learners at the base level (level-0). GB is a modern classification technique and enhanced version of AdaBoost (AB). AB starts with weak learners at the initial step for predicting the output. Further, the weak learners are improved by escalating the weight points of a higher order. GB is the minor deviation of AB, in which instead of escalating the data points, the latest learner at each step is launched. This approach can improve any differentiable loss function. At every iteration regression trees are built, and individual trees are added serially, i.e., the new tree is built, depending on the difference between the real and the projected value. Whereas the RF approach works on choosing the attributes and values that can construct some sequence of rules to create various decision trees, and finally takes the mean of the final outcomes.

Now instead of using majority voting or bayesian averaging techniques for final prediction, the learning of the level-1 model is done to combine the base model's predictions. This makes it more generalized compared to other ensemble techniques in terms of the predictions of the attack. The output of level-0 is the predictions for each record of the training dataset. To combine these outputs and predicting the final label for each request, XGBoost [22] is used.

Algorithm 3:Stacked ensemble Classification		
Input	:	$\hat{D_{train}}$(x), $\hat{D_{test}}$(x), f(x)
Output	:	Classify test data as DDoS and benign
Step1	:	Learn level-0 classifier (no. of classifier used=2) Learn Gradient Boost (GB) classifier Learn Random Forest (RF) classifier
Step2	:	Learn level-1 classifier (no. of classifier used=1) Learn eXtreme GB (XGB) classifier with the input from level-0 classifiers
Step3	:	Classify test data as DDoS and benign using learned stacked ensemble classifier

XGBoost is a decision tree-oriented ensemble classification technique that utilizes the GB algorithm over a known dataset and then considers the classification decision. The major motivation behind using XGBoost is its model performance, higher execution speed, memory efficiency, and high accuracy compared to other GB algorithm models [23]. Thus XGBoost is used in this work to obtain the final prediction of the request as attack and benign.

3.4 DDoS Attack Mitigation

Once the DDoS requests are identified after the classification process, these requests need to be processed with intensive care for future reference. Therefore, this Intensive Care Request Processing Unit (ICRPU) is set up to handle such attack requests. This unit confuses the attacker and makes him believe that their requests are actually being served. This impression helps the mitigation unit identify the attack source until the attacker is busy in question and answer round by this unit. As the attack requests are in the processing state, the attacker is fooled and believes that the service provider has found no suspicious activity out. This will create an illusion to the attacker. He will continue the attack without any changes and this makes it easy for the mitigation unit to identify the attack source. Once the attack source is identified all the request belonging to that source are dropped and even blocked for future reference.

4 Experimental Evaluations

The proposed approach is tested on Windows 10 on Dell series, having 64 bit i5 processor, 8 GB RAM. Python 3.0 is the language used to implement the proposed approach. NSL-KDD [24] is a publically available dataset used to validate the proposed ASAS-SEC approach. This dataset consists of various attacks however we used DoS and normal request in the dataset, which is of our interested are used to validate the proposed approach. The metrics used to asses ASAS-SEC are classification accuracy, F1-Score, Area Under Curve(AUC), and false alarm or False Positive Rate (FPR) [11].

4.1 Performance Metrics Used

The metrics used to assess ASAS-SEC are classification accuracy, F1-Score, Area Under Curve (AUC), and false alarm, also known as False Positive Rate (FPR). These metrics

are expressed in terms of True Positive (TP), True Negative (TN), False Positive (FP), False Negative (FN), respectively, where:

- TP: Specify the count of DDoS requests rightly predicted as DDoS
- TN: Specify the count of benign samples rightly predicted as benign
- FP: Count of benign requests falsely predicted as DDoS
- FN: Count of DDoS requests falsely predicted as benign

4.1.1 Accuracy

It is the percentage of correctly predicted DDoS and benign requests

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{3}$$

4.1.2 F1-Score

This score is calculated using Precision and Recall, therefore this score takes both FP and FN into account.

$$F1 - Score = 2 * \frac{(Recall * Precision)}{(Recall + Precision)} \tag{4}$$

where recall is the ratio of correctly predicted DDoS to the all observations in actual class

$$Recall = \frac{TP}{TP + FN}$$

and precision is the ratio of rightly predicted benign request to the entire predicted benign requests.

$$Precision = \frac{TP}{TP + FP}$$

4.1.3 FPR or False Alarm

It is the ratio of falsely predicted benign requests as DDoS to the actual number of benign requests.

$$FPR = \frac{FP}{FP + TN} \tag{5}$$

4.2 Result Analysis

The proposed approach utilizes MAD, IQR, and MedAD thresholding techniques to obtain a threshold value as mentioned in Sect. 3.2, based on which attributes selection is performed under each technique. In the literature, most of the methods uses fixed threshold values for the selection of attributes. However, techniques based on fixed threshold values cannot deal with the dynamic network behavior during the attack. As the size of the packet and values of the attributes changes drastically with various kinds of DDoS attack. Therefore, fixed threshold values are not able to tackle such situations and make the predictions accurately. Thus, to handle these limitations, adaptive threshold techniques are used as a part of the attribute selection process.

After selecting attributes under each adaptive thresholding technique, the attributes are further classified in two sets based on a fixed threshold value 'T_h' as AMAD-1, AMAD-2 for MAD thresholding technique, AIQR-1, AIQR-2 for IQR thresholding technique and AMedAD-1, AMedAD-2 for MedAD thresholding technique.

The most supreme and final attributes are shortlisted based on the significance of attribute in classifying the requests from these sets. Once the final attributes are selected, the stacked ensemble classifier as discussed in the Sect. 3.3 is used to classify the incoming request to cloud-assisted WBAN as DDoS and normal.

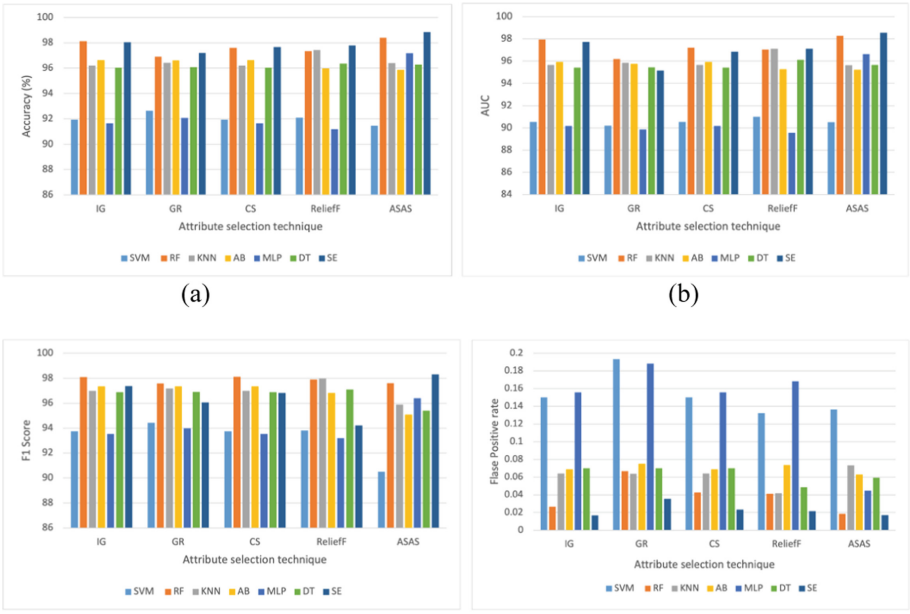


Fig. 4. Comparison between different threshold methods along side different classifier and proposed (ASAS+SE) approach for different metrics: (a) Accuracy, (b) AUC, (c) F1-Score, (d) FPR(false alarm)

After rigorous experimentations and comparisons it is observed that ASAS-SEC achieves the highest classification accuracy of 98.86%, F1 Score of 98.3%, AUC of 98.56, and lowest false alarm of 0.017. Thus ASAS-SEC is selected in the proposed approach.

Figure 4 shows the comparison of thresholding techniques with different classifiers. The classifiers used to compare the proposed approach are Decision Tree (DT), AdaBoost (AB), Support Vector Machine (SVM), K-Nearest Neighbor (KNN), Random Forest (RF), and Multi Layer Perceptron (MLP). From Fig. 4 (a), (b), (c), and (d), it is seen that the proposed ASAS-SEC attains the highest accuracy, F1-Score, Area Under Curve (AUC) in comparison to other amalgamations of thresholding technique and different classifiers. Moreover, ASAS-SEC achieves a low FPR which ensures very less false alarms.

The dominance of the proposed approach can also be seen by comparing it with the existing attribute selection techniques. The most widely used attribute selection techniques are Information Gain (IG), Gain Ratio (GR), Chi-Squared (CS), and ReliefF [25]. Figure 5 shows the comparative analysis of the proposed ASAS-SEC approach with existing feature selection and classification techniques.

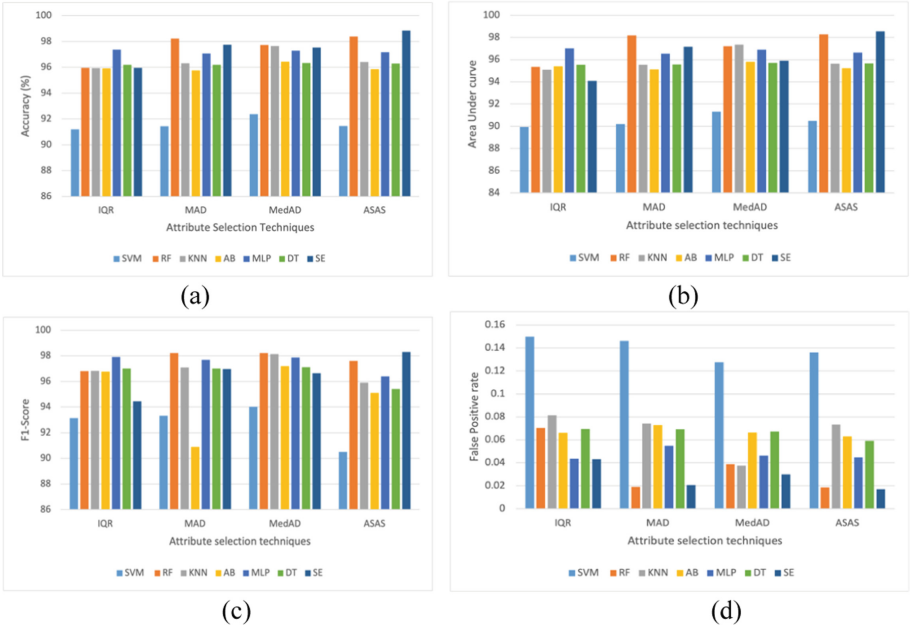


Fig. 5. Comparison between various attribute selection techniques along with different classifier and ASAS-SEC for different metrics: (a) Accuracy, (b) AUC, (c) F1-Score, (d) FPR (false alarm)

Figure 5 (a), (b), (c), and (d) shows the accuracy, AUC, F1-Score, and FPR comparison of the proposed approach with other attribute selection techniques. It is observed that the proposed ASAS-SEC proved to be superior over all the attribute selection techniques.

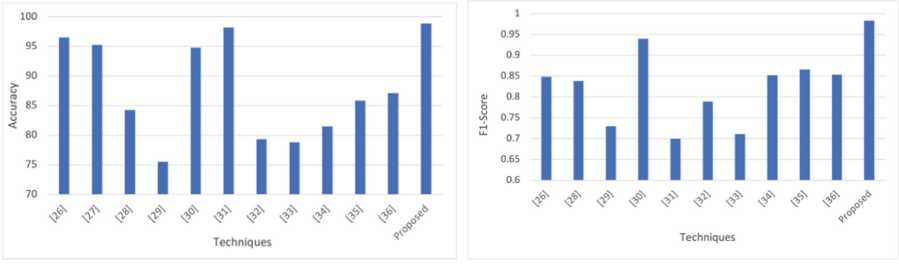
ASAS-SEC attains high accuracy, AUC, F1-Score, and lowest false alarm value compared to the above mentioned attribute selection techniques. As these attribute selection techniques cannot handle the dynamic behavior of traffic during the DDoS attack.

The proposed ASAS-SEC is also compared with the existing state-of-the-art approaches used to detect and classify DDoS attacks, as shown in Table 1. It is observed from Fig. 6 (a) that the proposed ASAS-SEC dominates other techniques and achieves high accuracy because it contains high TP and TN values.

Similarly, a comparative study on the F1-Score value of ASAS+SE with other existing methods is shown in Fig. 6 (b). Proposed approach attains highest F1-Score in comparison to state of the art approaches.

Table 1. Performance comparison of ASAS-SEC with state of the art techniques

Reference	Year	Accuracy	F1-Score	False alarm
[26]	2018	96.53	0.8484	0.56
[27]	2018	95.29	–	–
[28]	2018	84.25	0.8386	–
[29]	2019	75.51	0.73	2.87
[30]	2019	94.8	0.94	0.07
[31]	2018	98.23	0.7	0.32
[32]	2020	79.34	0.7888	–
[33]	2021	78.85	0.7111	–
[34]	2021	81.48	0.8523	–
[35]	2021	85.83	0.8661	–
[36]	2022	87.11	0.8533	–
Proposed	**–**	**98.86**	**0.983**	**0.017**



(a) (b)

Fig. 6. Comparison of accuracy and F1-Score of ASAS+SE with state of art techniques

5 Conclusion

This manuscript presents a DDoS attack defense approach in cloud-assisted WBAN to guarantee the accessibility of patient information to the healthcare system. The proposed approach ASAS-SEC is based on adaptive and supreme attribute selection and stacked ensemble classification. The adaptive threshold technique helps to deal with dynamic network traffic conditions due to various DDoS attack intensities. However, the fixed threshold value used in the literature are not capable to deal with such conditions. Therefore, using the adaptive threshold value depending on the present network statistics identifies the effective attributes for classification. Moreover, among the selected attributes under each thresholding technique (MAD, IQR, MedAD), furthermost supreme attributes are selected. After selecting an attribute, stacked ensemble classifier is used to classify the incoming request. The advantage of using stacked ensemble classification is that it overcomes the generalization capability for the predictions of the classifiers in the ensemble. The proposed approach ASAS-SEC is evaluated on the NSL-KDD dataset and proved to be best among the other techniques in the domain and state of the art approaches. However, proposed approach is unable to detect the other attacks. Thus in future proposed approach can be modified to identify the other attacks launched against the cloud-assisted WBAN.

References

1. Latif, R., Abbas, H., Latif, S.: Distributed denial of service (DDoS) attack detection using data mining approach in cloud-assisted wireless body area networks. Int. J. Ad Hoc Ubiquitous Comput. **23**(1–2), 24–35 (2016)
2. Irum, S., Ali, A., Khan, F.A., Abbas, H.: A hybrid security mechanism for intra-WBAN and inter-WBAN communications. Int. J. Distrib. Sens. Netw. **9**(8), 842608 (2013)
3. Hayajneh, T., Almashaqbeh, G., Ullah, S., Vasilakos, A.V.: A survey of wireless technologies coexistence in WBAN: analysis and open research issues. Wirel. Netw. **20**(8), 2165–2199 (2014). https://doi.org/10.1007/s11276-014-0736-8
4. Latif, R., Abbas, H., Assar, S., Latif, S.: Analyzing feasibility for deploying very fast decision tree for DDoS attack detection in cloud-assisted WBAN. In: Huang, D.-S., Bevilacqua, V., Premaratne, P. (eds.) ICIC 2014. LNCS, vol. 8588, pp. 507–519. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-09333-8_57
5. Wan, J., Zou, C., Zhou, K., Lu, R., Li, D.: IoT sensing framework with inter-cloud computing capability in vehicular networking. Electron. Commer. Res. **14**(3), 389–416 (2014). https://doi.org/10.1007/s10660-014-9147-2
6. Foster, I., Zhao, Y., Raicu, I., Lu, S.: Cloud computing and grid computing 360-degree compared. In: 2008 Grid Computing Environments Workshop, pp. 1–10 (2008)
7. Wang, H., Jia, Q., Fleck, D., Powell, W., Li, F., Stavrou, A.: A moving target DDoS defense mechanism. Comput. Commun. **46**, 10–21 (2014)
8. Sari, A.: A review of anomaly detection systems in cloud networks and survey of cloud security measures in cloud storage applications. J. Inf. Secur. **6**(02), 142 (2015)
9. Rajamohamed, R., Jose, T.J., Sumithra, S., Vijaya, J.: Multi model mitigation approach for network threats on cluster based linear chain routing protocol in wireless sensor networks at QoS development. Wirel. Pers. Commun. **102**(4), 3205–3224 (2018)

10. Idhammad, M., Afdel, K., Belouch, M.: Detection system of HTTP DDoS attacks in a cloud environment based on information theoretic entropy and random forest. Secur. Commun. Netw. (2018)
11. Verma, P., Tapaswi, S., Godfrey, W.W.: An Adaptive threshold-based attribute selection to classify requests under DDoS attack in cloud-based systems. Arab. J. Sci. Eng. **45**(4), 2813–2834 (2019). https://doi.org/10.1007/s13369-019-04178-x
12. Verma, P., Tapaswi, S., Godfrey, W.W.: A request aware module using CS-IDR to reduce VM level collateral damages caused by DDoS attack in cloud environment. Clust. Comput. **24**(3), 1917–1933 (2021). https://doi.org/10.1007/s10586-021-03234-2
13. Aburomman, A.A., Reaz, M.B.I.: A survey of intrusion detection systems based on ensemble and hybrid classifiers. Comput. Secur. **65**, 135–152 (2017)
14. Bharot, N., Verma, P., Sharma, S., Suraparaju, V.: Distributed denial-of-service attack detection and mitigation using feature selection and intensive care request processing unit. Arab. J. Sci. Eng. **43**(2), 959–967 (2018)
15. Shone, N., Ngoc, T.N., Phai, V.D., Shi, Q.: A deep learning approach to network intrusion detection. IEEE Trans. Emerg. Top. Comput. Intell. **2**(1), 41–50 (2018)
16. Choi, H., Kim, M., Lee, G., Kim, W.: Unsupervised learning approach for network intrusion detection system using autoencoders. J. Supercomput. **75**(9), 5597–5621 (2019). https://doi.org/10.1007/s11227-019-02805-w
17. Latif, R., Abbas, H., Assar, S.: Distributed denial of service (DDoS) attack in cloud-assisted wireless body area networks: a systematic literature review. J. Med. Syst. **38**, 128 (2014). https://doi.org/10.1007/s10916-014-0128-8
18. Shannon, C.E.: A mathematical theory of communication. ACM SIGMOBILE Mob. Comput. Commun. Rev. **5**(1), 3–55 (2001)
19. Sree, T.R., Bhanu, S.M.S.: Detection of http flooding attacks in cloud using dynamic entropy method. Arab. J. Sci. Eng. **43**(12), 6995–7014 (2018)
20. Alamri, H.A., Thayananthan, V.: Bandwidth control mechanism and extreme gradient boosting algorithm for protecting software-defined networks against DDoS attacks. IEEE Access **8**, 194269–194288 (2020)
21. Radivilova, T., Kirichenko, L., Ageiev, D., Bulakh, V.: Classification methods of machine learning to detect DDoS attacks. In: 2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), vol. 1, pp. 207–210 (2019)
22. Chen, T., Guestrin, C.: XGBoost: a scalable tree boosting system. In: Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, pp. 785–794 (2016)
23. Chakraborty, D., Elzarka, H.: Advanced machine learning techniques for building performance simulation: a comparative analysis. J. Build. Perform. Simul. **12**(2), 193–207 (2019)
24. NSL-KDD Dataset. http://www.unb.ca/cic/datasets/nsl.html
25. Pajouh, H.H., Dastghaibyfard, G., Hashemi, S.: Two-tier network anomaly detection model: a machine learning approach. J. Intell. Inf. Syst. **48**(1), 61–74 (2015). https://doi.org/10.1007/s10844-015-0388-x
26. Hamamoto, A.H., Carvalho, L.F., Sampaio, L.D.H., Abrão, T., Proença, M.L., Jr.: Network anomaly detection system using genetic algorithm and fuzzy logic. Expert Syst. Appl. **92**, 390–402 (2018)
27. Sharma, R., Chaurasia, S.: An enhanced approach to fuzzy C-means clustering for anomaly detection. In: Somani, A.K., Srivastava, S., Mundra, A., Rawat, S. (eds.) Proceedings of First International Conference on Smart System, Innovations and Computing, pp. 623–636. Springer, Singapore (2018). https://doi.org/10.1007/978-981-10-5828-8_60

28. Verma, P., Anwar, S., Khan, S., Mane, S.B.: Network intrusion detection using clustering and gradient boosting. In: 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT), pp. 1–7 (2018)
29. Ghosh, P., Karmakar, A., Sharma, J., Phadikar, S.: CS-PSO based intrusion detection system in cloud environment. In: Abraham, A., Dutta, P., Mandal, J.K., Bhattacharya, A., Dutta, S. (eds.) Emerging Technologies in Data Mining and Information Security. AISC, vol. 755, pp. 261–269. Springer, Singapore (2019). https://doi.org/10.1007/978-981-13-1951-8_24
30. Sreeram, I., Vuppala, V.P.K.: HTTP flood attack detection in application layer using machine learning metrics and bio inspired bat algorithm. Appl. Comput. Inform. **15**(1), 59–66 (2019)
31. Idhammad, M., Afdel, K., Belouch, M.: Semi-supervised machine learning approach for DDoS detection. Appl. Intell. **48**(10), 3193–3208 (2018)
32. Gohil, M., Kumar, S.: Evaluation of classification algorithms for distributed denial of service attack detection. In: AIKE, pp. 138–141. IEEE (2020)
33. Sudar, K.M., Beulah, M., Deepalakshmi, P., Nagaraj, P., Chinnasamy, P.: Detection of distributed denial of service attacks in SDN using machine learning techniques. In: IEEE International Conference on Computer Communication and Informatics (ICCCI), pp. 1–5 (2021)
34. Tonkal, Ö., Polat H., Başaran, E., Cömert, Z., Kocaoğlu, R.: Machine learning approach equipped with neighbourhood component analysis for DDoS attack detection in software-defined networking. Electronics **10**(11) (2021)
35. Ahuja, N., Singal, G., Mukhopadhyay, D., Kumar, N.: Automated DDOS attack detection in software defined networking. J. Netw. Comput. Appl. **187**, 103–108 (2021)
36. Pranto, M.B., Ratul, M.H., Rahman, M.M., Diya, I.J., Zahir, Z.B.: Performance of machine learning techniques in anomaly detection with basic feature selection strategy-a network intrusion detection system, J. Adv. Inf. Technol. **13**(1) (2022)