Denial of Service (DoS) Defences against Adversarial Attacks in IoT Smart Home Networks using Machine Learning Methods

Zahid Iqbal[1], Azhar Imran[1], Aman Ullah Yasin [1]and Adnan Alvi[1]
[1]Faculty of Computing & Artificial Intelligence, Air University, Islamabad, Pakistan
* Corresponding author email: azhar.imran@mail.au.edu.pk

Received: 16-12-2021, Received in Revised form: 10-03-2022
Accepted: 27-05-2022, Published: 30-06-2022

Abstract

The availability of information and its integrity and confidentiality are important factors in information and communication of the system security. The DDoS attack generally means Distributed denial of services generates many enormous packets to slow and down the Services for actual users who use services. The study examines the impact of a considerable rise in the number of connected devices in the IoT concept on the quantity and volume of DDoS attacks. Thanks to machine learning-based technology, intrusion Detection Systems (IDS) can be versatile and efficient. However, the advancement of machine learning systems, alongside the application of the uses for Adversarial Machine Learning, has also introduced a new potential attack vector; machine learning models which support the uses of the IDS' decisions may be subject to cyberattacks known as Adversarial Machine Learning (AML). AML is widely applicable to manipulating data and network traffic that transverse networked devices in the IoT setting. However, harmful network packets are frequently misclassified as benign perturbations in the machine learning classifier's decision bounds. Because of this, machine learning-based detectors such as malware scanners skip those flaws and reduce the risk of delaying detection and spreading malicious code and incurring issues such as personal information leaking, damaged hardware, and financial loss. Furthermore, this research investigates which DoS attack techniques should be implemented and how adversary samples should be constructed to strengthen the robustness of supervised models utilising adversarial training. The system obtained 99.98% accuracy with XGBoost and 99.96% accuracy achieved with the decision tree and AdaBoost.

Keywords: Adversarial Machine Learning (AML), Support Vector Machine (SVM), Convolutional Neural Network (CNN), Long Short Term Memory Network (LSTM), Recurrent Neural Network (RNN).

Introduction

Due to increasing IoT devices, IoT models are complicated daily. IoT and Machine Learning related applications are used in daily life. For example, disease taction using X-ray, pattern recognition, and brain signal modelling requires machine learning techniques and algorithms. And also, machine learning algorithms are used in the aerospace domain. The complexity of IoT infrastructure creates unwanted vulnerability in the system. So, anomalies and attacks are common nowadays. IoT devices are the wireless medium that makes them easier to attack. But in Normal communication, it is difficult to attack local nodes in the local network. A secured infrastructure is needed for protection from cybercriminals. Data is money for some stakeholders and entrepreneurs for their business. For government organisations, data is confidential [1]. Abnormalities in IoT device is a backdoor for an attacker to gather confidential data. The system's goal is to detect vulnerabilities and make reliable and secure IoT infrastructure. Here, Many machine learning techniques are used for Systems to protect from cybercriminals in abnormal conditions. As the number of IoT devices grows, more data is generated, rather than machine learning techniques to support IDS for IoT devices. We use the Supervised machine algorithm to detect malicious things on IoT devices. More system tests with supervised machine approach like the Random Forest, Decision Tree, and Support Vector Machine. Development of IoT concept and development in wireless networks (WSN) application and other technological advancements in the field leads to a higher risk of DDoS attacks in this area of the network infrastructure [2].

The taxonomy of DoS attacks conducted at WSN networks is described in the article. The document provides the methods of identifying the attacker, its capabilities, the aim of the attack exploited weakness and the outcomes of attacks. Paper [3] proposes that a complete taxonomy may aid in identifying various kinds of attacks and an improved understanding of these classifications of attacks. The paper shows the current taxonomy of DoS attacks and protection methods and propose a conceptual classification system of new features threats [4]. A detailed classification of protection measures was developed based on the suggested classification of DoS assaults. Paper describes botnet computer networks as commonly utilised danger in various cyberattacks against the ICS. Given that the modern detection methods of botnets target specific protocols and structures for control and management of such systems, the study's hypothesis is the inefficiency of such approaches in the event of changes in the structure and management and control techniques [5].

Collection of the Dataset from the IoT testbed and presenting the attack model. The first goal is to protect data in IoT devices. To protect IoT devices from cybercriminals, a secure IoT infrastructure is required [16]. There are a plethora of methods for protecting data from cybercriminals and hackers. Some companies say our data is our money. We use such a system as the trained model for the attack and introduce a new attack vector. These attacks are also helpful in targeting the machine learning model, which is referred to as an adversarial machine learning algorithm. Our mission is to identify the flaws in the pre-trained model for data transfer to IoT devices and then calculate the delay for detecting an IoT attack [17]. So, the model value decreases, and some vulnerabilities pass through machine learning-based detector approaches, which increases the delay in detecting an error in IoT devices. These attacks affect smart home devices like smart doors and smart light bulbs, making them unavailable for the user. Dos attack deploys by crafting customs packets in the network [6].

- Adversarial samples of IoT network dataset.
- Use IDs in IoT to find the behaviours of the machine learning algorithm.
- Increasing robustness for these types of models for adversarial training.

https://doi.org/10.24949/njes.v15i1.666

Machine learning and deep learning learn the pattern of the dataset, on the behave of the given dataset output model is dependent on the input dataset. Due to the experiment, we evaluate the performance of work. In which adversarial attack achieve high 100% misclassification rate. A conventional IT safety ecosystem comprises static network defences of perimeters (i.e., firewalls, IDSs), the all-embracing usage of endpoint (i.e., anti-viral) defences, and vendor software updates. However, these methods cannot support IoT deployments due to the heterogeneity of devices and their use cases and device/vendor restrictions. That indicates that existing ways to detect signs of attack are insufficient and non-scalable [3].

In IoT ecosystems, standard techniques for identifying abnormalities are inadequate, given the widespread and dynamic variety of possible ordinary devices compared to traditional IT settings. These can lead to catastrophic repercussions, damaged hardware, disruption of the system availability, system outages, and even bodily injury to people. In addition, computer demanding and latency-sensitive security activities that produce significant computing and communication loads are typically not viable for IoT devices with limited processing power, memory, radio bandwidth, and battery resources [15]. As a result, complicated and comprehensive safety measures cannot be implemented. Furthermore, given the diversity of these devices, developing and implementing a safety system that can withstand the scale and range of devices are quite hard. However, these techniques cannot manage IoT installations because of the variety of devices, their usage cases, and device/seller limitations. This means that existing approaches to identifying attack signatures are insufficient and unscalable (e.g., honeypots). Also, standard anomaly detection methods in IoT ecosystems are useless since the range of probable typical device behaviours is much wider and more dynamic than traditional IT environments [19].

Related Work

In related work, due to the invention of the latest machine learning algorithm and a considerable increase in IDSs used for these such techniques in IoT networks. Current research of AML mainly focuses on malware detection and spam email filter. AML targets IoT software, Android type, and sensor type application [7]. Researchers are working in the IoT area and developing the latest detectors and firewalls to overcome attacks in IoT devices. A machine learning algorithm is used to find the device connected to the IoT network. We use deep learning to detect data injection in IoT devices. The implementation of adversarial machine learning in IoT systems by mapping the strategies developed for exploratory, evasive, and causal attacks to diverse wireless networks[2]. Deep learning was used to construct a jamming threat and defence mechanisms while studying a spectrum poisoning attack. The retraining process was not considered in this research [4]. AML against standard Network IDSs and ICS has also been the subject of current research. Use the CICDDoS2019 dataset to produce adversarial samples and show how AML works against supervised algorithms [3]. Furthermore, demonstrate a basic AML attack against an LSTM classifier using an ICS dataset. To create adversarial samples, this assault necessitated the manual identification of characteristics that were to be disturbed. On a Simulink model of a steam condenser, assess a gradient-based search technique. This method was only effective against a small number of systems that used RNNs with smooth activation functions. Wireless communications have begun to use adversarial machine learning [9].

Several IoT security research sought to build IDS systems particularly designed for the IoT environment. The mapped data is analysed to identify all interference in the network. It appears to be promising its effectiveness in identifying other assaults. However, spoofing or altering information, sinkhole, and selective-forwarding attacks have only been tested. Intrusion detection module that employs an ETX measure to identify harmful network activities. A lightweight, adaptable, and knowledge-driven IDS. It gathers information on the monitoring network features and entities and users to dynamically configure the most efficient detecting strategies. New protocol standards can be expanded, but providing a mechanism for information sharing Allows the identification of collaborative events [5]. The IDS aims to identify benign node behaviour and any network traffic abnormalities. The results show that the system can identify benign and malicious knots well. However, the IDS performance is tested within a virtual network and not a real testbed [8]. Finding a broader spectrum of assaults and gadgets requires additional examination for efficiency testing in their system. To identify Distributed Denial of Service (DDoS) threats, utilise machine learning techniques in IoT networks. The selection of functionality in IoT network traffic is illustrated by the use of a variety of machines learner algorithms to achieve high-precision DDoS sensing, which focuses on the unrivalled IoT network conduct (e.g., limited endpoints and predictable time intervals between packets) [20].

Proposed Methodology

Data Acquiring

The dataset utilised comprises eighty network traffic and event records for seven different DDoS attacks, including no attack scenarios. The dataset is called the DDoS evaluation (CICDDoS2019) dataset [3], and the Canadian Institute for Cyber Security compiled it. In addition, the dataset was altered and evaluated for the distribution of output labels for various attack types by ensuring equal beauty smart distribution of every attack training.

Data Pre-processing

Data Processing is the job of changing data from a given form to a much more useable and desirable one, i.e., making it more relevant and informative. The way of remodelling uncooked records into an established layout by filling wanting values and tossing off loud, inconsistent, or unnecessary information is termed records preparation. Different operations are done at the data to retain its consistency and minimise the dimensionality and simplicity of processing. The following processes were carried out during the records preparation stage depicted in Figure 1.

Managing Missing Value

It has been shown that omitting details may negatively impact the research findings. Even though many strategies may be applied to fill misplaced block values, it is wonderful to disconnect the facts row having a missing value. It can create a bias within the estimate of parameters via the algorithms. As a

result, the dataset is checked for misplaced values, and the related rows are removed from the dataset due to many statistics and Dataset composition shown in Table 1.

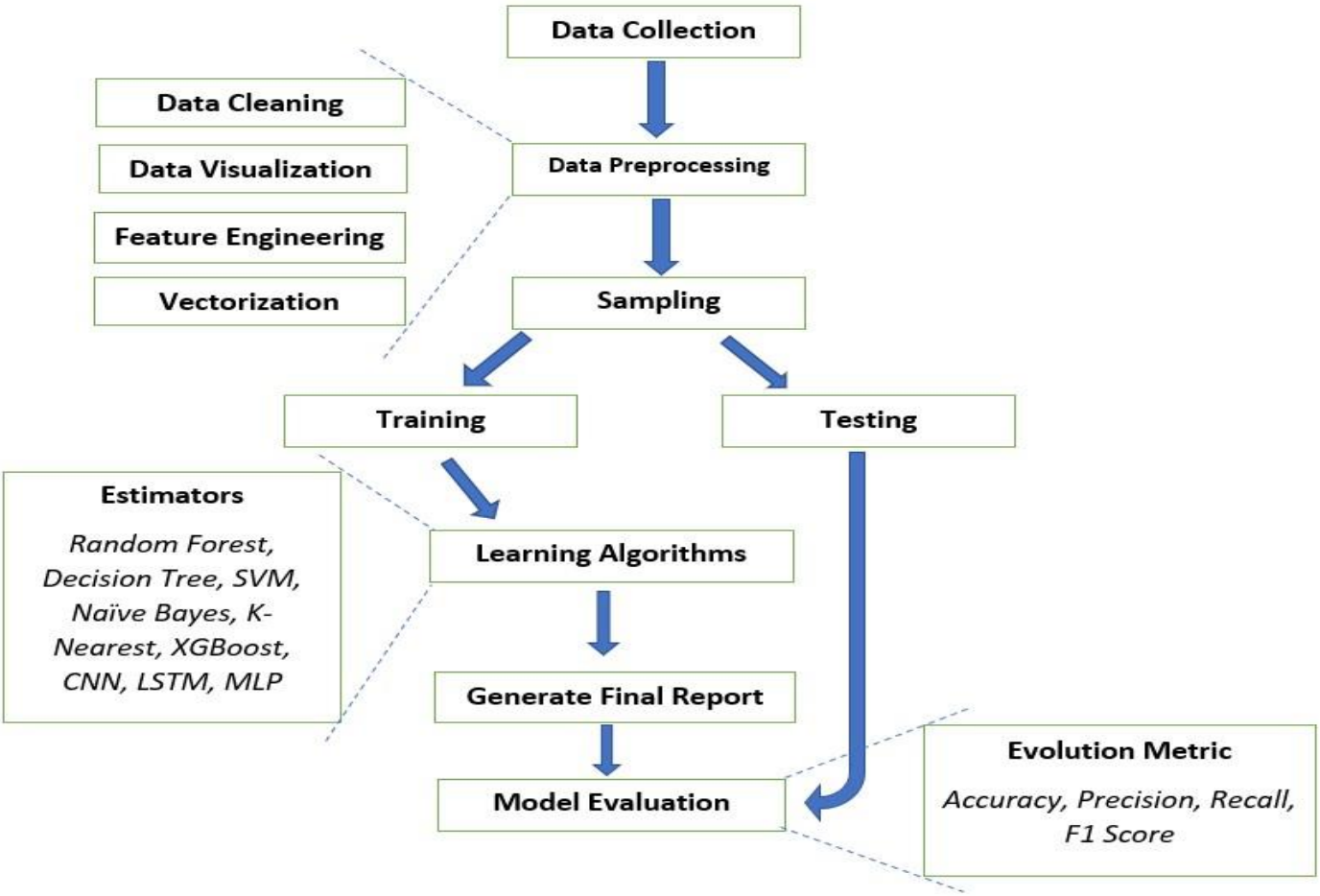

Fig. 1. The overall framework for attack and anomaly detection in IoT

Table 1. Dataset composition

Sr No.	Type	Frequency Count
1	DrDos-LDAP	5129
2	DrDos-MSSQL	4944
3	DrDos-NetBIOS	4934
4	DrDos-UDP	4921
5	DrDos-SNMP	4908
6	DrDos-DNS	4868
7	BENIGN	296

Handling Specific Records

Variables that reflect data separated into clusters are particular variables. The difficulty with particular data is that it cannot be examined using a set of rules until it is turned to a number value. On this take a look at, there had been three functions which had been categorical, especially IP address, timestamp, and label. Each sort of column was handled differently to store the data they conveyed [10]. Because machine learning models can only deal with integer or float data, IP addresses stated in quad-dotted notation could not be used for categorisation. It must be converted to its appropriate integer form by taking advantage of its binary structure. Because the timestamp declared the day and time of the assault, it became critical information to remember. Additional columns were created to maintain each timestamp component to convert it to a numerical representation. The output label had eight distinct values, seven of which signalled various types of attacks and one of which marked a normal connection. Using the only hot-encoding approach, these values have been converted to multi-column binary.

Standard Deviation Calculation

The measure of information diffusion is the standard deviation. It is critical to evaluate the unfold with each column since a zero deviation shows that the quantity is nearly constant over time and does not allow the class method to learn anything new about the data while extending the dimensionality and, thus, the computing expense. As a result, removing any columns with standard deviations close to zero is critical. This is based on the dataset that was used for this. I had a few columns where the standard

deviation was close to 0, such as PSHflags, URG flags, flag counts, forward and backward average bytes/bulk, and ahead and backward average packets/bulk. The flag columns, for example, The count number of certain flags and the average, were shown. Bytes/bulk signified the proportion of multiple bytes to bulk, whereas common packets/bulk denoted the proportion of sent and acquired packets to bulk [11].

Checking Correlation

The degree to which two or more variables are related linearly is a correlation. This is a good way to reduce record dimensionality by deleting attributes that have a weak association with the output label. With the aid of Python's sea-born package, a correlation heat map was created. The correlation coefficient is colour-coded, indicating the strength of the relationship between all aspects of the dataset. Features that have a nonzero correlation with the output label are beneficial in classification and are included in the study.

Standardisation Dataset

Standardisation is the process of transforming data such that its recommendations become zero and variance becomes one. It is designed to keep the size of all functions in a data set within a range, which reduces computation time and prevents fraud by algorithms that consider a function more important than its size value.

Handling Outliers

Noise as a database that differs from different data distribution rules. Work with changes that require data points to recognise data, data sales and data sets to assess data for data. In addition, the existence of a device blocks the knowledge of the algorithm and gets complexity to act the algorithm. As a result of removable external data, cleaning is a significant phase.

The contents of the data log can be found using visual methods such as cloud and bag chart analysis and statistical application as interquartile close results. Visual cues are particularly interesting because data points can be seen that do not follow the basic structure of the data [12].

However, they cannot be used when the dataset is large. Due to the large data set, the IQR method was used for detecting leaks. Interquartile rates for data records were obtained using this method by subtracting 70th and 30th percentiles.

Interquartile Range = Q3-Q1
Upper bound = Q1-1.5 x IQR
Lower bound = Q3+1.5 x IQR

Test Train Split

For this analysis, the dataset is divided into two halves in a 70-30 ratio. The more significant breakup is to train the algorithms; the test set is utilised to evaluate the trained algorithm's performance on the anonymous dataset using exceptional performance criteria.

Classification using ML and DL

This work used three deep learning algorithms and seven machine learning algorithms to detect DDoS attacks in networks. But the classification preliminary executed on the 20 decided features of the incoming network traffic. Finally, this model is compared with the training and testing datasets by considering the F1 scores, accuracy, and recall.

Extreme Gradient Boosting

This is a machine learning technique used in classification, regression, and many others. This prediction model is used in the decision tree algorithm to assemble week predictions. A decision tree is a weaker learner, so the resulting is called a gradient boosting tree. In which user decision tree technique in features for analysing the relationship. Using supervised input, create a tree and decrease and correct the error due to the creation of new trees via bottom trees. These models are added to the bottom tree till no further improvements. This algorithm uses memory resources efficiently to make it computationally friendly in a short amount of time, and this bosting gradient algorithm minimises the errors.

K-Nearest Neighbor

It is one of the simplest machine learning algorithms based on the supervised machine learning technique. Data points belong to the identical class, and new data is available on behalf of previous data of some other similar class. We can use KNN in some regression and classification but suitable and mostly used in classification. The similarity in a class and dissimilarity is shown in some among special classes. In which, assign data points to the class with the least distance. KNN is a lazy learner algorithm because it does not learn from the training set and stores the dataset. But in the case of classification, only act on the dataset.

Nanve Bayes

This is a supervised machine learning algorithm used to solve the classification problem—naïve Bayes theorem with the strong assumption between the features. In learning problem, this model is highly scalable require many parameters in the number of features. Use high dimensional training dataset for achieving text classification. This is a fast classification machine learning algorithm that makes a fast prediction. Their feature is independents of every other, but their feature has an equal impact on final results. Naïve Bayes algorithm used for spam filtering, medical data classifying, real-time prediction, credit scoring, and sentiment analysis. This algorithm is used for binary and multiclass classifications, and other algorithms perform well in multiclass classifications.

Support Vector Machine

Support vector machine makes the hyperplane used in outlier detection, which achieves good separation of the hyperplane near any class's largest training data point. Support vector machine is a supervised machine algorithm used for classification and regression. This algorithm creates the best line that separates the dimensional space into class, so this is easy for the future to put new data points incorrect categories. If the data is not labelled, it's not possible to use supervised learning but in case, use the unsupervised approach, which finds natural clustering of data into a group. SVM is used to categorise unlabeled data and is also used in industrial applications, which requires a clustering algorithm.

Decision Tree

It's like a tree structure that starts from the tree's root node and expands into further branches that look like a tree structure. The decision trees algorithm is used to is decide split two or more sub-nodes, and sub-nodes increase the homogeneity of any resultant sub-nodes. Decision trees are mostly used for classifying problems but also for classification and regression

problems. Again, it's like a tree structure. The internal node represents the dataset feature, identifies decision rules via branches, and results represent the leaf node, which has two nodes: decision and leaf nodes. Decision nodes are used for any decision for multiple branches, and leaf nodes are used for the output of this decision, which requires less data cleaning process than other algorithms.

Random Forest

Random forest is the supervised machine learning algorithm that performs classification and regression problems. The technique is based on ensemble learning which combines the multiple classifiers used to solve a complex problem. Build multiple decision trees and combine them to make a more accurate prediction. It contains many decisions tress in a given dataset on various subsets then average to predict the accuracy of datasets. Instead of decision trees, use the random forest to predict each decision tree and finally predict on behalf of more voting. Random forest used in banking, In Medicine, identify the risk of disease, Identify the similar area of Land, and identify the marketing trend.

AdaBoost

AdaBoost means adaptive learning used with other machine learning algorithms to improve performance. We can use this algorithm with others machine learning algorithms to improve performance. A weighted sum is the output of other algorithms representing the output of the boosted classifier. In an overfitting problem, this is less capable to another machine learning algorithm. This is used to boost the performance of another machine learning algorithm. A decision tree is used with AdaBoost to improve the accuracy. Instead of a binary classification problem, AdaBoost is used to classify the image and text.

Convolution Neural Network (CNN)

A convolutional neural network is a deep learning algorithm and a class of artificial neural networks used to analyse virtual memory. They are also called by space invariant artificial neural network based on the shared weight architecture and filter along with input feature and also provide translation is called as feature maps. CNN is mostly used in image recognition, image segmentation, and the medical field for image analysis and financial activities. This Convolutional Network is used in biological processes in pattern connectivity. Compared according to other image classification algorithm CNN use little preprocessing. Filter to optimised through network learning. This convolutional neural network is based on output, input, and hidden layers. Which middle layer is the hidden layer that performs convolution, and this convolution generates a feature map that moves to the input of the next layer.

Multi-layer Perceptron

The multi-layer perceptron is an artificial neural network used in supervised learning techniques like backpropagation for training. This multi-layer neural network consists of input, output, and hidden layers. The hidden and output layer uses non-layer activation functions. MLP uses backpropagation for training but in which data is not linear separately. It is used to solve a complex problem. In all neurons, the multi-layer perceptron has an activation function. Multi-layer perceptron is used to encode a database, monitor access, and check a database's security.

LSTM

Long short-term memory is an RNN Architecture based on deep learning. This model not only processes one data point (image) but all sequences of data (video). LSTM is used in speech and handwriting recognition and identifies attack and anemology in network traffic. LSTM unit is made with cell, input, output, and forget gate.

Performance and Evaluation

Overall performance evaluation is critical for properly determining how the model would work on unseen data. In this work, all five machine learning models had been evaluated using eight one-of-a-kind metrics. These metrics allow us to compare unique models against each different and evaluate the relevance of outcomes for every classification label. First, evaluate the model with a curve shown in figure 2. The following matrices were used for analysing the performance:

Accuracy

This is a subset of model performance. Accuracy measures the quality of classified observation overall numbers of observations. Accuracy discusses the percentage of classified input and the initial degree of model performance but is not a clear indicator for performance, which has many drawbacks. For example, it does not provide information of well classified, and that is being poorly classified through the model. Accuracy is described in Table 2.

Table 2. Applications of accident analysis techniques in different industries

Sr No.	Mechanism	Accuracy
1	Random Forest	99.88 %
2	Decision Tree	99.96 %
3	SVM	82.25 %
4	Naive Bayes	72.34 %
5	K-Nearest	96.72 %
6	XGBoost	99.98 %
7	Adaboost	99.96 %
8	CNN	79.68 %
9	LSTM	41.59 %
10	MLP	88.78 %

Precision

Precision is the positive predictive value, and this is used for evaluating the classification model. Precision measure with true positive and model claims to another number of positive. The ratio between true positive overall positive.

Recall

This model is used to correctly indent true positives-total positive instances over a percentage of positive instances.

F1 Score

F1 score is the harmonic mean of recall and precision, due to both recall and precision contribution achieved the higher f1 score.

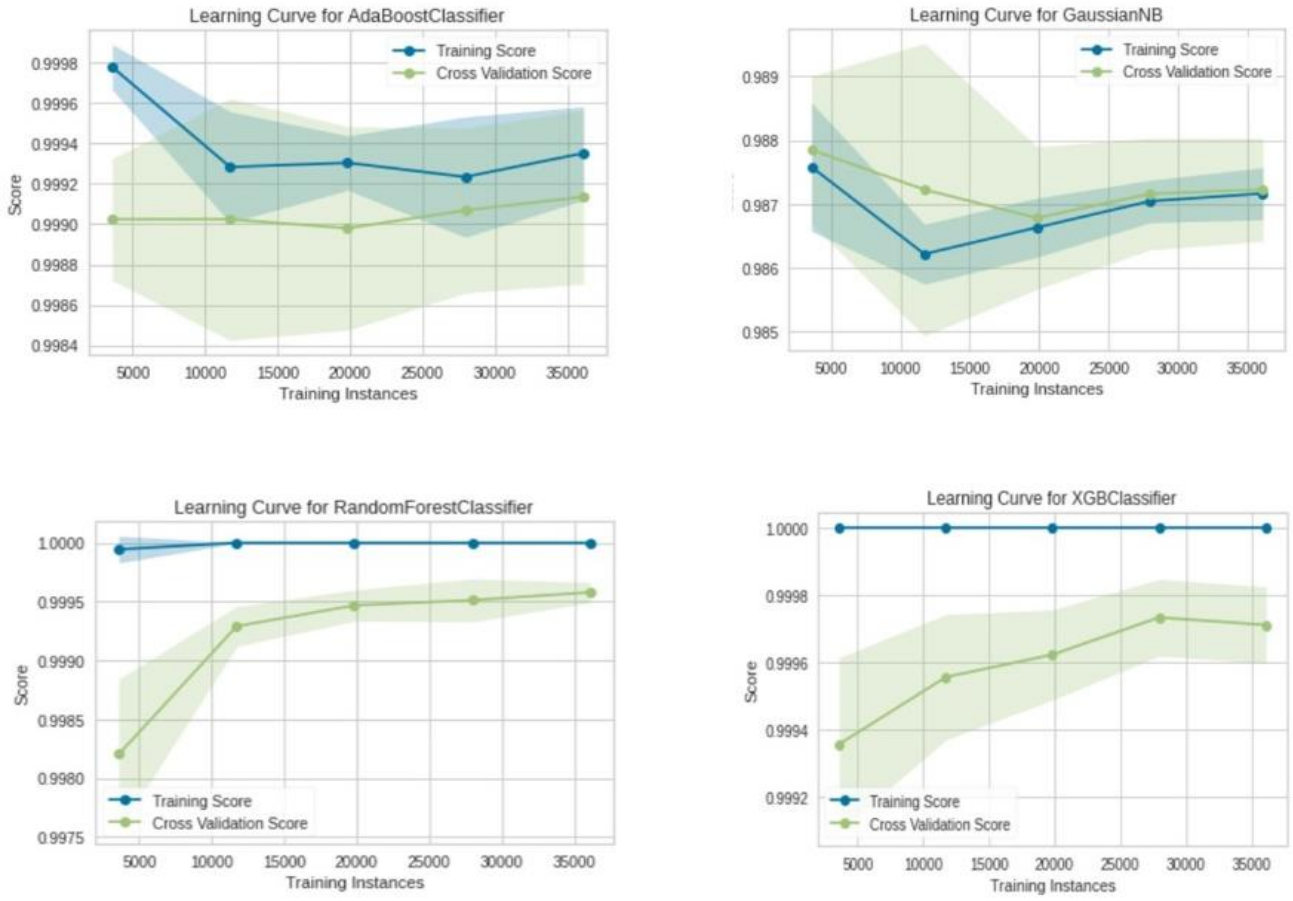

Fig. 2. Visualise the Learning curve of the Machine Learning Models

Table 3. Comparative description of proposed IoT attack detection with state of the art.

Author and Year	Dataset	Classification Type	Mechanism	Evaluation Metric (Accuracy)
Hasan et al. 2019 [3]	DS2OS	Multiclass	Logistic Regression Support Vector Machine Decision Tree Random Forest Artificial Neural Network	98.3% 98.2% 99.4% 99.4% 99.4%
Proposed Method	CICDDoS 2019	Multiclass	Random Forest Decision Tree SVM Naive Bayes K-Nearest XGBoost Adaboost CNN LST MMLP	99.88% 99.96% 82.25% 72.34% 96.72% 99.98% 99.96% 79.68% 41.59% 88.78%

Confusion Matrix

It is like a tabular form representing all predictions through the model shown in figure 3. Then, a confusion matrix is used to evaluate the machine learning algorithm's performance. The confusion matrix compares the actual value with the predicted value. This gives the result of our classification model how this works well and gives results about the error during the performance:

- Columns represent the actual values of the variable.

- Rows represent the predicted values of the variable.
- Variable has two values: Positive and Negative Value.

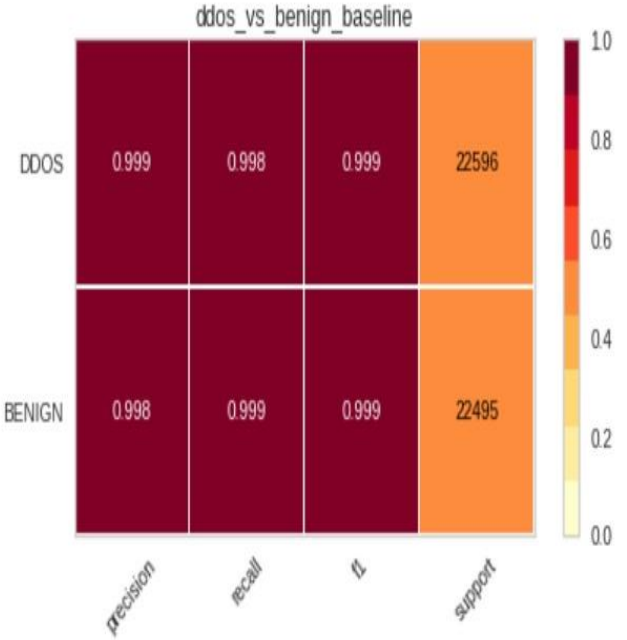

Fig. 3. Visualise Report with DDoS and Benign Baseline

True Positive

Predict the positive value, in which actual positive values are equal to predicted positive.

True Negative

Predict the negative value, in which actual negative values are equal to predicted negative.

False Positive

Predict wrong negative values as positive. The model predict the positive value for negative labelled data.

False Negative

Predict negative values as positive. The model predicted a negative value, but it's a positive in real.

Conclusion

Because of their dependability and versatility, Machine Learning IDs are known as basic methods for detecting cyber-attacks in IoT systems. However, as the results above reveal, machine learning detectors will be sensitive to attacks that seriously degrade or mislead their capacity. Furthermore, adversarial machine learning (AML) may major impact IoT infrastructures since opponents might change hostile DoS data points to avoid IDS, leading to delayed threat detection, secret data leaks, and major harm. This research examined how adverse attack can be employed by submitting generated Dos samples to a trained model and analysing their classification behaviours to target supervised classifiers. Use machine learning and deep learning model to improve accuracy. Achieve accuracy with XGBoost is 99.98%, and decision tree and Adaboost achieve 99.6% accuracy shown in Table 3. To support the experiments in this study, a benign and DoS network dataset of IoT has served to train and test several cutting-edge supervised classifiers, including the J48 Decision Tree, the best-performing IDS malicious and benign packets. The studies concentrated on DoS attack packets because it is one of the most serious assaults on IoT devices; it's hard to deploy through customised packages. Ultimately, due to the nature of DoS, an adversary can change packets without undoing the attack.

References

1. M. Pant, B.M. Singh, and D.V. Gupta. "3S-IoT an Algorithm to make the Network Secured and Smart". In: (2020).
2. D. Perakovic, M. Perisa, and I Cvitic. "Analysis of the IoT impact on volume of DDoS attacks". In: XXXIII Simpozijum o novim tehnologijama u postanskom i telekomunikacionom saobraˇ caju–PosTelˊ 2015 (2015), pp. 295–304.
3. M. Hasan et al. "Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches". In: Internet of Things 7 (2019), p. 100059.
4. H. Tyagi and R. Kumar. "Attack and Anomaly Detection in IoT Networks Using Supervised Machine Learning Approaches." In: Rev. d'Intelligence Artif. 35.1 (2021), pp. 11–21.
5. I. Ullah and Q.H. Mahmoud. "Design and development of a deep learning-based model for anomaly detection in IoT networks". In: IEEE Access 9 (2021), pp. 103906–103926.
6. Y.E. Sagduyu, Y. Shi, and T. Erpek. "IoT network security from the perspective of adversarial deep learning". In: 2019 16th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON). IEEE. 2019, pp. 1–9.
7. A. Abusnaina et al. "Adversarial learning attacks on graph-based IoT malware detection systems". In: 2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS). IEEE. 2019, pp. 1296–1305.
8. P. Maniriho et al. "Anomaly-based Intrusion Detection Approach for IoT Networks Using Machine Learning". In: 2020 International Conference on Computer Engineering, Network, and Intelligent Multimedia (CENIM). IEEE. 2020, pp. 303–308.
9. A.V. Deorankar and S.S. Thakare. "Survey on anomaly detection of (iot)-internet of things cyberattacks using machine learning". In: 2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC). IEEE. 2020, pp. 115–117.
10. K. Lee et al. "DDoS attack detection method using cluster analysis". In: Expert systems with applications 34.3 (2008), pp. 1659–1665.
11. Y. Al-Hadhrami and F.K. Hussain. "DDoS attacks in IoT networks: a comprehensive systematic literature review". In: World Wide Web (2021), pp. 1–31.
12. Y. Chen et al. "Design and implementation of IoT DDoS attacks detection system based on machine learning". In: 2020 European Conference on Networks and Communications (EuCNC). IEEE. 2020, pp. 122–127.
13. H. Sedjelmaci, S.M. Senouci, & M.A. Bahri (2016, May). A lightweight anomaly detection technique for low-resource IoT devices: A game-theoretic methodology. In 2016 IEEE international conference on communications (ICC) (pp. 1-6). IEEE.
14. Y. Meidan, M. Bohadana, Y. Mathov, Y. Mirsky, A. Shabtai, D. Breitenbacher, & Y. Elovici (2018). N-baiot—

network-based detection of iot botnet attacks using deep autoencoders. IEEE Pervasive Computing, 17(3), 12-22.

15. T. Golomb, Y. Mirsky, & Y. Elovici (2018). CIoTA: Collaborative IoT anomaly detection via blockchain. arXiv preprint arXiv:1803.03807.
16. I. Butun, B. Kantarci, & M. Erol-Kantarci (2015, June). Anomaly detection and privacy preservation in cloud-centric internet of things. In 2015 IEEE International Conference on Communication Workshop (ICCW) (pp. 2610-2615). Ieee.
17. V, Timčenko, & S. Gajin (2018). Machine learning based network anomaly detection for IoT environments. In ICIST-2018 Conference.
18. I. Ullah, & Q.H. Mahmoud (2021). Design and development of a deep learning-based model for anomaly detection in IoT networks. IEEE Access, 9, 103906-103926.
19. V. Mothukuri, P. Khare, R.M. Parizi, S. Pouriyeh, A. Dehghantanha, & G. Srivastava (2021). Federated Learning-based Anomaly Detection for IoT Security Attacks. IEEE Internet of Things Journal.
20. Y.M. Tukur, D. Thakker, & I.U. Awan (2021). Edge-based blockchain enabled anomaly detection for insider attack prevention in Internet of Things. Transactions on Emerging Telecommunications Technologies, 32(6), e4158.