Security and Performance Issues of IoT Devices on account of DDOS Attacks

Ahmet Yılmaz, Beraat Buz, Muhammed Enes Tırnakçı, Sercan Aydın

**Abstract**— Internet of Things (IoT) is a collection of internet-connected devices. Increasingly, organizations in various industries are using IoT technology to work more efficiently, provide better customer service, improve decision making and increase the value of the business, better understanding of customers. Thus, with this increase some manufacturers need to make some compromises to ensure their devices work at maximum performance to compete other competitors. These compromises let’s IoT devices more vulnerable to security threats. In this article, we discuss the security and performance issues of IoT devices with regard to Distributed Denial-of-Service (DDoS) attacks and propose a machine learning based solution that aims to detect attacks intelligently. We present a DDoS attack detection system based on incoming network packets types and design a machine learning model to identify DDoS attacks. To show how effective our model is we calculated model accuracy and model loss, and used a large dataset. In order to generate our model, we used sequential and K-V fold methods with Keras development library.

**Index Terms**— Artificial intelligence, Distributed Denial-of-Service (DDoS) attacks, Machine Learning, Deep Learning, Internet-of-Things (IoT) security.

————————————————

1. Ahmet Yılmaz is with the Department Faculty of Computer and Informatics Istanbul Technical University, Turkey. E-mail: yilmazahm16@itu.edu.tr
2. Beraat Buz is with the Department Faculty of Computer and Informatics Istanbul Technical University, Turkey. E-mail: buz16@itu.edu.tr
3. Muhammed Enes Tırnakçı is with the Department Faculty of Computer and Informatics Istanbul Technical University, Turkey. E-mail: tirnakci@itu.edu.tr.
4. Sercan Aydın is with the Department Faculty of Computer and Informatics Istanbul Technical University, Turkey. E-mail: aydinser17@itu.edu.tr

—————————— ◆ ——————————

# 1 Introduction

I

NTERNET of Things means that any object can be connected to the internet directly or indirectly at the simplest level. These objects can be anything you can think of like mobile phones, coffee machines, cameras, cars, industrial equipment, printers, computers, and even door bells. So we can think of something that can connect to the internet when we say object, or you can assume that anything can connect to the internet. Since, sensors started to appear everywhere in our lives with the growing diversity of sensors and the growth in the use of sensor devices, there was an increase in the number of Internet-connected objects much more than predicted. The ability of these devices to connect to the internet offers us a world where we can monitor and manage these objects on the internet. While IoT enables machines to talk to each other, artificial intelligence technology enables devices to command each other. This means that the devices can manage themselves. The biggest reason that the Internet of Things is so popular is that thousands or even millions of devices can be connected to the internet and can be used in many industries. Therefore, IoT is used in dozens of areas, including Smart Cities, Industry 4.0, Smart Homes, and Smart cars. Thus, this huge increase in devices and popularity let new manufacturers to get into to this market. In order to maintain profit, some manufacturers released devices with huge security vulnerabilities. For this reason, while IoT's market sharing and service domains are increasing increasingly, their conditions of protection remain undesirable. Companies make comprises in areas like the default software configuration, irregular updates of software installed, a long gap between patch release and it installation even some companies do not send updates to devices in the entire life time of devices. Since these devices are connected to the internet all the time and easy to get control of them, these devices become a potential tool for DDoS attacks. On the top of the DDoS attacks, Bot Nets that are random ware infection are also a very big threat for IoT devices. After IoT devices infected with a Bot Net malwares, these malwares lock devices with encryption and attackers want ransom to decrypt the device.

According to Gurunath, due to the default login credentials of some devices, the botnet called mirai has hacked many devices. Also Gurunath mentioned that use of unprotected internet protocols for internet scanning such as Zmap and Nmap can be resulted with intrusion by attackers [1].

Bhabad and Bagade described that some businesses need high processing power and operational control in application layer of IoT devices. Therefore, these businesses need high performance rather than spending resources for security checks. This affects security of IoT devices negatively [2].

Conceptual network anomaly detection model may also be new approach for detection of DDoS traffic generated by IoT devices. In addition to this, determining traffic deviations generated by IoT device compared to the legitimate traffic class is the good criterion for detection of DDos attacks. Using this model, IoT devices can be more secure [3].

In our proposed solution we have created a model to detect DDoS attacks intelligently. We used a detailed dataset to train our machine learning model to reduce model loss and maximize the model accuracy. Using supervised machine learning in our system will let IoT devices to make less performance sacrifice to secure itself.

Deep learning algorithms can also be used to train models, yet since deep learning requires high computing power and its complex training procedure causes to longer period of times to learn. Since IoT devices are usually low power devices, IoT devices cannot afford to use deep learning [4].

Before we dive into our proposed solution and its analysis, we collected and looked into some similar projects that are done for detecting and preventing DDoS attacks. We categorized these similar projects into three main sub-categories which are projects that are deep learning based DDoS defense techniques, projects that are machine learning based DDoS defense techniques and projects that are based on other DDoS defense techniques.

# 2 Background and Related Work

## 2.1 DDoS Attacks

Distributed Network Attacks are commonly known as Distributed Denial of Service (DDoS) attacks. These types of attacks take advantage of certain capacity limits that apply to any network resource, such as the infrastructure that provides a company's website. DDoS attacks aim to overcome or overload the website's capacity to process multiple requests, and prevent it from working correctly by sending multiple requests to the attacked web resource. The attacker sets up a zombie network of computers to send an extraordinary number of requests to the targeted resource. The scale of the attack can result in overloading the victim's web resources, as the attacker can control the actions of all infected computers in the zombie network. Since the number of requests that network resources such as web servers can serve simultaneously is limited, every time the number of requests exceeds the capacity limit of any component in the infrastructure, the service level will response to requests much slower than usual or some or all user requests can be completely ignored. In worst-case scenario, the entire service may even be down for a long time. Usually, the main goal of the attacker is to completely prevent the normal operation of the web resource. The attacker can also ask for money in exchange for stopping the attack. In some cases, a DDoS attack can also be an attempt to damage a competitor's reputation or damage its business.

## 2.2 Deep Learning Based DDoS Defense Techniques

Since DDoS attacks need to be detected while live internet traffic is ongoing, Doriguzzi-Corin et al. [5] present flexible and less heavy on performance deep learning DDoS detection system called LUCID which take advantage of the properties of Convolutional Neural Networks (CNNs) in order to find out traffic flows as either malicious or not. The authors observed that advantage of the CNN model is the elimination of the threshold configuration as required by approaches to statistical detection, and minimization of feature engineering. In their study, authors proposed a solution that lets CNNs to reuse parameters in terms of kernel weights to reduce performance impact on storage and memory usage, while every weight is used only once in a typical neural network. Their model automatically learns weights and biases of each filter during training to reduce the time-consuming feature engineering.

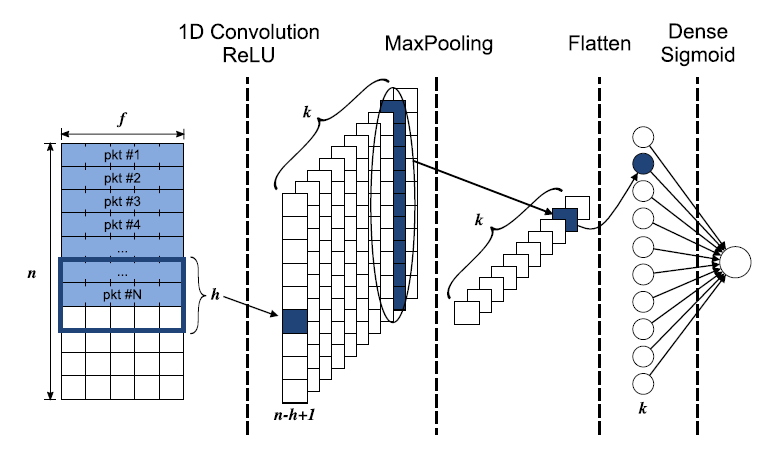


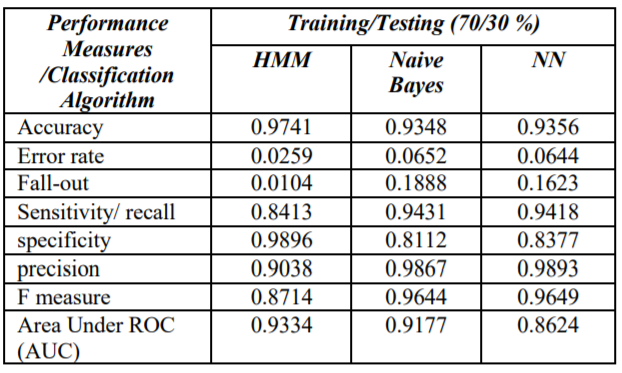
Fig. 1. LUCID Model

Deep learning approach has also been applied by ensemble convolutional neural network solution for distributed denial of service detection. Although CNN is a very effective mechanism used for image recognition, it is also used for DDOS detection. CNN works with various layers. In this approach Convolutional Layer is used to determine features. Then, it is provided to introduce non-linearity to the system by the Non-Linearity Layer, and Pooling (Down sampling) Layer reduces the number of weights and checks the fit. At the Flattening Layer, Data is prepared for the Classical Neural Network, and Fully-Connected Layer is Standard Neural Network used in classification

For example, [6] uses this technique to detect DDOS attack in SDN’s. It applies the algorithm as that from the dataset, 60:40 divisions of 140000 examples is made for grouping. Kindhearted traffic highlights are marked as 0 while DDoS as 1 in the stacked dataset. Dataset is part into preparing and testing with 0.2 test size. Highlights are scaled with Z-score standardization in pre-preparing stage. At that point dimensional reproduction of the highlights is done for before they put them into the Ensemble and single CNN model.

After they train the algorithm, they analyze the results by helping Keras Library with Tensorflow Backend. They noticeably get excellent detection accuracy 99.48% of the proposed ensemble CNN approach. Their accuracy is really successful compare to existing ones, and also their testing time is quite a short duration for all test set.

One of the applications of deep learning in detecting distributed denial service attacks is the using hidden Markov models. The Hidden Markov Model (HMM) is a widely used approach in the automatic learning literature to model time series. In this model, it is assumed that the observations are produced based on a conditional probabilistic rule on a hidden Markov state sequence. It has been used many deep learning areas such as speech recognition, computer vision and bioinformatics. Sulaiman Alhaidari, Ali Alharbi and Mohamed Zohdy have used this approach in their research [7]. The performance that is against to DDOS attacks of the HMM algorithm compares against two classification algorithms, Neural Network and Naive Bayes algorithm is shown at Table 1.

TABLE 1  
THE SUMMARILY OF THE EXPERIMENT RESULTS [7]

## 2.3 Machine Learning Based DDoS Defense Techniques

In order to detect, identify, classify, and mitigate DDoS attacks, Jia et al. [8] present system called FlowGuard based on traffic variations and two machine learning models which are long short-term memory (LSTM) and convolutional neural network (CNN). By using DDoS simulators like BoNeSi, SlowHTTPTest and CICDDoS2019 dataset, they showed their system outperforms other most used machine learning models that are used for detecting DDoS attacks. In order to detect suspicious flows of DDoS attacks are filtered according to filter rules that are created by machine learning algorithms. Filtered flows are handled by flow handler component of FlowGuard. To filter flows at maximum efficiency FlowGuard is deployed at edge servers as close as to the IoT network, so flow component can check all the packets passing through the edge servers. Authors use CICFlowMeter to get maximum features of each flow, to detect intention of flows. Their flow handler is based on a pre-designed LSTM model that is fed with flow-oriented attributes such as time period and length of each fragment and labels them as harmless or malicious. The harmless flows are sent to their destinations while the malicious ones are submitted for DDoS attack detection to the CNN model. While LSTM identify DDoS attacks, CNN classify DDoS attacks.

In order to protect network services, IoT servers and their resources from DDoS attacks, Ravi et al. [9] present a solution named learning-driven detection mitigation (LEDEM) that detects DDoS attacks with a semi-supervised machine-learning algorithm. Presented solution detect DDoS attacks via pre trained machine learning model. Model let local controllers to judge if traffic is malicious or not. Experimenting with various different learning technics like gradient-based learning, extreme learning machine (ELM) with its variants, and semi supervised deep extreme learning machine (SDELM) to determine base model for solution was SDELM selected by authors. The reason why SDELM is selected instead of ELM is SDELM is more robust and does not suffer from overfitting compared to ELM. Their system detects malicious DDoS attack by two different subsystems. One of is fIoT, and other one is mIoT. While fIoT is used for not moving objects like smoke alarm or door bells, mIoT is used for moving objects like wearable devices. Thus, while fIoT does not need authentication and authorization, mIoT does need authentication and authorization to ensure its security, so each time a moving object enter the range of access points, mIoT has to perform authentication and authorization process.

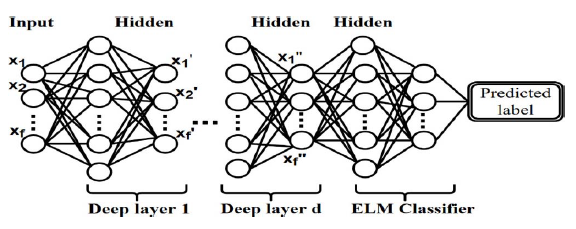


Fig. 2. SDELM Model

The detection system developed by the authors in this study [10] enables detection of DDoS attacks using machine learning technology and artificial neural networks (ANN) architecture. It uses a public data set for algorithms to develop. The Bot-IoT dataset used to detect attacks contains a small amount of benign data and a large amount of attack data. This creates an imbalance problem that needs to be solved. SMOTE (Synthetic Minority Over-Sampling Technique) was used to solve this imbalance problem during machine learning process. In the results, it is said that this approach can be an effective method in detecting DDoS attacks. This proposed detection system consists of four main parts: transformation, resampling, detecting, and alert generating. First of all, since the artificial neural network technology only processes numerical values, it is necessary to make a transformation process to represent the nominal values numerically. Then, a sampling architecture is developed with SMOTE, one of the high-speed sampling techniques, to solve the data imbalance problem. With a single hidden layer and an exit node, an artificial neural network is created to detect attacks. In addition, the neuron number similar to the input characteristics is put in the hidden layer. Using the Scikit-learn library, it is processed into the neural network architecture that created the sigmoid activation function. As a result of these actions, the system will give the necessary warning message when it detects an attack.

In this study [11], the authors demonstrate the Smart Detection-IoT system using machine learning method of DDoS attacks by analyzing the IP / TCP header to classify and interpret IoT network traffic without violating data privacy. The most important purpose of this system is to detect the attack as early as possible and to take action as soon as possible. The authors demonstrate that the Smart Sensing-IoT system proposed in this study has been evaluated for its performance using three classification algorithms and achieved good results compared to common approaches. The system has been tested with three datasets. These datasets are: CIC-DOS, CICIDS2017, and a customized containing several DoS / DDoS attacks, such as UDP flood, TCP flood, HTTP flood, and HTTP slow. As Fernandes S., Filho, Silva, Junior, and Felipe S. state that network traffic’s sampling rate (SR) %20, precision (PR) value is higher than 93%, attacks’s detection rate (DR) is higher than 96%, and it has low false alarm rate (FAR) (2020, p. 343).

In this study [12], the authors demonstrate the DDoS attack Detection-IoT system using machine learning method. They use pandemic modelling sources for IoT networks consisting of WSNs. In order to detect and abnormal defense behaviors, they establish a proposed framework. There are major difficulties, given the effect of IoT-specific features such as inadequate computing capacity, power constraints, and node density on the creation of a botnet. They use standard datasets for Mirai attacks which is the famous attack. They also use many machine learning methods. Data is collected and extracted from several IoT devices. There were many challenges for authors. These are dataset preparation, data preprocessing. The proposed framework reveals any strange movement by searching the traffic for IoT devices. In the experimental results, they found that the combination of random forest and decision tree algorithm achieves high accuracy for detection.

In this research [13], the authors simulate IoT network with 100 nodes using the simulation tool OMNET++ which includes DDoS attacks and is based in three tier IoT architecture. Also, OMNET++ simulator is a C++ based component simulation library. It provides a platform for the models to be generated. This 3-Tier architecture is composed of Perception Layer, Network Layer, Application Layer. In order to calculate the accuracy of detecting DDoS attacks on IoT networks using machine learning techniques, regular and attack-injected traffic is generated. A new IoT dataset is created by authors with different scenarios of normal traffic and traffic with attacks of different intensities. Due to the lack of public datasets, the main contribution of this research is the recognition of the need for an IoT DDoS attack dataset. Therefore, this created dataset used with machine learning tools to determine accuracy of the DDoS detection. Different ML algorithms in Azure ML studio used to analyze created dataset and evaluate the accuracy of the detection. The algorithms in research such as decision forest, decision jungle and boosted decision tree were used. Performance comparison of boosted tree in detecting DDoS attacks is higher than other two algorithms. The authors made this dataset publicly available. The dataset can be applied to different machine learning algorithms in order to develop different defensive mechanism to DDoS attacks.

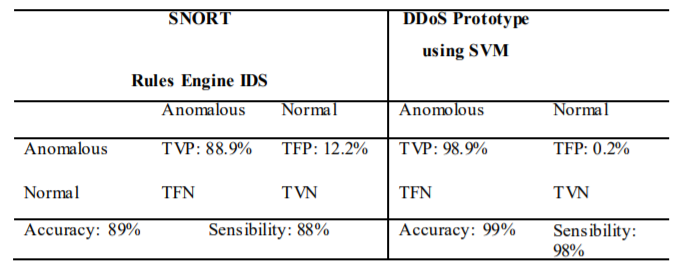
Another related work on this area is the using SVM machine learning method to detect DDOS attacks on IOT devices. Support Vector Machine is a classification algorithm like Logistic Regression. Both try to find the best line that separates the two classes. The algorithm allows the line to be drawn to be adjusted in two classes so that it passes from the furthest place to its elements. It is a classifier that takes no parameters (nonparametric). SVM can also classify linear and nonlinear data, but generally tries to classify the data linearly.

According to algorithm, firstly traffic is captured from TCP/IP Network. Then, the data that is captures is filtered, and this filtered data is normalized to get a normalized traffic. At the end, this data is trained and evaluated, and the results are stored.

In [14], they use the dataset in which the total standardized traffic data (typical 1349, anomalous 1349), are separated into the training stage, arbitrarily choosing 60% of the dataset (ordinary 809 irregulars 809), the other 40% (ordinary 539 abnormal 539) for testing. As a result, when they compare that SVM against a conventional Open Source IPS, they have great success that is shown Table 2.

TABLE 2

SVM DDOS PROTOTYPE PERFORMANCE RESULTS METRICS VS CONVENTIONAL IDS [14]



[15] have a semi-supervised machine learning approach for DDoS detection. As know, the labeled network traffic datasets are used by supervised ML, and the incoming network traffic that is going to be analyzed is used by unsupervised ML. Against these, this research has focused on datasets preprocessing, estimation of network traffic entropy, online co-clustering, information gain ratio computation and network traffic classification.

After datasets preprocessing the flow size distribution (FSD) that is a time-based sliding window algorithm is used for network traffic entropy estimation by comparing the packets count and bytes count of source and destination. Then, the estimation is clustered by an online co-clustering algorithm that is a proper strategy for classifying rows and columns of large sparse matric. At the end, according information gain ratio computation which is computed based on average entropy, network traffic is classified by using Extra-Trees ensemble which is a simple decision tree.

This approach is evaluated by three public datasets, and had accuracy 98.23%, 99.88% and 93.71% respectively.

## Other DDoS Defense Techniques

In this paper [16], the authors demonstrate an edge-based detection scheme using BPFabric, which uses a high-speed, programmable data-plane architecture and lightweight network functions to detect upstream anomalies. By this recommended detection method, it guarantees minimum resource usage and over-processing prevention. In addition, this system provides rapid detection of DDoS attacks on IoT devices. Gonzalez, Pastor, and Pezaros express that the solution gives 93%-95% accuracy, detection delays under 5ms, bandwidth overhead under 1%, when it compares with two well-known detection techniques (2019, p. 69). To realize platform independence and high performance levels are based on BPFabric specified in the study. The BPFabric platform can be considered complementary to other solutions as it allows programming the data plane of SDN network nodes. Because BPFabric focuses on high-speed processing, the Extended Berkeley Packet Filtering (eBPF) instruction set is used by BPFabric instead of Domain Specific Language (DSL).

In this article [17], the Manufacturer Usage Description (MUD) evaluation study was conducted by the authors. This system presents weaknesses of systems and improvements in architecture. In this research, a mechanism is put forward to identify and eliminate security vulnerabilities before creating a MUD profile. In this study, OWASP technology which discovers security vulnerabilities for Wi-Fi home routers is used. Devices can only request a MUD profile if their vulnerabilities are low. MUD is an Internet Engineering Task Force (IETF) standard that aims to describe the behaviour of IoT devices using Access Control Lists (ACLs) to communicate with or receive communications from a device. Also, in this study, there is a mechanism to perform both device MUD profile and MUD file generation operations. As an extra, there is talk about the application of home networks to perform a MUD profile using the firewall to protect from DDoS attacks.

In this article [18], the authors reveal a detection method with 3 main parts. One of these sections is a floating time window to fix the entropy calculation, another part is a one-way filter to perform early detection before the DDoS attack completely occurs and the last part is a quintile bias control algorithm to optimize results. The authors say that this method will give a real-time and highly efficient performance to recognize IoT DDoS attacks in the shortest time possible. Traffic data in the system is processed by the traffic processor and this data is sent to the entropy calculator. The entropy calculator that calculates real-time entropy values transmits the values to the detection module. Whether to give a warning or not is decided by the sensing module after the entropy values are matched with the risk models. As a result of these improvements, the entropy calculation process is optimized and a Quintile Deviation Check (QuinDC) algorithm has been designed to perform a real-time volumetric detection (RTVD). QuinDC, providing accurate performance and low latency, is also suitable for attack and defense systems with real-time requirements.

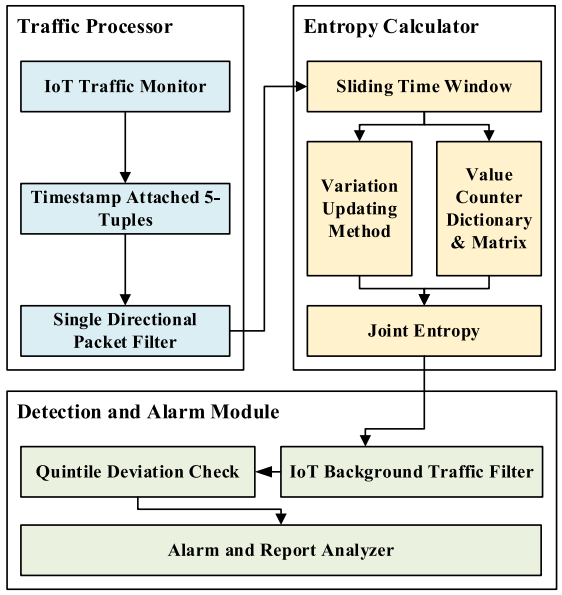


Fig. 3. Main Parts of Detection Method

In this article [19], the authors present the framework for the Internet of Things using the SDx paradigm. Then, an algorithm is proposed to detect and reduce DDOS attacks. In this algorithm, the threshold value of the cosine similarity of the packet input vectors is obtained at the port points of the SD-IoT limit switches. The threshold value is used by the algorithm to determine whether a DDoS attack has occurred, to find the true DDoS attacker, and to prevent the DDoS attack at its source. The framework consists of three layers: the application layer, control layer and infrastructure layer. The application layer consists of the IoT server containing SD-IoT controllers located in the cloud center and this server serves different services by using APIs. The control layer consists of controllers with SD-IoT controllers and runs a logical central control operating system for data transmission. The infrastructure layer contains many SD-IoT switches within it. Each switch performs the function of the IoT gateway and different IoT operating devices such as cameras, digital cameras, smartphones and personal This 3-Tier architecture is composed computers are accessed by these SD-IoT switches.

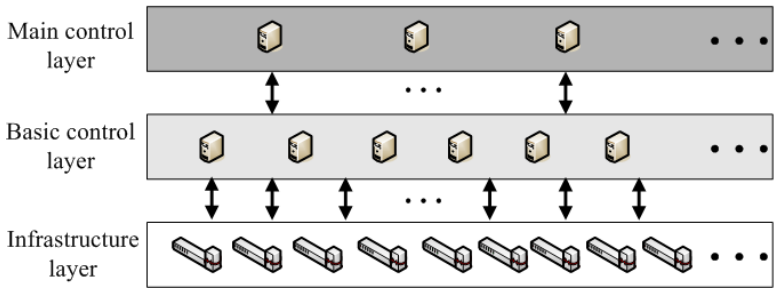


Fig. 4. Framework Layers

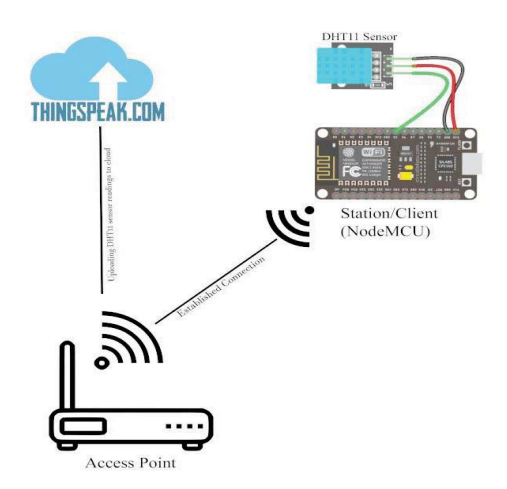
Several research papers are available on IoT devices and security issues faced by IoT devices. Most of the research are focusing on or are related to the problem statement that is at hand. In this paper [20], the Authors focuses on DDos attacks for IoT devices using Aircrack-ng carried out to reject fundamental services to microcontroller (NodeMCU) which is a gateway device. The system prevents most forms of attacks that target the victim IoT device using their MAC addresses. System has DHT11 and NodeMCu sensor. The system avoids most types of attacks using their MAC addresses targeting the victim's IoT devices. For this, it should serve as a station in order to connect to an access point. Therefore, proposed solution is that it adds an additional layer of security to the gateway by constantly changing its MAC address. Since MAC address is specific it’s easy for an attacker to launch an attack to the gateway by specifying the MAC address of the gateway device. By this proposed solution, we can change the MAC address continuously so that it becomes hard to find the its address of the gateway thus adding another layer of the security to gateway.

Fig. 5. System Architecture

In this article [21], the authors present the framework for detection of the depletion type DDoS attacks using Matching Pursuit algorithm. They use multiple network traffic features simultaneously to effectively detect low density DDoS attacks. The proposed method uses a dictionary created from network traffic parameters using KSVD algorithm. Network traffic dictionary generation offers legal traffic models and attacks. They discussed Wavelet and MP based DDoS detection approaches. These are, MPMP, Adaptive Matching Pursuit Based Detection (AMP), and Wavelet-based intrusion detection methods. In the AMP method, they combined anomaly detection and misuse detection using decision engine. And also, they evaluated both methods with and without the decision engine for the detection of TCP and UDP flood attacks. They also combined TCP and UDP flood datasets to test the efficiency of the methods in three traffic groups to detect DDoS attacks. Authors evaluated and compared these approaches using CAIDA datasets which are used as a combination of two datasets containing only DDoS attacks and only attack free traffic. And also, these approaches are compared and evaluated using BOUN DDoS dataset. As a result of this, they also implement DDoS detection methods using Matching Pursuit and Wavelet techniques and compare them using two distinct datasets. The experimental results show that the AMP method performs better compared to the Wavelet and MPMP methods with higher CID values.

# 3 Proposed Solutıon

We have designed an DDOS detection mechanism with using machine learning algorithm.

Our algorithm uses a simple feedforward network built in Keras to determine if incoming network packets are from one of four types of DDOS attacks or are a normal request.

Firstly, we shape our data into training data, test data, training label and test label by using 5 K-Fold cross validation. After shaping data, we create a sequential model of Keras library to fit. We fit our model with epoch size 2. At the end of our solution, we observe the evaluation results. We run this solution on Windows by using python 3.7. The requirements are Keras, Numpy, Arff Decoder that is needed for data, and Matplotlib.

To test the solution, we provided, we used a database that includes 60,000 data in it. In our database, there are lots of features such as source address, destination address, from node, to node, packet type, packet size, flag, flag identity, sequence number, number of packets, number of bytes, node name from, node name to, incoming packet, outgoing packet, packet rate, packet delay node, byte rate, average packet size, utilization, packet delay, packet delivery time, packet received time, first packet sent time, last packet received time and packet class.

Our algorithm’s pseudo code is shown at figure 6, and data model example is shown at figure 7.

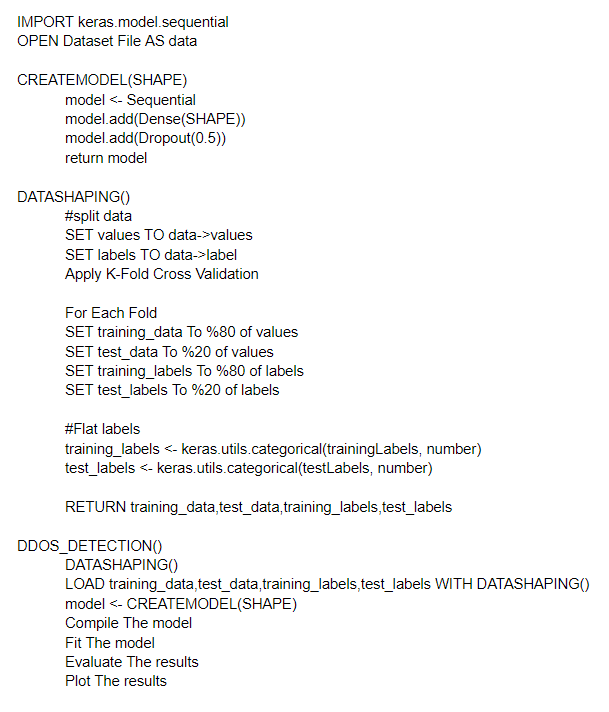


Fig. 6. Pseudo Code

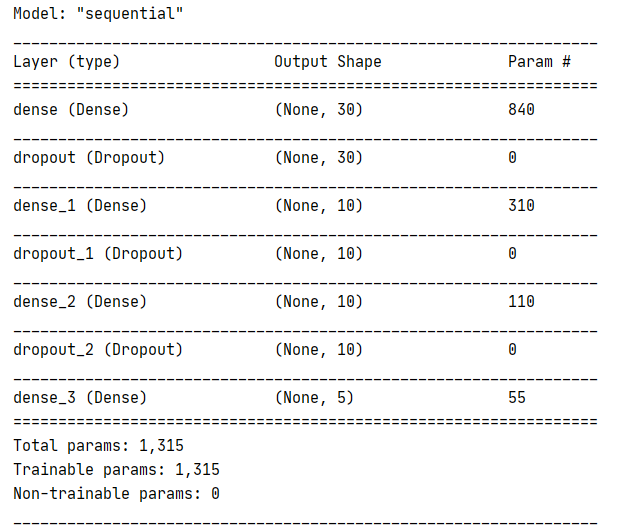


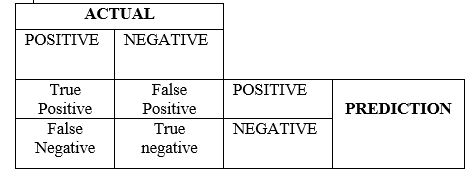
Fig. 7. One of the data model example

# 4 Analysıs of Proposed Solutıon

We need to know the following four terms: True Positive (TP): The number of attack instances identified as attacks: The performance test method to assess the performance of our proposed model and how reliable the model classifying and predicting the class mark of attack and natural. True Negative (TN): the number of instances of non-attacks known as non-attacks. False Negative (FN): The number of cases of attack defined as non-attacks. False Positive (FP): the number of cases of non-attacks classified as attacks. This terms are shown in the following table.

TABLE 3

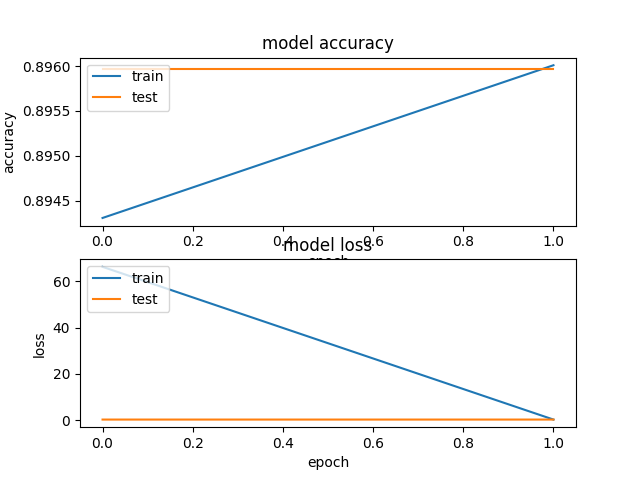
CONFUSION TERMS



With these TP, TN, FP, FN numbers, a matrix called Confusion Matrix is created and will be used in calculating the performance of our classification model.

Performance metrics calculated using the confusion matrix are:

1. **Accuracy**: The estimated correct classifications divided by the total number of classifications.
2. **Precision**: Used to determine how accurate it actually is when a positive estimate is obtained from the classification. This is divided by the number of correctly predicted positive predictions by the total number of positive predictions predicted, true or false.
3. **Recall**: Also known as Sensitivity or TPR (True Positive Rate). Which part of the positive predictions made by the classifier are used to find exactly this situation. In other words, it is the number of positive predictions divided by the number of positive classified values in the test data.
4. **False Positive Rate (FPR):** Recall goes by the name of True Positive Rate, as mentioned before, besides, there is another similar rate calculation that is False Positive Rate. FPR is used to calculate the odds of negative predictions. TPR and FPR are both used to draw a curve called a ROC (Receiver Operating Characteristic) curve. TPR and FPR formulas are:
5. **False Negative Rate (FNR):** The quickest way to calculate the false positive rate is to subtract one by the specificity of the test. However, if you do not know the specificity then you can calculate the false positive rate with following formula.



1. **F-measure:** F-measure helps to measure sensitivity and recall at the same time. It uses harmonic mean instead of arithmetic mean, punishing excess values more.
2. **True Negative Rate (TNR):** The specificity of the test, also referred to as the true negative rate (TNR), is the proportion of absolutely negative samples tested negative using the test in question.

TABLE 4  
OUR SOLUTION'S PERFORMANCE RESULTS

|  |  |
| --- | --- |
| Performance Measures | Our Proposed Solution |
| **Accuracy** | 0.8968 |
| **Precision** | 0.9073 |
| **Recall** | 0.8188 |
| **False Positive Rate (FPR)** | 0.0684 |
| **False Negative Rate (FNR)** | 0.1032 |
| **F-measure** | 0.9227 |
| **True Negative Rate (TNR)** | 0.8341 |

We used the K-Fold method to increase the accuracy of our algorithm. In the K-Fold method, we selected the number 5 suitable for the K value, and we printed the output of each fold value to show the development of our algorithm.

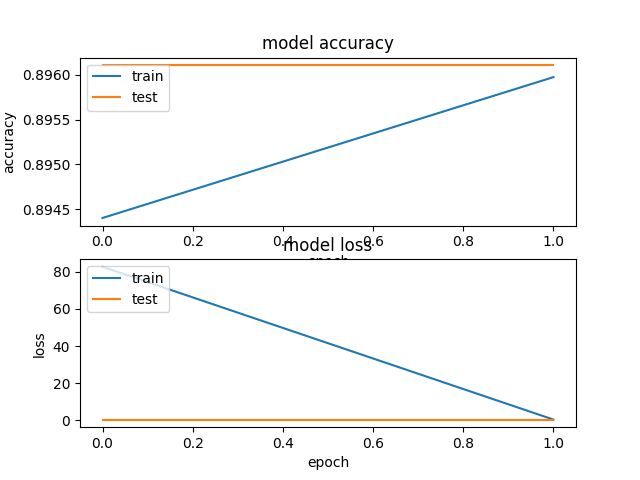


Fig. 8. First Fold

For the first fold, our model accuracy on train and validation dataset is 0.8958 & model loss on train and validation dataset is 1.5765.

Fig. 9. Second Fold

For the second fold, our model accuracy on train and validation dataset is 0.8959 & model loss goes from 67 to 1.69 on train and validation dataset.

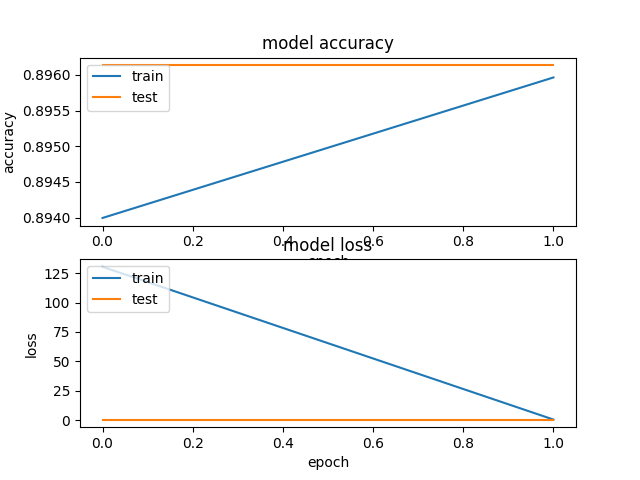


Fig. 10. Third Fold

For the third fold, our model accuracy on train and validation dataset is 0.8963 & model loss goes from 130 to 2.02 on train and validation dataset.

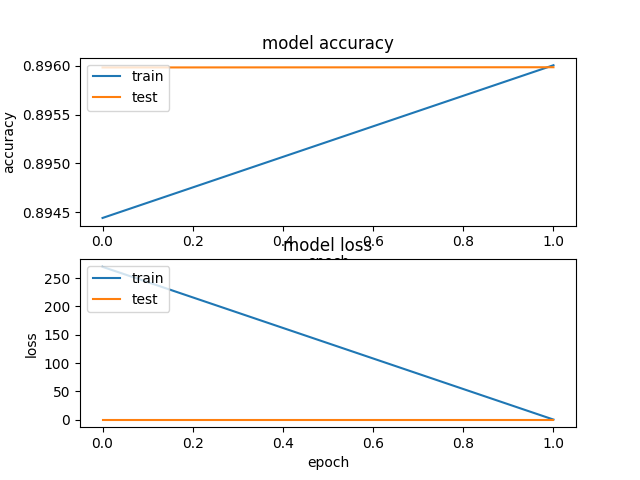


Fig. 11. Fourth Fold

For the fourth fold, our model accuracy on train and validation dataset is 0.8960 & model loss goes from 265 to 4.21 on train and validation dataset.

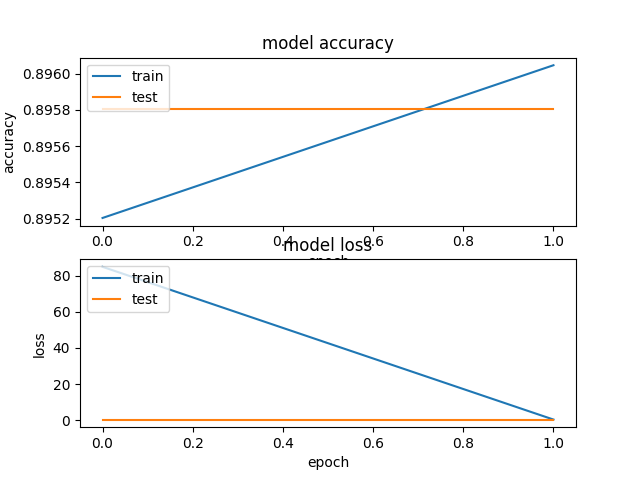


Fig. 12. Fifth Fold

For the fifth fold, our model accuracy on train and validation dataset is 0.8958 & model loss goes from 84 to 1.34 on train and validation dataset.

For our algorithm, average loss is 1.96 and this result shows us the algorithm works well because to do the model's prediction perfect, the loss should be closer to zero, and our solution's loss is considerably close to zero.

# 5 Conclusıon And Future Work

In this paper, we have proposed model using machine learning algorithm for DDos detection. We trained our machine learning model using comprehensive dataset to reduce model loss and increase the precision of the model. The implementation results show that proposed improvements improve the security. This project, being a small-scale model that presents an idea for improved security can be implemented in different IoT devices to detect DDos attacks. Also, future research scope for the project is huge as many attacks can be carried out and tested and the solution can be improved upon for a better and safe IoT system. Future work will focus on how to proactively defend against DDoS attacks.

**References**

1. R. Gurunath, M. Agarwal, A. Nandi and D. Samanta, "An Overview: Security Issue in IoT Network," *2018 2nd International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2018 2nd International Conference on*, Palladam, India, 2018, pp. 104-107, doi: 10.1109/I-SMAC.2018.8653728.
2. Mayuri A Bhabad and Sudhir T Bagade. Article: Internet of Things: Architecture, Security Issues and Countermeasures. *International Journal of Computer Applications* 125(14):1-4, September 2015. Published by Foundation of Computer Science (FCS), NY, USA.
3. Cvitić, I., Peraković, D., Periša, M. *et al.* Novel approach for detection of IoT generated DDoS traffic. *Wireless Netw* (2019). https://doi.org/10.1007/s11276-019-02043-1
4. R. Vishwakarma and A. K. Jain, "A Honeypot with Machine Learning based Detection Framework for defending IoT based Botnet DDoS Attacks," *2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI)*, Tirunelveli, India, 2019, pp. 1019-1024, doi: 10.1109/ICOEI.2019.8862720.
5. R. Doriguzzi-Corin, S. Millar, S. Scott-Hayward, J. Martínez-del-Rincón and D. Siracusa, "Lucid: A Practical, Lightweight Deep Learning Solution for DDoS Attack Detection," in *IEEE Transactions on Network and Service Management*, vol. 17, no. 2, pp. 876-889, June 2020, doi: 10.1109/TNSM.2020.2971776.
6. S. Haider, A. Akhunzada, G. Ahmed and M. Raza, "Deep Learning based Ensemble Convolutional Neural Network Solution for Distributed Denial of Service Detection in SDNs," *2019 UK/ China Emerging Technologies (UCET)*, Glasgow, United Kingdom, 2019, pp. 1-4, doi: 10.1109/UCET.2019.8881856.
7. Sulaiman Alhaidari, Ali Alharbi, & Mohamed Zohdy. (2018). Detecting Distributed Denial of Service Attacks Using Hidden Markov Models. International Journal of Computer Science Issues, 15(5), 9–15. http://doi.org/10.5281/zenodo.1467646.
8. Y. Jia, F. Zhong, A. Alrawais, B. Gong and X. Cheng, "FlowGuard: An Intelligent Edge Defense Mechanism Against IoT DDoS Attacks," in *IEEE Internet of Things Journal*, vol. 7, no. 10, pp. 9552-9562, Oct. 2020, doi: 10.1109/JIOT.2020.2993782.
9. N. Ravi and S. M. Shalinie, "Learning-Driven Detection and Mitigation of DDoS Attack in IoT via SDN-Cloud Architecture," in *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 3559-3570, April 2020, doi: 10.1109/JIOT.2020.2973176.
10. Y. N. Soe, P. I. Santosa and R. Hartanto, "DDoS Attack Detection Based on Simple ANN with SMOTE for IoT Environment," 2019 Fourth International Conference on Informatics and Computing (ICIC), Semarang, Indonesia, 2019, pp. 1-5, doi: 10.1109/ICIC47613.2019.8985853.
11. F. A. Fernandes Silveira, F. Lima-Filho, F. S. Dantas Silva, A. de Medeiros Brito Junior and L. F. Silveira, "Smart Detection-IoT: A DDoS Sensor System for Internet of Things," 2020 International Conference on Systems, Signals and Image Processing (IWSSIP), Niterói, Brazil, 2020, pp. 343-348, doi: 10.1109/IWSSIP48289.2020.9145265.
12. M. H. Aysa, A. A. Ibrahim and A. H. Mohammed, "IoT Ddos Attack Detection Using Machine Learning," *2020 4th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT)*, Istanbul, Turkey, 2020, pp. 1-7, doi: 10.1109/ISMSIT50672.2020.9254703.
13. I. A. Alnuman and M. Al-Akhras, "Machine Learning DDoS Detection for Generated Internet of Things Dataset (IoT Dat)," *2020 2nd International Conference on Computer and Information Sciences (ICCIS)*, Sakaka, Saudi Arabia, 2020, pp. 1-6, doi: 10.1109/ICCIS49240.2020.9257714.
14. Hoyos Ll M.S., Isaza E G.A., Vélez J.I., Castillo O L. (2016) Distributed Denial of Service (DDoS) Attacks Detection Using Machine Learning Prototype. In: Omatu S. et al. (eds) Distributed Computing and Artificial Intelligence, 13th International Conference. Advances in Intelligent Systems and Computing, vol 474. Springer, Cham. https://doi.org/10.1007/978-3-319-40162-1\_4
15. Idhammad, M., Afdel, K. & Belouch, M. Semi-supervised machine learning approach for DDoS detection. *Appl Intell* 48, 3193–3208 (2018). https://doi.org/10.1007/s10489-018-1141-2
16. A. Santoyo-González, C. Cervelló-Pastor and D. P. Pezaros, "High-performance, platform-independent DDoS detection for IoT ecosystems," 2019 IEEE 44th Conference on Local Computer Networks (LCN), Osnabrueck, Germany, 2019, pp. 69-75, doi: 10.1109/LCN44214.2019.8990862.
17. S. M. Sajjad, M. Yousaf, H. Afzal and M. R. Mufti, "eMUD: Enhanced Manufacturer Usage Description for IoT Botnets Prevention on Home WiFi Routers," in IEEE Access, vol. 8, pp. 164200-164213, 2020, doi: 10.1109/ACCESS.2020.3022272.
18. J. Li, M. Liu, Z. Xue, X. Fan and X. He, "RTVD: A Real-Time Volumetric Detection Scheme for DDoS in the Internet of Things," in IEEE Access, vol. 8, pp. 36191-36201, 2020, doi: 10.1109/ACCESS.2020.2974293.
19. D. Yin, L. Zhang and K. Yang, "A DDoS Attack Detection and Mitigation With Software-Defined Internet of Things Framework," in IEEE Access, vol. 6, pp. 24694-24705, 2018, doi: 10.1109/ACCESS.2018.2831284.
20. A. Raghuprasad, S. Padmanabhan, M. Arjun Babu and P. K. Binu, "Security Analysis and Prevention of Attacks on IoT Devices," *2020 International Conference on Communication and Signal Processing (ICCSP)*, Chennai, India, 2020, pp. 0876-0880, doi: 10.1109/ICCSP48568.2020.9182055.
21. D. Erhan and E. Anarim, "Hybrid DDoS Detection Framework Using Matching Pursuit Algorithm," in *IEEE Access*, vol. 8, pp. 118912-118923, 2020, doi: 10.1109/ACCESS.2020.3005781.