MACHINE LEARNING BASED NETWORK ATTACKS DETECTION FOR CONSUMER INTERNET OF THINGS DEVICES

Aditya Gupta, Apoorv Gupta, Archit Jain

Vellore Institute of Technology, Vellore - CSE with Specialization in Internet of Things

***Abstract*—The emergence of the Internet of Things (IoT) As the demand and use of IoT devices is increasing day-by-day, it has made network administration more complex and challenging. Fortunately, Software-Defined Networking (SDN) offers a simple and centralized method to manage numerous Internet of Things (IoT) devices and can significantly lessen the strain of network managers. As the use of IoT is increasing due to their user-friendliness and their effectiveness in our daily lives, it also attracts the attackers/hackers to exploit these for their benefits by getting their personal information, changing the actual data, or doing any kind of activity which the actual user is unaware of and doesn't want. Various types of attacks already prevail such as denial-of-service (DoS) attacks, man-in-the-middle (MitM) attacks, eavesdropping attacks, and malware attacks, ransomware attacks, supply-chain attacks, etc. These attacks are possible due to the various vulnerabilities in IoT devices, including security weaknesses in the communication protocols, lack of strong authentication and encryption, and the use of default or easily guessable passwords, and the ease with which they can be compromised. This highlights the need for improved security measures and the development of secure IoT devices that can protect against these types of attacks.**

I. Introduction

The last decade has seen an exponential growth in the number of IoT based devices and as WSN based networks have become cheap and are the norm now.[6] The number of Internet of Things (IoT) devices is projected to grow from 8 billion in 2017 to 20 billion in 2020.[1] Yet, many of these IoT devices are fundamentally insecure. One analysis of 10 currently popular IoT devices found 250 vulnerabilities, including open telnet ports, outdated Linux firmware, and unencrypted transmission of sensitive data [2], [3]. This has raised a major issue in the security domain of this sector and some of the major issues faced is Distributed Denial of Service which is performed by IoT based Botnets, phishing attacks performed by social engineers and man in the middle attacks performed by various eavesdroppers.

One of the major security concerns posed in this field is of Distributed Denial of Service or DDoS for short, refers to jamming of the services from a device due to flooding or crowding of unwanted or unnecessary requests from various services[3].These types of attacks have paralyzed many famous websites such as Twitter, Netflix, Github, and Amazon for several hours.One of the infamous software which is used in these types of attacks is "Mirai". Mirai is a malware which turns linux based devices into remotely controlled bots which are used in DDoS attacks. The mirai botnets had surfaced in august 2016 and has only seen increase in its popularity ever since.This has called for an immediate development in the field of security for IoT based networks[2].

Phishing attacks are performed by sending forged emails that look legitimate coming from a genuine entity to a victim or a group of victims [20] [23]. Their aim is to obtain users' confidential data or uploading some malicious software onto their systems. For example, the attackers can send an email with a redirection link to a malicious website where the user is prompted to provide some sensitive data, which may include bank account number or login and password or some other personal information that could be used for password guessing. The attacker can also attach a file to the fake email to be uploaded by the victim, which can automatically trigger the execution of embedded malware.

A Man In The Middle attack is a computer-based attack in which an outsider imposes as one or the other party in a two-manner contact situation, thereby successfully making a fool of the user and making them believe that they are conversing with the other. In such scenarios, the attacker can tune in to the correspondences between the two clueless gatherings to collect their data. These attacks can take place in both wired and remote organizations, with the last being more powerless. The identification of MITM attacks on Wi-Fi networks is

one of the bigger problems. Prevention and identification of these types of attacks is a very challenging area of research due to the importance of data traveling over the network, especially in cases similar to autonomous driving applications.[13][14][17]

There are a number of safety measures of IoT devices but their deployment depends upon the size and type of organisation in which it is imposed. The behaviour of users forces the security gateways to cooperate. In other words, we can say that the location, nature, application of IoT devices decides the security measures [18]. For instance, the smart IoT security cameras in the smart organisation can capture the different parameters for analysis and intelligent decision making.

There are several types of safety modules such as packet capture, firewall, IDS/IPS and Honeypot. However, those modules need periodic maintenance involving technical knowledge and cannot detect unknown attacks . Moreover, a detection module becomes a bottleneck and it may cause a system failure when the network is overloaded by attacks[12].

In this paper we will be presenting an efficient way to detect multiple network attacks at the same time. Most of the papers that we researched provide a very efficient method of detecting a particular type of attack but they won't be as effective if some other kind of attack is done on the network or a mutated form of the same attack is presented. Through this paper we will be contributing towards the creation of an integrated attack detecting system that can alert the users in case of common network attacks and can also adapt to new forms of attacks once faced with it. We will be creating the most accurate and precise ML/DL models to detect common network attacks so that the IDS/IPS won't be restricted to just detection of particular attacks based on the models integrated with them.

II. Literature Survey

Doshi, Rohan, Noah Apthorpe, and Nick Feamster proposed a systematic approach to detect the DDoS attack on the network by taking the help of machine learning algorithms. The model will be made to monitor the ingoing and outgoing traffic through each node and the algorithms will be used to classify the networking traffic as "normal" or an "anomaly" (in case of an attack). This paper uses the idea of monitoring the traffic which is ingoing and outgoing through a node with the help of "Middle boxes" (e.g. routers, firewalls, or network switches). This is because all the data packets which enter and leave a node pass through these devices and hence the monitoring of the data will be easier. The paper highlights two major points in solving this problem (A) Network Anomaly Detection

Anomaly detection: This means to identify the patterns in the traffic of the IoT network and checking if it matches with the available data on the normal network traffic pattern. The authors of the paper make their own small IoT set up consisting of a router, some popular consumer IoT devices for benign traffic, and some adversarial devices performing DoS attacks. The Machine Learning algorithms used in this paper are random forest, K-nearest neighbours and neural net classifiers. Using this algorithm on the self generated data, the authors claim to have an accuracy of the model, more than 0.999.

The second major point discussed in the paper is (B)Network Middlebox Limitations: Since the model uses middle boxes to monitor the data, the authors paid significant attention to them. The middle boxes are "Gate" devices such as firewalls or routers from which all the data has to pass. Due to this reason they play a role of monitoring the data entering and leaving the node. This, though, has certain limitations. These devices have limited processing power and a lower memory thereby imposing limitations on the Machine learning algorithms meaning that the algorithms used should be light weight and should consume a low memory for being implemented.

Muhammad Aslam et al. proposed Adaptive Machine Learning based SDN-enabled Distributed Denial-of-Services attacks Detection and Mitigation (AMLSDM) framework. The proposed AMLSDM framework develops an SDN-enabled security mechanism for IoT devices with the support of an adaptive machine learning classification model to achieve the successful detection and mitigation of DDoS attacks.

The proposed AMLSDM framework is based on an adaptive machine learning classification model to detect DDoS attacks for network traffic of SDN-enabled IoT. The AMLSDM framework also provides a DDoS mitigation system to switch network resources to normal network traffic. The multilayered feed-forwarding design of the AMLSDM framework utilizes SVM, NB, kNN, LR, and FR classifiers in the first layer. The output of the first layer is provided as input to the second layer EV, which accumulates the performance of first layer classifiers to detect the DDoS attacks. The trained adaptive machine learning model predicts the DDoS attacks for real-time network traffic at the third layer. We implement our proposed framework in four phases;
(i) training the adaptive classification model,
(ii) feature extraction of SDN-enabled IoT network traffic phase,
(iii) classification of real-time network traffic for DDoS

detection phase, and
(iv) DDoS mitigation phase. In every phase, we execute the adaptive classification module, feature extraction module, DDoS inspection module, and DDoS mitigation module. Our extensive simulation results validate the intelligent DDoS detection and mitigation of the AMLSDM framework to classify the real-time network traffic generated by two SDN-enabled IoT networks. Performance metrics of Accuracy, Precision, Recall, and F1 Score validate the better classification of adaptive setting AMLSDM-EV as compared to static AMLSDMSVM, AMLSDM-NB, AMLSDM-kNN, AMLSDM-LR, and AMLSDM-RF classification configurations. We also perform the simulation comparison with state-of-the-art LEDEM and CONA frameworks to validate the better performance of the AMLSDM framework. In the future, mitigation of DDoS attacks at SDN controller will be explored more deeply, as it is one of the key research area to further improve the utilization of SDN controllers in IoT networks. We will also extend the implementation of our proposed framework to detect phishing attacks.

Brij B. Gupta et al. acknowledged the tremendous growth in the field of IoT in the recent years. Due to this exponential growth, the paper shows the challenges which it has imposed on us with security being one of the major concerns. This is so because IoT devices use the Internet for inter-communication which attracts privacy and security issues. One of the major attacks which is performed by the hackers is DDoS (Distributed denial of Service). This means to flood the server with unwanted or useless traffic so that the useful request are not able to go through thereby paralyzing the system. One of the major DDoS attack using IoT devices triggered in October 2016. It is performed with the formation of the largest botnet army which is named as Mirai on the famous Security blogger Brian Krebs' website, krebsonsecurity.com.The aim of this paper is to contribute in the direction of DDoS attack traffic detection in local network and recognition of suspicious IoT device within that local network itself with the help of machine learning algorithms.The paper proposes a straight forward two step approach to this problem:
a) Detection
b) Mitigation
Detection phase: This phase monitors the networking traffic and checks if it contains the DDoS traffic in it. This step consists of traffic capture, Attribute extractor and classifier.
Traffic capture: in this part the benign packets are first captured and then the DDoS packets are captured and the information about these packets is gathered
Attribute extractor: This module deals with the separation of important attributes from the others which are required in the DDoS detection. Here two datasets are maintained. One for benign traffic and the other for DDoS traffic.
Classifier: Here the ML model is trained with the help of the datasets gained in the earlier step and this ML model will then work in real time to detect the DDoS traffic.

Mitigation phase: The ML model sends report to the network admin. The network admin checks for any anomaly or the malicious activity. If it is found that an attack is happening on the network from a node, the activity from the node is shut down and hence the network is protected from those types of attacks. The papers uses 4 different ML algorithms namely, SVM, Random forest, Logistic regression and Decision tree out of which the output was most prominent in Random forest with 99.17

Al Mtawa et al. proposed in this paper the depth insights on IoT based networks, the security threads possessed by them and ways in which these attacks can be detected and mitigated. The paper provides a short survey on protocols, investigates the IoT architecture and devices in-order to provide a better understanding on how to make the IoT based networks more secure. The paper also uses Machine Learning models in order to detect the attacks on the network and also to help mitigate the same (Mostly in the view of MIRAI botnet attacks). The paper states that the protocols used in the OS of pc's is ineffective when it comes to the case of ioT enabled devices. There were thousands of vulnerabilities which were found in the day to day used devices like backyard security camera which can be attacked. Hence the paper proposes safe protocols like: 6LoWPAN,RFID,Z-wave and Wifi.
ML-Based IoT Detection: This paper aims at utilising the special characteristics of IoT based networks like limited number of devices, patterned intervals of packet transportation and so on. To build the Machine learning model the following was done by the authors:
1) Building a network: the network which they built consisted of three hosts. With v switch as the middle box.
2) Traffic collection: The benign traffic is first sent through the host 3 by host1. This traffic is recorded and stored and then the DDoS attack is done by the host 2 on the host1. This data is too stored.
3) Feature Selection: The important features are then selected out of all the features which are required for accurate classification of network traffic as benign or as DDoS attack

Alex Medeiros et al. introduced the field IoT and one of the most promising fields in today's world where everything is connected to everything. It also sheds light on the security issues it possesses because of its increasing popularity. The threads and vulnerabilities are a little different when compared to the normal software as the IoT enabled devices are constantly connected to internet which makes the more prone to network attacks with botnets being a major issue and one of the major attacks which botnets perform is the Distributed denial of service attack (DDoS for short). The papers main aim is to detect the bots in order to prevent not the DDoS attack but also other cyber-attacks like capturing of sensitive information, spamming etc. The paper describes the details of an ANTicipating Botnet detection (ANTE) which maps the behavior of botnets with the ML to create models that anticipate the Botnet signals.This is a self adjusting algorithm which adjusts to changes in its environment. The proposed ML pipeline in this paper consists of 3 parts namely data collection and processing, feature processing and estimator. There are many ML algorithms to counter Botnets but not all Algorithms work well against all botnets. Hence ANTE framework decides which type of algorithm should be applied by checking which type of Botnet is causing the attack. This ANTE system is divided into 4 datasets

1) Information Security and Object Technology HTTP
2) Scenario 10
3) DDoS evaluation dataset
4) BoT-IoT dataset.

Since our discussion is mainly focused on DDoS detection and mitigation we will be focusing more on the 3rd data set that is the DDoS evaluation This ANTE system follows 5 steps:

1) Capture of network traffic
2) Extraction of host behavior
3) Identification of Best model
4) Anticipation of bots
5) Administrator notification

The monitoring of the network traffic is done with the help of the router and the router then sends the data to the network administrator. This collected input is then analyzed on the basis of source IP and MAC address, Destination IP and MAC address Port and so on. These data is then used for identifying the best model suited for the case. Depending on the decision feature extraction is done. And the relevant ML is applied. Once this is done, the ML searches for any anomalies in the network and if it find tone the algorithm then informs the administrator about it with the occurrence data and the probability of the device being a bot.

TABLE I
COMPARISON OF TECHNIQUES/ALGORITHMS FOR TRAFFIC MONITORING

S. No.	Author Name & Year	Actual Technique/Algorithm used	Limitations
1	Doshi et al. 2018	Traffic monitoring through edge devices, ML algorithms: K nodes, Random forest, LSVM	• Not suitable for real-time scenarios • Performance uncertainty for larger dataset • Prevention methods not discussed
2	Muhammad Aslam et al. 2022	A three layered approach: • First layer has ML algorithms like SVM, NV, KNN, LR and FR • Layer2: Ensemble voting • Layer3: Detection layer	• Implementation restricted to DDoS attacks • Further mitigation of DDoS attacks on SDN controllers can be done • Not enough testing on real-time data
3	Brij B. Gupta et al. 2019	Logistic regression, decision tree, RF	• Low accuracy • More advanced algorithms like CNN were not tested • Other metrics like precision and F1 score are not mentioned
4	Pooja Chaudhary et al. 2022	Gateway components like routers are used to monitor the traffic, Algorithms used: SVM, RF, LR, KNN, NB	• Simulation-based dataset not tested on real-time • Only use of supervised learning hence lacking adaptability • Mitigation is achieved by performing changes in pre-existing rules

III. Proposed Methodology

We will demonstrate that using IoT-specific network behaviors (e.g., limited number of endpoints and regular time intervals between packets) to inform feature selection can result in high accuracy DDoS detection in IoT network traffic with CNN algorithms. These results indicate that home gateway routers or other network middleboxes could automatically detect local IoT device sources of DDoS attacks using low-cost machine learning algorithms and traffic data that is flow-based and protocol-agnostic. Furthermore we will implement an alert system through email and sms which can inform a particular entity in-charge of the ecosystem about the happening of an attack.

A. Algorithms used

The implementation of the proposed system is divided into three major parts:

1.Data Preprocessing and Feature Selection: In this part, the data is first cleaned by removing the infinity values and the NA values. The data is then scaled using the min max algorithm which changes the value such that it ranges from 0 to 1 with zero being the minimum value and one being the maximum. In order to do feature selection, we use the chi square. We calculate it for all the available features and rank them in descending order and then remove the features which have a score lower than 0.2 as they do not effect the model much and would make the model be more overfitting and finally feature scaling is done.

2.Model building: The data which is obtained after feature scaling and data preprocessing, is then split into training and test data, with the ratio of 8:2. After splitting the data into training and test, we then make the ANN model. The model made by us consists of three layers. The first layer and the second layer use the "relu" curve as its activation function and since the final classification is either of "Binine" or "DDoS Attack" that is binary classification, the final activation function used in "Sigmoidal".

3.Prediction and application: The model which we made has an accuray of approximately 0.99 in training. This was then tested with the help of our test dataset, for which too the accuracy came out to be around 0.99. After detecting that the traffic flowing through the network is potentially a DDoS attack, we then send an alert message to the user in order to notify them about the potential attack. This is done through snitch API which provides autonomous messaging services like SMS, Email and Whatsapp messages. For our project we used the SMS service as it operates even in the absence of internet connectivity. One of the future which we would like to implement if we ran this in a real time IoT network is that when we would deploy this algorithm in the router (gateway, making the traffic monitoring easier), the flow of traffic from the particular IP address should directly be filtered in real time if an attack is detected by it.

B. Our Model

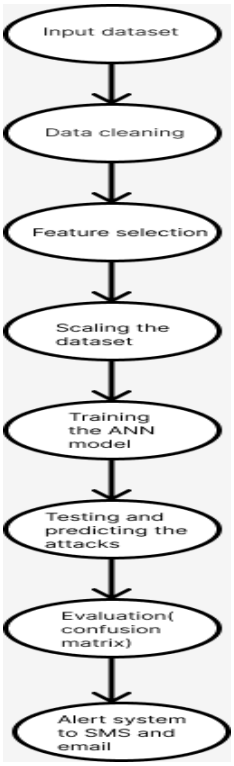

Fig. 1. Flow Diagram

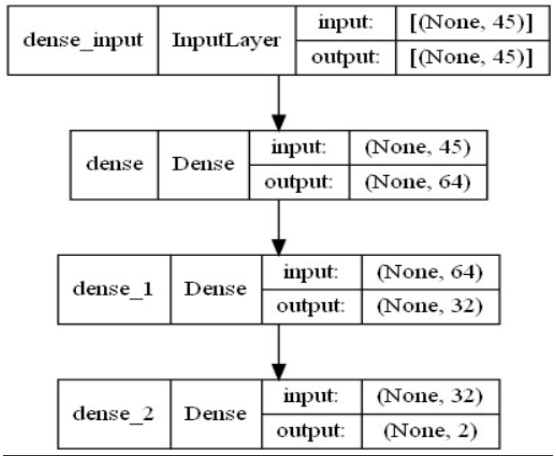

Fig. 2. Model Diagram

C. Simulation

To simulate the attack, we utilized a virtual machine running Kali Linux within VirtualBox on a separate host PC, which was isolated from the victim's PC via a router. The Kali Linux PC was configured with 4GB of hard disk, 45GB of memory, and 3 CPU cores, while the victim's PC had 8GB of RAM, 1TB of memory, and an i5 processor running Windows 11. We used the hping3 command in Kali Linux to perform various attacks, including DDoS, ICMP, and port scanning, and observed the effects on the victim's PC. We then used a deployed machine learning model that captured packets using PyShark and fed them to an artificial neural network (ANN) model to accurately detect the attack. When an attack was detected, we alerted the user via SMS and email.

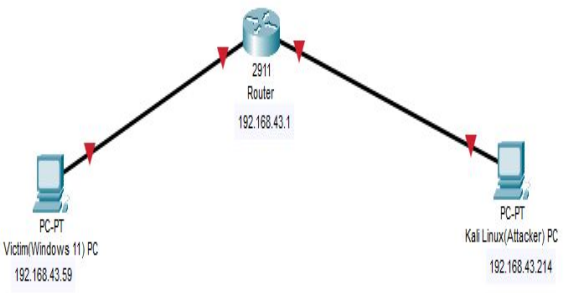

Fig. 3. Network topology

Fig. 4. Sending packets

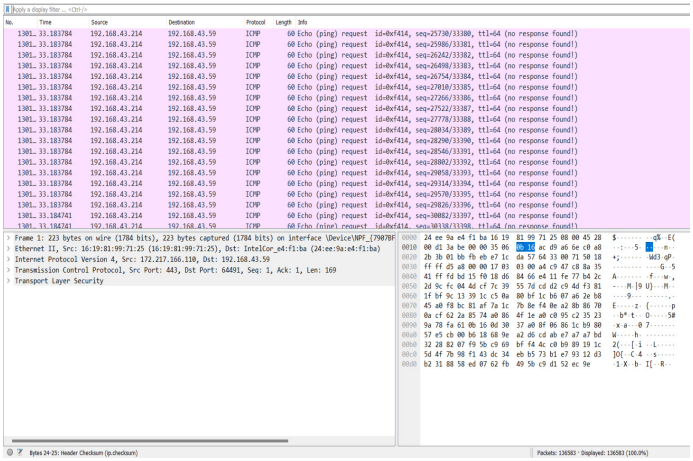

Fig. 5. Wireshark capturing the packets

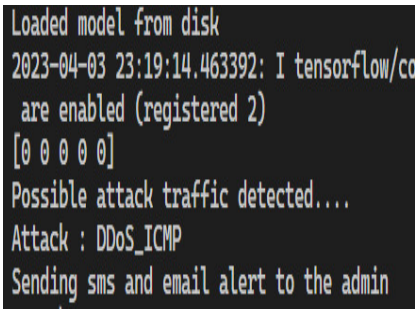

Fig. 6. Attack detected

IV. Research and Analysis

The correctness and accuracy of our model depends upon the corrleation between actual truth and the predicted value which can be shown as:

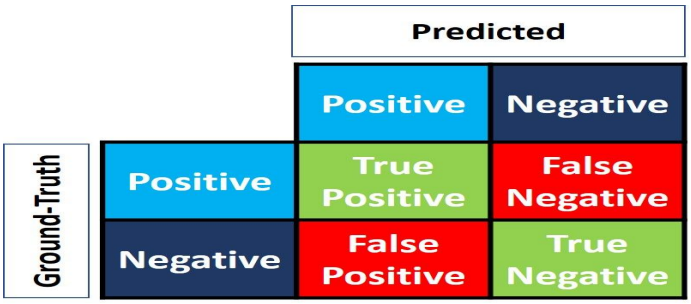

Fig. 7. Confusion Matrix for binary Classification

A. Equations

For data processing, we used min max scaling and for feature selection we used chi square score This examines the differences between categorical variables

from a random sample in order to determine whether the expected and observed results are well-fitting.

$$\chi^2 = \sum \frac{(O-E)^2}{E}$$

The following metrics define the behaviour of our model:

$\text{accuracy} = \frac{TP+TN}{TP+TN+FP+FN}$

$\text{precision} = \frac{\text{TP}}{\text{TP+FP}}$

$\text{recall} = \frac{\text{TP}}{\text{TP+FN}}$

O Observed Value
E Expected Value
TP True Positives
TN True Negatives
FP False Positives
FN False Negatives

B. Results

```
[36] from sklearn.metrics import accuracy_score
     accuracy_score(y_test, y_pred)

··· 0.9772252610641472
```

Fig. 8. Accuracy

Model	Accuracy
Decision Tree	92.17%
Random Forest	86.12%
KNeighbors Classifier	96.4%
ANN	97.7%

TABLE II
COMPARISON OF ACCURACIES

For finding the correct number of epochs, we used TensorBoard, a tool for providing the measurements and visualizations needed for the ML workflow.

```
In [52]: from sklearn.metrics import confusion_matrix
         cm= confusion_matrix(y_test, y_pred)
         print(cm)

[[1823    0    0    0    0   37  113    0    0    0]
 [   0 2618    1    0    0    0    0    0    0    0]
 [   0    0 2900    0    0    0    0    0    0    0]
 [   0    0    0   72    0    0    0    0    0    0]
 [   0    0    0    0 4820    0    0    0    0    0]
 [   0    0    1    0    0 1783    0    0    0    0]
 [   1    0    1    0    0   50 1886    0    0    0]
 [   0    0    0    0    0    0    0 2056    0    0]
 [   0    0    0    0    0    0    0    0 1635  377]
 [   0    0    0    0    0    0    0    0  102 1807]]
```

Fig. 9. Confusion Matrix

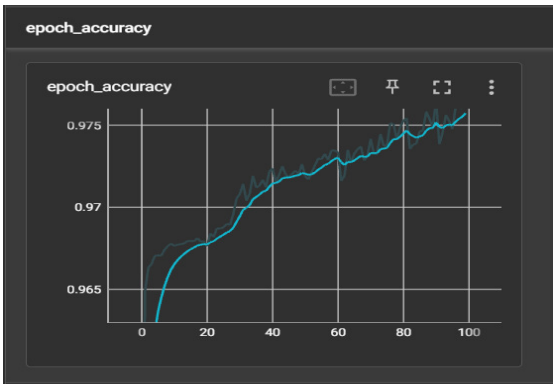

Fig. 10. epoch accuracy

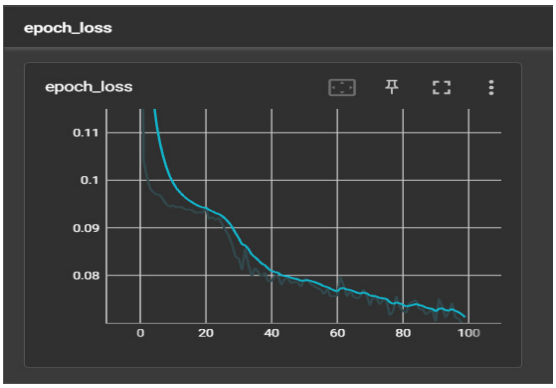

Fig. 11. epoch loss

We have also implemented an email and SMS service which will notify us during the time of attack.

Fig. 12. Email alert

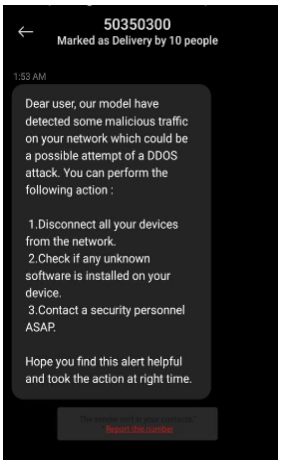

Fig. 13. SMS alert

REFERENCES

[1] Doshi, Rohan, Noah Apthorpe, and Nick Feamster. "Machine learning ddos detection for consumer internet of things devices." In 2018 IEEE Security and Privacy Workshops (SPW), pp. 29-35. IEEE, 2018.

[2] Aslam, Muhammad, Dengpan Ye, Aqil Tariq, Muhammad Asad, Muhammad Hanif, David Ndzi, Samia Allaoua Chelloug, Mohamed Abd Elaziz, Mohammed AA Al-Qaness, and Syeda Fizzah Jilani. "Adaptive Machine Learning Based Distributed Denial-of-Services Attacks Detection and Mitigation System for SDN-Enabled IoT." Sensors 22, no. 7 (2022): 2697

[3] Chaudhary, Pooja, and Brij B. Gupta. "Ddos detection framework in resource constrained internet of things domain." In 2019 IEEE 8th Global Conference on Consumer Electronics (GCCE), pp. 675-678. IEEE, 2019.

[4] Gupta, B. B., Pooja Chaudhary, Xiaojun Chang, and Nadia Nedjah. "Smart defense against distributed Denial of service attack in IoT networks using supervised learning classifiers." Computers & Electrical Engineering 98 (2022): 107726.

[5] Al Mtawa, Yaser, Harsimranjit Singh, Anwar Haque, and Ahmed Refaey. "Smart Home Networks: Security Perspective and ML-based DDoS Detection." In 2020 IEEE Canadian Conference on Electrical and Computer Engineering (CCECE), pp. 1-8. IEEE, 2020.

[6] McDermott, Christopher D., Farzan Majdani, and Andrei V. Petrovski. "Botnet detection in the internet of things using deep learning approaches." In 2018 international joint conference on neural networks (IJCNN), pp. 1-8. IEEE, 2018.

[7] Zakariyya, Idris, M. Omar Al-Kadri, and Harsha Kalutarage. "Resource Efficient Boosting Method for IoT Security Monitoring." In 2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC), pp. 1-6. IEEE, 2021.

[8] Vuppalapati, Jaya Shankar, Santosh Kedari, Anitha Ilapakurti, Chandrasekar Vuppalapati, Chitanshu Chauhan, Vanaja Mamidi, and Surbhi Rautji. "Cognitive secure shield-a machine learning enabled threat shield for resource constrained IoT devices." In 2018 17th IEEE International Conference on Machine Learning and Applications (ICMLA), pp. 1073-1080. IEEE, 2018.6

[9] Araujo, Alex Medeiros, Anderson Bergamini de Neira, and Michele Nogueira. "Autonomous machine learning for early bot detection in the internet of things." Digital Communications and Networks (2022).

[10] Silveira, Frederico Augusto Fernandes, Francisco Lima-Filho, Felipe Sampaio Dantas Silva, Agostinho de Medeiros Brito Junior, and Luiz Felipe Silveira. "Smart detection-IoT: A DDoS sensor system for Internet of Things." In 2020 International Conference on Systems, Signals and Image Processing (IWSSIP), pp. 343-348. IEEE, 2020.

[11] Kawamura, Tamotsu, Masaru Fukushi, Yasushi Hirano, Yusuke Fujita, and Yoshihiko Hamamoto. "An NTP-based detection module for DDoS attacks on IoT." In 2017 IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW), pp. 15-16. IEEE, 2017.

[12] Costa, Wanderson L., Matheus M. Silveira, Thelmo de Araujo, and Rafael L. Gomes. "Improving ddos detection in iot networks through analysis of network traffic characteristics." In 2020 IEEE Latin-American Conference on Communications (LATINCOM), pp. 1-6. IEEE, 2020.

[13] M. Saed and A. Aljuhani, "Detection of Man in The Middle Attack using Machine learning," 2022 2nd International Conference on Computing and Information Technology (ICCIT), Tabuk, Saudi Arabia, 2022, pp. 388-393, doi: 10.1109/ICCIT52419.2022.9711555.

[14] S. Malik and R. Chauhan, "Securing the Internet of Things using Machine Learning: A Review," 2020 International Conference on Convergence to Digital World - Quo Vadis (ICCDW), Mumbai, India, 2020, pp. 1-4, doi: 10.1109/ICCDW45521.2020.9318666.

[15] D. Wang, C. Li, S. Wen, S. Nepal and Y. Xiang, "Man-in-the-Middle Attacks Against Machine Learning Classifiers Via Malicious Generative Models," in IEEE Transactions on Dependable and Secure Computing, vol. 18, no. 5, pp. 2074-2087, 1 Sept.-Oct. 2021, doi: 10.1109/TDSC.2020.3021008.

[16] O. Toutsop, P. Harvey and K. Kornegay, "Monitoring and Detection Time Optimization of Man in the Middle Attacks using Machine Learning," 2020 IEEE Applied Imagery Pattern Recognition Workshop (AIPR), Washington DC, DC, USA, 2020, pp. 1-7, doi: 10.1109/AIPR50011.2020.9425304.

[17] A. Al-Hababi and S. C. Tokgoz, "Man-in-the-Middle Attacks to Detect and Identify Services in Encrypted Network Flows using Machine Learning," 2020 3rd International Conference on Advanced Communication Technologies and Networking (CommNet), Marrakech, Morocco, 2020, pp. 1-5, doi: 10.1109/CommNet49926.2020.9199617.

[18] M. Usmani, M. Anwar, K. Farooq, G. Ahmed and S. Siddiqui, "Predicting ARP spoofing with Machine Learning," 2022 International Conference on Emerging Trends in Smart Technologies (ICETST), Karachi, Pakistan, 2022, pp. 1-6, doi: 10.1109/ICETST55735.2022.9922925.

[19] Abbas, Syed Ghazanfar, et al. "Identifying and mitigating phishing attack threats in IoT use cases using a threat modelling approach." Sensors 21.14 (2021): 4816.

[20] T. A and A. John, "Phishing Website Detection Using LGBM Classifier With URL-Based Lexical Features," 2022 IEEE Silchar Subsection Conference (SILCON), Silchar, India, 2022, pp. 1-7, doi: 10.1109/SILCON55242.2022.10028793.

[21] T. A and A. John, "Phishing Website Detection Using LGBM Classifier With URL-Based Lexical Features," 2022 IEEE Silchar Subsection Conference (SILCON), Silchar, India, 2022, pp. 1-7, doi: 10.1109/SILCON55242.2022.10028793.

[22] Fetooh, Haytham Tarek Mohammed, M. M. El-Gayar, and A. Aboelfetouh. "Detection Technique and Mitigation Against a Phishing Attack." International Journal of Advanced Computer Science and Applications 12.9 (2021).

[23] Salloum, Said, et al. "A systematic literature review on phishing email detection using natural language processing techniques." IEEE Access (2022).

[24] Abbas, Syed Ghazanfar, et al. "Identifying and mitigating phishing attack threats in IoT use cases using a threat modelling approach." Sensors 21.14 (2021): 4816.

[25] Gopal, S. B., et al. “Autoencoder based Architecture for Mitigating Phishing URL attack in the Internet of Things (IoT) using Deep Neural Networks.” 2022 6th International Conference on Devices, Circuits and Systems (ICDCS). IEEE, 2022.