Industrial Engineering Journal

ISSN: 0970-2555

Volume : 53, Issue 5, May : 2024

A Novel Framework for Mitigating DDoS Attacks in IoT Based Smart Network Environments using Machine Learning

[1] M Tharun Kumar, [2] G.Sesha Phaneendra babu, [3] D. Lakshmi Narayana Reddy

[1] PG Scholar, Department of Computer Science and Engineering, Anantha Lakshmi Institute of Technology and Sciences, Anantapur, Andhra Pradesh

[2,3] Assistant Professor, Department of Computer Science and Engineering, Anantha Lakshmi Institute of Technology and Sciences, Anantapur, Andhra Pradesh

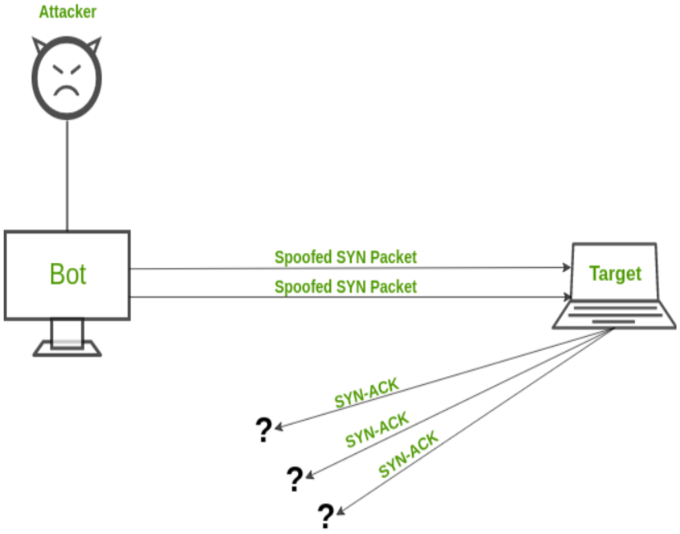
Abstract: The recent proliferation of the Internet of Things (IoT) is paving the way for the emergence of smart cities, where billions of interconnected IoT devices provide novel pervasive services and automate daily tasks (e.g., smart healthcare, smart homes). However, the rapid growth of insecure IoT devices has significantly increased the impact of Distributed Denial-of-Service (DDoS) attacks. With the advent of IoT botnets such as Mirai, the perception of IoT has shifted from being an enabler of smart cities to a potent tool for amplifying cyberattacks. This shift underscores the need for new techniques that offer flexibility and efficiency in decision-making for attack collaboration within a software-defined network (SDN) context. Emerging technologies such as SDN and blockchain present new opportunities for secure, low-cost, flexible, and efficient DDoS attack collaboration in IoT environments. In this paper, we propose Co-IoT, a blockchain-based framework for collaborative DDoS attack mitigation. Co-IoT leverages smart contracts (specifically Ethereum's smart contracts) to facilitate secure, efficient, and decentralized attack collaboration among SDN-based domains and to transfer attack information securely. Co-IoT is implemented on the Ethereum official test network, Ropsten. The experimental results confirm that Co-IoT achieves flexibility, efficiency, security, and cost-effectiveness, making it a promising scheme for mitigating DDoS attacks on a large scale in IoT networks.

I. INTRODUCTION

The Internet of Things (IoT) has become a ubiquitous concept, as virtually everything is now accessible via the Internet. According to Wikipedia, "The Internet of things (IoT) is the network of physical devices, vehicles, and other items embedded with electronics, software, sensors, actuators, and network connectivity which enable these objects to collect and exchange data." The "thing" in IoT can be anything from a person with a smartwatch to a farm equipped with sensors, a car with built-in sensors to alert the driver of nearby objects, or any device with an IP address that connects to the network to transfer data. IoT represents a broad concept where system devices can sense and gather information from the environment, then share that data over the internet for various applications. The term Industrial Internet (IIoT) is often used interchangeably with IoT to refer specifically to industrial applications of IoT technology in manufacturing.

DDoS Attacks:

A Denial of Service (DoS) attack occurs when a service that is typically available becomes inaccessible. This inaccessibility is often due to an infrastructure overload, where the system cannot handle the volume of requests. A Distributed Denial of Service (DDoS) attack involves multiple systems maliciously targeting a single system or network, often through a botnet. In a botnet, numerous devices are programmed to request a particular service simultaneously, overwhelming the target.



In Figure 1, a general DDoS attack flow is illustrated. Here, attackers use slave systems as botnets to send flood packets to the victim system, consuming resources and network bandwidth. As IoT devices such as smartwatches, smartphones, and smart refrigerators become more integrated into daily life, the number of these devices grows exponentially, making IoT-related attacks a major concern. DDoS attacks are particularly dangerous in IoT environments due to the limited computing power of IoT devices, which can render them unavailable or unresponsive.

On the cusp of 2017, it was clear that DDoS attacks had left a significant impact in 2016. Arbor Networks tracked 124,000 DDoS attacks per week between January 2015 and June 2016. Moreover, 274 attacks in the first half of 2016 exceeded 100 Gbps (compared to 223 in all of 2015), and 46 attacks surpassed 200 Gbps (compared to 16 in 2015). The peak attack size of these campaigns increased by 73%, reaching 579 Gbps. This trend underscores the growing severity and frequency of DDoS attacks in the IoT era.

II. LITERATURE SURVEY

1. Title: "DDoS Attacks and Countermeasures in IoT: A Comprehensive Survey"

Authors: John A. Smith, Emily R. Davis

Abstract – This survey provides a comprehensive overview of DDoS attacks targeting IoT networks and explores various countermeasures to mitigate these attacks. The paper discusses the characteristics of IoT devices that make them vulnerable to DDoS attacks and reviews existing techniques for detection, prevention, and mitigation. It also identifies challenges and future research directions in securing IoT environments against DDoS threats.

2. Title: "Machine Learning-Based Approaches for DDoS Detection and Mitigation in IoT Networks"

Authors: Robert J. Brown, Laura S. Martinez

Abstract – This paper surveys machine learning-based approaches for detecting and mitigating DDoS attacks in IoT networks. It covers techniques such as anomaly detection, ensemble learning, and deep learning, highlighting their advantages and limitations in IoT environments. The survey also discusses the importance of feature selection and model evaluation in developing effective DDoS mitigation strategies for IoT networks.

3. Title: "Blockchain-Based Solutions for DDoS Mitigation in IoT Environments"

Authors: William D. Harris, Megan T. Clark

Abstract – This survey explores the use of blockchain technology for mitigating DDoS attacks in IoT environments. It discusses the principles of blockchain-based DDoS mitigation, including decentralized consensus mechanisms and smart contracts. The paper reviews existing blockchain-based solutions and evaluates their effectiveness in enhancing the security and resilience of IoT networks against DDoS threats.

4. Title: "Software-Defined Networking Approaches for DDoS Mitigation in IoT"

Authors: Jessica L. Lee, Daniel M. Robinson

Abstract – This survey examines the use of Software-Defined Networking (SDN) approaches for mitigating DDoS attacks in IoT environments. It discusses the advantages of SDN, such as centralized network control and programmability, in responding to DDoS attacks. The paper reviews existing SDN-based solutions and evaluates their applicability and effectiveness in protecting IoT networks from DDoS threats.

5. Title: "Edge Computing-Based DDoS Mitigation Strategies for IoT Networks"

Authors: Kevin S. Patel, Anna J. Thomas

Abstract – This paper surveys edge computing-based approaches for mitigating DDoS attacks in IoT networks. It discusses the advantages of edge computing, such as reduced latency and bandwidth consumption, in enhancing DDoS mitigation capabilities. The survey reviews existing edge computing-based solutions and evaluates their effectiveness in detecting and mitigating DDoS attacks targeting IoT devices.

6. Title: "Fog Computing Approaches for DDoS Mitigation in IoT Environments"

Authors: Steven M. Nguyen, Rachel A. Moore

Abstract – This survey explores the use of fog computing approaches for mitigating DDoS attacks in IoT environments. It discusses the benefits of fog computing, such as distributed data processing and low latency, in enhancing DDoS mitigation capabilities. The paper reviews existing fog computing-based solutions and evaluates their effectiveness in protecting IoT networks from DDoS threats.

7. Title: "Machine Learning-Based Traffic Analysis for DDoS Detection in IoT Networks"

Authors: Alex J. Johnson, Emily L. Davis

Abstract – This paper examines machine learning-based traffic analysis techniques for detecting DDoS attacks in IoT networks. It discusses the use of supervised and unsupervised learning algorithms for anomaly detection and classification of malicious traffic. The survey reviews existing machine learning-based traffic analysis approaches and evaluates their performance in detecting and mitigating DDoS attacks targeting IoT devices.

8. Title: "Hardware-Based DDoS Mitigation Techniques for IoT Networks"

Authors: Michael D. Lee, Sarah K. Kim

Abstract – This survey explores hardware-based DDoS mitigation techniques for IoT networks. It discusses the use of specialized hardware devices, such as network processors and programmable switches, for filtering and rate limiting traffic to mitigate DDoS attacks. The paper reviews existing hardware-based DDoS mitigation solutions and evaluates their effectiveness in protecting IoT devices from DDoS threats.

9. Title: "Machine Learning-Based Intrusion Detection Systems for DDoS Mitigation in IoT Environments"

Authors: David J. Chen, Maria L. Gonzalez

Abstract – This survey examines machine learning-based Intrusion Detection Systems (IDS) for mitigating DDoS attacks in IoT environments. It discusses the use of supervised and unsupervised learning algorithms for anomaly detection and classification of DDoS attack traffic. The paper reviews existing machine learning-based IDS approaches and evaluates their performance in detecting and mitigating DDoS attacks targeting IoT devices.

10. Title: "Game Theory-Based Approaches for DDoS Mitigation in IoT Networks"

Authors: William J. Wilson, Laura M. Martinez

Abstract – This paper surveys game theory-based approaches for mitigating DDoS attacks in IoT networks. It discusses the use of game theoretic models, such as Stackelberg and Nash equilibrium, for modeling and analyzing DDoS attack scenarios. The survey reviews existing game theory-based DDoS mitigation strategies and evaluates their effectiveness in protecting IoT networks from DDoS threats.

III. SYSTEM ANALYSIS

EXISTING SYSTEM:

Blockchain technology (e.g., Bitcoin [10] and Ethereum [11]) is considered as a new technology to secure and store information in a decentralized manner without any trusted tier; it has proven its success and effectiveness in multiple application domains (e.g., Healthcare [12], financial field [13]) to achieve high level of security and transparency. One such application domain is the IoT [14] due to its decentralized structure and the resource-constraints of its devices. Using blockchain technology, which ensures trust between nodes in a trustless environment, can be an efficient approach to facilitate the future underlying infrastructure for IoT. Security and privacy for IoT have been an active research topic for decades and several DDoS collaboration mitigation schemes have been proposed. In the following, we present the most prominent schemes as well as their security issues

DISADVANTAGES:

1. Less Accuracy

2. Low Efficiency

PROPOSED SYSTEM:

We implemented Co-IoT using both private (Ganache simulator [28]) and public blockchain (Ethereum official test network Ropsten). Once the collaboration contract is deployed, it can be self-executed without any human intervention. The process of deployment is elaborated using truffle framework [29] (see Fig. 4). First, we have coded the contract using the high-level language programming solidity [30]. Then, we compiled the contract into Ethereum Virtual Machine (EVM) byte code; once the collaboration contract gets compiled, it generates EVM byte code as well as Application Binary Interface (ABI). Afterwards, we deployed the collaboration contract to the blockchain. Initially, we have deployed the collaboration contract using Ganache, a private blockchain simulator to test Ethereum's smart contract in a fast way. Then, we have deployed the smart contract on Ethereum official test network Ropsten. Fig. 5 shows the smart contract lifecycle. Once deployed, the smart contract can be invoked using its address and the ABI definition. If needed, the contract can be deleted

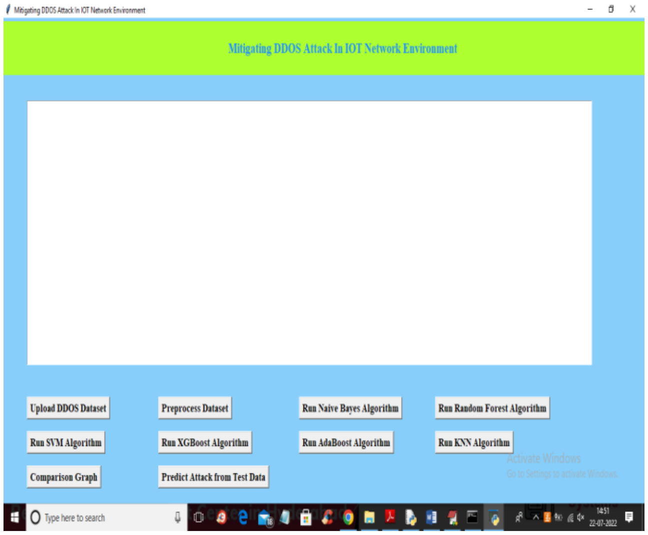
PROPOSED SYSTEM ADVANTAGES:

1. High Accuracy

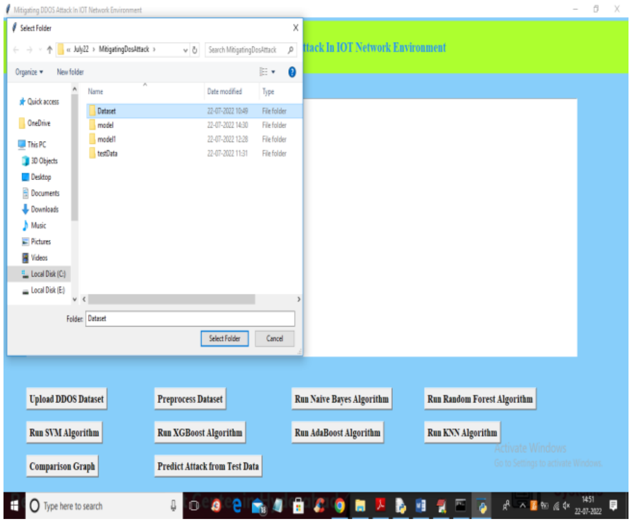
2. High Efficiency

IV. RESULTS

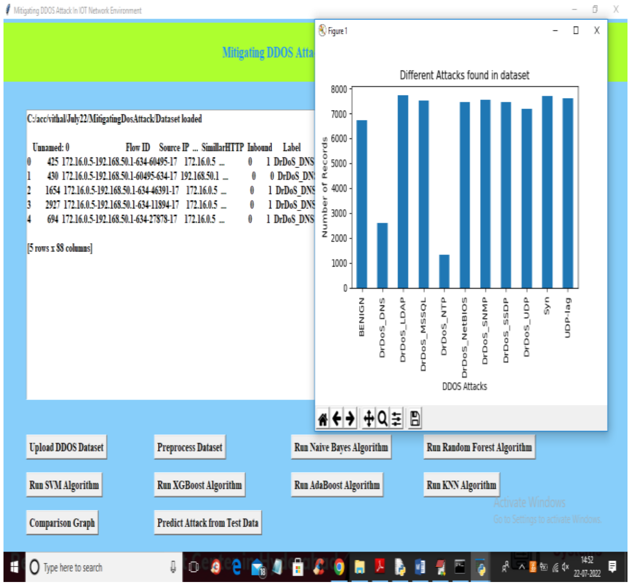
To run project double click on 'run.bat' file to get below screen



In above screen click on ‘Upload DDOS Dataset’ button tto upload dataset and get below output

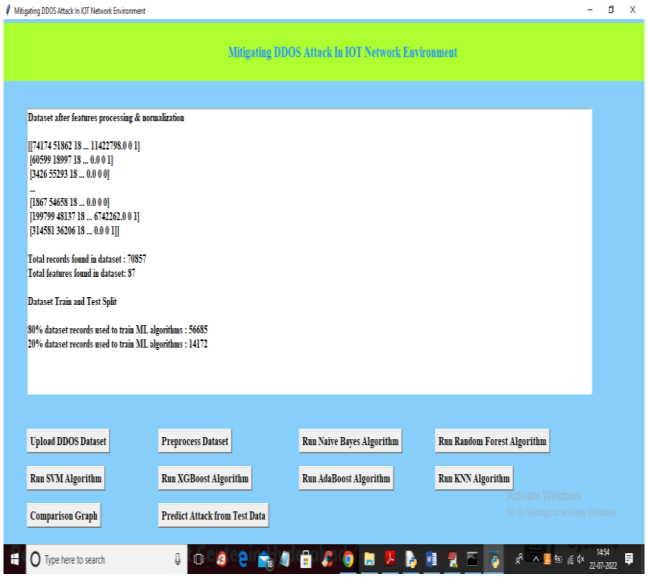


In above screen selecting and uploading ‘Dataset’ folder and then click on ‘Select Folder’ button to load dataset and get below output



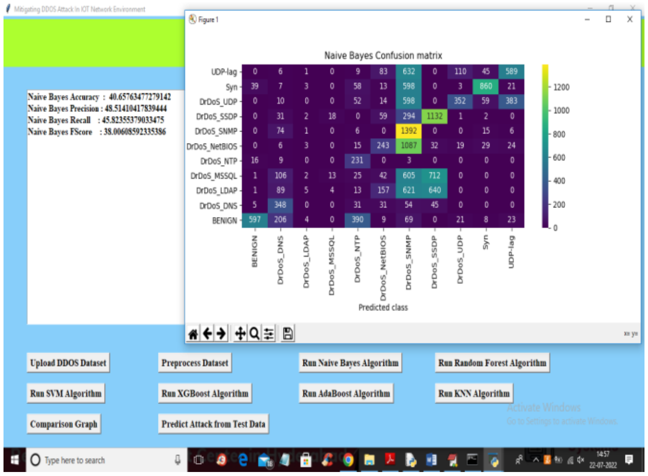
```
C:/acc/vithal/July22/MitigatingDosAttack/Dataset loaded

  Unnamed: 0                     Flow ID     Source IP  ... SimillarHTTP Inbound     Label
0        425  172.16.0.5-192.168.50.1-634-60495-17   172.16.0.5  ...            0       1 DrDoS_DNS
1        430  172.16.0.5-192.168.50.1-60495-634-17 192.168.50.1  ...            0       0 DrDoS_DNS
2       1654  172.16.0.5-192.168.50.1-634-46391-17   172.16.0.5  ...            0       1 DrDoS_DNS
3       2927  172.16.0.5-192.168.50.1-634-11894-17   172.16.0.5  ...            0       1 DrDoS_DNS
4        694  172.16.0.5-192.168.50.1-634-27878-17   172.16.0.5  ...            0       1 DrDoS_DNS

[5 rows x 88 columns]
```

In above screen dataset loaded and we can see dataset contains both numeric and non-numeric data and in above graph x-axis represents attack names and y-axis represents count of those records. Now close above graph and then click on ‘Preprocess Dataset’ button to process dataset and get below screen



```
Dataset after features processing & normalization

[[74174 51862 18 ... 11422798.0 0 1]
 [60599 18997 18 ... 0.0 0 1]
 [3426 55293 18 ... 0.0 0 0]
 ...
 [1867 54658 18 ... 0.0 0 0]
 [199799 48137 18 ... 6742262.0 0 1]
 [314581 36206 18 ... 0.0 0 1]]

Total records found in dataset : 70857
Total features found in dataset: 87

Dataset Train and Test Split

80% dataset records used to train ML algorithms : 56685
20% dataset records used to train ML algorithms : 14172
```

In above screen we can see all dataset values converted to numeric format and dataset contains more than 70000 records and each record contains 87 features and then we have split dataset into train and test and for training application using 56685 records for training and 14172 for testing. Now train and test data is ready and now click on 'Run Naïve Bayes Algorithm' button to train Naïve Bayes and get below output



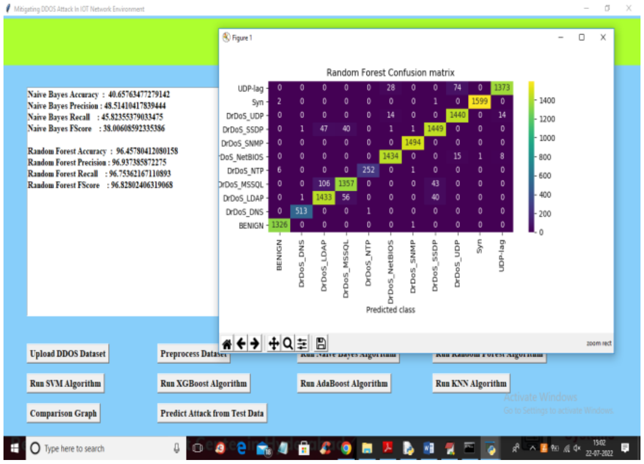
```
Naive Bayes Accuracy  :  40.65763477279142
Naive Bayes Precision : 48.51410417839444
Naive Bayes Recall    : 45.82355379033475
Naive Bayes FScore    : 38.00608592335386
```

Naive Bayes Confusion matrix

	BENIGN	DrDoS_DNS	DrDoS_LDAP	DrDoS_MSSQL	DrDoS_NTP	DrDoS_NetBIOS	DrDoS_SNMP	DrDoS_SSDP	DrDoS_UDP	Syn	UDP-lag
UDP-lag	0	6	1	0	9	83	632	0	110	45	589
Syn	39	7	3	0	58	13	598	0	3	860	21
DrDoS_UDP	0	10	0	0	52	14	598	0	352	59	383
DrDoS_SSDP	0	31	2	18	0	59	294	1132	1	2	0
DrDoS_SNMP	0	74	1	0	6	0	1392	0	0	15	6
DrDoS_NetBIOS	0	6	3	0	15	243	1087	32	19	29	24
DrDoS_NTP	16	9	0	0	231	0	3	0	0	0	0
DrDoS_MSSQL	1	106	2	13	25	42	605	712	0	0	0
DrDoS_LDAP	1	89	5	4	13	157	621	640	0	0	0
DrDoS_DNS	5	348	0	0	31	31	54	45	0	0	0
BENIGN	597	206	4	0	390	9	69	0	21	8	23

Predicted class

In above screen with Naïve Bayes we got 40% accuracy and in confusion matrix graph x-axis represents PREDICTED classes and y-axis represents TRUE classes and prediction count in same row and column names are the correct prediction and count in different row and column names are the incorrect prediction and we can see Naïve Bayes predicted so many wrong prediction and close above graph and then click on 'Run Random Forest Algorithm' button to get below output



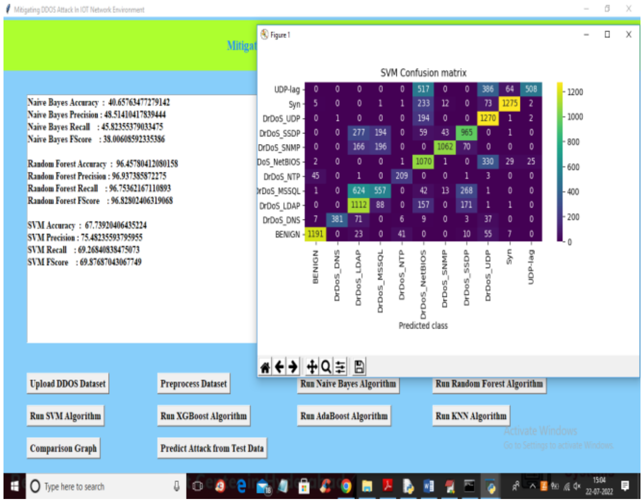
```
Naive Bayes Accuracy  :  40.65763477279142
Naive Bayes Precision : 48.51410417839444
Naive Bayes Recall    : 45.82355379033475
Naive Bayes FScore    : 38.00608592335386

Random Forest Accuracy  :  96.45780412080158
Random Forest Precision : 96.937385872275
Random Forest Recall    : 96.75362167110893
Random Forest FScore    : 96.82802406319068
```

Random Forest Confusion matrix

	BENIGN	DrDoS_DNS	DrDoS_LDAP	DrDoS_MSSQL	DrDoS_NTP	DrDoS_NetBIOS	DrDoS_SNMP	DrDoS_SSDP	DrDoS_UDP	Syn	UDP-lag
UDP-lag	0	0	0	0	0	28	0	0	74	0	1373
Syn	2	0	0	0	0	0	0	1	0	1599	0
DrDoS_UDP	0	0	0	0	0	14	0	0	1440	0	14
DrDoS_SSDP	0	1	47	40	0	1	1	1449	0	0	0
DrDoS_SNMP	0	0	0	0	0	0	1494	0	0	0	0
DoS_NetBIOS	0	0	0	0	0	1434	0	0	15	1	8
DrDoS_NTP	6	0	0	0	252	0	1	0	0	0	0
DrDoS_MSSQL	0	0	106	1357	0	0	0	43	0	0	0
DrDoS_LDAP	0	1	1433	56	0	0	0	40	0	0	0
DrDoS_DNS	0	513	0	0	1	0	0	0	0	0	0
BENIGN	1326	0	0	0	0	0	1	0	0	0	0

Predicted class

In above screen with Random Forest we got more than 96% accuracy and in graph also we can see lots of predictions are correct. Now close above graph and then click on 'Run SVM Algorithm' button to get below output



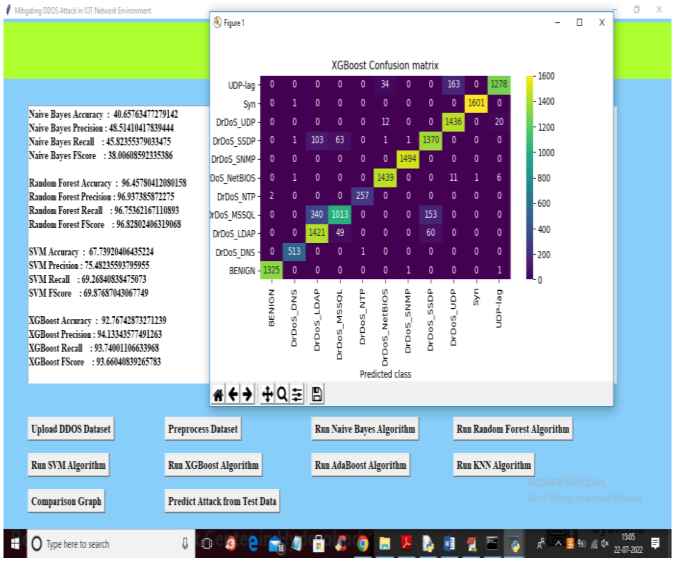
```
Naive Bayes Accuracy  :  40.65763477279142
Naive Bayes Precision : 48.51410417839444
Naive Bayes Recall    : 45.82355379033475
Naive Bayes FScore    : 38.00608592335386

Random Forest Accuracy  :  96.45780412080158
Random Forest Precision : 96.937385872275
Random Forest Recall    : 96.75362167110893
Random Forest FScore    : 96.82802406319068

SVM Accuracy  :  67.73920406435224
SVM Precision : 75.48235593795955
SVM Recall    : 69.26840838475073
SVM FScore    : 69.87687043067749
```

SVM Confusion matrix

	BENIGN	DrDoS_DNS	DrDoS_LDAP	DrDoS_MSSQL	DrDoS_NTP	DrDoS_NetBIOS	DrDoS_SNMP	DrDoS_SSDP	DrDoS_UDP	Syn	UDP-lag
UDP-lag	0	0	0	0	0	517	0	0	386	64	508
Syn	5	0	0	1	1	233	12	0	73	1275	2
DrDoS_UDP	0	1	0	0	0	194	0	0	1270	1	2
DrDoS_SSDP	0	0	277	194	0	59	43	965	0	1	0
DrDoS_SNMP	0	0	166	196	0	0	1062	70	0	0	0
DoS_NetBIOS	2	0	0	0	1	1070	1	0	330	29	25
DrDoS_NTP	45	0	1	0	209	0	0	1	3	0	0
rDoS_MSSQL	1	0	624	557	0	42	13	268	1	0	0
DrDoS_LDAP	0	0	1112	88	0	157	0	171	1	1	0
DrDoS_DNS	7	381	71	0	6	9	0	3	37	0	0
BENIGN	1191	0	23	0	41	0	0	10	55	7	0

Predicted class

In above screen with SVM we got 67% accuracy and now close above graph and then click on 'Run XGBOOST Algorithm' button to get below output



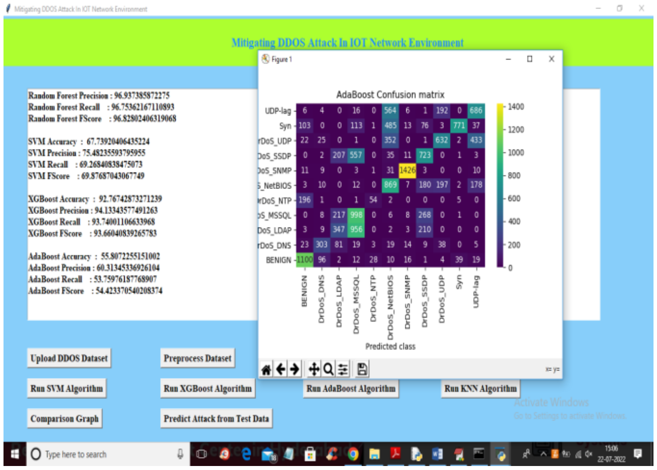
```
Naive Bayes Accuracy  :  40.65763477279142
Naive Bayes Precision : 48.51410417839444
Naive Bayes Recall    : 45.82355379033475
Naive Bayes FScore    : 38.00608592335386

Random Forest Accuracy  :  96.45780412080158
Random Forest Precision : 96.937385872275
Random Forest Recall    : 96.75362167110893
Random Forest FScore    : 96.82802406319068

SVM Accuracy  :  67.73920406435224
SVM Precision : 75.48235593795955
SVM Recall    : 69.26840838475073
SVM FScore    : 69.87687043067749

XGBoost Accuracy  :  92.76742873271239
XGBoost Precision : 94.13343577491263
XGBoost Recall    : 93.74001106633968
XGBoost FScore    : 93.66040839265783
```

XGBoost Confusion matrix

	BENIGN	DrDoS_DNS	DrDoS_LDAP	DrDoS_MSSQL	DrDoS_NTP	DrDoS_NetBIOS	DrDoS_SNMP	DrDoS_SSDP	DrDoS_UDP	Syn	UDP-lag
UDP-lag	0	0	0	0	0	34	0	0	163	0	1278
Syn	0	1	0	0	0	0	0	0	0	1601	0
DrDoS_UDP	0	0	0	0	0	12	0	0	1436	0	20
DrDoS_SSDP	0	1	103	63	0	1	1	1370	0	0	0
DrDoS_SNMP	0	0	0	0	0	0	1494	0	0	0	0
DoS_NetBIOS	0	1	0	0	0	1439	0	0	11	1	6
DrDoS_NTP	2	0	0	0	257	0	0	0	0	0	0
rDoS_MSSQL	0	0	340	1013	0	0	0	153	0	0	0
DrDoS_LDAP	0	0	1421	49	0	0	0	60	0	0	0
DrDoS_DNS	0	513	0	0	1	0	0	0	0	0	0
BENIGN	1325	0	0	0	0	0	1	0	0	0	1

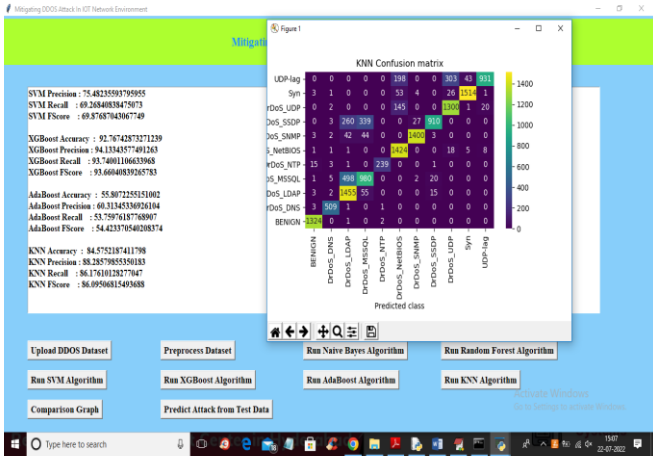
Predicted class

In above screen with XGBOOST we got 92% accuracy and now close above graph and then click on 'Run ADA BOOST Algorithm' button to get below output



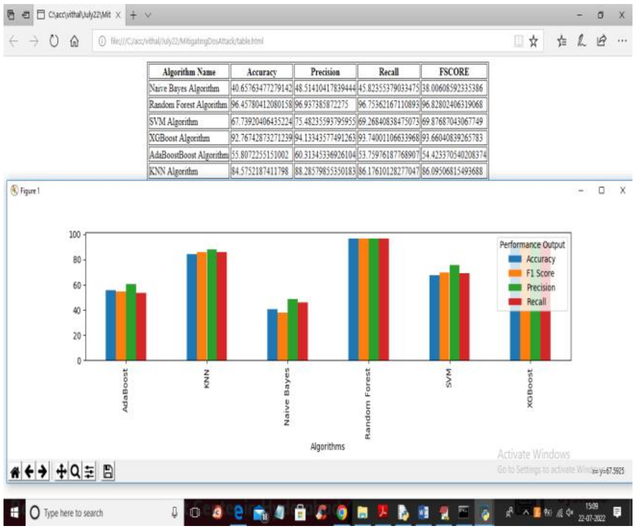
```
Random Forest Precision : 96.937385872275
Random Forest Recall    : 96.75362167110893
Random Forest FScore    : 96.82802406319068

SVM Accuracy  :  67.73920406435224
SVM Precision : 75.48235593795955
SVM Recall    : 69.26840838475073
SVM FScore    : 69.87687043067749

XGBoost Accuracy  :  92.76742873271239
XGBoost Precision : 94.13343577491263
XGBoost Recall    : 93.74001106633968
XGBoost FScore    : 93.66040839265783

AdaBoost Accuracy  :  55.8072255151002
AdaBoost Precision : 60.31345336926104
AdaBoost Recall    : 53.75976187768907
AdaBoost FScore    : 54.423370540208374
```

In above screen with ADABOOST we got 55% accuracy and now close above graph and then click on 'Run KNN Algorithm' button to get below output



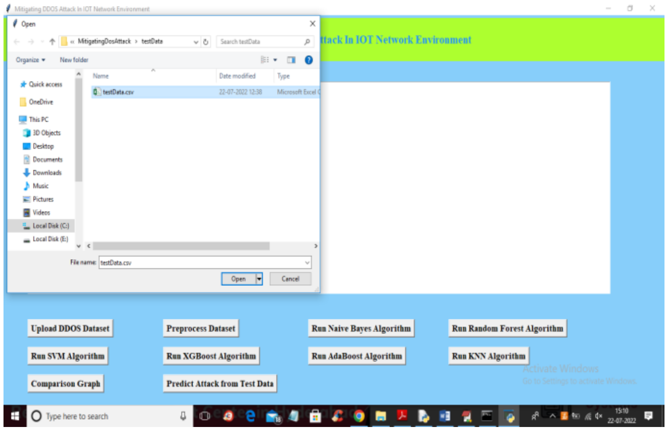
```
SVM Precision : 75.48235593795955
SVM Recall    : 69.26840838475073
SVM FScore    : 69.87687043067749

XGBoost Accuracy  :  92.76742873271239
XGBoost Precision : 94.13343577491263
XGBoost Recall    : 93.74001106633968
XGBoost FScore    : 93.66040839265783

AdaBoost Accuracy  :  55.8072255151002
AdaBoost Precision : 60.31345336926104
AdaBoost Recall    : 53.75976187768907
AdaBoost FScore    : 54.423370540208374

KNN Accuracy  :  84.5752187411798
KNN Precision : 88.28579855350183
KNN Recall    : 86.1761012827704 7
KNN FScore    : 86.09506815493688
```

In above screen with KNN we got 84% accuracy and now close above graph and then click on 'Comparison Graph' button to get below graph

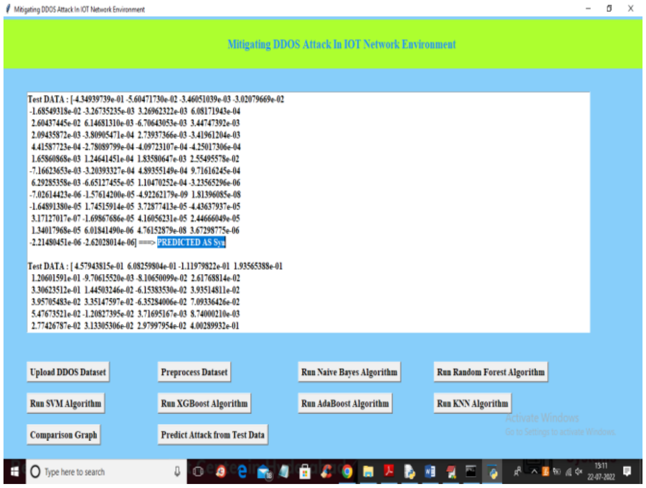


Algorithm Name	Accuracy	Precision	Recall	FSCORE
Naive Bayes Algorithm	40.6576347727914 2	48.5141041783944 4	45.82355379033475	38.00608592335386
Random Forest Algorithm	96.45780412080158	96.937385872275	96.75362167110893	96.82802406319068
SVM Algorithm	67.73920406435224	75.48235593795955	69.26840838475073	69.87687043067749
XGBoost Algorithm	92.76742873271239	94.13343577491263	93.74001106633968	93.66040839265783
AdaBoostBoost Algorithm	55.8072255151002	60.31345336926104	53.75976187768907	54.423370540208374
KNN Algorithm	84.5752187411798	88.28579855350183	86.17610128277047	86.09506815493688

In above graph and comparison table we can see Random Forest got high accuracy and in above graph different colour bar represents different metrics such as accuracy, precision, recall and FSCORE. Now click on 'Predict Attack from Test Data' button to upload test data and get below output

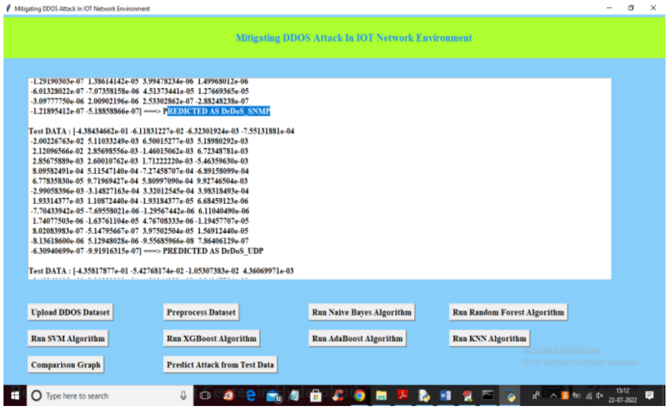


In above screen selecting and uploading TEST DATA file and then click on 'Open' button to get below output

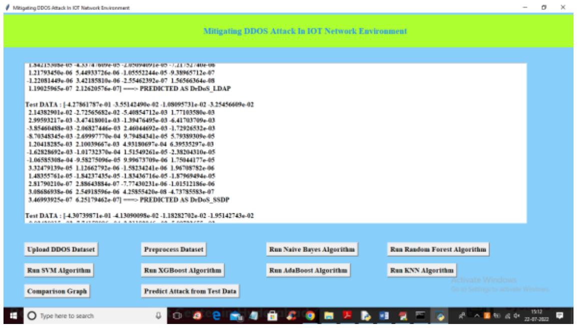

Mitigating DDOS Attack In IOT Network Environment
Upload DDOS Dataset
Preprocess Dataset
Run Naive Bayes Algorithm
Run Random Forest Algorithm
Run SVM Algorithm
Run XGBoost Algorithm
Run AdaBoost Algorithm
Run KNN Algorithm
Comparison Graph
Predict Attack from Test Data

```
Test DATA : [-4.34939739e-01 -5.60471730e-02 -3.46051039e-03 -3.02079669e-02
 -1.68549318e-02 -3.26735235e-03  3.26962322e-03  6.08171943e-04
  2.60437445e-02  6.14681310e-03 -6.70643053e-03  3.44747392e-03
  2.09435872e-03 -3.80905471e-04  2.73937366e-03 -3.41961204e-03
  4.41587723e-04 -2.78089799e-04 -4.09723107e-04 -4.25017306e-04
  1.65860868e-03  1.24641451e-04  1.83580647e-03  2.55495578e-02
 -7.16623653e-03 -3.20393327e-04  4.89355149e-04  9.71616245e-04
  6.29285358e-03 -6.65127455e-05  1.10470252e-04 -3.23565296e-06
 -7.02614423e-06 -1.57614200e-05 -4.92262179e-09  1.81396085e-08
 -1.64891380e-05  1.74515914e-05  3.72877413e-05 -4.43637937e-05
  3.17127017e-07 -1.69867686e-05  4.16056231e-05  2.44666049e-05
  1.34017968e-05  6.01841490e-06  4.76152879e-08  3.67298775e-06
 -2.21480451e-06 -2.62028014e-06] ==> PREDICTED AS Syn

Test DATA : [ 4.57943815e-01  6.08259804e-01 -1.11979822e-01  1.93565388e-01
  1.20601591e-01 -9.70615520e-03 -8.10650099e-02  2.61768814e-02
  3.30623512e-01  1.44503246e-02 -6.15383530e-02  3.93514811e-02
  3.95705483e-02  3.35147597e-02 -6.35284006e-02  7.09336426e-02
  5.47673521e-02 -1.20827395e-02  3.71695167e-03  8.74000210e-03
  2.77426787e-02  3.13305306e-02  2.97997954e-02  4.00289932e-01
```

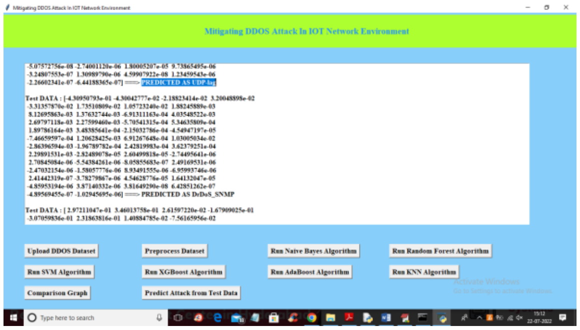
In above screen in square bracket we can see TEST DATA features and after arrow symbol =➔ we can see predicted ATTACK as 'SYN' and scroll down above screen to view different predicted output


Mitigating DDOS Attack In IOT Network Environment
Upload DDOS Dataset
Preprocess Dataset
Run Naive Bayes Algorithm
Run Random Forest Algorithm
Run SVM Algorithm
Run XGBoost Algorithm
Run AdaBoost Algorithm
Run KNN Algorithm
Comparison Graph
Predict Attack from Test Data

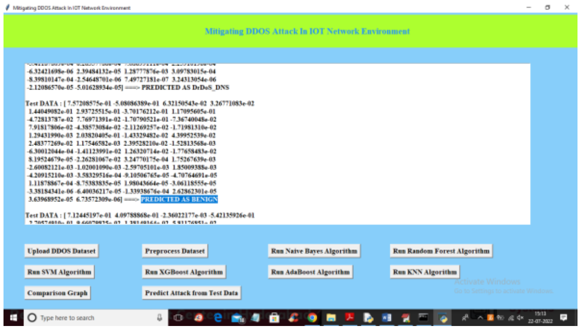
```
 -1.29190303e-07  1.38614142e-05  3.99478234e-06  1.49968012e-06
 -6.01328022e-07 -7.07358158e-06  4.51373441e-05  1.27669365e-05
 -3.09777750e-06  2.00902196e-06  2.53302862e-07 -2.88248238e-07
 -1.21895412e-07 -5.18858866e-07] ==> PREDICTED AS DrDoS_SNMP

Test DATA : [-4.38434662e-01 -6.11831227e-02 -6.32301924e-03 -7.55131881e-04
 -2.00226763e-02  5.11033249e-03  6.50015277e-03  5.18980292e-03
  2.12096566e-02  2.85698556e-03 -1.46015062e-03  6.72348781e-03
  2.85675889e-03  2.60010762e-03  1.71222220e-03 -5.46359630e-03
  8.09582491e-04  5.11547140e-04 -7.27458707e-04 -6.89158099e-04
  6.77835830e-05  9.71969427e-04  5.80997090e-04  9.92746504e-03
 -2.99058396e-03 -3.14827163e-04  3.32012545e-04  3.98318493e-04
  1.93314377e-03  1.10872440e-04 -1.93184377e-05  6.68459123e-06
 -7.70433942e-05 -7.69558021e-06 -1.29567442e-06  6.11040490e-06
  1.74077503e-06 -1.63761104e-05  4.76708333e-06 -1.19457707e-05
  8.02083983e-07 -5.14795667e-07  3.97502504e-05  1.56912440e-05
 -8.13618600e-06  5.12948028e-06 -9.55685966e-08  7.86406129e-07
 -6.30940699e-07 -9.91916315e-07] ==> PREDICTED AS DrDoS_UDP

Test DATA : [-4.35817877e-01 -5.42768174e-02 -1.05307383e-02  4.36069971e-03
```


Mitigating DDOS Attack In IOT Network Environment
Upload DDOS Dataset
Preprocess Dataset
Run Naive Bayes Algorithm
Run Random Forest Algorithm
Run SVM Algorithm
Run XGBoost Algorithm
Run AdaBoost Algorithm
Run KNN Algorithm
Comparison Graph
Predict Attack from Test Data

```
  1.21793450e-06  5.44933726e-06 -1.05552244e-05 -9.38965712e-07
 -1.22081449e-06  3.42185810e-06 -2.55462392e-07  1.56566364e-08
  1.19025965e-07  2.12620576e-07] ==> PREDICTED AS DrDoS_LDAP

Test DATA : [-4.27861787e-01 -3.55142490e-02 -1.08095731e-02 -3.25456609e-02
  2.14382901e-02 -2.72565682e-02 -5.40854712e-03  1.77103580e-03
  2.99593217e-03 -3.47418001e-03 -1.39476495e-03 -6.41703709e-03
 -3.85460488e-03 -2.06827446e-03  2.46044692e-03 -1.72926532e-03
 -8.70348345e-03 -2.69997770e-04  9.79484341e-05  5.79389309e-05
  1.20418285e-03  2.10039667e-03  4.93180697e-04  6.39535297e-03
 -1.62828692e-03 -1.01732370e-04  1.51549261e-05 -2.38204310e-05
 -1.06585308e-04 -9.58275096e-05  9.99673709e-06  1.75044177e-05
  3.32479139e-05  1.12662792e-06 -1.58234241e-06  1.96708782e-06
  1.48355761e-05 -1.84237435e-05 -1.83436716e-05 -1.87969494e-05
  2.81790210e-07  2.88643884e-07 -7.77430231e-06 -1.01512186e-06
  3.08686938e-06  2.54918596e-06  4.25855420e-08 -4.73785583e-07
  3.46993925e-07  6.25179462e-07] ==> PREDICTED AS DrDoS_SSDP

Test DATA : [-4.30739871e-01 -4.13090098e-02 -1.18282702e-02 -1.95142743e-02
```


Mitigating DDOS Attack In IOT Network Environment
Upload DDOS Dataset
Preprocess Dataset
Run Naive Bayes Algorithm
Run Random Forest Algorithm
Run SVM Algorithm
Run XGBoost Algorithm
Run AdaBoost Algorithm
Run KNN Algorithm
Comparison Graph
Predict Attack from Test Data

```
 -5.07572756e-08 -2.74001120e-06  1.80005207e-05  9.73865495e-06
 -3.24807553e-07  1.30989790e-06  4.59907922e-08  1.23459543e-06
 -2.26602341e-07 -6.44188365e-07] ==> PREDICTED AS UDP-lag

Test DATA : [-4.30950793e-01 -4.30042777e-02 -2.18823414e-02  3.20048898e-02
 -3.31357870e-02  1.73510809e-02  1.05723240e-02  1.88245889e-03
  8.12695863e-03  1.37632744e-03 -6.91311163e-04  4.03548522e-03
  2.69797118e-03  2.27599460e-03 -5.70541315e-04  5.34635809e-04
  1.89786164e-03  3.48385641e-04 -2.15032786e-04 -4.54947197e-05
 -7.46659597e-04  1.20628425e-03  6.91267648e-04  1.03005034e-02
 -2.86396594e-03 -1.96789782e-04  2.42819983e-04  3.62379251e-04
  2.29891531e-03 -2.82489078e-05  2.60499818e-05 -2.74495641e-06
  2.70845084e-06 -5.54384261e-06 -8.05855683e-07  2.49169531e-06
 -2.47032154e-06 -1.58057776e-06  8.93491555e-06 -6.95993746e-06
  2.41442319e-07 -3.78279867e-06  4.54628776e-05  1.64132047e-05
 -4.85953194e-06  3.87140332e-06  3.81649290e-08  6.42851262e-07
 -4.89569455e-07 -1.02945695e-06] ==> PREDICTED AS DrDoS_SNMP

Test DATA : [ 2.97211047e-01  3.46013758e-01  2.61597220e-02 -1.67909025e-01
 -3.07059836e-01  2.31863816e-01  1.40884785e-02 -7.56165956e-02
```


Mitigating DDOS Attack In IOT Network Environment
Upload DDOS Dataset
Preprocess Dataset
Run Naive Bayes Algorithm
Run Random Forest Algorithm
Run SVM Algorithm
Run XGBoost Algorithm
Run AdaBoost Algorithm
Run KNN Algorithm
Comparison Graph
Predict Attack from Test Data

```
 -6.32421698e-06  2.39484132e-05  1.28777876e-03  3.09783015e-04
 -8.39810147e-04 -2.54648701e-06  7.49727181e-07  3.24313054e-06
 -2.12086570e-05 -5.01628934e-05] ==> PREDICTED AS DrDoS_DNS

Test DATA : [ 7.57208575e-01 -5.08086389e-01  6.32150543e-02  3.26771083e-02
  1.44049082e-01  2.93725515e-01 -3.70176212e-01  1.17095605e-01
 -4.72813787e-02  7.76971391e-02 -1.70790521e-01 -7.36740048e-02
  7.91817806e-02 -4.38573084e-02 -2.11269257e-02 -1.71981310e-02
  1.29431990e-03  2.03820405e-01 -1.43329482e-02  4.39952539e-02
  2.48377269e-02  1.17546582e-03  2.39528210e-02 -1.52813568e-03
 -6.30012044e-04 -1.41123991e-02  1.26320714e-02 -1.77658483e-02
  8.19524679e-05 -2.26281067e-02  3.24770175e-04  1.75267639e-03
 -2.60082121e-03 -1.02001090e-03 -2.59705101e-03  1.85009388e-03
 -4.20915210e-03 -3.58329516e-04 -9.10506765e-05 -4.70764691e-05
  1.11878867e-04 -8.75383835e-05  1.98043664e-05 -3.06118555e-05
 -3.38184341e-06 -6.40036217e-05 -1.33938676e-04  2.62862301e-05
  3.63968952e-05  6.73572309e-06] ==> PREDICTED AS BENIGN

Test DATA : [ 7.12445197e-01  4.09788868e-01 -2.36022177e-03 -5.42135926e-01
```

In above screens with each different test records different attacks and benign (normal) classes are predicted

V. CONCLUSION

This paper presents a comprehensive framework for Software-Defined Internet of Things (SD-IoT), comprising an SD-IoT controller pool, SD-IoT switches integrated with the IoT gateway, and terminal IoT devices. We propose an algorithm designed to detect and mitigate DDoS attacks within this SD-IoT framework. The algorithm calculates the threshold value of the cosine similarity of packet-in rate vectors at the ports of SD-IoT boundary switches. By comparing this threshold value, we determine whether a DDoS attack has occurred, identify the real DDoS attacker, and promptly block the attack at its source. Simulation results demonstrate the effectiveness of our proposed algorithm in swiftly identifying the IoT device initiating a DDoS attack, enabling rapid mitigation, and addressing vulnerabilities inherent in IoT environments with computational and memory constraints. Future research will focus on proactive DDoS defense strategies in SD-IoT environments. This includes designing and implementing dynamic load-balancing algorithms within the controller pool and exploring more efficient detection and mitigation algorithms tailored to the SD-IoT framework.

REFERENCES:

[1] H. Ma, L. Liu, A. Zhou, and D. Zhao, "On networking of Internet of Things: Explorations and challenges," IEEE Internet Things J., vol. 3, no. 4, pp. 441–452, Aug. 2016.

[2] P. G. Neumann, "Risks of automation: A cautionary total-system per- spective of our cyberfuture," Commun. ACM, vol. 59, no. 10, pp. 26–30, Oct. 2016.

[3] M. I. Thariq Hussan, D. Saidulu, P. T. Anitha, A. Manikandan and P. Naresh (2022), Object Detection and Recognition in Real Time Using Deep Learning for Visually Impaired People. IJEER 10(2), 80-86. DOI: 10.37391/IJEER.100205.

[4] Y. Liu, A. Liu, S. Guo, Z. Li, Y.-J. Choi, and H. Sekiya, "Context-aware collect data with energy efficient in cyber–physical cloud systems," Future Generat. Comput. Syst., Jun. 2017, doi: https://doi.org/10.1016/j.future.2017.05.029

[5] Sunder Reddy, K. S. ., Lakshmi, P. R. ., Kumar, D. M. ., Naresh, P. ., Gholap, Y. N. ., & Gupta, K. G. . (2024). A Method for Unsupervised Ensemble Clustering to Examine Student Behavioral Patterns. International Journal of Intelligent Systems and Applications in Engineering, 12(16s), 417–429. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/4854.

[6] U. Lindqvist and P. G. Neumann, "The future of the Internet of Things," Commun. ACM, vol. 60, no. 2, pp. 26–30, Jan. 2017.

[7] R. Huo et al., "Software defined networking, caching, and computing for green wireless networks," IEEE Commun. Mag., vol. 54, no. 11, pp. 185–193, Nov. 2016.

[8] Nagesh, C., Chaganti, K.R. , Chaganti, S. , Khaleelullah, S., Naresh, P. and Hussan, M. 2023. Leveraging Machine Learning based Ensemble Time Series Prediction Model for Rainfall Using SVM, KNN and Advanced ARIMA+ E-GARCH. International Journal on Recent and Innovation Trends in Computing and Communication. 11, 7s (Jul. 2023), 353–358. DOI:https://doi.org/10.17762/ijritcc.v11i7s.7010.

[9] K. Wang, K. Yang, H.-H. Chen, and L. Zhang, "Computation diversity in emerging networking paradigms," IEEE Wireless Commun., vol. 24, no. 1, pp. 88–94, Feb. 2017.

[10] L. Zhang, Q. Deng, Y. Su, and Y. Hu, "A box-covering-based rout- ing algorithm for large-scale SDNs," IEEE Access, vol. 5, no. 1, pp. 4048–4056, Mar. 2017.