Identification Of Network Intrusion and Anomaly Detection in Network Security and Digital Forensics

ALK Bilahari*
*Reasearch Scholar, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Hyderabad-500075, Telangana, Hyderabad, Email: bilahari89@klh.edu.in

Dr. M Saidi Reddy,
Associate Professor, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Hyderabad-500075, Telangana, Hyderabad
Email: msreddy33@klh.edu.in

ABSTRACT

Currently, cloud conditions are confronting a gigantic test from the aggressors regarding different assaults tossed to the cloud specialist co-ops. In both industry and scholastics, the discovery and moderation of DDoS assaults is presently a problematic issue. Distinguishing Distributed Denial of Service dangers is primarily a characterization issue that can be tended to utilizing information mining, AI, and profound learning methods. DDoS assaults can happen in any of the seven-layer OSI model's organizations. Thus, distinguishing the DDoS assaults is a significant undertaking for cloud specialist organizations to defeat perilous assaults and misfortune by partners and suppliers.

1. INTRODUCTION

Denial of service (DoS) and dispensed refusal of administration (DDoS) attacks have ended up being a rising number of renowned in current years, with assailants sending an enormous wide assortment of parcels to the substantial individual gadget as a method for making online structures inaccessible for them. DoS attacks are venomous tasks that save legitimate clients from gaining admittance to a device, local area, programming, or records. The cutting-edge examples have just approved the development of cyberattacks. There are, for the most part, styles of dispensed dos attacks:

Unmarried stock attacks begin from an available gadget, and dispensed dos attacks start from multiple designs. DDoS (Conveyed Refusal of Administration) attacks are covered withinside the DoS class. DDoS attacks pick objective Web frameworks, switches, DNS servers, data transmission, and servers, among various things.DDoS volumetric attacks represent more prominent than 65% of all attacks.

The aggressors consistently utilize those systems and online entertainment, email, and web applications to play out the attack and send the code contaminating the gadget. They occasionally choose the methodology of endlessly utilizing a botnet, moreover called a local area of commandeered machines. If their attack is effective, the assailant could be fit to deal with the device in any way they need. This could be all finished from wherein they might be sitting without the gadget's owner, in any event, knowing.

Peculiarity location is a top-notch subject for local area clients in vogue mechanical time. Likewise, clients of the local area are developing; this intends that there are more prominent guests in the local area in light of the improvement of various local area techniques. This makes it extremely challenging to recognize phenomenal styles. The structure/model's precision degree changed into moreover referenced in this paper, along the edge of a high-level perspective on the various ML methodologies used to determine the vagueness identification inconvenience and their advantages and impediments. Techniques for sorting out and moderating local area guests' peculiarities are referenced and thought about in this review in expressions of exactness and sort of abnormality. Network guests' oddity identification concentrates on holes, and fundamental inquiries are referenced exhaustively. We expect that the scientists could be directed withinside the appropriate way to project unrivaled examinations on this area through the assessment, correlations, and next personality of holes.

Advanced change, digitization, venture 4.0, etc., are popular expressions, and the essential role is to apply time and records to upgrade precision, efficiency, and effectiveness. The Key empowering influence is equipped to remove valuable records from a colossal amount of records, permitting capacity improvement, time investment funds, and cost decrease. There are a lot of procedures used to separate gainful documents. Information is examined through many methodologies as part of the records assessment process. In current cases, the fine of contributions and security in immense scope networks have offered a customary undertaking to various local gatherings. These well-being issues might be followed through many inward or outside components. Outside components incorporate taking well-being records or closing down all contributions; inward features include design mistakes, guest blockage, energy blackouts, and server crashes.

Notwithstanding those issues, an unmarried well-being danger called an oddity, is now boundless. The styles of various datasets fluctuate from the ones of the regular dataset, or the records occasionally veer off from the common dataset. Irregularity is the call given to this deviation, severely affecting local area tasks and significantly affecting local area contributions. There are many ways to deal with frame oddity. Lakhina et al. country that [1] "oddities are unmistakable styles and a moderate extra de withinside the guest's scopes of a local area".

2. LITERATURE REVIEW

In light of contraption getting to be aware and profound getting to know strategies, the ensuing rule considerations for local area IDPS work. In recent years, quick upgrades in age and organizations have come about because of the colossal utilization of Web contributions throughout all enterprises. Since falsifying has raised, and a few current designs were compromised, it's now urgent to increment measurements security answers that might choose new attacks.

Et., M. Mithem al; distinguished obscure attack programs utilizing a profound brain local area and an ever-evolving interruption discovery contraption with unprecedented local area execution [4]. Using both paired classes or multiclass classes might recognize assaults—the suggested techniques created promising outcomes in expressions of exorbitant precision. Security is problematic because many measurements are traded through all spaces every hour. Information security might be protected by utilizing a brain's local area within the way characterized in [5]. Various IDS and Interruption Counteraction Frameworks (IPS) have been tried and in examination on this view.
What's more, the differentiation of various strategies is completed. Different styles and designs for interruption recognition are additionally referenced here. The view recommends how related inconveniences might be settled with brain organizations.

Chewet et al.2020). This paper's three strategies for NIDS have been covering a situation to win over their permeability issues [10]. A choice tree-fundamentally based absolute correction is made to the pruning calculations. By settling on the most extreme fundamental arrangements, this structure jam protection and any little changes haven't any effect on the technique decision approach anyway affect the device's presentation. With the guide of utilizing Bhatiet al. (2020), this paper makes a structure that is, to a great extent, applied with the help of MATLAB programming. A person classifier is developed and gifted inside this system, and it makes a definitive determination essentially founded absolutely on the superb part vote. The conclusion is the leftover of this system's four most significant stages, which envelop insights assortment, pre-handling, preparing, and testing. On various datasets, it gives over-the-top location exactness. The paper's weakness is that it provides a mind-boggling system structure.

D'Souza, D. J., and others2021) Exception recognition in unstructured measurements changed into the worry of this paper [12].t might be addressed the utilization of a chart. An overview of static, dynamic, and gadget getting-to-know strategies for irregularity location is similarly safeguarded in this paper, with more accentuation on charts essentially based on absolute procedures. The device will become more noteworthy complex because it utilized more than one diagram situation, a weakness.

The point of the work [8] is to apply profound getting-to-know-principally based absolutely interruption location and counteraction systems that may double forestall attacks like DOS, R2L, and U2R. The interruption changed into pictured the utilization of an in-force getting-to-know rendition, that is, a multi-degree cognizance gifted with unreasonable accuracy withinside the kddcup99 dataset. The Showcase Profound Learning rendition gathers the ideal local area insights and recoveries it as a CSV record to gauge the achieve real-time. In the subsequent stage, the interruption stays away from the guide of utilizing legacy scripts. The content will likely complete the counteraction segment with the direction to suggest various attack exceptional deterrent measures. The Multi-facet Perceptron class part's measurements might be utilized to make a choice. Specific interruption recognition and counteraction structures are mixed solidly into an unmarried device to work with faster and more prominent green interruption discovery and avoidance.

Following a proof of IDS, the examine [10] gives a class principally based absolutely at the most extreme regular spot strategies to the coming of Organization fundamentally based absolutely IDS (NIDS) structures, comprehensive of contraption getting to be aware and profound getting to be knowledgeable. The current NIDS-essentially based thorough research is evaluated in power, accentuating proposed replies, advantages, and disadvantages. The proposed approach, appraisal rules, and dataset decision are undeniably referenced after current ML and DL-essentially based absolutely NIDS upgrades and attributes are referenced. The blemishes in the introduced methodologies were utilized to feature various examination issues and the potential for additional examination concerning upgrading ML and DL-based NIDS. A portion of the benefits and burdens of different techniques, as well as challenges in building a model.

Challenges:

- Looking at the qualities of assaults — like their low or high rate — as well as the security issues welcomed on by the variety of associated objects
- Recognizing the assault as a particular sort of assault.
- Creating procedures for spotting assaults
- Tracking down the harmony between scholarly recommendations and the modern act of battling DDoS.
- Conquering the deficiency of cash.
- Confirmation, client security, and information spillage stay significant deterrents for distributed computing conditions.

3. METHODOLOGY

Below are the research methodologies previously used.
Load the dataset, Drop the lines with null, infinite values, Standardize the dataset and increase with 255, Convert the dataset into number sort, Find the mean of each column, Element Component requested Connection (FFoR): FFoR of a component fi with any remaining highlights fj of an item Oi is characterized utilizing beneath Condition. Normal FFoR (AFFoR): We characterize the AFFoR of an article Oi as the mean worth of its individual FFoR values, and it tends to be communicated utilizing underneath Condition. The Deviation vector (Dev): The deviation vector of article O I can be characterized as the outright distinction between the FFoR upsides of the item and its related AFFoR esteem. The Dev of an element fj is registered to utilize beneath Condition. FF-score (FFSc): We characterize the FFSc of an article Oi as the level of likeness as far as its Dev and mean worth, given by the underneath Condition.

$$FFoR\left(O_i^{f_i}\right) = \sum_{j=1\&i\neq j}^{n} \left(|f_i - f_j|\right)$$

$$where\ l\ \leq i \leq n.$$

$$AFFoR(O_i) = \frac{\sum_{j=1}^{n} (\mathrm{FFoR}(O_i^{f_j}))}{n}$$

$$Dev\left(O_i^{f_j}\right) = lAFFoR(O_i) - FFoR(O_i^{f_j})|, \forall j$$
$$= 1,2, \ldots n$$

$$FFSc(O_i) = \frac{(O_i \times Dev(O_i)T)}{(mean(O_i) + mean(Dev(O_i)))}$$

• Distance Clustering

Load the dataset, Drop the lines with invalid, endless qualities, and Standardize the dataset by separating each worth with the most extreme price of that particular class mark segment. Track down the Mean and Standard Deviation of every detail in the dataset. Contrast mean qualities and values in the dataset. The numerator mainly has three conditions: If both rates are not equivalent to 0, then 0.5(1+e-(meani-datai/σi)2). If any of the worth is 0, - 1, Else 0, Contrast mean qualities and values in the dataset. There are mainly three conditions in the denominator: If the two rates are 0, 0 Else , Favg=ΣNumerator/ΣDenominator, Sim=1+Favg/2.

The proposed strategy introduced here needs to be revised to overcome the issues and limitations. The exploratory consequences of different AI characterization calculations are analyzed on the interruption set dataset in this segment. Unaided and directed learning are the two most customary ways to deal with AI. For preparing analyses, marked models, for example, a contribution with a picked yield, are utilized. Cases without marks are prepared through unaided learning. Investigating the information and discovering some designs are the two goals of solo learning. Semi-regulated learning and support learning are likewise utilized [12], notwithstanding these methodologies.

An assortment of records is alluded to as an informational index. The csv documents are the sort of information we're utilizing here. The condensing for "comma isolated esteem" is "csv." We want an informational index to secure the model and train it. We start with the csv information in this paper. It will be changed into pictures from now on, and those pictures act as the model's feedback. For this situation, we have used the CIC Ddos 2017, CICDdos 2019, and NSL-KDD informational indexes.

Perceiving, understanding, and ordering objects into foreordained "sub-populaces" is the most common grouping method. The ML calculations group future datasets utilize various calculations and pre-sorted preparing datasets. In AI, characterization calculations use preparing information to foresee whether new information will be named clearly. To put it compactly, the order is a subset of "design acknowledgment" that utilizes characterization procedures in preparing a report to find an example in the informational collections [13]. The following grouping calculations were used to distinguish and group meddlesome assaults for this situation: Arbitrary Timberland, AdaBoost, Additional Trees, Angle Lift, Direct Relapse, and Multi-facet Perceptron.

First and foremost, we should comprehend and envision each element; in any case, it is tough to dissect and picture these highlights. In this way, we want to diminish the number of highlights in the informational collection and guarantee that the most significant ones are incorporated. Confirm that the elements are not copies or exceptions. We should apply Andrew Bends' idea to the informational collection after eliminating the bothersome highlights to imagine the informative group. We can switch high-layered information completely to two-layered information utilizing Andrew Bends, which is highly advantageous.

While working with an AI model, the piece of the element choice interaction where we ensure we have the right highlights to prepare the model well is vital. High-layered highlights, then again, present a test while preparing an enormous number of elements since imagining high-layered data is troublesome. Andrew bends are used here.
The Andrew bend is utilized to show a lot of information. To handle them, we want to envision the high-layered highlights in our dataset appropriately. For this reason, we want Andrew to bend. The Andrew bend decides if the information is straightforward, nonlinear, or straight.

Andrew bends are needed for the accompanying reasons:

- To imagine high-layered information.
- To comprehend the way of behaving of the informational collection.
- To break down the methodology and the procedure.
- To ensure if we need to utilize the administered or solo calculations.

We can picture the information, which is two layered, yet when we have the informational collection with additional aspects, we want Andrew Bends to envision that informational index aspect. Andrew's turns are utilized to imagine high-layered information. Moreover, by planning every perception onto a capability, all Means, distances, and changes were saved.

The plotting module's Andrews bends () technique can be utilized to plot Andrews bends on a chart. Multivariate information groups can be imagined using the matplotlib plot of Andrews turns created by this program. Coming up next are a portion of the assault classes distinguished in the datasets: DoS (Forswearing of Administration): Root to Client (U2R): Neighborhood to Remote (R2L): Probe: The different Organization Oddities and Organization Assaults carried out in this paper are portrayed in Fig. 1 below.

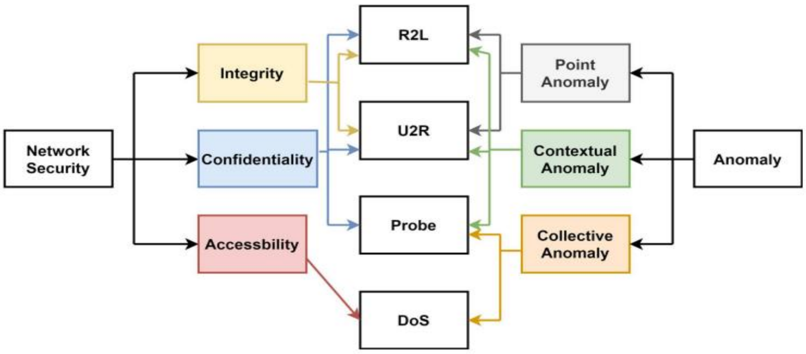

Fig. 1. Framework of Network Anomalies Attacks

4. IMPLEMENTATION

Because of the exceptionally nonlinear nature of the datasets, an assortment of AI and Profound Learning strategies can be utilized to rapidly recognize typical traffic from pernicious traffic. Another technique for accurately identifying traffic is created by joining different profound learning, and AI draws near. This framework can be utilized in cloud, Mist, SDN, and IoT conditions to distinguish assaults and protect the climate. In this paper, alongside other datasets referenced, we executed the dataset Utilitarian Portrayal is CIC-DDoS2019.

We have chosen the CICDdos 2019 informational index to do this assignment. At the point when we followed the connection to http://205.174.165.80/CICDataset/CICDDoS2019/, we found that there are two unmistakable record types: These are known as Pcaps or bundle catch documents, and they contain the crude information from two-day explore. CSVs, or comma-isolated esteem records, are a sort of document where the data is put away in csv design, and the kind of assault is physically marked. First, we thought about involving cvs as a contribution to the model. When the information in the CSV records is finished and clean, we can apply them as contributors to the model. Even so, there are a couple of issues with it:

The two records that are absent and the vastness of records are unimportant to profound learning calculations. Another problem is that a couple of the information sections contain critical figures. Subsequently, we are again recovering the CSV documents from the Pcap records to address this issue. Which CICFlowMeter empowers us to complete. CICFlowMeter, created by the Canadian Organization for Network Protection, can produce roughly 83 highlights from Parcel Catch Documents and audit those elements.

Andrew Curves for DDoS Evaluation Dataset (CIC-DDoS2019)

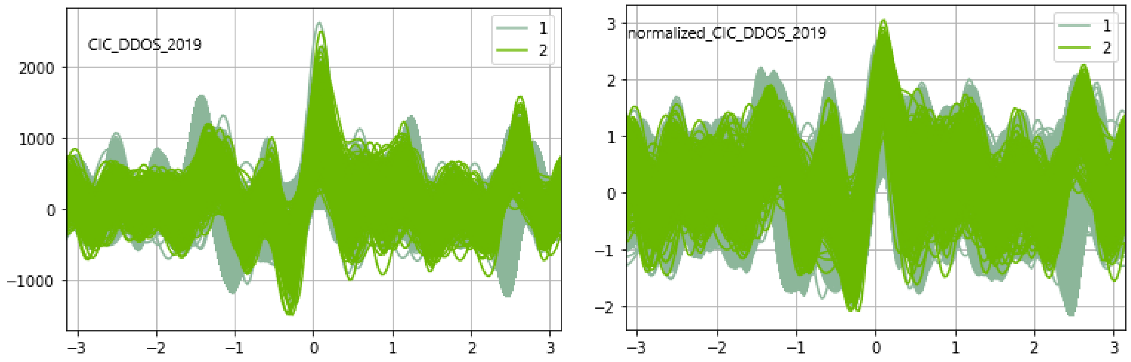

Fig.2. CIC DDoS 2019 dataset and Normalized CIC DDoS 2019 dataset Andrew Curve

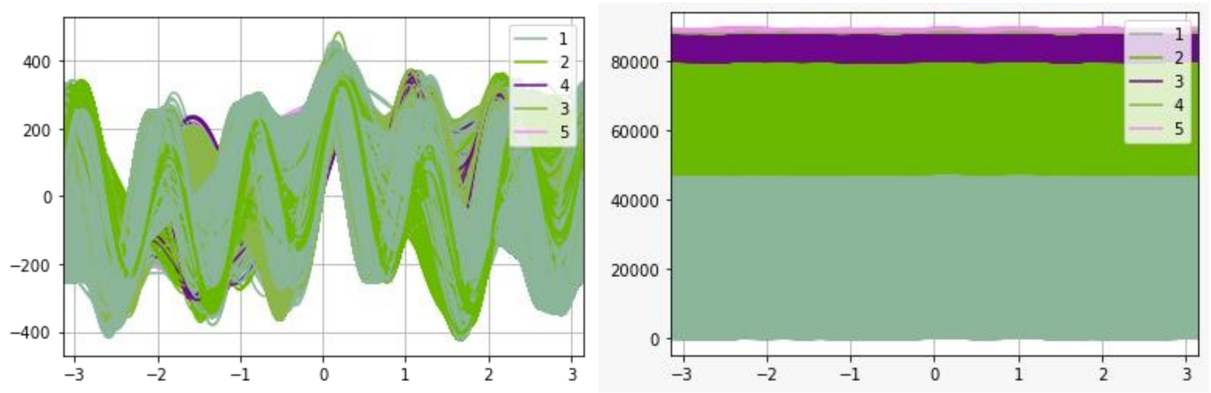

Fig. 3. NSL-19 KDD and Normalized NSL-19 dataset Andrew curve

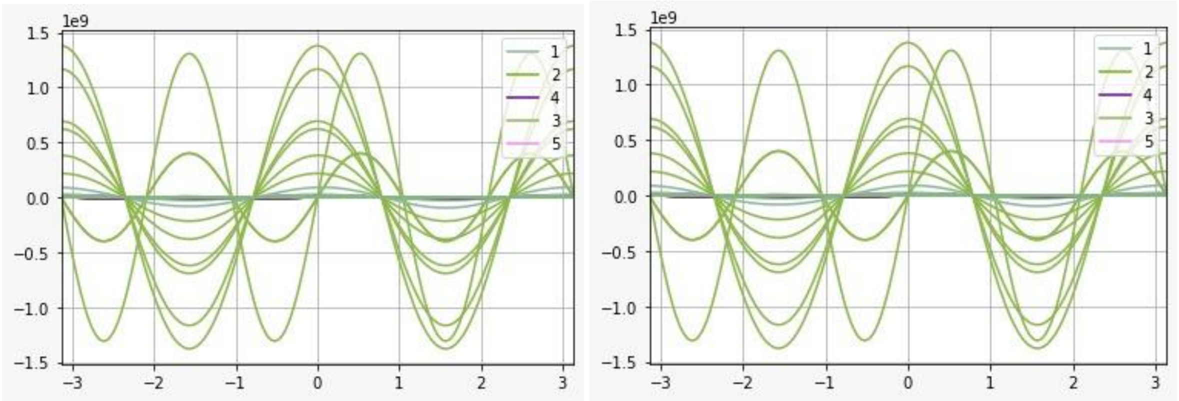

Fig. 4. NSL-41 and Normalized NSL-41 Andrew curve

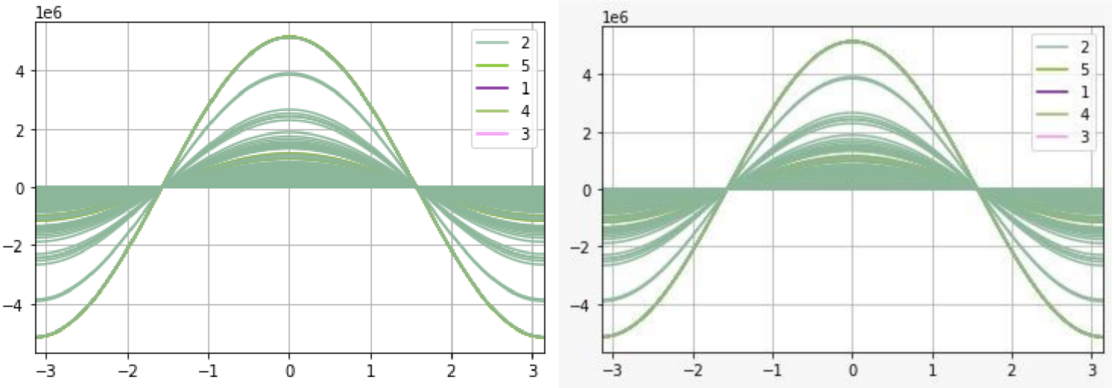

Fig. 5. KDD and Normalized KDD-19 Andrew curve

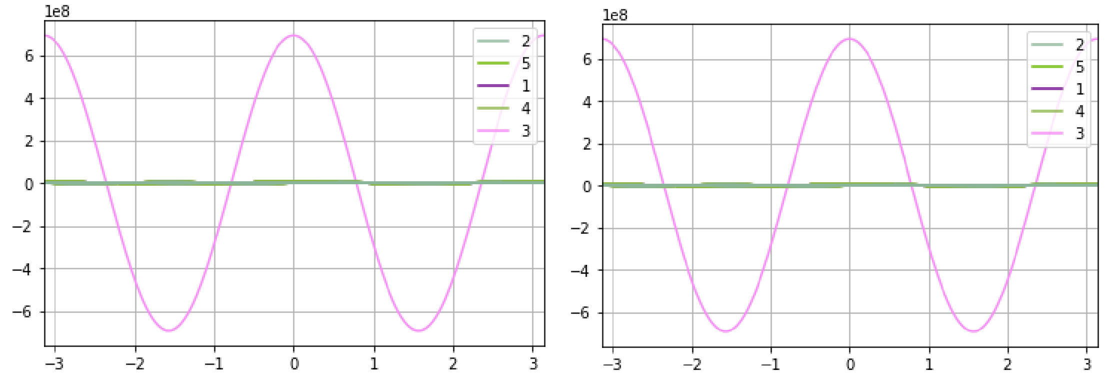

Fig. 6. KDD-41and Normalized KDD-41 Andrew curve

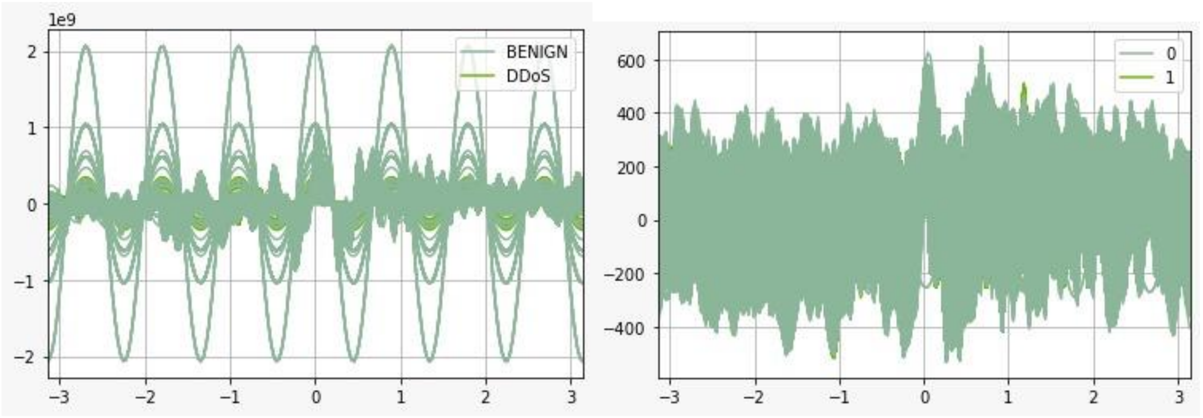

Fig. 7. CICIDS-2017 and Normalized CICIDS-2017 datasets Andrew curve

From Fig 2 to Fig 7, Andrew Bends applied on occasions utilizing the datasets. At long last, after seeing the Andrew bends of all the datasets, we can reason that the idea of the datasets is exceptionally non-direct.

5. RESULTS AND DISCUSSION

In this paper, we have added AI, and a few strategies have been carried out. Six calculations are utilized in this work: Naive Bayes, KNN, and SVM with FFSC and without FFSC. Result with Component Element Score (FFSC): Point-by-point depiction of the Train informational index, Number of traffic occurrences: 27686, Number of highlights: 63, Class names with Number of traffic examples in each: Assault - > 25186 and Harmless - > 2500. Nitty gritty depiction of the Test informational collection Number of traffic occasions: 12622, Number of elements: 63, Class marks with Number of traffic occasions in each: Assault - > 11606 and Harmless - > 1016, Created Andrew bends:

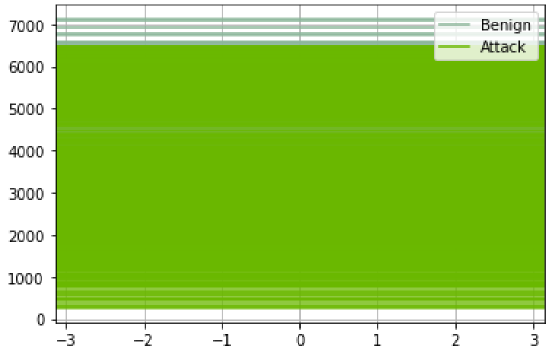

Fig. 8. FFSC dataset Andrew curves

Naive Bayes Results: Train dataset for: confusion matrix:

```
[[25186     0]
 [ 2500     0]]
```

Overall result:

- Accuracy -> 90.97016542656938, Precision -> 90.97016542656938, Recall -> 90.97016542656938, F-score -> 90.97016542656938

Class	Sensitivity	Specificity	Balanced a ccuracy
Attack	0.0	1.0	0.5
Benign	1.0	0.0	0.5

Classification Report

Class	Precision	Recall	F-1 Score	Support
Attack	0.9	1.00	0.95	25186
Benign	0.00	0.00	0.00	2500

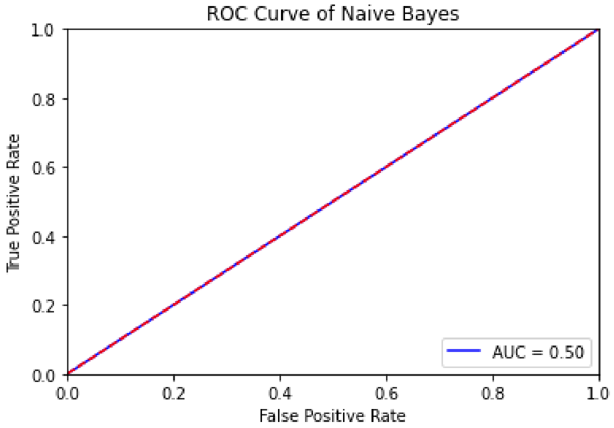

Fig. 9. Training data-set ROC curve for Naïve Bayes

Test dataset: confusion matrix:

```
[[11606     0]
 [ 1016     0]]
```

Overall result:

- Accuracy -> 91.95056250990335, Precision -> 91.95056250990335, Recall -> 91.95056250990335, F-score -> 91.95056250990335

Class	Sensitivity	Specificity	Balanced ac curacy
Attack	0.0	1.0	0.5
Benign	1.0	0.0	0.5

Classification Report

Class	Precision	Recall	F-1 Score	Support
Attack	0.91	1.00	0.95	25186
Benign	0.00	0.00	0.00	2500

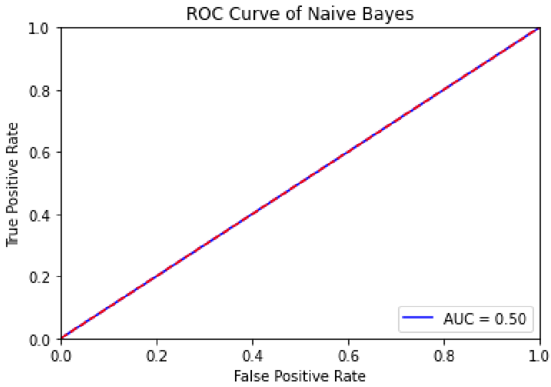

Fig. 10. Testing data-set ROC curve for Naïve Bayes

K Neighbors Classifier Results: n value -> 1

Train dataset for confusion matrix:

```
[[25186     0]
 [    0  2500]]
```

Overall result:

- Accuracy -> 100.0, Precision -> 100.0, Recall -> 100.0, F-score -> 100.0

Classification Report:

Class	Sensitivity	Specificity	Balanced accuracy
Attack	0.0	1.0	1.0
Benign	1.0	1.0	1.0

Class	Precision	Recall	F-1 Score	Support
Attack	1.00	1.00	1.00	25186
Benign	1.00	1.00	1.00	2500

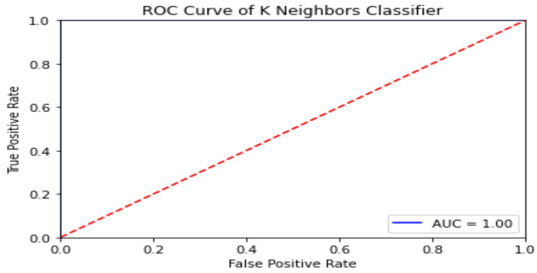

Fig. 11. Training data-set ROC curve for K Neighbors

Test dataset: confusion matrix:

```
[[10920   686]
 [  914   102]]
```

Overall result:

- Accuracy -> 87.32372048803676, Precision -> 87.32372048803676, Recall -> 87.32372048803676, F-score -> 87.32372048803676

Classification Report:

Class	Sensitivity	Specificity	Balanced accuracy
Attack	0.100394	0.940893	0.520643
Benign	0.940893	0.100394	0.520643

Class	Precision	Recall	F-1 Score	Support
Attack	1.00	1.00	1.00	25186
Benign	1.00	1.00	1.00	2500

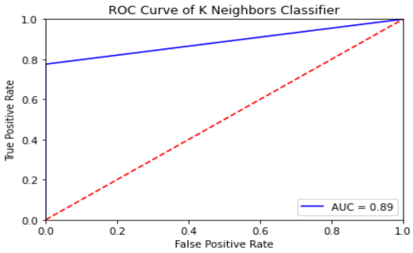

Fig. 12. Testing data-set ROC curve for K Neighbors

Support Vector Machine Results: Kernel selected -> RBF

Train dataset for confusion matrix:

```
[[25084   102]
 [  414  2086]]
```

Overall result:

- Accuracy -> 98.13624214404392, Precision -> 98.13624214404392, Recall -> 98.13624214404392, F-score -> 98.13624214404392

Classification Report:

Class	Sensitivity	Specificity	Balanced accuracy
Attack	0.83440	0.99595	0.915175
Benign	0.99595	0.83440	0.915175

Class	Precision	Recall	F-1 Score	Support
Attack	0.98	1.00	0.99	25186
Benign	0.95	0.83	0.89	2500

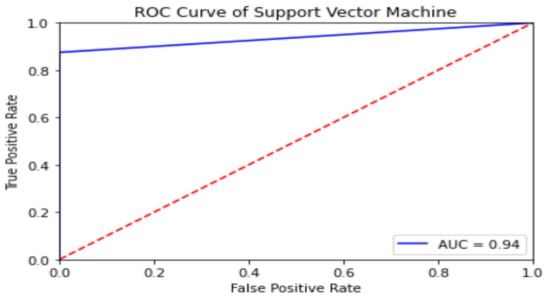

Fig. 13. Training data-set ROC curve for Support Vector Machine

Test dataset: confusion matrix:

```
[[11111   495]
 [  941    75]]
```

Overall result:

- Accuracy -> 88.623039138013, Precision -> 88.623039138013, Recall -> 88.623039138013, F-score -> 88.6 23039138013

Classification Report:

Class	Sensitivity	Specificity	Balanced accuracy
Attack	0.07819	0.957350	0.515584
Benign	0.957350	0.073819	0.515584

Class	Precision	Recall	F-1 Score	Support
Attack	0.98	1.00	0.99	25186
Benign	0.95	0.83	0.89	2500

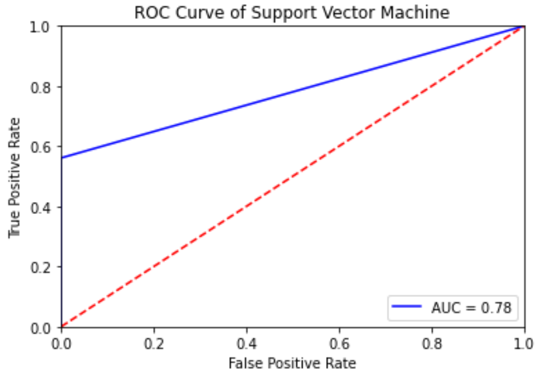

Fig. 14. Testing data-set ROC curve for Support Vector Machine

Decision Tree Entropy Results: Train dataset for confusion matrix:

```
[[24976   210]
 [  820  1680]]
```

Overall result:

- Accuracy -> 96.27970815574659, Precision -> 96.27970815574659, Recall -> 96.27970815574659, F-score -> 96.27970815574659

Classification Report:

Class	Sensitivity	Specificity	Balanced accuracy
Attack	0.672000	0.991662	0.831831
Benign	0.991662	0.672000	0.831831

Class	Precision	Recall	F-1 Score	Support
Attack	0.97	0.99	0.98	25186
Benign	0.89	0.67	0.77	2500

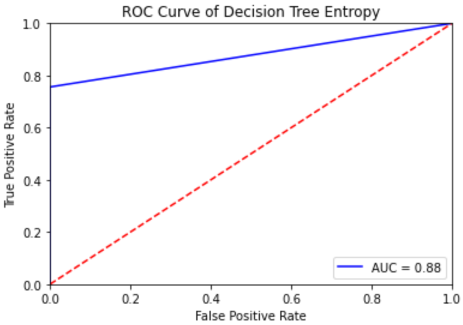

Fig. 15. Training data-set ROC curve for Decision Tree

Test dataset: confusion matrix:

```
[[11302   304]
 [ 1008     8]]
```

Overall result:

- Accuracy -> 89.60545080019014, Precision -> 89.60545080019014, Recall -> 89.60545080019014, F-score -> 89.60545080019014

Classification Report:

Class	Sensitivity	Specificity	Balanced accuracy
Attack	0.007874	0.973807	0.49084
Benign	0.973807	0.007874	0.49084

Class	Precision	Recall	F-1 Score	Support
Attack	0.97	0.99	0.98	25186
Benign	0.89	0.67	0.77	2500

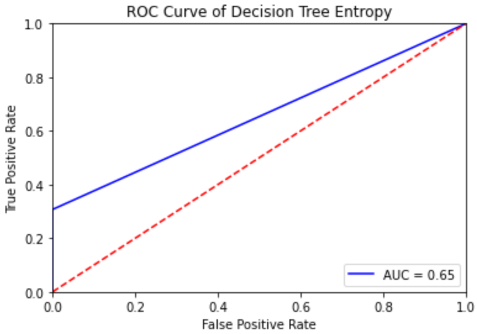

Fig. 16. Testing data-set ROC curve for Decision Tree entropy

Feature Score (FFSC) Train data set: Number of traffic instances: 27686, Number of features: 63, Class labels wit h number of traffic instances in each: Attack -> 25186, Benign -> 2500
Test Dataset: Number of traffic instances: 12622, Number of features: 63, Class labels with number of traffic instan ces in each: Attack -> 11606, Benign -> 1016
Generated Andrew curves without FFSC:

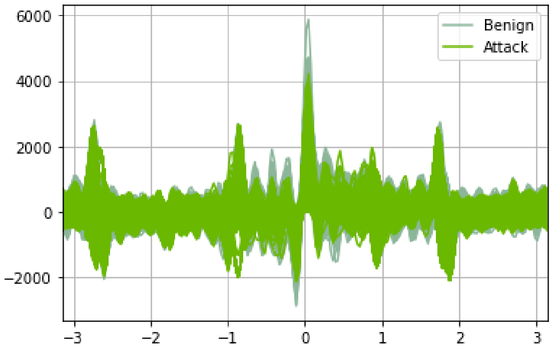

Fig. 17. Output generated without FFSC

Naive Bayes Results: Train dataset for: confusion matrix:

```
[[22420  2766]
 [   23  2477]]
```

Overall result:

- Accuracy -> 89.92631654988081, Precision -> 89.92631654988081, Recall -> 89.92631654988081, F-score -> 89.92631654988081

Classification Report:

Class	Sensitivity	Specificity	Balanced accuracy
Attack	0.990800	0.890177	0.940489
Benign	0.890177	0.990800	0.040489

Class	Precision	Recall	F-1 Score	Support
Attack	1.00	0.89	0.94	25186
Benign	0.47	0.99	0.64	2500

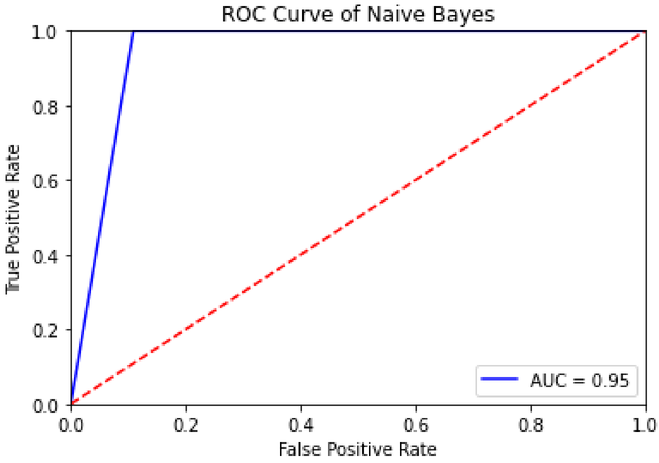

Fig. 18. Navie Bayes for training data-set without FFSC

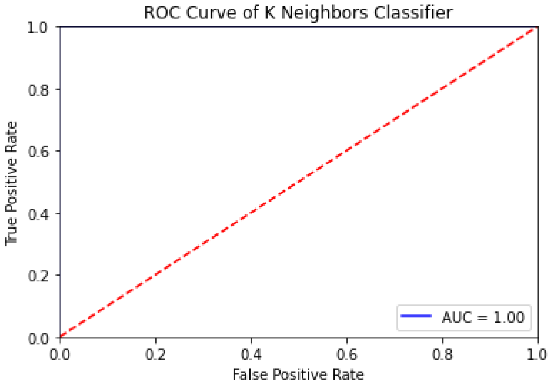

Fig. 19. K Neighbors Classifier for training data-set without FFSC

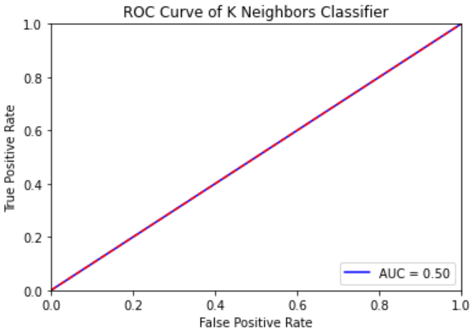

Fig. 20. K Neighbors Classifier for testing data-set without FFSC

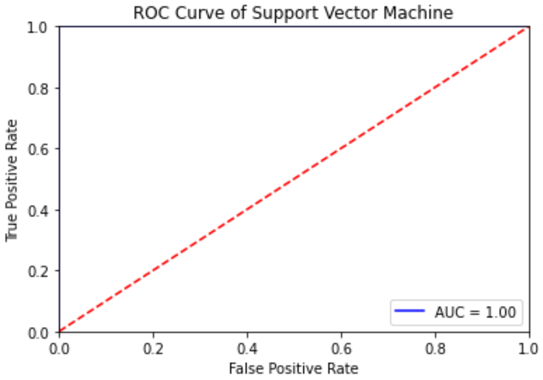

Fig. 21. Support Vector Machine for training data-set with out FFSC

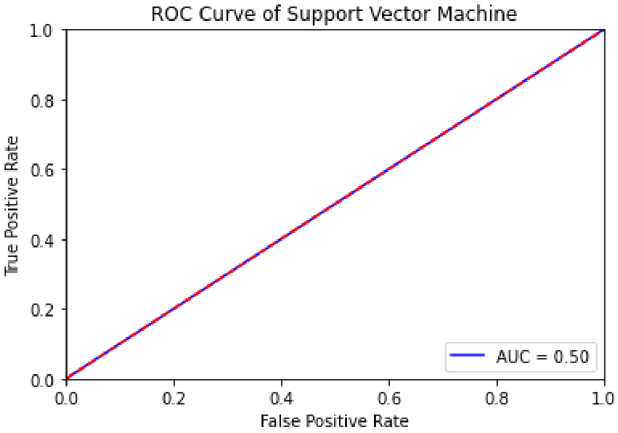

Fig. 22. Support Vector Machine for testing data-set with out FFSC

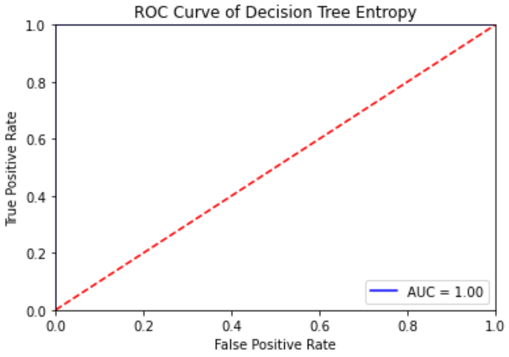

Fig. 23. Decision Tree for training data-set with out FFSC

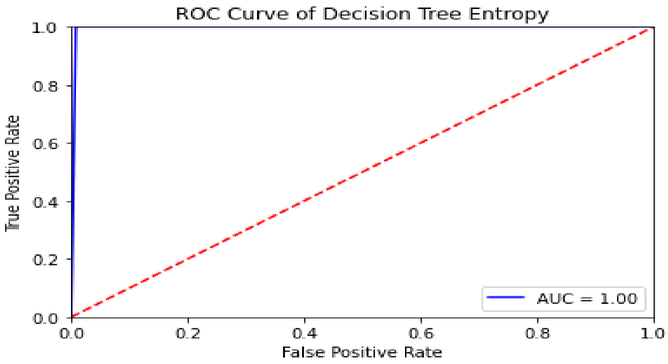

Fig. 24. Decision Tree for training data-set with out FFSC

6. CONCLUSION

The principal thought about the proposed methodology is to recognize low-rate DDoS attacks effectively by using a couple of stages, like pre-dealing with and incorporating decisions and requests. There is an assortment of subclassified assaults that must likewise be accurately distinguished. The proposed technique should give the most elevated levels of accuracy, review, and F-measure exactness. We suggest executing a web or versatile application to exhibit the learning model's carried-out functionality for better cognizance of the framework's activity. Utilizing different instruments and innovations like Carafe, Nodejs, HTML, CSS, Javascript, Precise, Bootstrap, Information base.

REFERENCES

1. Frederico A. F. Silveira,Agostinho de Medeiros Brito Junior,Genoveva Vargas-Solar, and Luiz F. Silveira, "Smart Detection: An Online Approach for DoS/DDoS Attack Detection Using Machine Learning",Volume 2019 |Article ID 1574749
2. Ivandro Ortet Lopes, Deqing Zou,Francis A Ruambo,Saeed Akbar, and Bin Yuan, "Towards Effective Detection of Recent DDoS Attacks: A Deep Learning Approach", Volume 2021 |Article ID 5710028
3. P. RENUKA ,Dr. B. BOOBA, Professor ,"Analysis on Detecting DDoS Attack in IoT Environment ",2018, ISSN : 0731-6755
4. Yuanyuan Wei; Julian Jang-Jaccard; Fariza Sabrina; Amardeep Singh; Wen Xu; Seyit Camtepe,"AE-MLP: A Hybrid Deep Learning Approach for DDoS Detection and Classification",IEEE Access (Volume: 9)
5. Zecheng He; Tianwei Zhang; Ruby B. Lee,"Machine Learning Based DDoS Attack Detection from Source Side in Cloud",2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud)
6. Muhammad Aamir &Syed Mustafa Ali Zaidi, "DDoS attack detection with feature engineering and machine learning: the framework and performance evaluation", Published: 11 April 2019
7. Isha Sood, Dr. Varsha Sharma, "Comparing Computational Intelligent Techniques forDDOS Attacksdetection", Vol.12 No.6(2021), 4774-4789
8. RojalinaPriyadarshini, Rabindra KumarBarik, "A deep learning based intelligent framework to mitigate DDoS attack in fog environment",24 April 2019
9. Kolawole Abubakar Sadiq, Aderonke Thompson, "Mitigating DDoS Attacks in Cloud Network using Fog and SDN: A Conceptual Security Framework", DOI:10.5120/ijais2020451877, August 2020

10. Swathi Sambangi,Lakshmeeswari Gondi, ”A Machine Learning Approach for DDoS (Distributed Denial of Service) Attack Detection Using Multiple Linear Regression”, 25 December 2020.
11. Er. Sakshi kakkar , Er. Dinesh kumar, “A Survey on Distributed Denial of Services (DDOS) “,Vol.5(3), 2014,3863-3866.
12. Nazrul Hoque; Dhruba K Bhattacharyya; Jugal K Kalita,”A novel measure for low-rate and high-rate DDoS attack detection using multivariate data analysis”, 2016 8th International Conference on Communication Systems and Networks.
13. Ankit Agarwal, Manju Khari & Rajiv Singh, “Detection of DDOS Attack using Deep Learning Model in Cloud Storage Application”, Wireless Pers Commun (2021).
14. Abdullah EmirCil, KazimYildiz, AliBuldu, “Detection of DDoS attacks with feed forward based deep neural network model”, Expert Systems with Applications ,Volume 169, 1 May 2021, 114520.
15. Abdul Raoof Wani , Q.P. Rana , U. Saxena , Nitin Pandey,” Analysis and Detection of DDoS Attacks on Cloud Computing Environment using Machine Learning Techniques “,2019 Amity International Conference on Artificial Intelligence (AICAI)
16. Thapanarath Khempetch, Pongpisit Wuttidittachotti,”DDoS attack detection using deep learning”,IAES International Journal of Artificial Intelligence (IJ-AI)Vol. 10, No. 2, June 2021, pp. 382~388 ISSN: 2252-8938, DOI: 10.11591/ijai.v10.i2.pp382-388.
17. Dasari, K.B., Devarakonda, N. (2022). Detection of TCP-based DDoS attacks with SVM classification with different kernel functions using common uncorrelated feature subsets. International Journal of Safety and Security Engineering, Vol. 12, No. 2, pp. 239-249. https://doi.org/10.18280/ijsse.120213.
18. Dasari, K.B., Devarakonda, N. (2022). TCP/UDP-based exploitation DDoS attacks detection using AI classification algorithms with common uncorrelated feature subset selected by Pearson, Spearman and Kendall correlation methods. Revue d'Intelligence Artificielle, Vol. 36, No. 1, pp. 61-71. https://doi.org/10.18280/ria.360107.
19. Dasari, K.B., Devarakonda, N. (2021). Detection of different DDoS attacks using machine learning classification algorithms. Ingénierie des Systèmes d’Information, Vol. 26, No. 5, pp. 461-468.
https://https://doi.org/10.18280/isi.260505.