VAWKUM Transactions on Computer Sciences
http://vfast.org/journals/index.php/VTCS@ 2024, ISSN(e): 2308-8168, ISSN(p): 2411-6335
Volume 12, Number 2, July-December 2024 *pp: 311-325*

Comprehensive Model Comparison for Intrusion Detection in UNR-IDD Dataset: Evaluating Naïve Bayes, Decision Tree, Random Forest, K-Neighbors, and LSTM

Muhammad Zulkifl Hassan [1], **Muhammad Zunnurain Hussain** [2*], **Muzzamil Mustafa** [3], **Muhammad Atif Yaqub** [4], **Hooria Umar** [5], **Hoor Fatima Yousaf** [2]

[1]Faculty of Information Technology University of Central Punjab, Lahore, 54000, Pakistan;
[2]Department of Computer Science, Bahria University Lahore Campus, Lahore, 54000, Pakistan;
[3]Department of Artificial Intelligence, University of Management & Technology Lahore Pakistan;
[4]Department of Computer Science, National College of Business Administration and Economics, Pakistan; [5]Software Developer

Keywords: *Intrusion Detection, UNR-IDD Dataset, Machine Learning, Naïve Bayes, Decision Tree, Random Forest, K-Neighbors (KNN), Long Short-Term Memory (LSTM).*

Journal Info:
Submitted:
October 08, 2024
Accepted:
December 19, 2024
Published:
December 31, 2024

Abstract

This paper compares the efficiency of five supervised learning algorithms, Namely Naïve Bayes, Decision Tree, Random Forest, K-Neighbors (KNN), and Long Short-Term Memory (LSTM) on intrusion detection using the UNR-IDD dataset. We analysed the results of the models considering the accuracy, precision, and F1-score. The Decision Tree, Random Forest, and LSTM models were also shown to be the best performers with scores of 1 for accuracy, F1-score, and area under the curve on the testing set. The Naïve Bayes yielded low standard error of 0.038165 but the precise values of precision at 0.773218 and F1-score at 0.872107 depict how the model contributed slightly fewer true positives but more false positives. From such outcomes obtained above, it is evident that Decision Tree, Random Forest and LSTM have high accuracy and appropriateness for this intrusion detection problem, although the accuracies of 100% are questionable because of the possibilities of over fitting. In terms of classification too, K-Neighbors has very good results and rarely misclassifies patterns. Despite this, Naïve Bayes is not the most suitable method in the present case for this particular dataset. This analysis also demonstrates the specific advantages and disadvantages of each model and gives the understanding of real-world usability of intrusion detection systems.

***Correspondence author email address:** Zunnurain.bulc@bahria.edu.pk
DOI: 10.21015/vtcs.v12i2.1929

1 Introduction

A Denial of Service (DoS) attack is a kind of cyber attack in which several attackers attack different network resources like servers or websites. Like other classes of attacks, a DDoS assault happens when vulnerabilities are taken advantage of. It is done by preventing the flow of automobiles on the road. It is more of a non- intrusive attack and that tells you that the attacker does not require any level of control of the resources in order to execute the attack. DDoS is an ability to attack targeted internet-based devices.

A bot, which is more than one bots, is used to launch an attack on the server or the website. However, if there are many requests at once, the functioning of the resources will be significantly worse due to their limitations, as well as the time required to process the requests for providing the services. Consequently, the natural stream of traffic may be barred from the services, which is the tenet of the Denial of Service in a DDoS attack[1].

The term "Distributed" in a Distributed Denial of Service (DDoS) attack is used to distinguish between this and the Denial of Service (DoS) attack. The attack emanates from several infected devices deployed systematically at different locations in the world network. Each bot in a botnet is a real device and reachable via a valid IP address on the Internet, therefore it is hard to tell between a malicious traffic and a legitimate one.

Table 1. Literature Survey

No	Author(s)	Year	Title	Source	Focus/ Keywords	Main Findings/Contributions
1	M, S.	2020	DDoS botnet attack on IoT devices	Kaggle	DDoS, Botnet, IoT	Dataset for DDoS botnet attacks on IoT devices. Provides data for analysis and model development in DDoS detection.
2	Tapadhir Das		UNR-IDD Intrusion Detection Dataset	Kaggle	Intrusion detection, IoT	Dataset for intrusion detection related to IoT devices. Useful for training and testing IDS models.
3	Hani Alshahrani	2021	Attacks and Targeted Layers in IoT	ResearchGate	IoT security, DDoS, Attack Layers	A diagrammatic representation of attack vectors and target layers within IoT systems, highlighting critical points for security implementation.
4	Vishwakarma, R. & Jain, A.K.	2019	A survey of DDoS attacking techniques and defense mechanisms in the IoT network	SpringerLink	DDoS, IoT, defense mechanisms, survey	Comprehensive survey on DDoS attack types and mitigation techniques, focusing on IoT environments.
5	Tripathi, N., et al.	2022	Application layer denial-of-service attacks and Defense Mechanisms: A Survey	ACM Computing Surveys	Application layer, DDoS, defense, survey	Extensive analysis of application-layer DDoS attacks and countermeasures, with emphasis on mitigating attacks in complex network architectures.

No	Author(s)	Year	Title	Source	Focus/ Keywords	Main Findings/Contributions
6	Gupta, B. B., Chaudhary, P., Chang, X., Nedjah, N., et al.	2022	Smart defense against distributed denial of service attack in IoT networks using supervised learning classifiers	Computers and Electrical Engineering	DDoS, IoT, machine learning, supervised learning	Proposes a machine learning-based approach using supervised classifiers to detect and mitigate DDoS attacks in IoT networks.
7	Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J.	2017	DDoS in the IoT: Mirai and other botnets	IEEE Computer	DDoS, Botnets, IoT	Discusses the infamous Mirai botnet attack and other similar botnets, focusing on their impact on IoT networks.
8	Osanaiye, O., Choo, K. K. R., & Dlodlo, M.	2016	Distributed denial of service (DDoS) resilience in cloud: Review and conceptual cloud DDoS mitigation framework	Journal of Network and Computer Applications	DDoS, Cloud Computing, resilience, mitigation framework	Proposes a conceptual framework for mitigating DDoS attacks in cloud environments, emphasizing resilience and scalability.
9	Adedeji, K. B., Abu-Mahfouz, A&. M., & Kurien, A. M.	2024	DDoS attack and detection methods in internet-enabled networks: Concept, research perspectives, and challenges	Journal of Sensors and Actuator Networks	DDoS, IoT, detection methods	Surveys detection methods for DDoS attacks in IoT networks, outlining emerging techniques and ongoing challenges.
10	Bensaid, R., Labraoui, N., Abba Ari, A. A., Maglaras, L., Saidi, H., Lwahhab, A. M. A., & Benfriha, S.	2024	Toward a real-time TCP SYN Flood DDoS mitigation using adaptive neuro-fuzzy classifier and SDN assistance in fog computing	Security and Communication Networks	DDoS, TCP SYN Flood, fog computing, neuro-fuzzy classifier	Presents an adaptive neuro-fuzzy classifier for mitigating TCP SYN Flood DDoS attacks, incorporating SDN assistance in fog computing environments.
11	Khozam, S., Blanc, G., Tixeuil, S., & Totel, E.	2024	DDoS mitigation while preserving QoS: A deep reinforcement learning-based approach	IEEE NetSoft	DDoS, QoS, deep reinforcement learning	Uses deep reinforcement learning to mitigate DDoS attacks while maintaining Quality of Service (QoS) in critical systems.
12	Wang, T., Xie, X., Zhang, L., Wang, C., Zhang, L., & Cui, Y.	2024	ShieldGPT: An LLM-based Framework for DDoS Mitigation	Asia-Pacific Workshop on Networking	DDoS, GPT, large language models, mitigation	Introduces a framework leveraging large language models for DDoS mitigation, enabling more sophisticated and adaptive countermeasures.

No	Author(s)	Year	Title	Source	Focus/ Keywords	Main Findings/Contributions
13	Xia, X., Chen, F., He, Q., Luo, R., Liu, B., Chua, C., Buyya, R.,& Yang, Y.	2024	EdgeShield: Enabling collaborative DDoS mitigation at the edge	IEEE Transactions on Mobile Computing	DDoS, edge computing, collaborative mitigation	Proposes a collaborative DDoS mitigation framework for edge computing environments, enhancing response time and resource efficiency.
14	Zhao, Z., Liu, Z., Chen, H., Zhang, F., Song, Z., & Li, Z.	2024	Effective DDoS mitigation via ML-driven in-network traffic shaping	IEEE Transactions on Dependable and Secure Computing	DDoS, traffic shaping, machine learning	Describes a machine learning-driven approach to shaping in-network traffic to mitigate DDoS attacks efficiently.
15	Zhou, Y., Cheng, G., Ouyang, Z., & Chen, Z.	2024	Resource-efficient low-rate DDoS mitigation with moving target defense in edge clouds	IEEE Transactions on Network and Service Management	DDoS, low-rate, moving target defense, edge clouds	Discusses resource-efficient DDoS mitigation strategies using moving target defense techniques in edge cloud environments.
16	Banoula, M.	2023	Naive Bayes classifier - machine learning	Simplilearn	Machine learning, Naive Bayes	Tutorial explaining the Naive Bayes classifier, a fundamental machine learning technique, with applications in classification tasks.

2 Distinction Of DDoS From DOS

The difference between DDoS and DoS can be summed up by the fact that where in a DoS attack, the arilist starts the attack using one device or even network a DDoS attack is started using several sources.

Every bot in the context of a botnet is a real node possessing a legitimate IP address on the Internet. This is why it is practically hard to differentiate the ill-favored traffic with the permissible traffic[2].

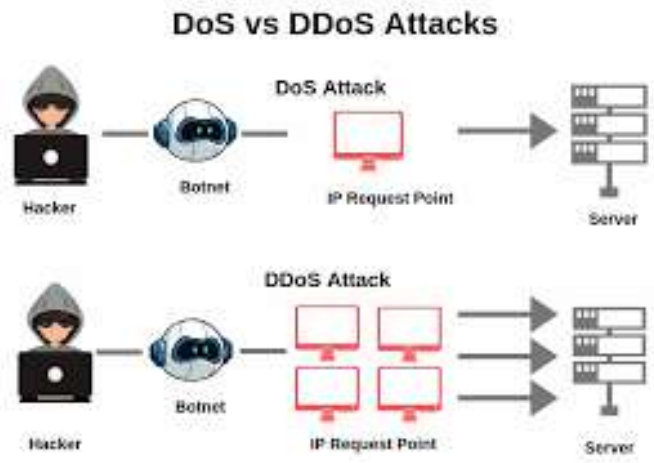

Figure 1. Diagram Showing Difference Between DDoS and Dos Attacks.

3 Working Of DDoS

Sources divers make numerous demands. A number of computers may be infected with malware to stage an attack and especially against any device connected to the Internet.

These floods of attacks interfere with the flow of traffic of the aspired resource and results into denial of services such as emails, websites and business related sites such as e-commerce sites [3].

The devices that have been infected and turned into tools for starting attack are called bots and a group of such bots is termed as botnet. Each bot is in fact a hacked device interacting with the Internet; it has a genuine Internet Protocol or IP address, thus it cannot really be singled out or differentiated from harmless Internet traffic.

It is often when a targeted resource is flooded with a constant influx of requests beyond its recommended limits that it ceases to provide services to authorized or 'normal' traffic pa. It seems to be more like a traffic jam [4].

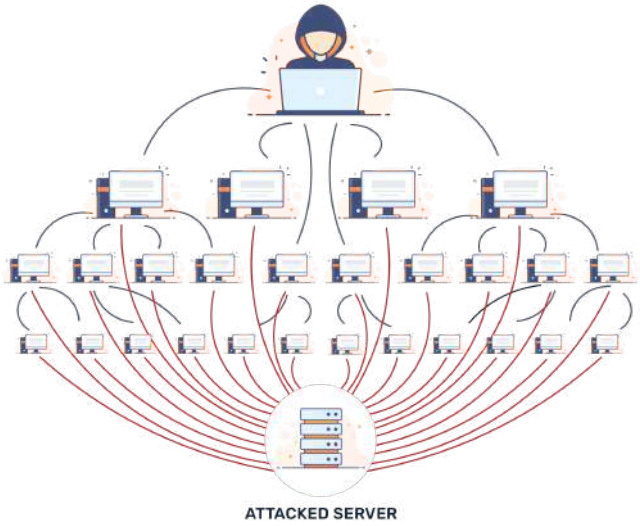

Figure 2. Server Attacked Using DDoS

4 Detection Of DDoS Attack

DDoS attacks, which include employment of bots with legitimate IP addresses may be detected by watching for high levels of traffic channeling from a single source or through an IP address.

The other sign may be an unprecedented rise in requests for using a particular commodity, be it a site or a server.C. Abnormal traffic may be detected by observing the increase in a specific resource usage at fixed time intervals. high levels of traffic originating from a single source or IP address.

Another indicator may be a rapid surge in the demands for a certain resource, such as a website or a server [5].

Abnormal traffic may be identified by monitoring the sudden increases in activity at precise intervals of a particular resource. If there is an irregularity in the normal flow of activities it may actually be due to a Distributed Denial of Service (DDoS) attack.

5 Types Of DDoS Attack

DDoS attacks specifically target Internet of Things resources, whereas other forms of Denial of Service attacks concentrate on different levels of the OSI model.

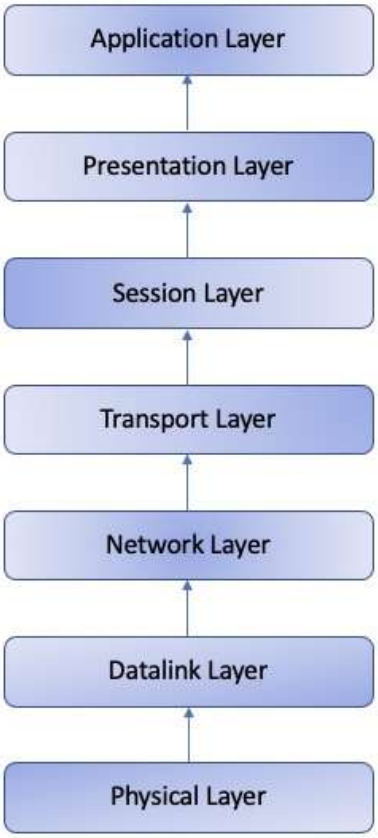

Figure 3. OSI Model

Application Layer assault: This refers to an assault that targets the seventh layer of the OSI Model, known as the Application Layer. This attack involves rendering the resources of an application inaccessible to authorized users by overwhelming the program with an excessive number of requests for resource consumption.

An HTTP Flood Attack is a kind of Application Layer Attack where the server is overwhelmed by repeatedly sending a large number of HTTP requests [6].

Protocol attacks, also known as state exhaustion attacks, target the Network Layer and Transport Layer of the OSI (Open System Interconnection) Model. This attack involves the excessive use of network resources, such as servers, firewalls, or load balancers, at the targeted source.

SYN Flood: This is an attack where the attacker sends a large number of "Initial Connection Requests" SYN packets during a TCP handshake. This approach employs a falsified IP address of the source.

Volumetric assaults involve depleting the target's bandwidth. The whole bandwidth between the target and the Internet is fully used by transmitting a substantial volume of data, using amplification techniques, or generating a significant quantity of traffic by other methods.

DNS Amplification is a kind of attack that involves the use of the target's IP address. The attacker generates a falsified IP address that matches the IP address of the intended source, and then inundates the target's IP address with an overwhelming volume of answers from the server [7].

Figure 4. Types of DDoS Attacks

6 Hazards Of DDoS Attacks

DDoS (Distributed Denial of Service) attacks pose challenges in both identification and mitigation. Due to the attacker's use of tactics that obfuscate the malicious data, distinguishing it from regular traffic becomes challenging, resulting in significant potential for harm. For many firms, this might result in significant financial losses, since they cannot afford to restrict all traffic to their resources. Several techniques are used to avoid or reduce the impact of assaults [8].

(A) Can firewalls be utilized? firewalls may also fall prey to similar assaults, rendering them ineffective in distinguishing between malicious traffic and approved or regular traffic. Therefore, they are insufficient on their own to effectively address the risks posed by DDoS assaults. Load balancers and other forms of IPS (Intrusion Prevention System) devices are incapable of guaranteeing network availability.

(B) B.DDoS assaults have grown more prevalent in cloud computing due to the widespread use of this technology by enterprises.

7 Mitigation Of DDoS Attacks

Managing DDoS is not an easy task. There are tools which are used to be as an antidote or reducer to the DDoS attacks. These services depend on various factors like:

1. Scalability: The services should be scalable enough to accommodate the growing needs of the enterprises and the growing waves of DDoS attacks.
2. Flexibility: The threats also need to be scanned and evaluated as they occur in order to let the client know the status of the website's functioning. In order to manage and resolve threats, flexibility is evident and required.
3. Reliability: Mitigation services need to be available and functioning properly right from the start of a DDoS (Distributed Denial of Service) attack.
4. Network Size: Contrary to this view, the size of the network itself predicts the success of mitigation services. It also becomes clear that the response time of the mitigation service elevates as the number of nodes in the network scales up.

8 Prevention Of DDoS On Cloud

An Approach Toward Safeguarding The Cloud Against Ddos Attacks Is Employing A Cloud Ddos Protection Service.Tion. These Services Apply A Combination Of Tools Such Hardware And Software Like Firewalls, Ids/Ips, Traffic Analyzer Etc That Scans The Traffic And Prevents Malicious Traffic From Getting Into The Servers Or Networks. Besides, Thes E Systems Have The Features That Allow For Their Real-Time Streaming And Reporting And Their Ability To Block Any Offending Communication. Cite Recent Findings, Works, Or Studies Have Brought Out That

Cloud Based Ddos Protection Systems Had The Potential Of Identifying Such Attacks & Overcome Them And Thus Greatly Reducing The Impact That A Particular Ddos Assault Posed To A Particular Resource.

With A Cdn, We May Perhaps Spread The Traffic Across Several Servers, And This May Perhaps Make It More Challenging For Would Be Attackers To Overload A Server Or Network. Ddos Attack May Also Be Reduced By This Strategy Since The Targeted Website Traffic Is Spread Across Many Sites. From The Current Studies It Is Evident That Cdn Is Capable Of Handling Ddos Attacks And/Or Reduce The Impact To The Targeted Resources.C. Cloud Providers Use The Virtual Private Cloud (Vpc) To Created Subnets Of Your Network, And Limit Exposure Of Your Resources To The Internet.Nd Software, Including Firewalls, Intrusion Detection And Prevention Systems, And Traffic Analyzers, To Detect And Block Harmful Traffic Before It Reaches The Intended Server Or Network. Additionally, These Systems Have The Capability To Monitor And Report In Real-Time, As Well As Automatically Block Any Communication That Is Deemed Suspicious. Research Has Shown That Cloud-Based Ddos Protection Systems Had The Capability To Accurately Identify And Counteract Ddos Assaults, Therefore Substantially Minimizing The Adverse Effects Of An Attack On The Specific Resources Being Attacked [9][10].

By Using A Content Delivery Network (Cdn), We May Effectively Divide Traffic Across Several Servers, Hence Increasing The Level Of Difficulty For Potential Attackers To Overwhelm A Single Server Or Network. This Strategy May Also Mitigate The Effect Of A Ddos Attack By Dispersing The Traffic Across Many Sites. Research Has Shown That Content Delivery Networks (Cdns) Are Capable Of Efficiently Mitigating Distributed Denial Of Service (Ddos) Assaults And Minimizing The Impact On The Specific Resources That Are Being Attacked.

Cloud Providers Use The Virtual Private Cloud (Vpc) To Partition Your Network And Restrict The Vulnerability Of Your Resources To The Internet. The Adoption Of This Strategy May Well Serve To Reduce The Thinenddate That Might Be Targeted By Prospective Adversaries, Thereby Raising The Level Of Challenge That Such Parties Would Face In Identifying Specific Targets Of Opportunity [11]. Several Studies In The Problem Area Have Indicated That Vpcs Can Effectively Mitigate Ddos Attacks By Limiting The Exposure Of Resources To The Internet And The Surface Of The Attack.D. Ddos Attack Mitigation Consists Of A Firewalling Mechanism That May Have Been Configured To Limit Or Block Traffic From Certain Compromised Ip Addresses Or Blocks Of Them, Or Limit The Quantity Of Connections From A Specific Ip Address.Systems, And Traffic Analyzers, To Detect And Block Harmful Traffic Before It Reaches The Intended Server Or Network. Additionally, These Systems Have The Capability To Monitor And Report In Real-Time, As Well As Automatically Block Any Communication That Is Deemed Suspicious. Research Has Shown That Cloud-Based Ddos Protection Systems Had The Capability To Accurately Identify And Counteract Ddos Assaults, Therefore Substantially Minimizing The Adverse Effects Of An Attack On The Specific Resources Being Attacked[12].

Ddos Attack Mitigation Involves Using A Firewall That May Be Customized To Restrict Or Limit Traffic From Certain Ip Addresses Or Ranges, As Well As To Restrict The Number Of Connections From A Single Ip Address. Firewalls Have Proven Style Of Blocking Ddos Soruces And Getting Rid Of Dangerous Traffic From The Network.

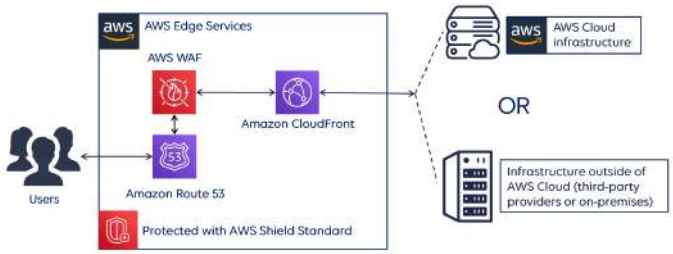

Figure 5. Example of AWS Cloud

9 Dataset Of DDoS

(A) Data Preprocessing: We have performed data processing on the datasets to accomplish the following tasks:
   1. Eliminate null values or discard columns that contain only one value.

(B) Remove categorical columns that have just one dominant category.

(C) Remove columns that have above 50% missing data.

(D) Remove rows that have missing values in a column exceeding 5%.

We used the dataset supplied via Kaggle. The dataset has a grand total of 83 columns.

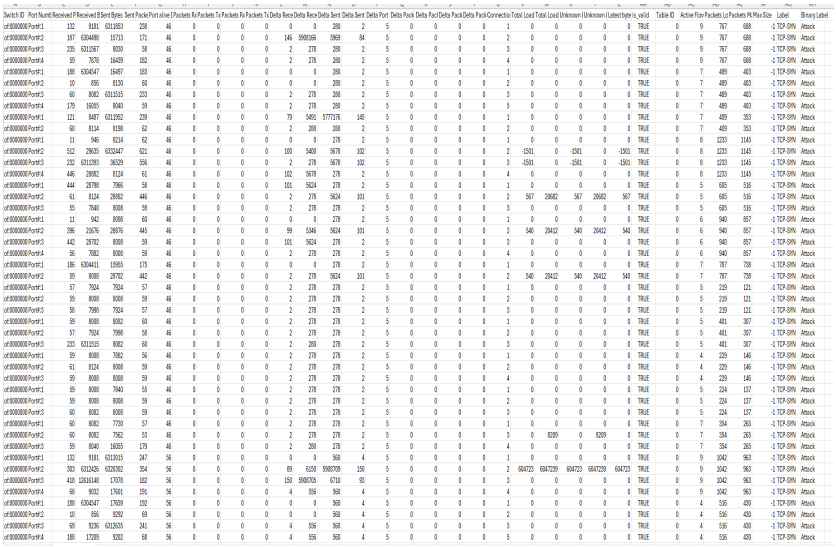

Figure 6. Dataset of DDoS

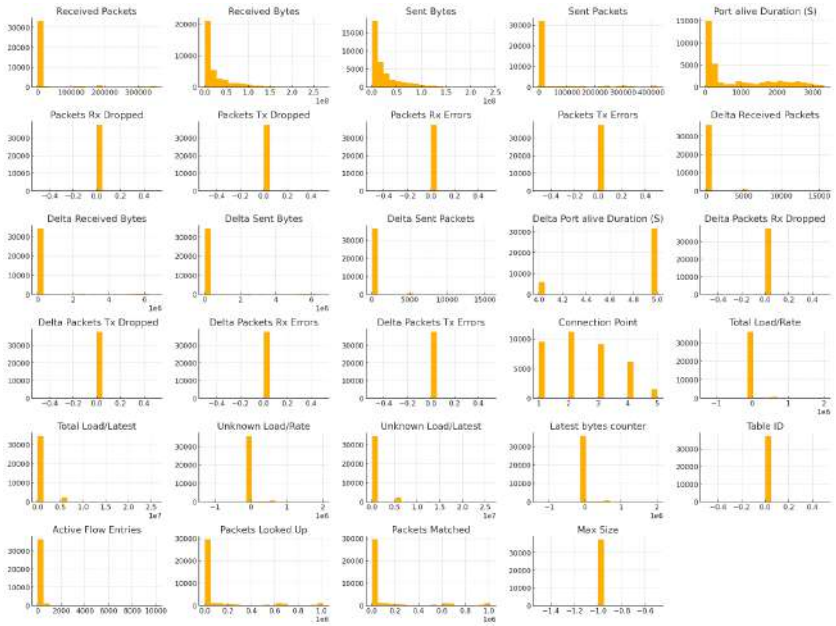

Figure 7. Bar Graph for all feilds

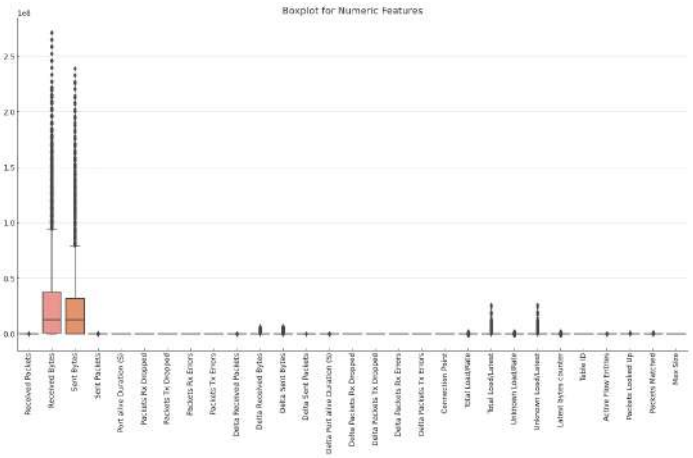

Figure 8. Box Plot for features

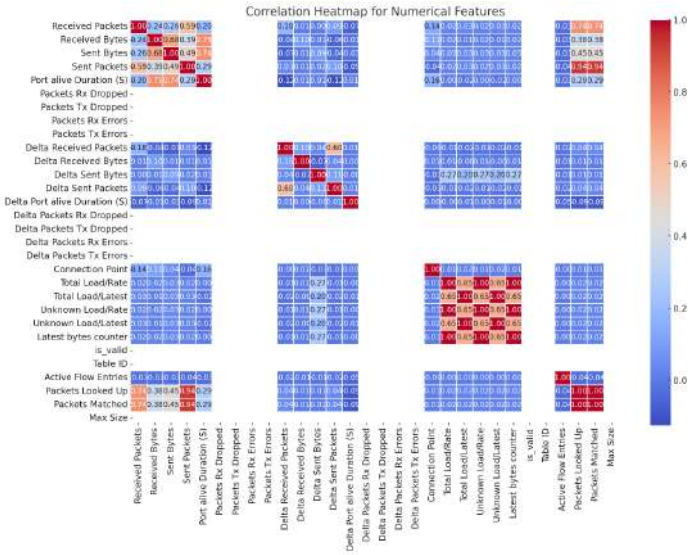

Figure 9. Correlation Matrix

Table 2. Model Comparison

	Model	Accuracy
0	Naïve Bayes	0.971936
1	Decision Tree	1.000000
2	Random Forest	1.000000
3	K-Neighbors	0.999733

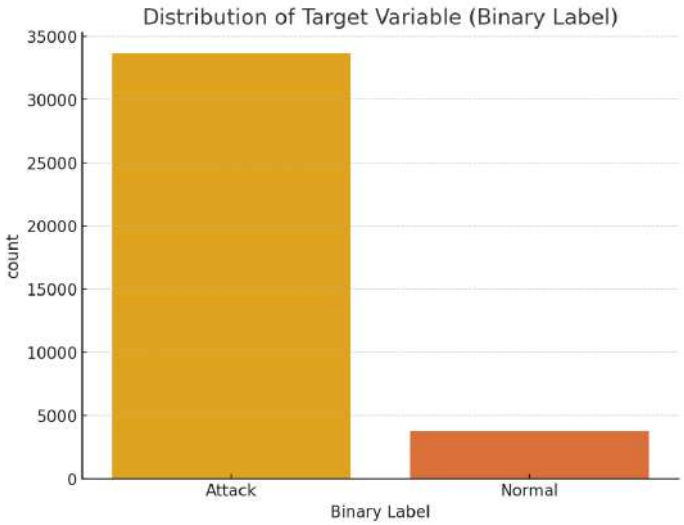

Figure 10. Target VaVariables (Binary Label)

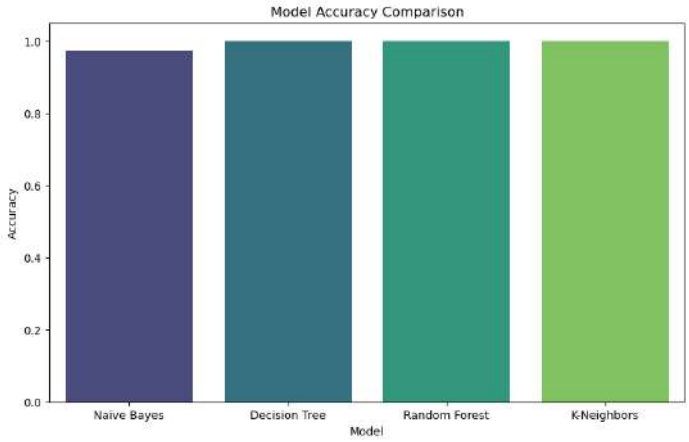

Figure 11. Model Accuracy Comparison

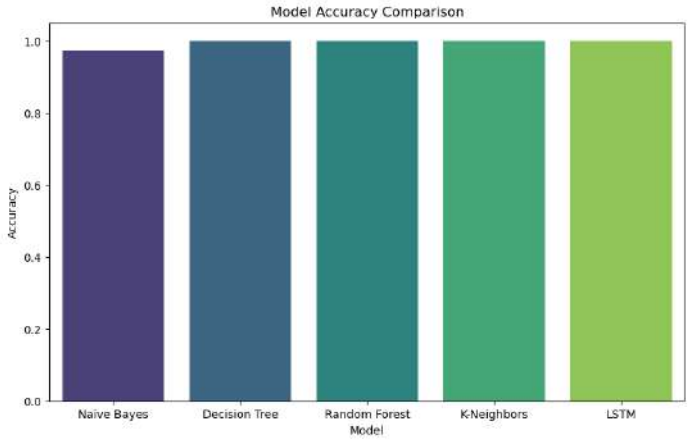

Figure 12. Model Accuracy Comparison

Table 3. Model Comparison

	Model	Accuracy	Precision	F1-Score
0	Naïve Bayes	0.971936	0.773218	0.872107
1	Decision Tree	1.000000	1.000000	1.000000
2	Random Forest	1.000000	1.000000	1.000000
3	K-Neighbors	0.999733	1.000000	0.998601
4	LSTM	1.000000	1.000000	1.000000

The provided Model Comparison offers a detailed evaluation of five different machine learning models: The machine learning algorithms that are used in this project include Naïve and Bayes, Decision Tree, Random Forest, K-Neighbors (KNN) and Long Short Term (LSTM). Each model has been evaluated based on three key metrics: Accuracy, Precision, and F1 Score metrics all are formulated in the same way as defined above with different parameters.Let's break down each metric and explain the table:

Accuracy is calculated as the percentage of total rightful predictions of the outcomes among all the inputs to the model. It is by far the simplest method of evaluating the model's performance, but it may not be the best method when the data set has a diverse distribution. In this case: Decision Tree, Random Forest, and LSTM had 1.000 in accuracy which means these algorithms classified all instances of the test set correctly [13].

K-Neighbors also had high accuracy of 0.999733 suggesting that very small number of observations were misclassified. Regardless, naïve Bayes performed rather well with an accuracy of 0.971936 but still slightly lower than the other models. This can be attributed to the fact that Naïve Bayes make the assumption that features are independent and this assumption might not be valid in case of this dataset.

Precision the ratio of accurate positive predictions made by the model in relation to all the positive predictions made by the model with regard to the actual class. It derives from the aspect of how right the positive classifications are. Overall higher degree of accuracy can results in fewer false alarms. In this case: All the positive predictions of each model were correct since the models scored a perfect precision of 1.000 for Decision Tree, Random Forest, K-Neighbors, and LSTM.

Naïve Bayes produced a precision of 0.773218; this shows that Naïve Bayes model's high number of TP indicates that while it correctly identified many actual positives, it also marked several actual negatives as positives than the other models.

The F1-score is the harmonic mean of precise and recall so nothing really since exists, it just provides a better metric for unbalanced datasets or those where we care about both false positives false negatives. This is important because it considers two measures: precision and recall, and delivers one measure that comprehensively encompasses these two parameters. In this case: The best results were achieved by Decision Tree, Random Forest, and LSTM with F1-score of 1.000 which means that there were no false posiitives and false negatives [14][15].

K-Neighbors had impressive F1-score of 0.998601 thus implying that the model had effortlessly categorized all the instances. Naïve Bayes yielded an F1-score of 0.872107 which, though is not as high as the other models, is quite good.

The results of the experiment show that Naïve Bayes has slightly lower accuracy, precision, recall rate and F1-measure compared to the other models. The new model has an accuracy of 0.971936 and an F1-score of 0.872107, which proves it is still a feasible model; however, the lower value of precision, 0.773218, indicates that the model provided more false positives.

In terms of scores, Accuracy, Precision, and F1-score model Decision Tree, Random Forest, and LSTM all performed with zeros for both datasets. This means that these models were extensively accurate in assigning the

test data into the respective classes without an error, which can well explain overfitting. Baseline-K was almost perfect with the highest F1-score of 0.998601, which showed that K-Neighbors classified almost all the instances as positive instances.

Thus, Decision Tree, Random Forest, and LSTM are the best models, and K-Neighbors model exhibits good results a little worse F1-score. Decision tree algorithm was not utilized due to longer training time, but its precision was quite poor and F1 score was even worse and proved that this model is might not suitable for this kind of dataset.

While the result shows that Decision Tree, Random Forest, and LSTM models achieve an accuracy of 100 percent, such values are often considered as an overfitting [16]. This may be due to the characteristics of the dataset, or restricted variation in test parameters. To corroborate such conclusions, the use of cross-validation methods which includes k fold cross validation should be used to check validity across different data splits. Further research should also be conducted with the aim of verifying how these models work in practice when they are evaluated on completely different data samples."

10 Conclusion

In this broad comparative analysis, we compared the five machine learning models on the UNR-IDD dataset for the intrusion detection feature. Decision Tree, Random forest and LSTM were ranked as top performing model based on accuracy, precision, and F1score metrics, as these models obtained an accolade of score results equal to 1.000. This implies that these models where very efficient in feeding into the dataset and where able to classify the instances without any mistake. However, the perfect scores also give an indication of overfitting especially in Decision Trees which lack generalization settings.

Another algorithm that showed great results was K-Neighbors (KNN), which had an accuracy of 99.9733% and the F-measure of 0.98601% which also means the program has very low error rate and it classifies the data very well. Nevertheless, Naïve Bayes yielded relatively high accuracy, 0.971936, but lower precision, 0.773218, which indicated that this tool had more false positives. This might be due to feature independence, an assumption used in construction of this algorithm, failing to operate well given the dataset at hand.

The outcome shows that Decision Tree, Random Forest, and LSTM are indeed powerful models for this particular intrusion detection problem. K-Neighbors has a good performance as well and Naïve Bayes is still a contender for situations when computational complexity or simplicity is the issue. However, these are issues of overfitting and the need to generalize the model best understood in cases where the score is already one hundred percent. Because of this, high perfect scores for all the algorithms namely Decision Tree, Random Forest, and LSTM means they are the best algorithms in terms of classification ability but also signifies that the model has learned the data input-output correlation too well and may result to overfitting. In real life functioning of the model there are chances that an overfitting model is not able to recognize new kind of attacks which violates the security of the network. Hence, implementing these models should involve scheduling of data updating and checking on new data sets to measure the predictive accuracy. Some of the practical uses in relation to computational usage includes; In the use of these models in enterprise level intrusion detection systems practicality involves a comparison of simpler models such as Naïve Bayes to complex models like LSTM.-hidden Layers.

Author Contributions

Muhammad Zulkifl Hasan: Conceptualization, Methodology,moi[. **Muhammad Zunnurain Hussain**: Supervision, Data curation.**Muzammil Mustafa**: Visualization, Investigation. **Waqas Ali**: Software, Validation. **Muhammad Atif Yaqub**: Writing- Reviewing and Editing **Hooria Umar** Writing- Original draft preparation. **Hoor Fatima Yousaf** Software, Reviewing and Editing.

Compliance with Ethical Standards

It is declared that all authors don't have any conflict of interest. It is also declared that this article does not contain any studies with human participants or animals performed by any of the authors. Furthermore, informed consent was obtained from all individual participants included in the study.

References

[1] M, S. (2020) DDoS botnet attack on IOT devices, Kaggle. Available at: https://www.kaggle.com/datasets/siddharthm1698/ddos-botnet-attack-on-iot-devices

[2] UNR-IDD Intrusion Detection Dataset (no date) Kaggle. Available at: https://www.kaggle.com/datasets/tapadhirdas/unridd-intrusion-detection-dataset

[3] Attacks and targeted layers in IOT. | download scientific diagram (2021). Available at: https://www.researchgate.net/figure/Attacks-and-Targeted-Layers-in-IoT_fig3_350595140

[4] Vishwakarma, R. and Jain, A.K. (2019) A survey of ddos attacking techniques and defence mechanisms in the IOT network - telecommunication systems, SpringerLink. Springer US. Available at: https://link.springer.com/article/10.1007/s11235-019-00599-z .

[5] Nikhil Tripathi Fraunhofer Institute for Secure Information Technology et al. (2022) Application layer denial-of-service attacks and Defense Mechanisms: A Survey: ACM Computing Surveys: Vol 54, no 4, ACM Computing Surveys. Available at: https://dl.acm.org/doi/abs/10.1145/3448291

[6] panelB.B.GuptaabcdPersonEnvelopePoojaChaudharyaXiaojunChangeNadiaNedjahf, A.links open overlay et al. (2022) Smart defense against distributed denial of service attack in IOT networks using supervised learning classifiers, Computers & Electrical Engineering. Pergamon. Available at: https://www.sciencedirect.com/science/article/abs/pii/S0045790622000404

[7] Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J. (2017). DDoS in the IoT: Mirai and other botnets. Computer, 50(7), 80-84. https://doi.org/10.1109/MC.2017.201.

[8] Osanaiye, O., Choo, K. K. R., & Dlodlo, M. (2016). Distributed denial of service (DDoS) resilience in cloud: Review and conceptual cloud DDoS mitigation framework.*Journal of Network and Computer Applications*, 67, 147-165. https://doi.org/10.1016/j.jnca.2016.01.001).

[9] Adedeji, K. B., Abu-Mahfouz, A. M., & Kurien, A. M. (2024). DDoS attack and detection methods in internet-enabled networks: Concept, research perspectives, and challenges.*Journal of Sensors and Actuator Networks*, 12(4), 51.

[10] Bensaid, R., Labraoui, N., Abba Ari, A. A., Maglaras, L., Saidi, H., Abdu Lwahhab, A. M., & Benfriha, S. (2024). Toward a real-time TCP SYN Flood DDoS mitigation using adaptive neuro-fuzzy classifier and SDN assistance in fog computing. Security and Communication Networks, 2024, 1–20. https://doi.org/10.1155/2024/6651584

[11] Khozam, S., Blanc, G., Tixeuil, S., & Totel, E. (2024). DDoS mitigation while preserving QoS: A deep reinforcement learning-based approach. 2024 IEEE 10th International Conference on Network Softwarization (NetSoft), 369–374.

[12] Wang, T., Xie, X., Zhang, L., Wang, C., Zhang, L., & Cui, Y. (2024). ShieldGPT: An LLM-based Framework for DDoS Mitigation. Proceedings of the 8th Asia-Pacific Workshop on Networking, 108–114.

[13] Xia, X., Chen, F., He, Q., Luo, R., Liu, B., Chua, C., Buyya, R.,& Yang, Y. (2024). EdgeShield: Enabling collaborative DDoS mitigation at the edge.*IEEE Transactions on Mobile Computing*, PP(99), 1–12. https://doi.org/10.1109/tmc.2024.3443260

[14] Zhao, Z., Liu, Z., Chen, H., Zhang, F., Song, Z., & Li, Z. (July-Aug 2024). Effective DDoS mitigation via ML-driven in-network traffic shaping.*IEEE Transactions on Dependable and Secure Computing*, 21(4), 4271–4289. https://doi.org/10.1109/tdsc.2023.3349180

[15] Zhou, Y., Cheng, G., Ouyang, Z., & Chen, Z. (2024). Resource-efficient low-rate DDoS mitigation with moving target defense in edge clouds. *IEEE Transactions on Network and Service Management*, PP(99), 1–1. https://doi.org/10.1109/tnsm.2024.3413685.

[16] Banoula, M. (2023) Naive Bayes classifier - machine learning [updated]: Simplilearn, Simplilearn.com. Simplilearn. Available at: https://www.simplilearn.com/tutorials/machine-learning-tutorial/naive-bayes-classifier