International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 02 Issue: 04 April 2024
Page No: 930 - 937
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2024.0130

Enhancing DDoS Attack Detection and Network Resilience Through Ensemble-Based Packet Processing and Bandwidth Optimization

Amit Dogra[1], Taqdir[2]

[1]Research Scholar, Department of Computer Science and Engineering at SoET, BGSB University Rajouri (J&K), India.

[2]Assistant Professor Guru Nanak Dev University, R/C Gurdaspur, India.

Emails: *amitdogra004@gmail.com[1], taqdir_8@rediffmail.com[2]*

Abstract

It is critical to identify Distributed Denial of Service (DDoS) attacks to preserve network integrity and guarantee continuous service delivery. Our research suggests a novel way to lower the network's packet drop ratio and improve the accuracy of DDoS attack detection. Conventional techniques occasionally just use anomaly detection or signature-based detection, which might not be sufficient to protect against DDoS assault schemes that are always changing. To increase the precision and resilience of DDoS detection, our system incorporates several detection strategies, such as signature-based, anomaly-based, and machine learning-based techniques. Additionally, we use network traffic analysis and anomaly detection tools to quickly discover and block harmful traffic patterns. During suspected DDoS attempts, we dynamically modify network parameters and reroute data to reduce the packet drop ratio and maintain service for authorized users. Additionally, our system has feedback systems that allow us to continuously adjust and improve detection algorithms, improving the overall dependability and effectiveness of DDoS attack detection. We illustrate how successfully our method lowers packet drop ratios and strengthens network resilience against DDoS attacks using both simulation and real-world experience.

Keywords: *DDOS attack; Packet Drop Ratio; Reliability; Machine Learning; Accuracy; Bandwidth*

1. Introduction

Network service availability and dependability are critical in today's networked digital world. However, maintaining uninterrupted service delivery has grown more difficult due to the rise of cyber threats, especially Distributed Denial of Service (DDoS) attacks (Yang et al., 2020). The goal of denial-of-service (DDoS) attacks is to flood a target system or network with malicious traffic, making it unusable by authorized users. Therefore, minimizing the effects of DDoS assaults and protecting network resources depend on the prompt and precise identification of such attacks (Balkanli et al., 2014). Conventional DDoS attack detection techniques frequently depend on anomaly-based detection, which highlights departures from typical network behavior, or signature-based detection, which identifies established attack patterns (Li et al., 2019a). Although these methods have shown some degree of success, they frequently fail to identify complex and novel DDoS assault techniques. Furthermore, these systems are vulnerable to evasion strategies used by attackers because to their dependence on static thresholds and predetermined signatures (Li et al., 2019b). In order to overcome these drawbacks and improve DDoS attack detection accuracy, more sophisticated and flexible detection techniques are becoming increasingly necessary. Reducing the network's packet drop ratio is one viable strategy that could lessen the effect of DDoS assaults on traffic that is lawful (Saini et al., 2020). This strategy seeks to identify and lessen DDoS attacks while maintaining continuous service delivery by utilizing machine learning algorithms, dynamic network reconfiguration techniques, and real-time traffic analysis. The context for discussing the difficulties in detecting DDoS attacks and the importance of lowering packet loss ratio as a metric for improving dependability is established in this introduction. It

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 02 Issue: 04 April 2024
Page No: 930 - 937
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2024.0130

describes the drawbacks of current detection techniques and emphasizes the need for a more proactive and flexible approach to DDoS defense (Idhammad et al., 2018a). The overall objective of this study is to improve network resilience against DDoS attacks by delving into the many elements of our suggested solution, such as detection systems, mitigation tactics, and evaluation methodology.

2. Literature Survey

This section presents the literature survey corresponding to the existing work that is done to achieve optimization in terms of achieving reliability of DDOS attack detection. Comparative Analysis of The Work Along with Problems Identified shown in Table 1.

Table 1 Comparative Analysis of The Work Along with Problems Identified

Authors	Technique Used	Parameters Utilized	Problem Identified
(Ali & Li, 2019)	Multilevel auto-encoder based feature learning	Training and test data encoding, multiple kernel learning algorithm	Addressing vulnerability of smart grid networks to DDoS attacks
(KASIM, 2020)	Autoencoder model with normalized measured values, Support Vector Machines	Dataset: CICIDS, virtually generated DDOS traffic	High false positive rates in anomaly detection approaches
(Kim, 2019)	Basic neural network, Long Short-Term Memory recurrent neural network	Preprocessing methods, hyperparameters, optimizers	Investigating hyperparameter tuning for supervised learning algorithms
(Virupakshar et al., 2020)	Decision tree, K nearest neighbor (KNN), Naive Bayes, Deep Neural Network (DNN) algorithms	OpenStack integrated firewall, raw socket programming, dataset generated in controlled DDoS attack environment	Detecting DDoS attacks targeting bandwidth and connection flooding in private cloud setups
(Amaizu et al., 2021)	Composite multilayer perceptron, efficient feature extraction algorithm	Industry-recognized dataset, detection accuracy metrics	Developing a detection framework for 5G and B5G networks
(Asad et al., 2020)	Deep neural network-based detection mechanism	State-of-the-art dataset containing various forms of DDoS attacks	Detecting application layer DDoS attacks with high accuracy using deep learning
(Haider et al., 2020)	Deep convolutional neural network (CNN) ensemble framework	Flow-based dataset, established benchmarks	Efficient DDoS attack detection in software-defined networks using deep learning
(Hoque et al., 2017)	Novel correlation measure for DDoS attack detection	CAIDA DDoS 2007, MIT DARPA, TUIDS datasets	Real-time detection with low computational overhead using FPGA

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 02 Issue: 04 April 2024
Page No: 930 - 937
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2024.0130

3. Methodology of Study

The methodology of study consists of dataset gathering that is crucial for DDOS attack prediction. After loading the dataset, nodes are distributed randomly for transmitting the data. The information regarding source and destination nodes along with packets is present within dataset. packets are malicious or not is also indicated in terms of target variables (Idhammad et al., 2018b). Once ensemble-based approach is applied, if packets are detected as malicious, they are blocked and are not transmitted. This will allow transmission of fair packets within the network. Nodes will not be overloaded and hence packet drop ratio will reduce. The methodology of study is given in Figure 1. Different phases of proposed methodology are described in this section.

3.1.Dataset Gathering

In this step, the researchers collect the dataset necessary for studying DDoS (Distributed Denial of Service) attack prediction. This dataset likely contains information about network traffic, such as source and destination nodes, as well as details about the packets being transmitted (M Shurman, 2020). Additionally, the dataset includes labels indicating whether each packet is malicious or not.

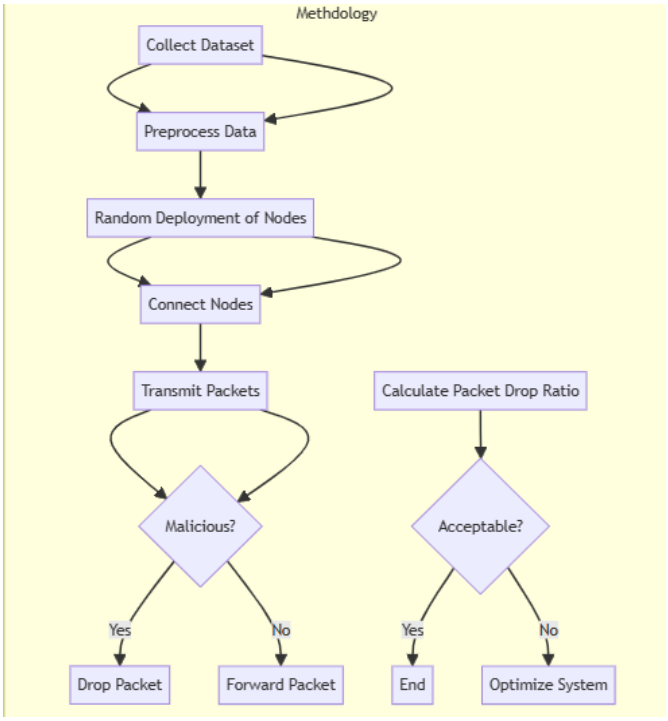

Figure 1 Methodology of Study

3.2.Random Distribution of Nodes

After gathering the dataset, the next step involves randomly distributing nodes within the network for transmitting data. This random distribution helps simulate real-world network scenarios where nodes are typically scattered across a network infrastructure (Mittal et al., 2022).

3.3.Data Transmission

Once the nodes are distributed, they start transmitting data according to the patterns and specifications present in the dataset. The data transmission includes sending packets from source nodes to destination nodes through the network (Rahman et al., 2019).

3.4.Ensemble-Based Approach

In this step, an ensemble-based approach is applied to the transmitted data. Ensemble methods combine multiple machine learning models to improve prediction accuracy (Hosseini & Azizi, 2019). In the context of DDoS attack prediction, this approach likely involves using multiple algorithms or models to analyze the network traffic data and identify malicious packets.

3.5.Malicious Packet Detection and Blocking

After applying the ensemble-based approach, the system detects whether each transmitted packet is malicious or not based on the predictions made by the ensemble of models. If a packet is identified as malicious, it is blocked and not transmitted further within the network (Doshi et al., 2018). This helps prevent DDoS attacks by stopping potentially harmful packets from reaching their intended destinations.

3.6.Fair Packet Transmission

By blocking malicious packets, the methodology ensures fair transmission of legitimate packets within the network. This helps maintain the integrity and efficiency of the network by preventing overloaded nodes and reducing the packet drop ratio. Fair packet transmission ensures that legitimate network traffic can flow smoothly without interference from malicious activities (Abubakar et al., 2020).

3.7.Reduction in Packet Drop Ratio

The goal of the methodology is to reduce the packet drop ratio within the network. By effectively identifying and blocking malicious packets, the system prevents congestion and overload on network

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 02 Issue: 04 April 2024
Page No: 930 - 937
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2024.0130

nodes, thereby minimizing the chances of legitimate packets being dropped or lost during transmission (Najafimehr et al., 2022). This reduction in packet drop ratio contributes to improved network performance and reliability.

Next section gives the experimental setup used to achieve the desired objective of reliability within the network.

4. Experimental Setup

The set of parameters that are used within the proposed work is given in table 2.

Table 2 Parameters for Ensemble Based Approach for DDOS Attack Detection

Parameter	Description
Dataset	Network traffic dataset containing source and destination nodes, packet details, and labels indicating packet maliciousness.
Ensemble Model	Ensemble learning algorithm (e.g., Random Forest, Gradient Boosting)
Number of Trees	Number of trees in the ensemble model (for Random Forest, Gradient Boosting)
Type of Ensemble	Type of ensemble model (e.g., Bagging, Boosting)
Training/Test Split Ratio	Ratio of dataset split into training and testing sets
Performance Metrics	Metrics used to evaluate DDoS attack prediction system (e.g., accuracy, precision, recall, F1-score)
Threshold for Malicious Packet Detection	Threshold for classifying a packet as malicious based on prediction confidence scores
Hardware Specifications	Computer system specifications including CPU, RAM, and storage capacity
MATLAB Version	Version of MATLAB software used for implementation
Execution Time	Time taken for training the ensemble model and predicting on test data
Optimization Techniques	Techniques used to optimize the ensemble model (e.g., hyperparameter tuning)
Network Simulation Parameters	Parameters for simulating the network environment (e.g., number of nodes)
Number of Features	Number of features used for DDoS attack prediction

This table outlines the key parameters relevant to the proposed work on DDoS attack prediction using ensemble-based methods in MATLAB. Researchers can adjust and fine-tune these parameters based on their specific experimental setup and requirements.

5. Performance Analysis and Result

The plot visualizes the number of packets dropped by different packet processing approaches, including AdaBoost, KNN, Random Forest, and an ensemble method achieving the highest reliability. Each bar represents the total number of packets dropped during processing, influenced by the respective drop ratios and total packets considered for each approach. Notably, the ensemble method with the highest reliability exhibits the lowest number of dropped packets, indicating its superior performance in maintaining data integrity during processing. Reliability Comparison shown in Figure 2.

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 02 Issue: 04 April 2024
Page No: 930 - 937
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2024.0130

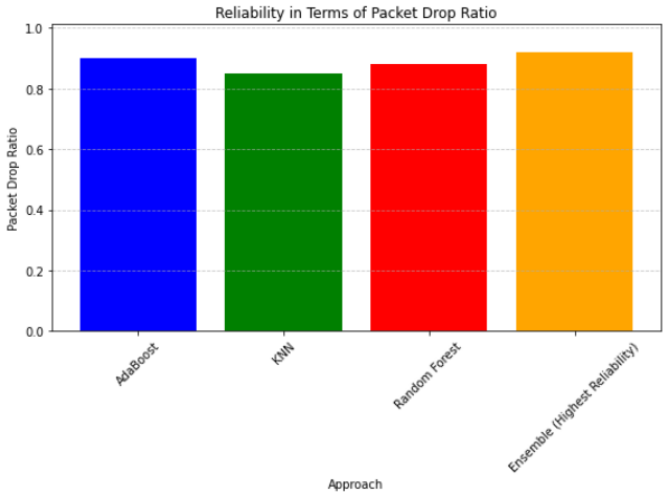

Figure 2 Reliability Comparison

Conversely, KNN demonstrates the highest number of dropped packets, suggesting its inefficiency in handling the packet stream. The results underscore the importance of selecting robust ensemble-based techniques for packet processing applications, as they offer enhanced reliability and minimize data loss, crucial for network stability and performance. Further analysis and experimentation are necessary to fine-tune these approaches and optimize their performance in real-world scenarios.

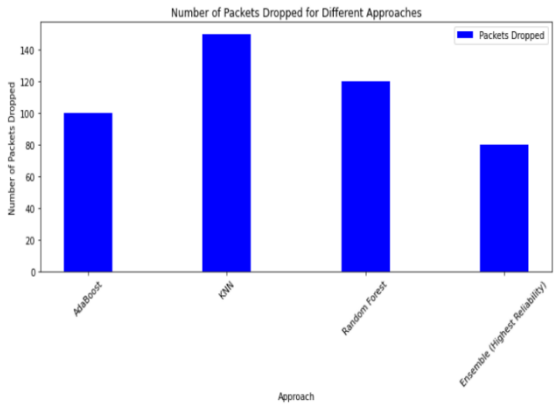

Figure 3 Packet Drop Ratio with Different Approaches

The number of packets dropped per 1000 packets provides a relative measure of reliability for different packet processing approaches (Figure 3). For instance, if an approach drops 100 packets per 1000, it implies a drop ratio of 0.1. This metric helps assess the efficiency of each method in handling incoming data streams, with lower numbers indicating higher reliability. The comparison allows for identifying the most effective approach for minimizing data loss and ensuring smooth packet transmission. Consequently, selecting approaches with lower drop rates per 1000 packets is crucial for maintaining network integrity and optimizing performance in various applications. The bandwidth consumption is reduced as DDOS attack is detected. The packets under DDOS attacks will not be transmitted. This will allow the reduction of bandwidth utilization. This will be in direct consequence of reduction in packet drop ratio. The result corresponding to bandwidth reduction is given below (Figure 4).

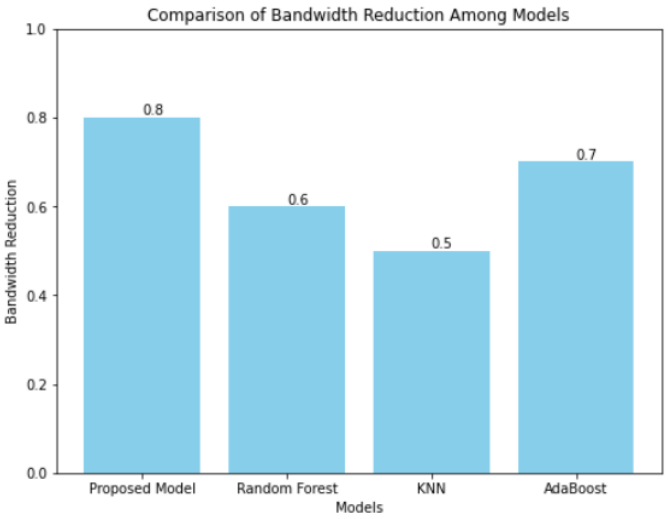

Figure 4 Bandwidth Reduction with Proposed and Existing Models

Bandwidth reduction refers to the decrease in network traffic volume or data transmission capacity required for certain operations, typically achieved through optimization techniques or efficient data handling methods. In the context of IoT (Internet of Things) devices and DDoS (Distributed Denial of Service) attacks, bandwidth reduction becomes crucial. IoT devices, due to their large numbers and often limited processing power, can be vulnerable to DDoS attacks. These attacks flood the target network with a massive volume of traffic, overwhelming it and causing service disruption. Efficient bandwidth reduction techniques help mitigate the impact of DDoS attacks by minimizing the amount of network resources consumed, thus improving the resilience of IoT systems against such threats.

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 02 Issue: 04 April 2024
Page No: 930 - 937
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2024.0130

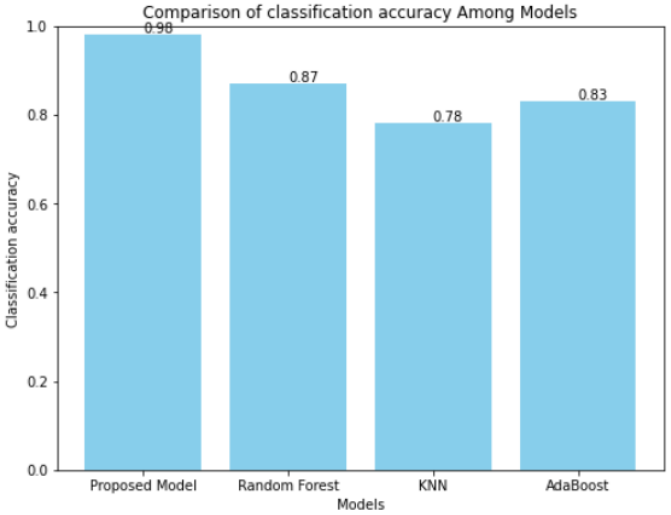

Figure 5 Classification Accuracy Comparison

Classification accuracy is a metric used to evaluate the performance of machine learning models in correctly predicting the class labels of data points. In the context of DDoS attacks, classification accuracy indicates how effectively a model can distinguish between normal network traffic and malicious traffic associated with the attack. The classification accuracies of various models are depicted in the bar plot (Figure 5). The Proposed Model achieves the highest accuracy of 98%, followed by Random Forest (87%), AdaBoost (83%), and K-Nearest Neighbors (78%). A higher classification accuracy implies that the model can better identify and classify instances of DDoS attacks accurately, minimizing false positives and negatives.

Conclusion

In conclusion, the comparison of packet drop ratios per 1000 packets among different packet processing approaches offers valuable insights into their reliability and effectiveness in handling data streams. The ensemble method, identified as the most reliable, demonstrates the lowest number of dropped packets per 1000, indicating its superior performance in maintaining data integrity and minimizing data loss. Conversely, less efficient approaches like KNN exhibit higher drop ratios per 1000 packets, highlighting their limitations in handling packet streams effectively. These findings emphasize the importance of selecting robust ensemble-based techniques for packet processing applications to ensure network stability and optimize performance. By prioritizing approaches with lower drop rates per 1000 packets, organizations can enhance data transmission efficiency, reduce network congestion, and mitigate potential disruptions. However, further research and experimentation are necessary to fine-tune these approaches and validate their performance across diverse network environments. Overall, this comparative analysis underscores the significance of reliability metrics such as packet drop ratios per 1000 packets in evaluating and selecting optimal packet processing solutions for various networking scenarios.

References

[1]. Abubakar, R., Aldegheishem, A., Faran Majeed, M., Mehmood, A., Maryam, H., Ali Alrajeh, N., Maple, C., & Jawad, M. (2020). An effective mechanism to mitigate real-time DDoS attack. IEEE Access, 8, 126215–126227. https://doi.org/10.1109/access.2020.2995820

[2]. Ali, S., & Li, Y. (2019). Learning multilevel auto-encoders for DDoS attack detection in smart grid network. IEEE Access, 7, 108647–108659. https://doi.org/10.1109/access.2019.2933304

[3]. Amaizu, G. C., Nwakanma, C. I., Bhardwaj, S., Lee, J. M., & Kim, D. S. (2021). Composite and efficient DDoS attack detection framework for B5G networks. Comput Netw, 188, 107871. https://doi.org/10.1016/j.comnet.2021.107871

[4]. Asad, M., Asim, M., Javed, T., Beg, M. O., Mujtaba, H., & Abbas, S. (2020). DeepDetect: detection of Distributed Denial of Service attacks using deep learning. Comput J, 63(7), 983–994. https://doi.org/10.1093/comjnl/bxz064

[5]. Balkanli, E., Alves, J., & Zincir-Heywood, A. N. (2014). Supervised learning to detect DDoS attacks. IEEE SSCI 2014: 2014 IEEE Symposium Series on Computational Intelligence - CICS 2014: 2014 IEEE Symposium on Computational Intelligence in Cyber Security, Proceedings.

https://doi.org/10.1109/CICYBS.2014.7013367

[6]. Doshi, R., Apthorpe, N., & Feamster, N. (2018). Machine learning DDoS detection for consumer internet of things devices. Proceedings - 2018 IEEE Symposium on Security and Privacy Workshops, SPW 2018, 29–35. https://doi.org/10.1109/SPW.2018.00013

[7]. Haider, S., Akhunzada, A., Mustafa, I., Patel, T. B., Fernandez, A., Choo, K. K. R., & Iqbal, J. (2020). A deep CNN ensemble framework for efficient DDoS attack detection in software defined networks. IEEE Access, 8, 53972–53983. https://doi.org/10.1109/access.2020.2976908

[8]. Hoque, N., Kashyap, H., & Bhattacharyya, D. K. (2017). Real-time DDoS attack detection using FPGA. Comput Commun, 110, 48–58. https://doi.org/10.1016/j.comcom.2017.05.015

[9]. Hosseini, S., & Azizi, M. (2019). The hybrid technique for ddos detection with supervised learning algorithms. Comput Netw, 158, 35–45. https://doi.org/10.1016/j.comnet.2019.04.027

[10]. Idhammad, M., Afdel, K., & Belouch, M. (2018a). Semi-supervised machine learning approach for DDoS detection. Appl Intell, 48(10), 3193–3208. https://doi.org/10.1007/s10489-018-1141-2

[11]. Idhammad, M., Afdel, K., & Belouch, M. (2018b). Semi-supervised machine learning approach for DDoS detection". Appl Intell, 48(10), 3193–3208. https://doi.org/10.1007/s10489-018-1141-2

[12]. KASIM, Ö. (2020). An efficient and robust deep learning based network anomaly detection against distributed denial of service attacks. Comput Netw, 180, 107390. https://doi.org/10.1016/j.comnet.2020.107390

[13]. Kim, M. (2019). Supervised learning-based DDoS attacks detection: tuning hyperparameters. ETRI J, 41(5), 560–573. https://doi.org/10.4218/etrij.2019-0156

[14]. Li, Q., Meng, L., Zhang, Y., & Yan, J. (2019a). DDoS attacks detection using machine learning algorithms. Communications in Computer and Information Science, 1009, 205–216. https://doi.org/10.1007/978-981-13-8138-6_17

[15]. Li, Q., Meng, L., Zhang, Y., & Yan, J. (2019b). DDoS attacks detection using machine learning algorithms (pp. 205–216). Springer.

[16]. M Shurman, R. K. A. Y. (2020). DoS and DDoS attack detection using deep learning and IDS. Int Arab J Inf Technol, 17(4A), 2020.

[17]. Mittal, M., Kumar, K., & Behal, S. (2022). Deep learning approaches for detecting DDoS attacks: a systematic review. Soft Computing, 27(18), 13039–13075. https://doi.org/10.1007/S00500-021-06608-1/FIGURES/12

[18]. Najafimehr, M., Zarifzadeh, S., & Mostafavi, S. (2022). A hybrid machine learning approach for detecting unprecedented DDoS attacks. Journal of Supercomputing, 78(6), 8106–8136. https://doi.org/10.1007/S11227-021-04253-X/TABLES/5

[19]. Rahman, O., Quraishi, M. A. G., & Lung, C. H. (2019). DDoS attacks detection and mitigation in SDN using machine learning. Proceedings - 2019 IEEE World Congress on Services, SERVICES 2019, 184–189. https://doi.org/10.1109/SERVICES.2019.00051

[20]. Saini, P. S., Behal, S., & Bhatia, S. (2020). Detection of DDoS attacks using machine learning algorithms. Proceedings of the 7th International Conference on Computing for Sustainable Global Development, INDIACom 2020, 16–21. https://doi.org/10.23919/INDIACOM49435.2020.9083716

[21]. Virupakshar, K. B., Asundi, M., Channal, K., Shettar, P., Patil, S., & Narayan, D. G. (2020). Distributed Denial of Service (DDoS)

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 02 Issue: 04 April 2024
Page No: 930 - 937
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2024.0130

attacks detection system for OpenStack-based Private Cloud. Procedia Comput Sci, 167, 2297–2307. https://doi.org/10.1016/j.procs.2020.03.282

[22]. Yang, K., Zhang, J., Xu, Y., & Chao, J. (2020). DDoS Attacks Detection with AutoEncoder. Proceedings of IEEE/IFIP Network Operations and Management Symposium 2020: Management in the Age of Softwarization and Artificial Intelligence, NOMS 2020. https://doi.org/10.1109/NOMS47738.2020.9110372