Int. Jrl. of **Human Computations & Intelligence**
Vol. 02, Issue 04, 2023
ISSN: 2583-5696

LITERATURE / REVIEW ARTICLE

Machine Learning Techniques to Detect DDoS Attacks in IoT's, SDN's: A Comprehensive Overview

Sudhanva Manjunath[1]. Athreya Abhay Pratap Singh[1] . Naveen Chandra Gowda[1] . Yerriswamy T[1]. Veena H N[2]

[1] School of Computer Science and Engineering, REVA University, Bengaluru, India
[2] Department of Computer Science and Engineering, SJB Institute of Technology, Bengaluru, India

Received: 30 April 2023 / Revised: 24 May 2023 / Accepted: 08 June 2023

DOI: 10.5281/zenodo.8027034

Abstract – Attacks known as distributed denial of service (DDoS) compromise user privacy while disrupting internet services and posing a serious danger to network security. DDoS attack detection using machine learning (ML) techniques has showed promise, but the evolving nature of these attacks presents challenges in accurately distinguishing between attack patterns and normal traffic. This paper presents a comprehensive overview of effective ML techniques for DDoS attack detection, focusing on IoTs, SDNs, and cloud. The literature survey analyzes research findings, categorized according to a suggested taxonomy, providing insights into the strengths and limitations of different approaches. Deploying and evaluating ML-based models in real-world environments is crucial to assessing practical effectiveness. This paper highlights the potential of ML techniques in detecting DDoS attacks while emphasizing the need for further research to address evolving attack tactics, establish evaluation practices, and develop adaptive defenses for real-world scenarios. By pursuing these avenues, network systems can significantly enhance security and resilience against DDoS attacks.

Index Terms – DDoS attack detection, Machine learning techniques, Deep learning methods, ML/DL-based defense mechanisms, IoTs, SDNs

I. INTRODUCTION

Attacks known as Distributed Denial of Service (DDoS) have grown to be a serious problem for network security and have the potential to cause severe disruption to online services. These attacks work by overwhelming a service with malicious traffic, making it unavailable to users. With the emergence of new types of attacks, it is essential to detect DDoS attacks effectively to prevent damage to the online service and protect user privacy. Machine learning algorithms have been used in various applications for prediction and analysis [1]. Machine learning (ML) algorithms have shown significant promise in detecting DDoS attacks. Researchers have proposed various ML techniques for DDoS attack detection,

ranging from traditional statistical approaches to modern deep learning-based algorithms [2][5]. Convolutional neural networks (CNN), recurrent neural networks (RNN), and RNN variants (e.g., Long Short-Term Memory [LSTM], Bidirectional Long Short-Term Memory [BLSTM], Stacked Long Short-Term Memory [SLSTM], and Gated Recurrent Units [GRU]) are a few of the methods used.

In this paper, we will focus on surveying effective ML techniques for DDoS attack detection and provide a comprehensive overview of the current state of research in this field. We will analyze the various ML techniques that have been used to detect DDoS attacks and provide insights into their strengths and weaknesses. We will focus on techniques that have been published in research papers from various sources, including academic journals, conferences, and technical reports. Our aim is to provide a comprehensive review of the most effective ML techniques for DDoS attack detection to help researchers and practitioners gain a better understanding of the field and make informed decisions about the most appropriate detection methods for their applications. We will also highlight the challenges that still exist in this field and suggest future research directions to improve the accuracy and efficiency of DDoS attack detection.

II. SELECTION CRITERIA

We conducted a systematic literature review and analyzed papers focused on using ML-based techniques for the detection and prevention of DDOS attacks.

Literature Search Strategy

To ensure a comprehensive analysis of the research on DDoS attack detection techniques, a systematic literature search was conducted. The search was conducted until 5/13/23 and covered five relevant databases (IEEE Xplore, ACM Digital Library, SpringerLink, ScienceDirect, and arXiv) for relevant articles, conference proceedings, and technical reports. Specific keywords and syntax (i.e., abstract, title, or keywords containing “DDoS attack,” “detection,” “prevention,” “mitigation,” “Machine Learning,” “Deep Learning,” "Neural Networks," "Artificial Intelligence," "Intrusion Detection," and "Cybersecurity") were used to identify articles that met the inclusion criteria. The inclusion criteria included articles that were published in English, peer-reviewed, and published within the past five years. A total of 26 articles met the inclusion criteria and were thoroughly analyzed. To ensure the latest research was included, a forward search was also performed, and additional relevant articles were added to the final selection. The selected articles cover various ML techniques, traditional techniques, and their combinations for DDoS attack detection. The analysis of the literature provides insights into the most effective and promising techniques for DDoS attack detection. Furthermore, the study identifies gaps in the research and highlights future research directions to improve the accuracy and efficiency of DDoS attack detection.

Quality criteria for study identification

In this study, only peer-reviewed international publications, including journal articles and conference proceedings, were considered to ensure the inclusion of high- quality and substantial

research work. Papers such as poster sessions, editorials, interviews, commentaries, and research- in-progress were excluded. template is used to format your paper and style the text.

III. LITERATURE SURVEY

In this study, we reviewed several existing machine learning algorithms for the detection and the mitigation of DDOS attacks. Many of the machine learning and deep learning have been proposed for security purposes [6][7]. The following is a review of the twelve latest algorithms considered in this study.

Support Vector Machine

Support Vector Machines (SVM) is a popular machine learning algorithm used in DDoS attack detection. SVMs work by identifying the boundary that separates two classes, normal and malicious traffic, in a high-dimensional feature space. SVMs are known for their ability to generalize well on unseen data, which makes them an effective choice for DDoS attack detection. SVM-based models have been shown to achieve high accuracy and efficiency in detecting DDoS attacks when compared to traditional techniques. SVMs can also handle non-linear relationships between features, making them suitable for detecting complex DDoS attack patterns. However, selecting the optimal parameters and kernel function for SVM models can be challenging, and overfitting can occur in some cases, which can lead to reduced performance.

SVM, a well-liked supervised learning method in machine learning, is used for regression and classification. SVM has been utilised in a number of studies on DDoS and DoS detection. In a Software Defined Network (SDN), Jin Ye et al.[10] suggested a method for DDoS detection using SVM by gathering flow status data and deriving six-tuple characteristic values associated with DDoS attacks. The traffic is subsequently evaluated using the SVM algorithm in order to detect DDoS attacks. By gathering system data to train the SVM classifier to differentiate between legitimate and malicious actions of the VM, Adel Abusitta et al.'s [9] suggested an SVM-based framework for detecting DoS attacks in a virtualized cloud. To keep a filter of resource adjustments effect, the hypervisor measures and tracks the impact of making resource adjustments on the data that has been acquired.

Vipin Das et al.[8] conducted a study on classifying DOS attacks using rough set theory (RST) and SVM, showing that RST and SVM can efficiently detect DOS attacks and improve false positive ratios. T. Subbulakshmi et al. aimed to track online networks and instantly activate security techniques when suspicious behavior was detected. Enhanced Support Vector Machines (ESVM) are utilized to detect processes for recognizing spoofed IPs in this strategy, which enables the identification of both non-spoofed and spoofed IPs. RST and SVM were combined by Rung-Ching Chen et al. [11] to recognize DOS assaults by feeding SVM a specific feature set obtained from RST. The DDoS dataset was created and detected using Enhanced Support Vector Machines (ESVCM) and SVM for evaluation by T. Subbulakshmi et al.

A real-time anomaly detection system is also suggested by A. Ramamoorthi et al. [12] to identify and categorize DDoS attacks at the application and network layers. To distinguish between regular and

attack incoming flows, the system employs ESVM with string kernels. The findings demonstrate the proposed system's capability to identify and categorize DDoS attacks, with string kernels outperforming other kernel functions in terms of classification accuracy. The report makes additional recommendations for future work to preserve detection accuracy against novel DDoS attack types including port scanning and DNS spoofing. The support vector regression is also used for predicting the trust of end devices over the attacks [13] as it is most important to manage and maintain the trust for secured communication [14]. Overall, SVM has shown promising results in DDoS and DoS detection in both cloud and SDN environments.

Naïve Bayes

Naive Bayes is a classification model that uses the Bayesian approach. It is a simple and straightforward method for creating classifiers by defining prototypes that assign class labels to new cases based on the values of their features, which are represented as vectors. The class labels are chosen from a finite set of possibilities. It was discovered in a study by Kanagalakshmi R. et al.[17] that utilising Hidden Naive Bayes (HNB) gave findings that were more trustworthy than those from the traditional Naive Bayes model. Using dynamic properties and massive network data stream capabilities, HNB is a data mining technique that foresees infiltration issues like DOS attacks. This method differs from the simplistic Bayes presumption of implicit impartiality methods. In a separate study, Mouhammad Alkasassbeh et al. acquired a fresh dataset of DDOS attacks in different tiers of the network and employed three different approaches, including Naive Bayes and Random Forest, for DDoS detection. In a different work, Jasreena Kaur Bains et al. suggested a hierarchically layered approach for determining attack rates that used a Naive Bayes classifier with K2 learning method between each attack class on a condensed NSL KDD dataset. The output of one layer was passed on to another layer to increase the detecting rate once the layers were trained to recognise a specific type of attack.

According to Singh et al.'s research, employing information gain in addition to the Gaussian Naive Bayes classifier method results in a higher accuracy (above 99%) in detecting Distributed Denial of Service (DDoS) assaults than using the Gaussian Naive Bayes algorithm alone. Additionally, this combined approach reduces computation time by 46%. The authors suggest future implementation of this technique in conjunction with IP blacklisting to block abnormal IPs and recommend evaluating its performance using other standard datasets, such as DARPA datasets, for comparison with the results obtained from CIADA datasets. In the paper by Abdul Fadil et al. [18], the authors introduce a DDoS attack detection approach using Gaussian Naive Bayes. The method uses the average and standard deviation to create a set of classes, with the average denoting the centre of each class and the standard deviation denoting the size of the set of classes. Each class set's width provides specificity to each of its members.

The Gaussian Naive Bayes method demonstrates accurate and precise predictions. The authors suggest that future research should involve processing more data to further evaluate the accuracy of the Gaussian Naive Bayes method. The Hidden Naive Bayes (HNB) Multiclass classification model, enhanced with various discretization and feature selection methods, exhibits improved performance in detecting denial-of-service (DoS) attacks compared to traditional naive Bayes and extended naive Bayes

models, according to the study's findings by Setiadi et al. [16]. Due to its simplicity and superiority over the conditional independence assumption of the naive Bayes model, the HNB model shows promise for datasets containing dependent attributes, such as the KDD-99 intrusion detection dataset.

Decision Tree

Decision trees have emerged as a popular approach for detecting DDoS attacks due to their effectiveness, interpretability, and structured classification capabilities. Algorithms like C4.5, CART, and Random Forest enable the identification of normal and malicious network flows by utilizing a range of features, including traffic volume, packet attributes, and flow statistics. This enables informed decision-making in real-time detection scenarios, empowering network security against DDoS threats. A lightweight decision-tree (DT) approach is proposed by Lucky et al. [15] for accurate and effective DDoS flooding attack detection. With just 7% of the CPU used, their architecture manages to achieve detection accuracy of above 99.9%. The system shows promise for implementation in low-cost contexts and makes use of a robust feature selection technique. Future work aims to improve performance at higher line rates through distributed monitoring using hardware such as Field Programmable Gate Arrays (FPGAs). Decision tree techniques are suggested by Lakshminarasimman et al. [19] for application in identifying DDoS attacks. They specifically contrast the J48 decision tree algorithm's performance with that of the random forest decision tree technique. Through dataset analysis, they find that the J48 algorithm provides a more preferable solution in terms of detecting different features related to DDoS attacks.

The study utilizes the KDDCup'99 dataset and emphasizes the importance of anomaly detection in securing wireless nodes from DDoS attacks. The research aims to identify attack patterns and develop effective countermeasures to enhance network security. The goal of a research by Liguo Chen et al.[20] is to use Spark and the Random Forest method to identify DNS DDoS attacks. The report draws attention to the importance of DNS security and the rise in volume-based DDoS attacks. The suggested model, which is based on Random Forest, successfully classifies traffic on Spark with a high accuracy of 99.2%, making it appropriate for handling massive DNS query volumes. The study presents a novel approach to traffic filtering utilising machine learning algorithms to decrease DDoS traffic on Top Level Domain (TLD) servers. Future work will focus on extracting features, using the model to make real-time rules using streaming technology, and developing a real-time detection and prevention system using the traffic filtering model.

KNN

Madathi et al.[21], focuses on detecting DDoS attacks in SDN environments using the KNN algorithm. They achieve a 96% accuracy in detecting DDoS attacks by preprocessing a DDoS detection dataset, eliminating outliers, and applying various classification techniques, including KNN. Shi Dong et al.[4], addresses the challenge of DDoS attack detection in SDN networks. The authors propose four features (flow length, flow duration, flow size, and flow ratio) and introduce the concept of the "degree of attack" to detect DDoS attacks. They present two detection algorithms: DDADA and DDAML, which outperform existing solutions and demonstrate higher detection rates in experimental evaluations. The DDAML algorithm shows particular promise for future application in real SDN environments.

K-Means Clustering

K-means clustering is used in DDoS detection by grouping network traffic based on similarities. Features such as packet size and frequency are considered, allowing for the identification of anomalous patterns. It helps differentiate between normal traffic and DDoS attacks, aiding in their detection and mitigation. In their study, She et al.[22] propose a novel approach for detecting application-layer DDoS attacks using the Affinity Propagation (AP) clustering algorithm. They extract features from normal users' sessions and employ AP clustering to form K clusters. The resulting models are then utilized to identify application-layer DDoS attacks. The authors' method focuses on building user behavior models based on session features to enhance detection accuracy. Aamir et al.[23] present a semi-supervised machine learning technique for classifying DDoS attacks using the K-Means clustering algorithm. Their approach leverages a hybrid feature selection method and employs the CICIDS2017 dataset for training and evaluation. By identifying two centroids representing DDoS and normal traffic, the proposed algorithm effectively categorizes network traffic. The authors suggest future work, including online traffic labeling, integration of additional machine learning algorithms, and utilizing the proposed centroids for online detection frameworks.

Pedroso et al.'s [24] proposal for an enhanced K-means clustering approach addresses the problem of DDoS assault detection. By using an integrated feature selection method and a deep autoencoder (DAE), they improve the K-means clustering technique by extracting encoded information that more effectively distinguish between good and bad network flows. The authors show that the performance of the K-means model is greatly enhanced by their hybrid approach, putting it on par with cutting-edge supervised machine learning and deep learning techniques for DDoS attack detection. Pramana et al.[25] present a modified K-means clustering algorithm for effective DDoS detection. Their method incorporates chain initialization over a landmark window to handle large datasets. The authors evaluate the proposed algorithm using the DARPA 98 dataset and achieve satisfactory results in detecting denial-of-service traffic. The modified K-means algorithm demonstrates high detection rates and accuracy while maintaining a low false positive rate. Future work involves enhancing chain initialization stability, further improving detection rates and accuracy, and exploring additional features for enhanced performance.

Deep Learning-based approaches

Deep learning techniques such as Recurrent Neural Networks (RNNs), Convolutional Neural Networks (CNNs), and Long Short-Term Memory (LSTM) networks have proven effective in detecting DDoS attacks. RNNs excel at capturing temporal dependencies in network traffic, while CNNs are adept at extracting spatial features from multidimensional matrices representing traffic data. LSTM networks [3] address the vanishing gradient problem in RNNs and effectively capture long-term dependencies. By leveraging these deep learning techniques, systems can automatically differentiate normal network traffic from DDoS attacks, making them adaptable and effective in this dynamic security domain.

A time-stamped bi-directional gated recurrent unit (GRU) model for detecting DDoS assaults in IoT situations is proposed by Chun-Yu Chen et al. in their paper[26]. Comparing their method to earlier ones, it has higher accuracy and requires less training. The bi-GRU model performs well in identifying DDoS assaults when paired with diverse datasets. Roheen Qamar et al.[27] aim to identify the best algorithm for detecting DDoS attacks. They use the recurrent neural network (RNN) to train and classify input traffic. Three algorithms—gradient descent with momentum, scaled conjugate gradient, and variable learning rate gradient descent—are the subject of their research. Among these, the variable learning rate gradient descent algorithm achieves the highest accuracy (99.9%) and short training time (2 minutes and 29 seconds).

Harish Kumar et al.[28] propose a lightweight CNN model for detecting DDoS attacks in distributed scenarios. They leverage deep hybrid learning to detect various types of minimal DDoS attacks. Their model successfully detects low-rate DDoS attacks like Slow-Headers, Slow-Body, Slow-Read, and Shrew assaults by building multi-type constrained DDoS threat datasets and using CNN-RF hybrid learning. Dingyang Lv et al.[29] introduce FLDDoS, a system that combines federated learning (FL) and convolutional neural network (CNN) for DDoS attack detection. An technique for data preprocessing and a CNN model are used by FLDDoS to extract features from DDoS traffic data. The federated learning architecture allows for distributed data model training while protecting data privacy. Their method detects DDoS attacks with high accuracy (99%) and classifies multiple attacks with good accuracy (90%).

A Long Short-Term Memory (LSTM) based system called LSTM-CLOUD is proposed by Hakan Aydn et al.[30] for identifying and combating DDoS attacks on public cloud networks. They have two modules in their system: defence and detection. On the CICDDoS2019 dataset, the detection module uses an LSTM DL model and achieves an accuracy rate of 99.83%. The defense module activates the defense mechanism upon attack detection, protecting cloud systems. DDoSLSTM, a deep learning model for the detection of Distributed Denial-of-Service (DDoS) assaults on IoT devices, is the solution put up by Gaur et al. [31]. A Long Short-Term Memory (LSTM) network, which can handle time series data and lengthy time-dependent inputs, is used in the model. The study's main goal is to improve the LSTM model's classification performance. The maximum accuracy that the authors can get using a multi-layer LSTM model for binary and multiclass data is 99.46% for the 1-Layer LSTM with binary data and 99.16% for the 2-Layer LSTM with multiclass grouped data. In comparison to existing cutting-edge methods, such as deep neural networks (DNNs), recurrent neural networks (RNNs), convolutional neural networks (CNNs), and Transformers, the suggested DDoSLSTM model performs better.

IV. CONCLUSION

In conclusion, the field of machine learning and deep learning has made significant advancements in detecting and mitigating Distributed Denial of Service (DDoS) attacks. However, the evolving nature of DDoS attacks poses challenges in accurately distinguishing between attack patterns and normal traffic. Researchers have proposed various ML/DL methods over the years, but the applicability of these techniques remains limited due to the dynamic tactics employed by attackers. It is worth highlighting that the future of DDoS attack detection and mitigation lies in the continued exploration and utilization

of advanced machine learning techniques, such as transformers and deep learning methods. These approaches have demonstrated immense potential in various domains and have the capacity to revolutionize the field of DDoS defense. While the reviewed literature demonstrates the potential of ML/DL methods in detecting DDoS attacks, further research is needed to address the challenges posed by evolving attack tactics, establish standardized evaluation practices, and develop adaptive defense mechanisms that can be deployed effectively in real-world scenarios. By pursuing these avenues, the field can make significant strides towards enhancing the security and resilience of network systems against DDoS attacks.

REFERENCES

1. Rekha, K. B., & Gowda, N. C. (2020, October). A framework for sentiment analysis in customer product reviews using machine learning. In *2020 International Conference on Smart Technologies in Computing, Electrical and Electronics (ICSTCEE)* (pp. 267-271). IEEE.
2. Suresh, M., & Anitha, R. (2011). Evaluating machine learning algorithms for detecting DDoS attacks. In *Advances in Network Security and Applications: 4th International Conference, CNSA 2011, Chennai, India, July 15-17, 2011 4* (pp. 441-452). Springer Berlin Heidelberg.
3. Hochreiter, S., & Schmidhuber, J. (1997). Long short-term memory. *Neural computation*, *9*(8), 1735-1780.
4. Dong, S., & Sarem, M. (2019). DDoS attack detection method based on improved KNN with the degree of DDoS attack in software-defined networks. *IEEE Access*, *8*, 5039-5048.
5. He, Z., Zhang, T., & Lee, R. B. (2017, June). Machine learning based DDoS attack detection from source side in cloud. In *2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud)* (pp. 114-120). IEEE.
6. Shalini, L., Manvi, S. S., Gowda, N. C., & Manasa, K. N. (2022, June). Detection of Phishing Emails using Machine Learning and Deep Learning. In *2022 7th International Conference on Communication and Electronics Systems (ICCES)* (pp. 1237-1243). IEEE.
7. Shalini, L., Manvi, S. S., Gardiner, B., & Gowda, N. C. (2022, December). Image Based Classification of COVID-19 Infection Using Ensemble of Machine Learning Classifiers and Deep Learning Techniques. In *2022 International Conference on Data Science, Agents & Artificial Intelligence (ICDSAAI)* (Vol. 1, pp. 1-6). IEEE.
8. Vipin, Das & Vijaya, Pathak & Sattvik, Sharma & Sreevathsan, & MVVNS.Srikanth, & T, Gireesh. (2010). Network Intrusion Detection System Based On Machine Learning Algorithms. International Journal of Computer Science & Information Technology.
9. Abusitta, Adel & Bellaiche, Martine & Dagenais, Michel. (2018). An SVM-based framework for detecting DoS attacks in virtualized clouds under changing environment. Journal of Cloud Computing.
10. Ye, J., Cheng, X., Zhu, J., Feng, L., & Song, L. (2018). A DDoS Attack Detection Method Based on SVM in Software Defined Network. *Security and Communication Networks*, *2018*, 9804061.
11. Chen, R. C., Cheng, K. F., Chen, Y. H., & Hsieh, C. F. (2009, April). Using rough set and support vector machine for network intrusion detection system. In *2009 First Asian Conference on Intelligent Information and Database Systems* (pp. 465-470). IEEE.
12. Ramamoorthi, A., Subbulakshmi, T., & Shalinie, S. M. (2011, June). Real time detection and classification of DDoS attacks using enhanced SVM with string kernels. In *2011 international conference on recent trends in information technology (ICRTIT)* (pp. 91-96). IEEE.
13. Gowda, N. C., & Malakreddy, B. (2023, February). A Trust Prediction Mechanism in Edge Communications using Optimized Support Vector Regression. In *2023 7th International Conference on Computing Methodologies and Communication (ICCMC)* (pp. 784-789). IEEE.
14. Manvi, S. S., & Gowda, N. C. (2019). Trust Management in Fog Computing: A Survey. In *Applying Integration Techniques and Methods in Distributed Systems and Technologies* (pp. 34-48). IGI global.

15. Lucky, G., Jjunju, F., & Marshall, A. (2020, December). A lightweight decision-tree algorithm for detecting DDoS flooding attacks. In *2020 IEEE 20th international conference on software quality, reliability and security companion (QRS-C)* (pp. 382-389). IEEE.
16. Setiadi, F. F., Kesiman, M. W. A., & Aryanto, K. Y. E. (2021). Detection of dos attacks using naive bayes method based on internet of things (iot). *Journal of Physics: Conference Series*, *1810*(1), 012013.
17. Koc, L., Mazzuchi, T. A., & Sarkani, S. (2012). A network intrusion detection system based on a Hidden Naïve Bayes multiclass classifier. *Expert Systems with Applications*, *39*(18), 13492-13500.
18. Fadil, A., Riadi, I., & Aji, S. (2017). A novel ddos attack detection based on gaussian naive bayes. *Bulletin of Electrical Engineering and Informatics*, *6*(2), 140-148.
19. Lakshminarasimman, S. & Ruswin, S. & K., Sundarakantham. (2017). Detecting DDoS attacks using decision tree algorithm. 1-6.
20. Chen, L., Zhang, Y., Zhao, Q., Geng, G., & Yan, Z. (2018). Detection of dns ddos attacks with random forest algorithm on spark. *Procedia computer science*, *134*, 310-315.
21. Madathi, M., Harini, R., Monikaa, R., & Gowthami, N. (2022). Detection of DDoS attack in SDN environment using KNN algorithm. *IJRAR-International Journal of Research and Analytical Reviews (IJRAR)*, *9*(2), 252-257.
22. Yerriswamy, T., & Gururaj, M. (2022). An Efficient Hybrid Protocol Framework for DDoS Attack Detection and Mitigation Using Evolutionary Technique. *TECHNOLOGY*, 77.
23. Ahmed, S. T. (2017, June). A study on multi objective optimal clustering techniques for medical datasets. In 2017 international conference on intelligent computing and control systems (ICICCS) (pp. 174-177). IEEE.
24. Aamir, M., & Zaidi, S. M. A. (2021). Clustering based semi-supervised machine learning for DDoS attack classification. *Journal of King Saud University-Computer and Information Sciences*, *33*(4), 436-446.
25. Yerriswamy, T., & Murtugudde, G. (2021). An efficient algorithm for anomaly intrusion detection in a network. *Global Transitions Proceedings*, *2*(2), 255-260.
26. Pramana, M. I. W., Purwanto, Y., & Suratman, F. Y. (2015, August). DDoS detection using modified K-means clustering with chain initialization over landmark window. In *2015 International Conference on Control, Electronics, Renewable Energy and Communications (ICCEREC)* (pp. 7-11). IEEE.
27. Chen, C. Y., Chen, L. A., Cai, Y. Z., & Tsai, M. H. (2020, December). RNN-based DDoS detection in IoT scenario. In *2020 International computer symposium (ICS)* (pp. 448-453). IEEE.
28. Raja, D. K., Kumar, G. H., Basha, S. M., & Ahmed, S. T. (2022). Recommendations based on integrated matrix time decomposition and clustering optimization. International Journal of Performability Engineering, 18(4), 298.
29. Qamar, Roheen & Zardari, Baqir & Arain, Aijaz & Khoso, Fida & Jokhio, Ahmed. (2022). Detecting Distributed Denial of Service attacks using Recurrent Neural Network.
30. Kumar, Harish & Aoudni, Yassine & Ortiz, Geovanny & Jindal, Latika & Miah, Shahajan & Tripathi, Rohit. (2022). Light Weighted CNN Model to Detect DDoS Attack over Distributed Scenario. Security and Communication Networks. 2022. 1-10.
31. Murtugudde, G. (2022). Signature-based Traffic Classification for DDoS Attack Detection and Analysis of Mitigation for DDoS Attacks using Programmable Commodity Switches. *International Journal of Performability Engineering*, *18*(7).
32. Aydın, H., Orman, Z., & Aydın, M. A. (2022). A long short-term memory (LSTM)-based distributed denial of service (DDoS) detection and defense system design in public cloud network environment. *Computers & Security*, *118*, 102725.
33. Ambika, B. J., & Banga, M. K. (2021). Energy-Efficient MPLS-MANET Using Ant Colony Optimization and Harmony Search Algorithm. In *Cognitive Informatics and Soft Computing: Proceeding of CISC 2020* (pp. 195-209). Springer Singapore.
34. Al-Shammari, N. K., Syed, T. H., & Syed, M. B. (2021). An Edge–IoT framework and prototype based on blockchain for smart healthcare applications. Engineering, Technology & Applied Science Research, 11(4), 7326-7331.