International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Dynamic DDoS Detection using Deep Learning

S. Rishikanth[1] | *M. Mohammed Ejaz*[2] | *P. Muthuram*[3] | *Mr. A. Vinish*[4]

(Department of Computer Science, UG Scholar, Rathinam College of Arts and Science, Coimbatore, rishikanths3524 @gmail.com)[1]
(Department of Computer Science, UG Scholar, Rathinam College of Arts and Science, Coimbatore, jannathejaz@gmail.com)[2]
(Department of Computer Science, UG Scholar, Rathinam College of Arts and Science, Coimbatore,muthuram260303 @gmail.com)[3]
(Department of Computer Science, Senior Faculty, Rathinam College of Arts and Science, Coimbatore, alikkalvinish@gmail.com)

ABSTRACT :

A Cyber Attack is a purposeful, malicious attempt to breach, harm, or obtain unauthorized access to computer systems or networks. A DDoS attack is an intentional attempt to overwhelm a system or network with excessive internet traffic, resulting in a denial of service for authorized users. The goal of deep learning, a branch of artificial intelligence, is to train deep neural networks to automatically learn and represent data. This will enable the networks to perform tasks like natural language processing and image recognition more effectively. In a cloud-based project, real-time network traffic is analyzed for DDoS attack patterns using deep learning, specifically with models such as LSTM. Scalability, effective resource management, and integration with security services are made possible by the cloud infrastructure, which guarantees efficient detection and response systems. Constant monitoring and model updates help create a strong defense system. The goal of this project is to use deep learning, specifically LSTM, in a cloud architecture to create an intelligent and adaptive DDoS detection system. Our mission is to protect network infrastructure by offering scalability, effective mitigation, real-time detection, and constant adaptation to DDoS attack strategies. The expected outcomes include automated reactions, timely alerts, and real-time DDoS attack detection. In addition to effectively mitigating attacks, the system should scale to accommodate fluctuating traffic loads, integrate with cloud services with ease, and continually adapt through periodic updates to threats that evolve over time. Analytics and system logs offer information about overall performance and potential threats.

Keywords: DDoS attack, deep learning, LSTM

Introduction :

In the modern world, technology is now a necessary aspect of living. In actuality, everything has moved from offline to online during the Covid-19 pandemic, including businesses and educational institutions. As a result, attacks and intrusions using Internet-based technologies increase exponentially. An intentional, malicious attempt to take advantage of, harm, or obtain unauthorized access to computer systems, networks, or digital devices is referred to as a cyberattack. Cyberattacks can take many different forms, with the goal of jeopardizing the availability, confidentiality, or integrity of data and systems. Ransomware, phishing, malware infections, denial-of-service (DoS) attacks, and data breaches are examples of common cyberattacks.

Attackers, also known as hackers, use a variety of methods and instruments to take advantage of holes in software, networks, or human behavior. Cyberattacks can be carried out for a variety of reasons, such as espionage, financial gain, service interruption, or theft of confidential data. The techniques employed in cyberattacks change along with technology, so cybersecurity is a field that is always developing to combat these threats.

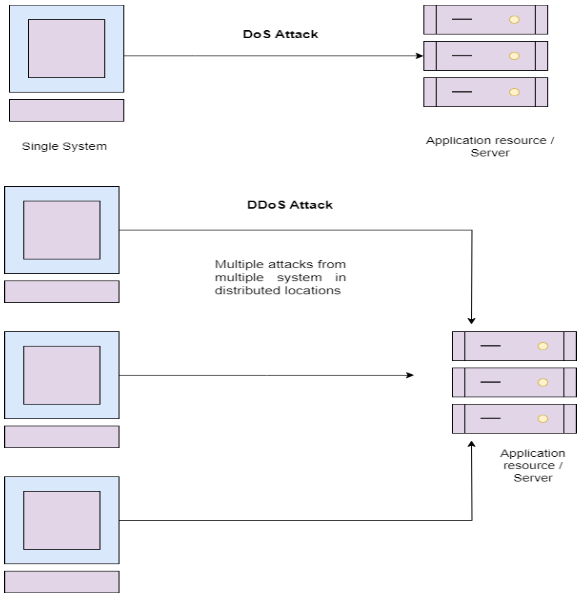

DoS Attack
Single System
Application resource / Server
DDoS Attack
Multiple attacks from multiple system in distributed locations
Application resource / Server

Fig 1.1 Difference Between DoS and DDoS attack

The Distributed Denial of Service (DDoS) attack is a deadly threat that can quickly bring down Internet-based services and applications Attacks known as Distributed Denial of Service (DDoS) are deliberate attempts by malicious parties to overload a network, service, or website with excessive traffic in order to prevent it from operating normally. When a DDoS attack occurs, the attacker usually uses a botnet, a network of compromised computers to overwhelm the target with too many requests, stopping it from processing requests from legitimate users. The target's resources are depleted by the sheer volume of incoming traffic, which prevents legitimate users from accessing the targeted system and causes a denial of service.

DDoS attacks can be carried out in a number of ways, including by overloading particular infrastructure components, flooding the target with traffic, or taking advantage of vulnerabilities. These assaults represent serious risks to internet services, frequently leading to the targeted entities to suffer financial losses, service degradation, and outages.

Artificial intelligence (AI) encompasses machine learning, of which deep learning is a subset. It entails processing vast volumes of data in order to train artificial neural networks to execute tasks. Neural networks, especially those with numerous layers, or "deep" neural networks, can automatically learn to represent data through hierarchical abstraction in deep learning.

Multiple-layered neural networks, or deep neural networks, are essential to deep learning. Examples of deep neural networks include convolutional neural networks (CNNs), which are used for image recognition and natural language processing, and recurrent neural networks (RNNs), which are used for sequential data. In a number of AI applications, such as speech and picture recognition, natural language processing, and strategic game play, deep learning has demonstrated impressive results.

The application of Long Short-Term Memory (LSTM) networks in this project is essential to strengthening the DDoS detection system. Recurrent neural networks (RNNs) of the LSTM type are particularly well-suited to the dynamic nature of network traffic because of their prowess in capturing temporal dependencies within sequential data. The main goal is to improve the system's capacity to recognize and adjust to DDoS attack patterns over time. Leveraging LSTMs gives the model the ability to identify dynamic and subtle abnormalities in network behavior, which improves detection accuracy and flexibility.

LSTMs' sequential data processing powers enable the system to function in real-time, quickly detecting anomalies in typical patterns and enabling an adaptive defense mechanism. to put it simply, the addition of LSTMs is essential to improving the DDoS detection system's sensitivity, accuracy, and responsiveness in the cloud architecture. The system performs predefined actions, like updating cloud-based firewall rules or alerting administrators, in response to detected anomalies. The cloud infrastructure's scalability is utilized to effectively manage different traffic volumes. The overall security infrastructure is improved through seamless integration with current cloud security services.

The LSTM model is updated periodically and is continuously monitored to guarantee that it can adapt to changing DDoS attack tactics. The goal of this all-encompassing strategy is to develop a DDoS detection system that is intelligent and adaptive and can offer real-time. the expected output includes real-time detection of DDoS attacks, timely alerts, and automated responses. The system should efficiently mitigate attacks, scale with varying traffic loads, seamlessly integrate with cloud services, and continuously adapt to evolving threats through periodic updates. System logs and analytics provide insights into threats and overall performance.

Problem Statement

The increasing frequency of Distributed Denial of Service (DDoS) attacks presents a significant risk to the dependability and accessibility of internet-based services, thereby requiring sophisticated defense systems that can adjust to changing attack tactics. Real-time and flexible solutions are frequently lacking from traditional DDoS mitigation techniques, particularly in the dynamic environment of cloud-based infrastructures. Creating a DDoS detection system that is both intelligent and scalable while integrating seamlessly with cloud environments and utilizing Long Short-Term Memory (LSTM) networks to identify subtle patterns indicative of attacks is the challenge. In order to protect network infrastructures from the increasingly sophisticated DDoS attacks, maintain the availability of online services, and minimize possible financial and reputational losses for businesses, it is imperative that this issue be resolved.

Proposed Method

The initial step in the process of LSTM-based DDoS detection is to gather network traffic data from various sources. Examples of these could be packet captures, network logs, and traffic flow data.

These resources provide valuable insights into the network's behaviour and can be used to identify patterns that indicate DDoS attacks. However, the information that has been acquired may contain inconsistent, irrelevant, or missing values.

Pre-processing is necessary to ensure data uniformity and correctness.

This means cleaning the data to eliminate abnormal values, standardizing the data to a consistent scale, and filtering out unrelated or unreliable information. Subsequently, the pre-processed data provides a reliable foundation for feature extraction. After pre-processing, the network traffic data must be taken and relevant features must be extracted. These attributes aim to capture the essential components of network traffic that are useful in differentiating between DDoS and normal traffic.

Often utilized features for DDoS detection include packet size, packet count, protocol type, source and destination IP addresses, and port numbers. The raw network traffic data needs to be transformed into a numerical representation that the LSTM model can handle quickly in order to extract these features. It may be necessary to scale, normalize, or encode the characteristics in order to ensure that they fall into the right range and preserve their fundamental relationships.

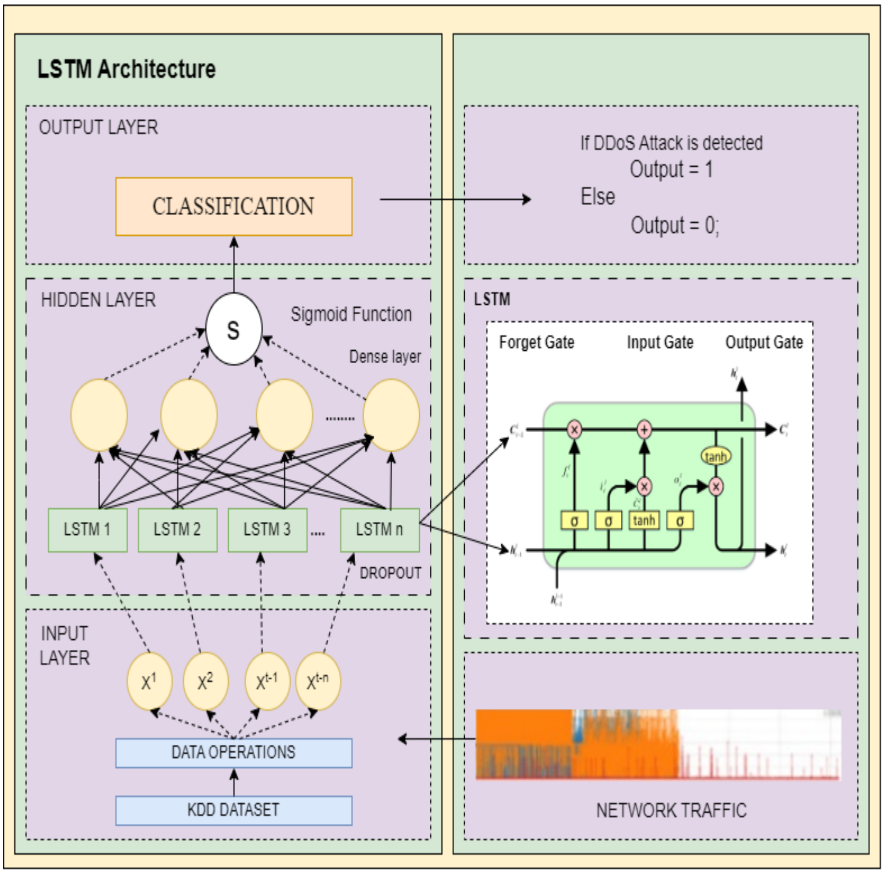


Fig 1.2 LSTM Architecture

Several parts make up the LSTM architecture:

The diagram's (Refer fig 1.2) top horizontal line represents the cell state. Its job is to keep the network's long-term memory in good condition. The LSTM can retain information for extended periods of time because the cell state may transport information over several time steps.

The Forget Gate (f_t) is responsible for determining whether cell state data should be ignored or forgotten. It creates a forget gate activation vector (f_t) with values between 0 and 1 using input from the current input (x_t) and the prior hidden state (h_{t-1}). The LSTM may selectively recall or forget information thanks to this gate.

The input gate (i_t) determines which data from the input stream should be kept in the cell state. The input gate layer and the tanh layer make up its two components. The tanh layer generates a vector of new candidate values that might be added to the cell state, while the input gate layer selects which values to update.

The Output Gate (o_t) determines which cell state data should be produced at the given time step. It generates an output gate activation vector (o_t) with values between 0 and 1 using input from the previous hidden state (h_{t-1}), the current input (x_t), and the current cell state (C_t). The data that is output to the next concealed state is controlled by this gate.

Hidden State (h_t) is the LSTM unit's output, which stands for the network's short-term memory. Based on the gate activations and the cell state, it is computed. Either the next time step or estimates are made using the concealed state.

The LSTM model can be trained after the data has been preprocessed and the pertinent features have been extracted. Three sets of data are created during the training process: training, validation, and testing. The LSTM model learns the patterns connected to both regular and DDoS traffic from the training set.

The purpose of the validation set is to keep an eye on the model's performance while it is being trained and guard against overfitting, a condition in which the model performs poorly on newly discovered data because it is too closely aligned with the training set. The model's final performance on untrained data is assessed using the testing set, which offers an objective appraisal of the model's capacity for generalization.

Workflow

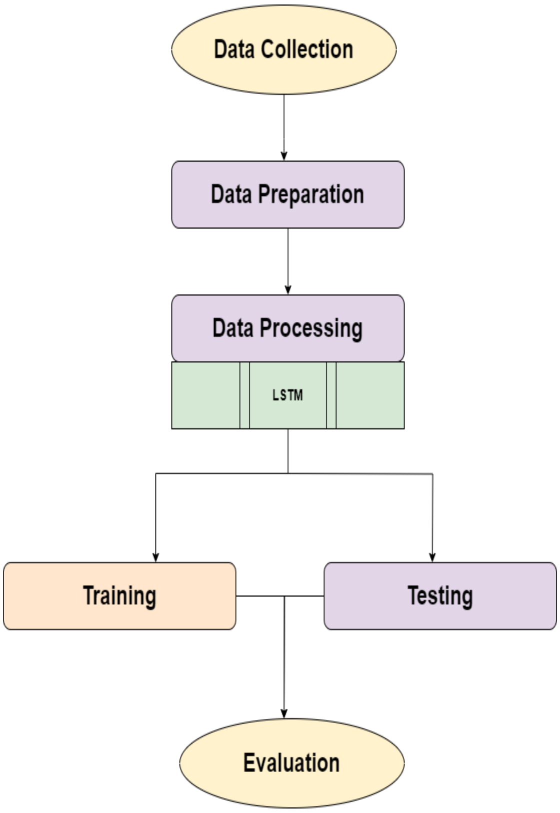
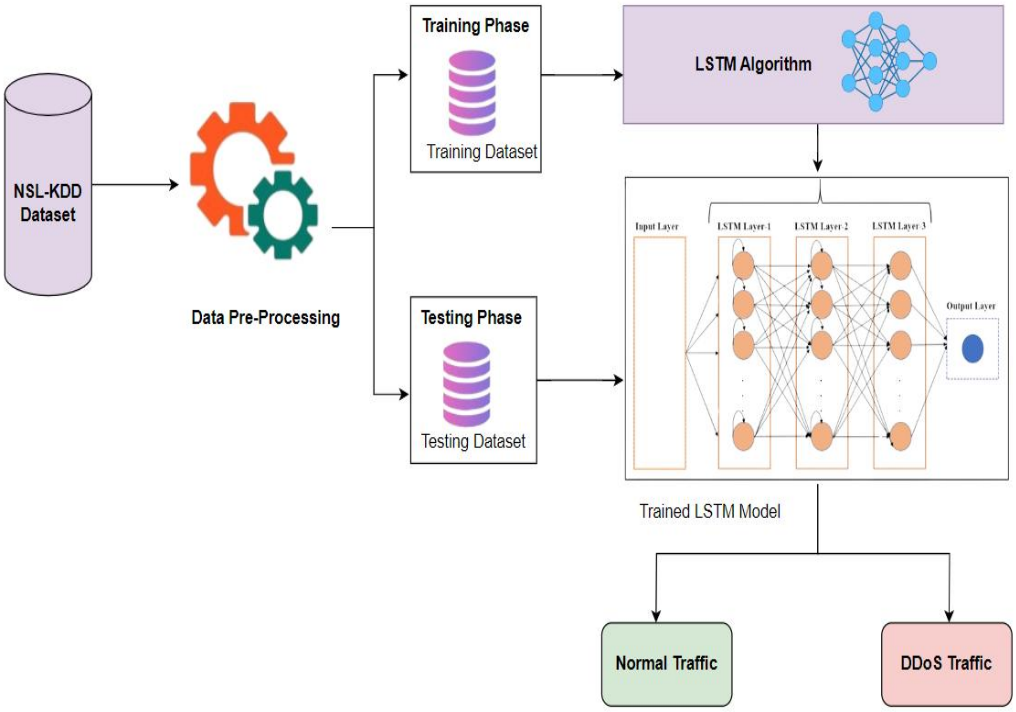


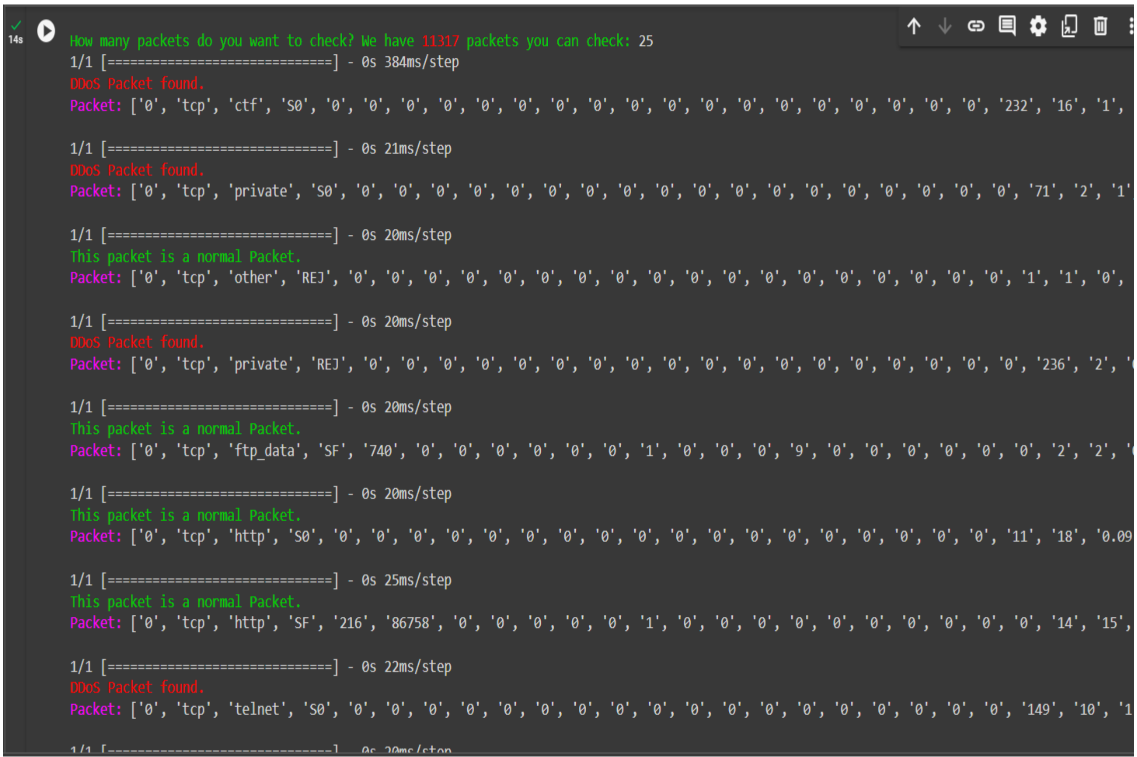
Fig 1.4 Workflow of DDoS attack

Data Collection: Acquiring data from various sources.
Data Preparation: Cleaning and organizing the data for analysis
Model Training: Using algorithms like LSTM (Long Short-Term Memory) to train the model on the data.
Model Testing: Evaluating the model's performance with a separate set of data.
Evaluation: Assessing the accuracy and effectiveness of the model.

System Design :



5.1 Detection



```
How many packets do you want to check? We have 11317 packets you can check: 25
1/1 [==============================] - 0s 384ms/step
DDoS Packet found.
Packet: ['0', 'tcp', 'ctf', 'S0', '0', '0', '0', '0', '0', '0', '0', '0', '0', '0', '0', '0', '0', '0', '0', '0', '0', '0', '232', '16', '1',

1/1 [==============================] - 0s 21ms/step
DDoS Packet found.
Packet: ['0', 'tcp', 'private', 'S0', '0', '0', '0', '0', '0', '0', '0', '0', '0', '0', '0', '0', '0', '0', '0', '0', '0', '0', '71', '2', '1'

1/1 [==============================] - 0s 20ms/step
This packet is a normal Packet.
Packet: ['0', 'tcp', 'other', 'REJ', '0', '0', '0', '0', '0', '0', '0', '0', '0', '0', '0', '0', '0', '0', '0', '0', '0', '0', '1', '1', '0',

1/1 [==============================] - 0s 20ms/step
DDoS Packet found.
Packet: ['0', 'tcp', 'private', 'REJ', '0', '0', '0', '0', '0', '0', '0', '0', '0', '0', '0', '0', '0', '0', '0', '0', '0', '0', '236', '2', '

1/1 [==============================] - 0s 20ms/step
This packet is a normal Packet.
Packet: ['0', 'tcp', 'ftp_data', 'SF', '740', '0', '0', '0', '0', '0', '0', '1', '0', '0', '0', '9', '0', '0', '0', '0', '0', '0', '2', '2', '

1/1 [==============================] - 0s 20ms/step
This packet is a normal Packet.
Packet: ['0', 'tcp', 'http', 'S0', '0', '0', '0', '0', '0', '0', '0', '0', '0', '0', '0', '0', '0', '0', '0', '0', '0', '0', '11', '18', '0.09

1/1 [==============================] - 0s 25ms/step
This packet is a normal Packet.
Packet: ['0', 'tcp', 'http', 'SF', '216', '86758', '0', '0', '0', '0', '0', '1', '0', '0', '0', '0', '0', '0', '0', '0', '0', '0', '14', '15',

1/1 [==============================] - 0s 22ms/step
DDoS Packet found.
Packet: ['0', 'tcp', 'telnet', 'S0', '0', '0', '0', '0', '0', '0', '0', '0', '0', '0', '0', '0', '0', '0', '0', '0', '0', '0', '149', '10', '1

1/1 [==============================] - 0s 20ms/step
```

Fig 1.6 DDoS detection demo using KDD Dataset

6. Conclusion and Future Work

It is true that DDoS detection is not perfect, even when the attacking or DDoS packets are known. Future methods will always be distinct from one another. But with to advancements in artificial intelligence, particularly the RNN's Long Short-Term Memory technique, it is now always feasible to search for packet patterns and sequences. The second-generation machine learning framework from Google, TensorFlow, made it much easier to train many models in a short period of time. The accuracy of the SVM model was 96%, which is 3% less accurate than the LSTM RNN. It has been demonstrated that the LSTM recurrent neural network algorithm detects DDoS attacks more accurately than other widely used machine learning techniques.

Future work on the project can focus further on refining the LSTM and other deep learning models that are being used, with the goal of increasing detection accuracy and reducing false positives. To achieve significant performance improvements, this means investigating innovative methods in model construction, feature selection, and hyperparameter modification. In order to present a more comprehensive picture of possible dangers, there is also potential for integrating a larger range of data sources outside network traffic, such as system logs, user behaviour analytics, and threat intelligence feeds. The system's capacity to identify complex DDoS attacks in real time may be greatly increased by creating methods for efficiently fusing and analysing multi-modal data. Additionally, studies might concentrate on strengthening the system's resistance to hostile attacks, looking at methods like adversarial training and robust optimization to lessen vulnerabilities.

7. REFERENCE :

[1] Akgun, D., Hizal, S., Cavusoglu, U.: A new DDoS attacks intrusion detection model based on deep learning for cybersecurity. Comput. Secur. 118, 102748 (2022)

[2] Elsayed, M.S., Le-Khac, N.A., Dev, S., Jurcut, A.D.: DDoSNet: a deep-learning model for detecting network attacks. In: 2020 IEEE 21st International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM), pp. 391-396 (2020)

[3] Alamri, H.A., Thayananthan, V.: Bandwidth control mechanism and extreme gradient boosting algorithm for protecting software-defined networks against DDoS attacks. IEEE Access 8, 194269-194288 (2020)

[4] Shurman, M.M., Khrais, R., Yateem, A.A.: DoS and DDoS attack detection using deep learning and IDS. Int. Arab J. Inf. Technol. 17, 655-661 (2020)

[5] Pontes, C.F.T., de Souza, M.M.C., Gondim, J.J.C., Bishop, M., Marotta, M.A.: A new method for flow-based network intrusion detection using the inverse potts model. IEEE Trans. Netw. Serv. Manage. 18, 1125-1136 (2019)

[6] Zhou, H., Zheng, Y., Jia, X., Shu, J.: Collaborative prediction and detection of DDoS attacks in edge computing: a deep learning-based approach with distributed SDN. Comput. Netw. 225, 109642 (2023)

[7] Ganeshan, E.S.G.S.R, R., Jingle, I.D.J., Ananth, J.P.: FACVO-DNFN: deep learning-based feature fusion and distributed denial of service attack detection in cloud computing. Knowl.- Based Syst. 261, 110132 (2023)

[8] S. Das, D. Venugopal, S. Shiva and F. T. Sheldon, "Empirical evaluation of the ensemble framework for feature selection in DDoS attack", *Proc. 7th IEEE Int. Conf. Cyber Secur. Cloud Comput. (CSCloud)*, pp. 56-61, 2020.

[9] M. Sakurada and T. Yairi, “Anomaly detection using autoencoders with nonlinear dimensionality reduction,” in Proc. MLSDA 2014 2nd Workshop on Machine Learning for Sensory Data Analysis, 2014, pp. 4–11.

[10] C. Yin, Y. Zhu, J. Fei, and X. He, “A deep learning approach for intrusion detection using recurrent neural networks,” IEEE Access, vol. 5, pp. 21954–21961, 2017.

[11] F. Jiang, Y. Fu, B. B. Gupta, F. Lou, S. Rho, F. Meng, and Z. Tian, “Deep learning based multi-channel intelligent attack detection for data security,” IEEE transactions on Sustainable Computing, 2018.

[12] Y. Bengio, P. Lamblin, D. Popovici, and H. Larochelle, “Greedy layerwise training of deep networks,” in Advances in neural information processing systems, 2007, pp. 153–16

[13] Ujjan, Raja Majid Ali, et al. "Towards sFlow and adaptive polling sampling for deep learning-based DDoS detection in SDN." *Future Generation Computer Systems* 111 (2020): 763-779.

[14] Wei, Yuanyuan, et al. "Ae-mlp: A hybrid deep learning approach for ddos detection and classification." *IEEE Access* 9 (2021): 146810-146821.

[15] Wei, Y., Jang-Jaccard, J., Sabrina, F., Singh, A., Xu, W., & Camtepe, S. (2021). Ae-mlp: A hybrid deep learning approach for ddos detection and classification