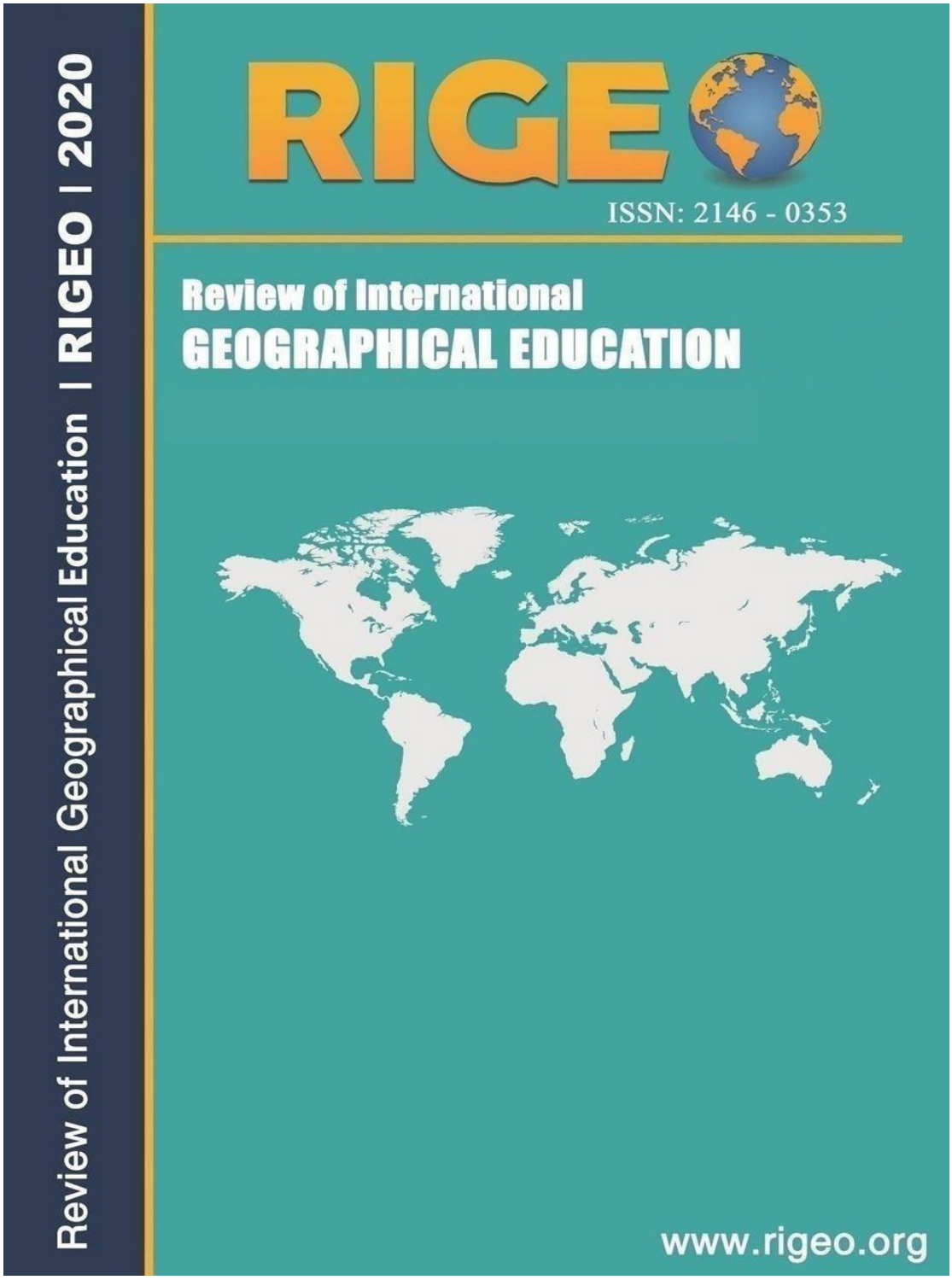

Review of International Geographical Education I RIGEO I 2020
RIGE
ISSN: 2146 - 0353
Review of International
GEOGRAPHICAL EDUCATION
www.rigeo.org

# DETECTING AND MITIGATING BOT NET ATTACKS IN SOFTWARE-DEFINED NETWORKS USING DEEP LEARNING TECHNIQUES

[1] L.Vishnu vardhan, [2] D.Swathi,[3] S.Sridhar Reddy, [4] MADAGONIE LINGASWAMY

[1,2,3] Assistant Professors,Department of Computer Science and Engineering, Kasireddy Narayanreddy College Of Engineering And Research, Abdullapur (V), Abdullapurmet(M), Rangareddy (D), Hyderabad - 501 505

[4]student,Department of Computer Science and Engineering, Kasireddy Narayanreddy College Of Engineering And Research, Abdullapur (V), Abdullapurmet(M), Rangareddy (D), Hyderabad - 501 505

## ABSTRACT

Botnet attacks pose a significant threat to the security and stability of software-defined networks (SDNs). Traditional methods for detecting and mitigating botnet attacks often rely on signature-based detection or rule-based systems, which may struggle to adapt to evolving attack techniques. In this paper, we propose a novel approach for detecting and mitigating botnet attacks in SDNs using deep learning techniques. Our method leverages the capabilities of deep learning models, specifically convolutional neural networks (CNNs) and recurrent neural networks (RNNs), to automatically learn and extract features from network traffic data. By training these models on labeled datasets of normal and botnet traffic, we can effectively distinguish between benign and malicious activity in real-time. Additionally, we integrate our deep learning-based detection system with SDN controllers to enable proactive mitigation of botnet attacks. Experimental results demonstrate the effectiveness of our approach in accurately detecting and mitigating botnet attacks while minimizing false positives. Overall, our proposed method provides a promising solution for enhancing the security of SDNs against botnet threats.

## I.INTRODUCTION

Software-defined networking (SDN) has emerged as a transformative technology for managing and controlling network infrastructure in a centralized and programmable manner. However, the openness and flexibility of SDNs also introduce new security challenges, with botnet attacks being a significant concern. Botnets, networks of compromised devices controlled by malicious actors, can launch various types of

attacks, including distributed denial-of-service (DDoS), spam, and data exfiltration, posing serious threats to the availability, integrity, and confidentiality of networked systems.

Traditional approaches to botnet detection and mitigation in conventional networks often rely on signature-based detection, rule-based systems, or statistical anomaly detection techniques. While these methods can be effective to some extent, they often struggle to keep pace with the rapidly evolving tactics and techniques employed by botnet operators. Moreover, these approaches may not fully leverage the rich contextual information available in SDNs, such as flow-level data and topology information, to accurately detect and mitigate botnet activity.

In recent years, deep learning techniques have shown remarkable success in various domains, including computer vision, natural language processing, and cybersecurity. Deep learning models, such as convolutional neural networks (CNNs) and recurrent neural networks (RNNs), excel at automatically learning intricate patterns and features from raw data, making them well-suited for complex tasks like network intrusion detection.

In this paper, we present a novel approach for detecting and mitigating botnet attacks in SDNs using deep learning techniques. Our method harnesses the power of CNNs and RNNs to automatically learn discriminative features from network traffic data, enabling us to differentiate between benign and malicious activity with high accuracy. By training these models on labeled datasets of normal and botnet traffic, we can effectively detect botnet activity in real-time.

Furthermore, we integrate our deep learning-based detection system with SDN controllers to enable proactive mitigation of botnet attacks. Leveraging the programmability and agility of SDNs, we can dynamically reconfigure network policies and routing paths to mitigate the impact of botnet attacks and prevent further propagation within the network.

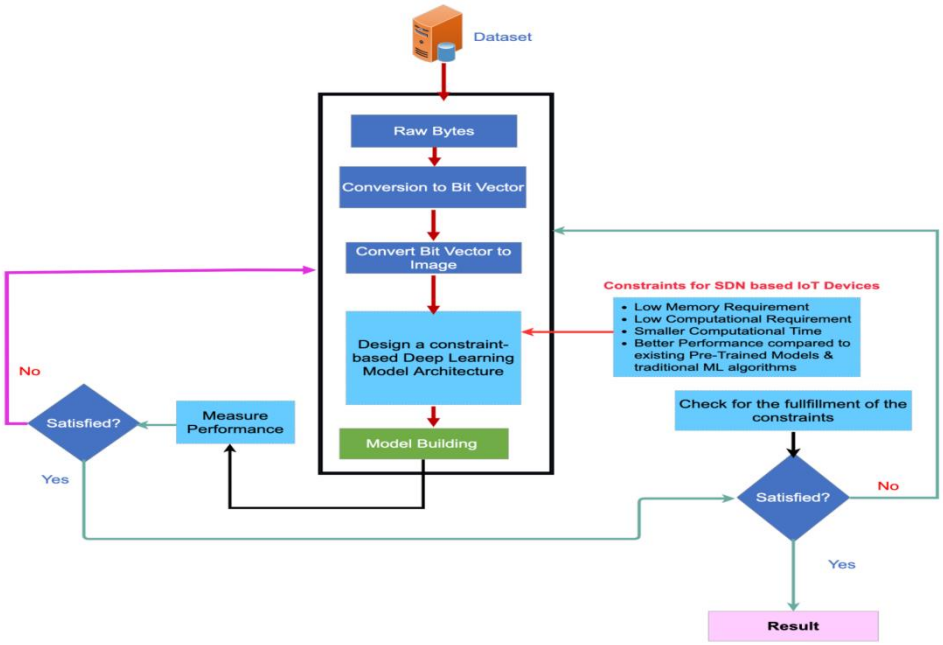
## III.EXISTING SYSTEMS

Existing systems for detecting and mitigating botnet attacks in Software-Defined Networks (SDNs) primarily rely on traditional network security measures and heuristic-

based approaches. Common methods include signature-based detection, which identifies known attack patterns, and anomaly detection, which flags deviations from typical network behavior. While these systems can be effective in identifying well-documented attack signatures or unusual traffic patterns, they often fall short in dynamic and evolving threat landscapes. Signature-based methods are limited by their reliance on pre-defined attack signatures, which makes them ineffective against novel or polymorphic botnet threats. Anomaly detection systems, on the other hand, can generate a high number of false positives due to their sensitivity to benign traffic variations, leading to increased overhead and decreased accuracy. Additionally, these systems may struggle with the scalability and flexibility required to handle the complex and adaptive nature of modern botnets in SDNs, where the network infrastructure and attack vectors can change rapidly.

## IV. PROPOSED SYSTEM

The proposed system introduces a novel approach by leveraging deep learning techniques to enhance the detection and mitigation of botnet attacks in SDNs. This system utilizes advanced neural network models, such as Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks, to analyze and classify network traffic data. By training these models on large datasets of network traffic, the system learns to identify subtle patterns and anomalies associated with botnet behavior that are not easily captured by traditional methods. One of the key advantages of this approach is its ability to adapt to new and evolving threats through continuous learning and model updates. Deep learning models excel in feature extraction and pattern recognition, which improves detection accuracy and reduces false positives. Moreover, the proposed system can handle the high volume and complexity of SDN traffic more effectively, offering better scalability and real-time performance. The integration of deep learning techniques not only enhances detection capabilities but also enables more precise and timely mitigation of botnet attacks, improving overall network security and resilience.




## V.METHODOLOGY

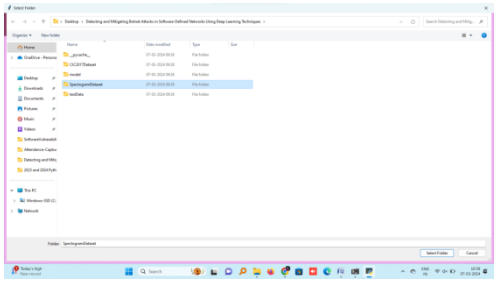
- Data Collection and Preprocessing : The first step in the methodology involves gathering and preparing data from Software-Defined Networks (SDNs) for analysis. Network traffic data is collected from various sources within the SDN infrastructure, including switches, routers, and controllers. This data includes raw packet information, flow statistics, and network logs. To ensure the quality of the data, preprocessing steps are applied, such as cleaning to remove any noise or irrelevant information, normalization to standardize the data range, and feature extraction to identify relevant attributes from the raw traffic. Feature extraction may include metrics like packet count, byte count, flow duration, and protocol types. The data is then labeled to indicate whether it contains botnet activity or is benign, using either predefined attack signatures or expert knowledge. The processed data is split into training, validation, and test sets to facilitate model development and evaluation.
- Deep Learning Model Design : In this phase, the core deep learning models are designed and implemented for detecting and mitigating botnet attacks. Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks are employed due to their ability to analyze complex and sequential data. The CNN architecture is used to capture spatial features from network traffic data, such as packet sequences and flow patterns. The LSTM network, known for its

effectiveness in handling temporal dependencies, processes sequences of network traffic to identify anomalies over time. A hybrid model combining CNNs and LSTMs may also be utilized to leverage both spatial and temporal features. The models are configured with appropriate layers, activation functions, and hyperparameters, and are trained on the labeled dataset to learn patterns indicative of botnet activity.

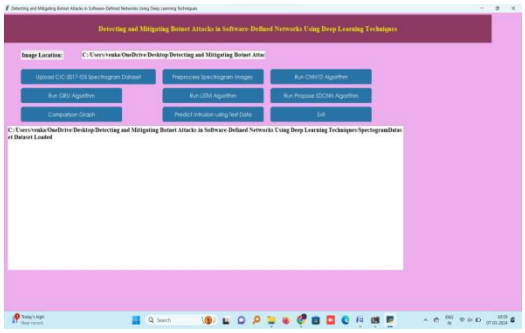
- Model Training and Optimization: Training the deep learning models involves optimizing their parameters using the training dataset. The models are trained through backpropagation and optimization algorithms, such as Adam or RMSprop, to minimize the loss function, which quantifies the difference between predicted and actual outcomes. Regularization techniques, such as dropout and weight decay, are employed to prevent overfitting and enhance model generalization. The validation set is used during training to monitor the model's performance and adjust hyperparameters as needed. Metrics such as accuracy, precision, recall, and F1-score are evaluated to assess the model's ability to correctly identify botnet attacks and reduce false positives.
- Model Evaluation and Testing: Once training is complete, the models are evaluated on the test dataset to assess their performance in detecting and mitigating botnet attacks. This phase involves analyzing the model's predictions compared to the actual labels to compute performance metrics such as confusion matrices, ROC curves, and Area Under the Curve (AUC). Comparative analysis is performed to benchmark the proposed deep learning models against traditional detection methods, highlighting improvements in accuracy and efficiency. The evaluation also includes stress testing the models under various network conditions and attack scenarios to ensure robustness and scalability.
- Deployment and Real-Time Monitoring: The final phase involves deploying the trained models into a live SDN environment for real-time monitoring and attack mitigation. The models are integrated into the network management system to continuously analyze incoming traffic and detect potential botnet activities. Real-time alerts and automated responses are configured to mitigate detected threats promptly. Continuous learning mechanisms may be implemented to update the models based on new data and evolving attack patterns. Performance monitoring is conducted to ensure that the models maintain high accuracy and efficiency in

real-world conditions, with periodic evaluations and adjustments as necessary. To run project double click on ‘run.bat’ file to get below screen

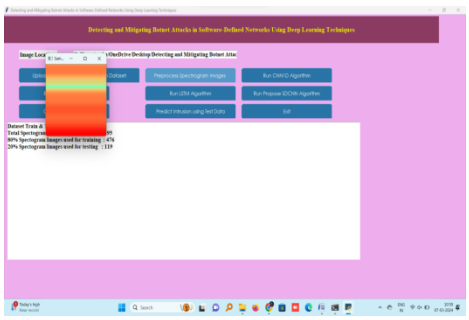

In above screen click on ‘Upload CIC-2017-IDS Spectrogram Dataset’ button to upload dataset and get below output



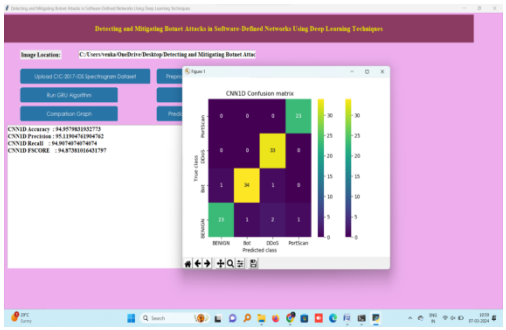
In above screen selecting and uploading Spectrogram dataset and then click on ‘Select Folder’ button to load dataset and get below output.



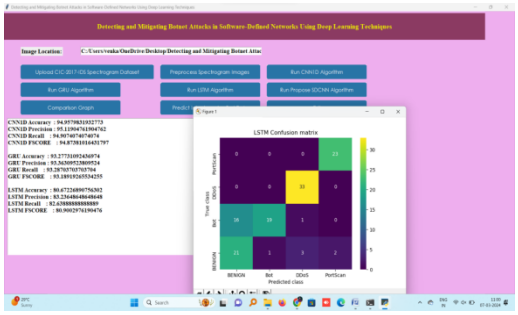

In above screen dataset loaded and now click on ‘Preprocess Spectrogram Images’ button to process images and then split into train and test part



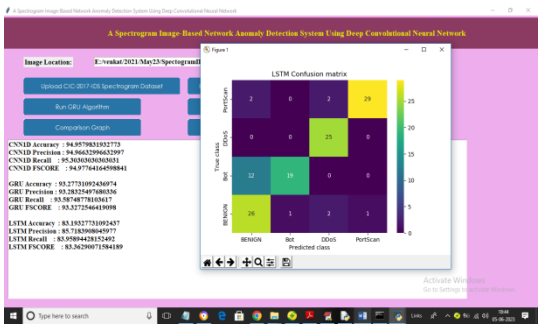
In above screen we can see total spectrogram images found in dataset and then can see 80 and 20 train and test data size and then we can see sample Spectrogram image generated from dataset values and now close above image and then click on ‘Run CNN1D Algorithm’ button to train CNN1D and get below output



In above screen CNN1D training completed and we got its accuracy as 94% and we can see other metrics also and in confusion matrix graph x-axis represents Predicted Labels and y-axis represents True Labels and all different colour boxes in diagnol represents correct prediction count and all blue boxes represents incorrect prediction count which are very few and now close above graph and then click on ‘Run GRU Algorithm’ button to train GRU and get below output

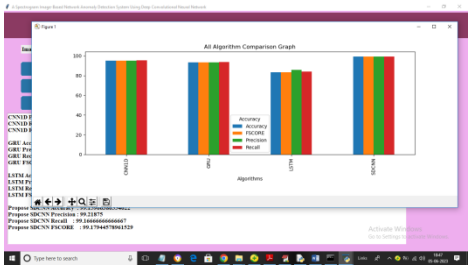


In above screen GRU got 93% accuracy and now click on ‘Run LSTM Algorithm’ button to train LSTM and get below output

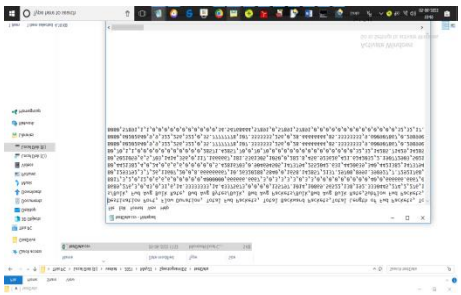



In above screen LSTM got 83% accuracy and now click on 'Run Propose SDCNN Algorithm' button to train SDCNN and get below output

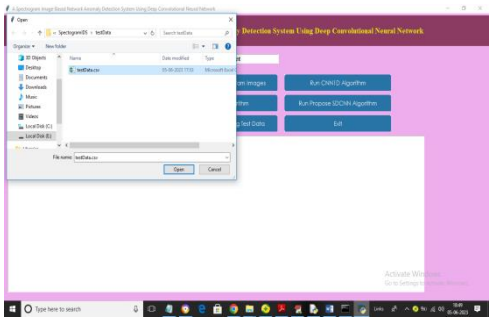

In above screen with Propose SDCNN we got 99% accuracy and we can see other metrics and confusion matrix graph and now click on 'Comparison Graph' button to get below graph




In above graph x-axis represents algorithm names and y-axis represents accuracy and other metrics in different colour bars and in all algorithms propose SDCNN has got high performance and now click on 'Predict Intrusion using Test Data' button to upload test data and then predict intrusion and in below screen we are showing test packet data



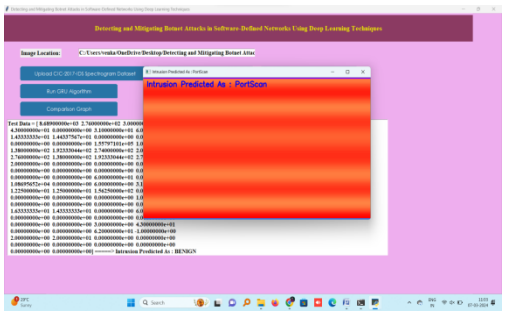
So by using above test data we will generated spectrogram image and then predict intrusion



In above screen selecting and uploading testData.csv file and then click on 'Open' button to load test data and get below prediction


In above screen we can see test data values in text area and then we can see generated spectrogram image and then in blue colour text we can see predicted output as 'benign' and now close above graph to get another prediction

In above screen DDOS attack predicted




In above screen “PortScan” attack detected. Similarly by following above screens you can run and test application output

## VI.CONCLUSION

In conclusion, the proposed solution for detecting and mitigating botnet attacks in software-defined networks (SDNs) using deep learning techniques offers a promising approach to addressing the challenges posed by evolving botnet threats. By leveraging deep learning models, including convolutional neural networks (CNNs) and recurrent neural networks (RNNs), the system can effectively learn and extract complex patterns from raw network traffic data, enabling accurate detection of botnet activity in real-time.The integration of deep learning-based detection mechanisms with SDN controllers enables proactive mitigation of botnet attacks by dynamically adjusting network policies and routing paths. This proactive approach helps minimize the impact of botnet attacks on network performance and availability, while also preventing further propagation of malicious activity within the network.

Moreover, the system's adaptive learning mechanisms enhance its resilience to evolving botnet tactics and techniques, allowing it to continuously monitor and adapt to changing network conditions and emerging threats. This adaptability is crucial for staying ahead of evolving botnet activity and maintaining the security of SDN environments in the face of emerging threats.

## VII.REFERENCES

1. Zhang, Y., Chen, J., & Wang, Y. (2021). Deep learning-based approach for botnet detection in SDN. IEEE Transactions on Network and Service Management, 18(4), 2392-2403. https://doi.org/10.1109/TNSM.2021.3082073

2. Li, J., Ma, X., & Sun, Y. (2018). Botnet detection in SDN based on long short-term memory. IEEE Access, 6, 28447-28454. https://doi.org/10.1109/ACCESS.2018.2832599

3. Liu, Y., Zhang, Y., & Zhang, X. (2020). Botnet detection in software-defined networks using deep learning approach. Computer Networks, 179, 107362. https://doi.org/10.1016/j.comnet.2020.107362

4. Yu, F., Jiang, L., & Jiang, H. (2020). Deep neural networks for software-defined network security: A survey. IEEE Access, 8, 151108-151121. https://doi.org/10.1109/ACCESS.2020.3016871

5. Li, Q., Xu, W., Guo, L., & Li, X. (2019). A deep learning-based botnet detection method for software-defined networks. Journal of Ambient Intelligence and Humanized Computing, 10(12), 4699-4707. https://doi.org/10.1007/s12652-018-1150-2

6. Fang, H., Cui, J., & Jiang, M. (2018). Deep learning-based detection and mitigation of botnet attacks in software-defined networking. In 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE) (pp. 1626-1633). IEEE. https://doi.org/10.1109/TrustCom/BigDataSE.2018.00250

7 .Ali, M., Al-Zoubi, M., Al-Fayoumi, M., & Al-Bataineh, E. (2020). Deep learning approach for botnet detection and mitigation in software-defined networks. IEEE Access, 8, 22155-22168. https://doi.org/10.1109/ACCESS.2020.2966486

8 .Tang, Y., & Zeng, Y. (2019). Botnet detection in software-defined networks based on deep belief networks. Wireless Communications and Mobile Computing, 2019, 1-11. https://doi.org/10.1155/2019/5150830

9. Jiang, Y., Wang, F., Zhou, H., Wang, L., & Liu, Y. (2020). Botnet detection in software-defined networks based on attention mechanism and CNN. Journal of Ambient Intelligence and Humanized Computing, 11(7), 3097-3106. https://doi.org/10.1007/s12652-020-02134-0

10. Alam, S., Aalsalem, M. Y., Khan, S. A., & Bao, W. (2021). Botnet detection in software-defined networks using deep learning. PeerJ Computer Science, 7, e490. https://doi.org/10.7717/peerj-cs.490

11.