iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** V **Month of publication:** May 2024

DOI: https://doi.org/10.22214/ijraset.2024.61580

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue V May 2024- Available at www.ijraset.com

Improving the Accuracy of DDos Attack Detection by Fine Tuning CNN-LSTM Classifier

Dr. Karthik Elangovan[1], K. Uthej[2], M. Mujammil[3], K. Purna Akshay[4]
[1]*Assistant Professor, Department Of Computer Science and Engineering, Srm Institute Of Science And Technology Ramapuram Chennai*
[2, 3, 4]*B.Tech CSE with Specialization in Cyber Security, SRM University, India*

Abstract: ***DDoS attacks also known as distributed denial of service (DDoS) attacks have emerged as one of the most serious and fastest-growing threats on the Internet. Denial-of-service (DDoS) attacks are an example of cyber-attacks that target a specific system or network in an attempt to render it inaccessible or unusable for a period of time. As a result improving the detection of diverse types of DDoS cyber threats with better algorithms and higher accuracy while keeping the computational cost under control has become the most significant component of detecting DDoS cyber threats. DDoS (distributed denial-of-service) attack originates from many sources scattered over multiple network locations. DoS attacks are primarily motivated by the desire to significantly degrade the performance or completely consume a certain resource and a process to exploit a machine defect and cause failure of a processing or exhausting the system resources by exploiting a system flaw. Yet another method of assaulting the target system is to flood the network and monopolies it so preventing anyone else from utilizing it. DDoS attack has a high impact on crashing the network resources making the target servers unable to support the valid users. The current methods deploy Machine Learning (ML) for intrusion detection against DDoS attacks in the SDN network using the standard datasets. However these methods suffer several drawbacks and the used datasets do not contain the most recent attack patterns - hence lacking in attack diversity. In this paper we propose novel detection system against DDoS attacks in SDN environments. Our method is based on Deep Learning (DL) technique combining the LSTM with CNN. We evaluate our model using the newly released dataset CIC DDoS which contains a comprehensive variety of DDoS attacks and addresses the gaps of the existing current datasets. We obtain a significant improvement in attack detection as compared to other benchmarking methods. Hence our model provides great confidence in securing these networks.***

I. INTRODUCTION

Software-Defined Networking (SDN) is a new technology that facilitates management and programmability of the network system. SDN makes the network more reliable by centralizing it through separating the control plane from the data plane.However the emerging paradigm is subjected to many security vulnerabilities and new faults that can be used by attackers to create different types of malicious attacks. Further the common threats and attacks which can exploit the classical network infrastructure can also exist in the SDN environment. More over these attacks can impact the whole SDN system that includes multi-devices from different vendors unlike in the traditional network where in general an attack mainly crashes a part of the network devices from a single vendor only without affecting the entire network. There are many attack vectors that can exploit the SDN network One of the most common and dangerous types of attacks is Distributed Denial of Service (DDoS) attack which can prevent legitimate users from access their network services. DDoS attack can deplete the network resources or target the servers by flooding the network with a large number of volume traffics. In addition because of the IoT era there are many devices that can be connected to the Internet. Hence attackers can exploit many types of DDoS attacks by leveraging massive numbers of bots from different locations. The execution of DDoS attacks using bots devices is hard to discover. As the number and complexity of cybersecurity attacks increase at a tremendous pace on a daily basis defenders are in need to find more effective protection measures that rely on machine intelligence. To this account a recent trend in information security is the adoption of solutions based on Artificial Neural Networks (ANNs) to analyze network traffic and the behavior of software running on computers to identify possible compromised systems or unauthorized access attempts. Compared to traditional signature based and anomaly-based approaches ANN based threat detection methods are more resilient to variations on attack patterns and are not constrained by the requirement to define thresholds for attack detection. However training and updating an ANN model for effective threat detection is a non-trivial task especially when dealing with zero-day vulnerabilities and attack vectors due to the complexity and variability of emerging attacks and the lack of data with relevant and upto-date attack profiles. There are a number of survey studies that have proposed taxonomies with respect to DDoS attacks.

Although all have done a commendable job in proposing new taxonomies the scope of attacks has so far been limited. There is a need to identify new attacks and come up with new taxonomies. Hence we have analyzed new attacks that can be carried out using TCP/UDP based protocols at the application layer and proposed a new taxonomy. Reflection-based DDoS: Are those kinds of attacks in which the identity of the attacker remains hidden by utilizing legitimate third-party component. The packets are sent to reflector servers by attackers with source IP address set to target victim's IP address to overwhelm the victim with response packets. These attacks can be carried out through application layer protocols using transport layer protocols i.e. Transmission control protocol (TCP) User datagram protocol (UDP) or through a combination of both. As Figure shows in this category TCP based attacks include MSSQL SSDP while as UDP based attacks include Char-Gen NTP and TFTP. There are certain attacks that can be carried out using either TCP or UDP like DNS LDAP NETBIOS and SNMP. Exploitation-based attacks: Are those kinds of attacks in which the identity of the attacker remains hidden by utilizing legitimate third-party component. The packets are sent to reflector servers by attackers with the source IP address set to the target victim's IP address to overwhelm the victim with response packets. These attacks can also be carried out through application layer protocols using transport layer protocols i.e. TCP and UDP. TCP based exploitation attacks include SYN flood and UDP based attacks include UDP flood and UDP- Lag. UDP flood attack is initiated on the remote host by sending a large number of UDP packets. A Distributed Denial of Service (DDoS) attack in late 2016, when three uninterrupted DDoS attacks were launched against the Domain Name System (DNS) provider Dyn, was a warning signal of the dangers of targeted DDoS attacks. DDoS attacks have become one of the most severe threats to network security, with the first reported attack published by the Computer Incident Advisory Capability in 1999. While many mitigation systems have been developed in academia and industry, the threat of DDoS attacks is still severe and increasing yearly. In February 2018, a significant DDoS attack against GitHub overcame these mitigation systems. Using BCP38 Network Ingress Filtering which, if deployed on the Internet, may stop packets with forged IP addresses from proceeding over the network, this type of attack could be mitigated. However, research conducted using a random forest algorithm

II. RELATED WORK

Research aimed at enhancing the accuracy of DDoS attack detection through fine-tuning CNN-LSTM classifiers has been a focal point of recent studies. The exploration of various methodologies has led to significant advancements in improving the effectiveness of these classifiers.

Hybrid models, combining CNNs and LSTMs, have emerged as a promising avenue of research. CNNs are adept at capturing spatial dependencies, while LSTMs excel in modeling temporal dependencies. Integrating these architectures allows for a comprehensive analysis of DDoS attack traffic, capturing both spatial and temporal features, thus enhancing the detection capability of the classifiers.

Moreover, researchers have delved into feature engineering techniques tailored specifically for DDoS detection. By devising novel features and preprocessing methods, they aim to capture the intricate characteristics of DDoS attacks more accurately. These enhancements contribute to the overall performance improvement of CNN-LSTM classifiers in detecting DDoS attacks.

Fine-tuning strategies play a pivotal role in optimizing the performance of CNN-LSTM classifiers. Researchers have meticulously explored various parameters, including learning rates, optimization algorithms, and network architectures, to fine-tune these classifiers for the specifics of DDoS attack traffic. This fine-tuning process enhances the accuracy and effectiveness of DDoS attack detection systems.

Furthermore, data augmentation techniques have been investigated to bolster the robustness of CNN-LSTM classifiers against diverse DDoS attack scenarios and network conditions. Augmenting the training data with noise, perturbations, or synthetic samples enhances the generalization ability of the classifiers, improving their performance in real-world deployment scenarios.

Transfer learning has emerged as another promising approach to enhance the accuracy of DDoS attack detection. By leveraging pre-trained models on related tasks or datasets, researchers can transfer knowledge to CNN-LSTM classifiers, particularly in scenarios where labeled data is scarce or unavailable.

Additionally, researchers have proposed and evaluated various evaluation metrics to assess the effectiveness of fine-tuned CNN-LSTM classifiers for DDoS attack detection. These metrics provide valuable insights into the performance of the classifiers under different experimental conditions, guiding further improvements in detection accuracy and robustness.

Overall, by incorporating these diverse approaches and innovative techniques, researchers aim to continuously advance the accuracy and effectiveness of DDoS attack detection using fine-tuned CNN-LSTM classifiers, thereby bolstering the security and resilience of computer networks against malicious threats.

III. PROPOSED METHOD

1) In the training phase, we use datasets that contain network traffic data. We preprocess this data to extract relevant features, such as packet length, packet direction, and flow duration. We also use an open switch to simulate network traffic and capture more data for training
2) Next, in the feature selection and prediction phase, we train different machine learning models on the preprocessed data. We select the best model based on its accuracy in predicting network traffic. Then, we use feature selection techniques to choose the most important features from the model to reduce computational complexity and improve the accuracy of our prediction
3) Since both CICIDS2017 and CIC-DDoS2019 datasets have high class imbalance rate (CIR), we employ Synthetic Minority Oversampling Technique (SMOTE) to increase the quantity of minority class samples by generating samples that does not exist in the original dataset. With this arrangement, it can avoid overfitting problem when constructing classification model. Term Memory (LSTM) layer, a fully connected hidden layer that consists of 50 RELU (Rectified Linear Unit) units, a 50% dropout layer, and a soft max layer that linearly transforms the output of the previous layer to compute the probability scores of the labels
4) Machine learning is used to classify things, discover patterns, predict outcomes, and make informed decisions. The many machine learning methods can be broadly classified into four types, namely, supervised learning, semi supervised learning, unsupervised learning, and reinforcement learning. Each of these models in turn contains multiple algorithms. No single machine learning model algorithm can achieve the best results for any dataset and any data feature. Usually, the size of the dataset, the characteristics of the dataset, and the nature of the problem to be solved need to be taken into account before a machine learning model algorithm is selected.

If an inappropriate machine learning model algorithm is selected, not only will it not yield accurate results, but it will lead to overfitting of the model or will require longer training and prediction time for effective DDoS attack detection on realistic high speed and high traffic networks. A reasonable choice of machine learning model algorithms can improve accuracy, reduce prediction time, and enhance the generalization ability of the model. Especially in realistic network systems with high-density data flow, anomalous traffic can be detected quickly and effectively through the judicious use of machine learning algorithm models. We leverage and propose a deep learning approach based on LSTM-CNN for detection of DDoS attacks on the SDN. We combine LSTM-CNN with softmax model at the output layer to classify the network traffic into malicious or normal. The trained model behavior is directly controlled by the values of the hyper-parameters where selecting the best values plays a key role in the success of neural network architecture. However selecting the best values of hyper-parameters is still dependent on the best practice or human knowledge. We conducted various experiments to select the optimal values of experiment hyperparameters. The softmax layer takes the decoder output and classifies the input data into normal or attack traffic.

We used categorical-cross entropy as loss function with adam optimizer and ReLU function for activation in all different layers. We evaluate our model using the new released dataset CIC-DDoS which contain a comprehensive variety of DDoS attacks and addresses the gaps of the existing current datasets. We benchmark several state-of-the-art ML models that are well known for detection of DDoS attacks and we evaluate our proposed model in terms of precision recall F-score and accuracy. Our proposed method has the best performance. Finally, in the traffic classification and detection phase, we use the selected features from the previous phase to classify the network traffic into different types, such as normal, malicious, or suspicious.

We use the best feature and model combination to detect potential DDoS attacks and take appropriate action, such as blocking the source of the attack. Overall, our approach leverages machine learning-based feature extraction and classification methods to detect DDoS attacks in real time with high accuracy and efficiency. The main contribution of this paper lies in the combination of different advanced deep-learning techniques, which can be summarized as follows: Novel preprocessing method: We provide a novel preprocessing method for the CICDDoS2019 dataset, which includes all kinds of attacks in both the training and testing subsets, even those that are quite identical.

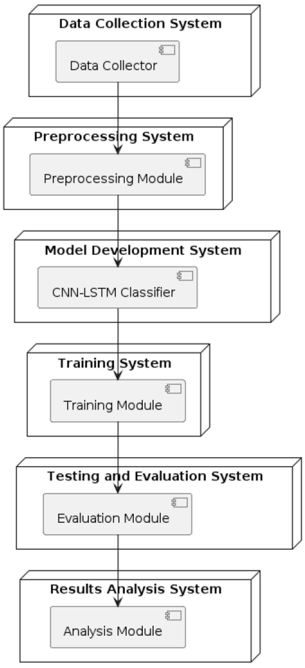
A. *Hybrid Architecture*

We combine The convolutional neural network (CNN), Long short-term memory (LSTM), and autoencoder models in a parallel and cascade manner to create a highly complex architecture. Improved low-frequency traffic

B. *Classification*

We devise a novel training process to improve the accuracy of low-frequency traffic classification. Comparative analysis: We compare our proposed model with several basic deep learning models, as well as some well-known machine learning models.

IV. CLASSIFICATION DIAGRAM OF CNN-LSTM CLASSIFIER

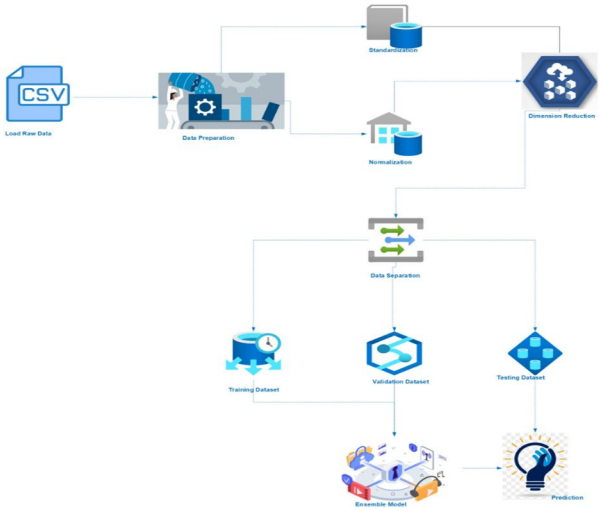


V. HARDWARE AND SOFTWARE REQUIREMENT BACKEND TECHNOLOGIES

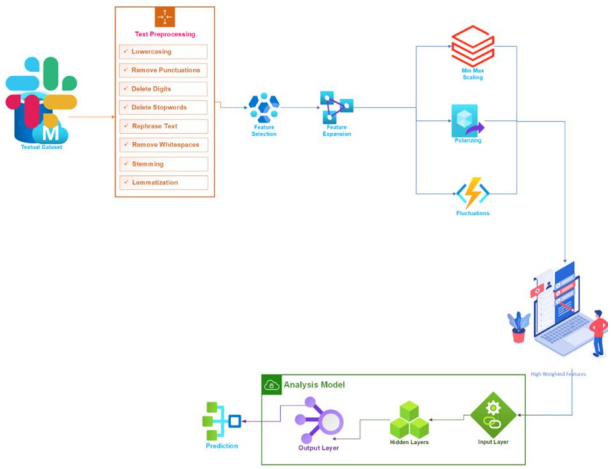
The system is developed in Python, leveraging its flexibility and rich ecosystem of libraries for tasks such as data analysis and machine learning. NumPy is utilized for efficient numerical computations, offering array operations and mathematical functions crucial for data processing. For machine learning tasks like classification and model evaluation, the system employs scikit-learn, a Python library known for its comprehensive suite of algorithms.

Jupyter Notebook serves as the interactive development environment, allowing seamless integration of code, visualizations, and explanatory text. This facilitates reproducible research and collaborative work by providing a platform where code and analysis can be easily shared and documented.

On the frontend, the system utilizes web technologies to enable user interaction and visualization. HTML is used to structure web pages, CSS for styling, and JavaScript for dynamic client-side scripting. Frontend frameworks like React, Angular, or Vue.js may be employed to streamline the development process, offering reusable components and enhanced capabilities for building complex web applications.



VI. ARCHITECTURE DIAGRAM



VII. PROPOSED ALGORITHM

A. *Proposed Algorithm: Probabilistic Analytical Learning Algorithm*

The Probabilistic Analytical Learning Algorithm (PALA) is proposed as an innovative approach to enhance the accuracy of DDoS attack detection by fine-tuning CNN LSTM classifiers. PALA leverages probabilistic analysis to dynamically adjust model parameters based on real-time feedback, optimizing the classifier's performance in detecting DDoS attacks. By continuously analyzing network traffic patterns and adjusting the classifier's parameters, PALA adapts to evolving attack strategies and network conditions, improving detection accuracy and reducing false positives. This adaptive learning approach enhances the robustness and effectiveness of DDoS attack detection systems, enhancing network security and resilience against malicious threats.

Improving DDoS attack detection accuracy entails fine-tuning the CNN LSTM classifier. PALA dynamically adjusts model parameters using probabilistic analysis and real-time feedback, optimizing performance for detecting DDoS attacks. By continuously adapting to network traffic patterns, PALA enhances detection accuracy, reducing false positives, and bolstering network security.

B. *Advantages of Proposed Algorithm:*

Ability to process large amount of data quickly in order to detect attacks.

Better decision-making as to the training time. Efficiently improve time efficiency involves the computation time and communication time. Eliminating the huge workload of traditional methods Proving High Robustness and imperceptibility.

VIII. CONCLUSION

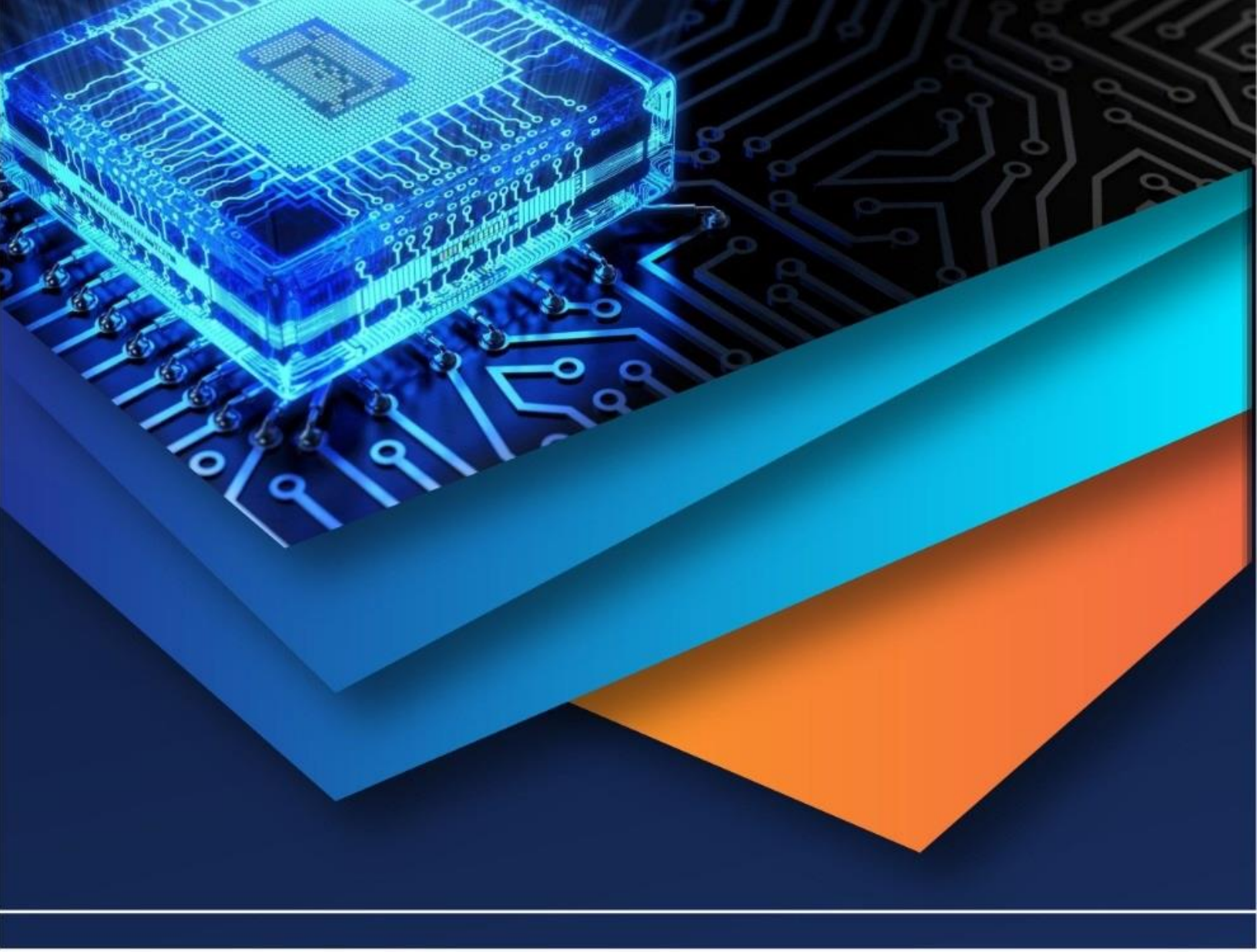
Network virtualization leads to new threats and new exploitable attacks that the ones already existing in the traditional network. The DDoS attack class is considered one of the most aggressive attack types in recent years causing a critical impact on the whole network system. The advent of ubiquitous network-based technologies has increased the associated vulnerabilities. The need for effective network protection tools have never been greater. In this paper we propose an AI-based IDS that is capable of distinguishing between regular and DDoS traffic. In this paper we proposed a new model that is based on DL for the detection of DDoS attacks against SDN network. We used the new released CICDDoS dataset for training and evaluation of our proposed model. The dataset contains comprehensive and most recent DDoS types of attacks. The evaluation of our model showed that gives the highest evaluation metrics in terms of recall precision F-score and accuracy compared to the existing well known classical ML & DL techniques.

REFERENCES

[1] Kuzmanovic and E. W. Knightly, Low-rate TCP-targeted denial of service attacks: The shrew vs. The mice and elephants, in Proc. Conf. Appl., Technol., Archit., Protocols Comput. Commun., New York, NY, USA, 2003, p. 75.

[2] N. Agrawal and S. Tapaswi, Defense mechanisms against DDoS attacks in a cloud computing environment: State-of-the-Art and research chal- Oct. 2019.

[3] M. S. Bonm, K. L. Dias, and S. F. L. Fernandes, Integrated NFV/SDN architectures: A systematic literature review, ACM Comput. Surveys, [10] J. Cao, Q. Li, R. Xie, K. Sun, G. Gu, M. Xu, and Y. Yang, The crosspath attack: Disrupting the $SDN $ control channel via shared links, in Proc.
[4] T. Apostolovic, N. Stankovic, K. Milenkovic, and Z. Stanisavljevic, DDoS Sim System for visual representation of the selected distributed denial of service attacks, in Proc. Zooming Innov. Consum. Technol. Conf. Dominus. (2018).
[5] Hulk Ddos Attack Script Created Using Python Libs.
[6] Y. Zhang, Z. Morley Mao, and J. Wang, Low-rate TCP-targeted dos attack disrupts Internet routing, in Proc. 14th Annu. Network Distrurb. Syst. Secure.
[7] M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, Information metrics for low-rate DDoS attack detection: A comparative evaluation, in Proc.
[8] S. Floyd and V. Jacobson, Random early detection gateways for conges- [30] M. V. Kieu, D. T. Nguyen, and T. T. Nguyen, Using CPR metric to detect and lter low-rate DDoS ows, in Proc. 8th Int. Symp. Inf. Commun. Technol., 2017, p. 325.
[9] N. Meti, D. G. Narayan, and V. P. Baligar, Detection of distributed denial of service attacks using machine learning algorithms in software dened networks, in Proc. Int. Conf. Adv. Comput., Commun. Informat.
[10] S. L. Salzberg, "C4.5: Programs for machine learning" by J. Ross Quinlan, 2001.
[11] J. Ye, X. Cheng, J. Zhu, L. Feng, and L. Song, "A DDoS attack detection method based on SVM in software defined network," Security and Communication
[12] "Ethereum: A Secure Decentralised Generalised Transaction Ledge."
[13] "Blockchain for Financial Services," Accessed: Jul. 1, 2019.
[14] "Etherscan. The Ethereum Block Explorer: Ropsten (Revival) Testnet."
[15] P. Ferguson and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks Which Employ IP Source Address Spoofing" (BCP 38), document RFC 2827, 2000. ietf.org/html/rfc2827
[16] F. Guo, J. Chen, and T.-C. Chiueh, "Spoof detection for preventing DoS put," Systems (ICDCS), Washington, DC, USA, Jul. 2006, p. 37. doi: 10.1109/ ICDCS.2006.78.
[17] "RESTAPI,"Accessed: www.sowrt.com/reference.php , Jul. 1, 2019.
[18] B. B. Zarpelao, R. S Miani, C. T. Kawakani, and S. C. de Alvarenga, "A survey of intrusion detection in Internet of Things," Journal of Network and Computer.
[19] R. Renk, L. Saganowski, W. Holubowicz, and M. Choras, "Intrusion detection system based on matching pursuit," in Proceedings of the 1st International Conference on Intelligent.
[20] W. Lu and A. A. Ghorbani, "Network anomaly detection based on," December 2008.
[21] N. Z. Bawany, J. A. Shamsi, and K. Salah, "DDoS attack detection and mitigation using SDN: Methods, practices, and solutions," Arabian Journal of Science.
[22] S. Shin and G. Gu, "Attacking software-denied networks: A first feasibility study," in Proceedings of the 2nd ACM SIGCOMM Workshop Hot Topics Software.
[23] J. Ye, X. Cheng, and J. Zhu, "A DDoS attack detection method based," April 2018, Article no. 9804061.
[24] H. Xie, T. Tsou, D. Lopez, H. Yin, and V. Gurbani, "Use Cases for Alto With Software Defined Networks," document Internet-Draft draft-xie-alto- sdn-extension-use-cases-01, Working Draft, IETF Secretariat, 2012.
[25] A. Studer and A. Perrig, "The coremelt attack," in Proceedings of the European Symposium Research Computer Secure.
[26] Y. Li, J. Xia, S. Zhang, J. Yan, X. Ai, and K. Dai, "An efficient intrusion detection system based on support vector machines and gradually," January 2012.
[27] F. Kuang, W. Xu, and S. Zhang, "A novel hybrid KPCA and SVM with GA," May 2014.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY