Analysis of Machine Learning Based DDoS Attack Detection Techniques in Software Defined Network

Akshat Gaurav[1], Varsha Arya[2], and Domenico Santaniello[3]
[1]Ronin Institute, Montclair, New Jersey 07043, U.S.(e-mail: akshat.gaurav@roninstitute.org)
[2]Independent Researcher, Taiwan. (email: varshaarya21@gmail.com)
[3]University of Salerno, Italy. (email:dsantaniello@unisa.it)

ABSTRACT Software Deffned Network (SDN) is a novel way of network management. In SDN, control plane and data plane are separated and the incoming traffic is controlled by control plane. Incoming data packets are not handled by the network switches, if there is no matching entry in the forwarding tables, the inbound packet is routed to the controller, the SDN's operating system, for further processing. However, due to this SDN becomes prime target of Distributed denial of services (DDoS) attack. Due to DDoS attack the services of SDN becomes unavailable to its users. Hence, the purpose of this study is to analysis of machine learning based DDoS attack detection techniques in Software defined network (SDN). We analysis the Scopes indexed papers in this study and present a comparative analysis from them.

KEYWORDS DDoS, Machine learning, Software-defined network (SDN)

I. INTRODUCTION

SDN is the latest network virtualization technique, which separates the data plane from the control plane. Before software-defined networking (SDN), network-based algorithms were often implemented on the hardware to govern and monitor data flow in the network, manage routing patterns, and determine how various devices are coupled. These routing rules and algorithms are often implemented on special hardware. But this hardware implementation makes an alteration of the rotting algorithm a difficult task. Because, to change the routing rules, one has to change the hardware of the switch [1]. This problem is solved by the introduction of SDN, as in SDN the data plane and control plane are separated. All control planes are centrally controlled; hence, it is possible to change the network traffic rules of any switch at any time.

The basic architecture of SDN is presented in Figure 1. SDN has two layers or planes [2]:

- Infrastructure Layer: This layer consists of all the physical devices such as router and switches.
- Control Layer: This layer is used to control the infrastructure layer. This layer consists of a flow table that has all the routing rules. The traffic through the infrastructure layer is controlled by the flow tables.

However, single-point control makes the SDN vulnerable to different types of security attacks [3]–[5] such as distributed denial-of-services attacks (DDoS) [6], [7]. DDoS attacks [8], [9] are decade-old cyber-attacks in which attacker flood the victims system with many compromised devices. The basic operation of DDoS attack is presented in Figure 2. As represented in the Figure 2 the attacker traffic consumes all the resources of the victim; hence, it is not available for the legitimate users [10]. In this context, we analysis different DDoS attack detection strategies related to SDN, in this paper.

TABLE 1: Main Information

Description	Results
Time Duration	2018:2022
Sources Information	67
Published Articles	102
Total References	3853
Total Keywords	275
Unique Authors	343

II. LITERATURE REVIEW

Researchers have proposed many techniques for the detection of DDoS attacks [11]–[13] for different enviroments such as cloud [14]–[17], [17]–[19], IoT [20]–[23], SDN, VANET [24]–[26] and healthcare [27]–[31]. The author in [32] proposed a DDoS attack detection technique based on game theory. In other work, author [33] proposed DOM-based attack detection ttechniqie. The authors in [34] proposed DNS based bot net detection technique. Authors in [35] explains different security issues and mitigation techniques for social media. Authors in [36], [37] different encryption and decryption techniques for attack detection. Author in [38]

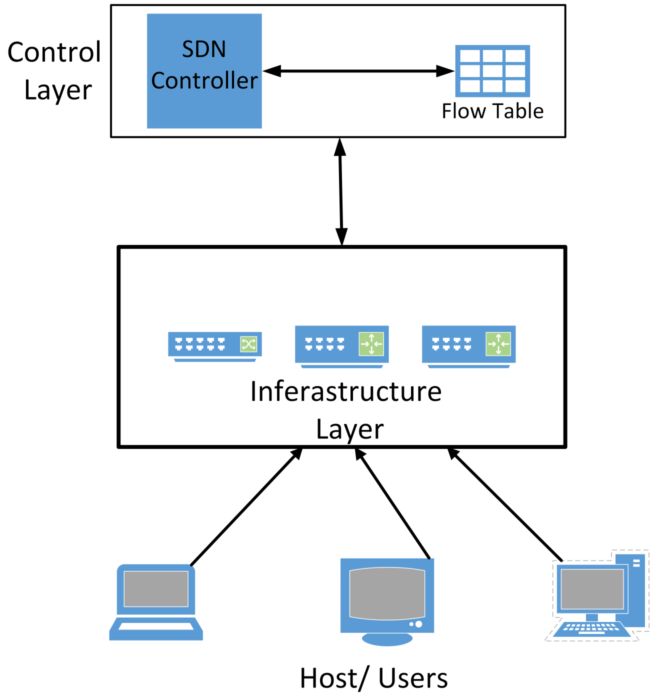


FIGURE 1: SDN Architecture

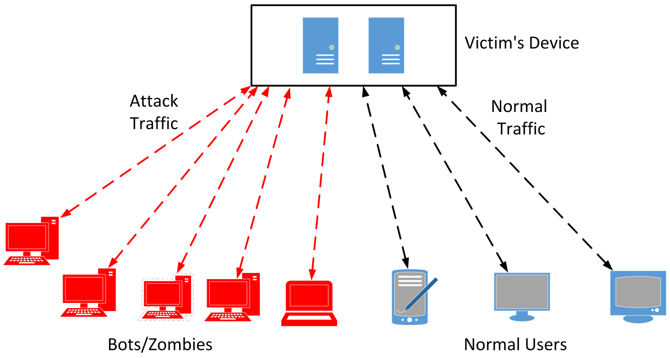


FIGURE 2: DDoS Attack Structure

proposed statistical techniques for DDoS attack detection. The RFID based security measures are propsed by author in [39], [40]. Authors in [41] proposed DDoS attack detection technique for the MEANET environment. Authors in [42] proposed an attack detection technique using 3D technology. Authors in [43] proposed packet filtering methods for DDoS detection. Authors in [44] proposed a SIP based technique for DDoS attack detection. Authos in [45] presents different testbeds for attack detection. Author in [46] proposed a URL-based attack detection technique. The author in [47] presents a risk assessment technique. A cooperative attack detection technique is presented by the author in [48]. Authors in [49] DDoS attack detection technique in healthcare systems. Author in [50] proposed a identity based attack detection technique for maritime environment.

The authors in [51] proposed a machine learning-based attack detection technique. The author in [27] proposed a deep learning-based attack detection technique. In other work, the authors [20] proposed a deep learning-based attack detection technique for cloud computing. The author in [52] proposed an attack detection technique using the fuzzy technique. Author in [53] proposed attack detection technique for smart homes. Author in [11] the big-data-based attack detection technique. Author in [54] proposed reinforcement machine learning based technique for attack detection. Author in [55] proposed an attack detection technique using the search engine technique. The author presented the review of smart card security in [56]. The authors in [57] presented a review of different attack detection technique. The author in [58] present a neural network based technique for attack detection. Author in [59] presents a matching technique for attack detection. The author in [60] proposed a feature detection technique. Author in [61] proposed an attack detection technique based on graph technique.

III. RESEARCH METHODOLOGY

In this paper, we try to analysis the machine learning based techniques for DDoS attack detection for SDN environment. We selected the Scopus database for our study; as it include papers from majority of the journals.

A. SELECTION CRITERIA

We include all the journal papers publish in-between 2018 to 2022 in English language. Few papers were disqualified because they were irrelevant to the study's fundamental objectives. Our study, for instance, is limited to the field of computer science.

B. DATA SOURCE

The information was collected in October of 2022 using the Scopus database. The search strategy used to address the study topic used the following key phrases.

- SDN
- Software defined network
- DDoS
- Distributed denial of services
- Machine learning

C. SEARCH QUERY SELECTION

We used different queries to get required information form the Scopus database.

- **Stage 1**:

  "(TITLE-ABS-KEY(SDN OR "software defined network") AND TITLE-ABS-KEY("distributed network" OR ddos))AND TITLE-ABS-KEY("machine learning")) AND (LIMIT-TO (LANGUAGE,"English"))"

- **Stage 2** :

  (TITLE-ABS-KEY(SDN OR "software defined network") AND TITLE-ABS-KEY("distributed network" OR ddos))AND TITLE-ABS-KEY("machine learning")) AND (LIMIT-TO (

LANGUAGE,"English")) AND LIMIT-TO (DOCTYPE , "ar"))

IV. THEORETICAL AND PRACTICAL IMPLICATIONS

We used the Scopus database in this research. As Scopus database contains majority of papers, we get the latest development related to the research topic. The development in the field of detection of DDoS attacks in the SDN network using the machine learning method is presented by Figure 3a. The details of selected paper for this research is presented in Table 1. From Figure 3a, it is clear that the annual growth rate is 78.93% for the papers.

We then examine the most recent trends and developments in the field of study. To kick off the investigation, we check at how the paper's keywords are laid together. The keywords in a document are a shorthand for the paper's central argument. Figure 3b represents the important keywords; the size of the keyword in Figure 3b depends on its occurrence in the literature.

We look at how the sources are broken up as well. The quantity of papers produced by a source is used to rank the sources in order of their productivity and influence. The ranking of the sources are represented in Figure 3c. We also try to find out the most popular authors. One method to find the most popular author is according to the number of published documents. The author statistics is presented in Figure 3d. The details of most cited papers are presented in Table 2. In Table 2, the documents are represented according to the citation.

V. CONCLUSION

SDN, or software-defined networking, is a method of designing networks that makes it possible to deploy software programs for centralized, high-level network administration and scheduling. Its adaptability, agility, and scalability are the driving force behind its increasing appeal. By moving the control layer to the data layer, SDN increases network programmability and speeds up network variation. However, SDN is vulnerable to different types of cyber-attacks such as DDoS attack. In this Research Paper, we review some of the important DDoS attack detection techniques. We analyze only the papers included in the Scopus database in the future, we include the papers from the ore database.

REFERENCES

[1] F. Hu, Q. Hao, and K. Bao, "A survey on software-defined network and openflow: From concept to implementation," IEEE Communications Surveys & Tutorials, vol. 16, no. 4, pp. 2181–2206, 2014.

[2] L. Barki, A. Shidling, N. Meti, D. Narayan, and M. M. Mulla, "Detection of distributed denial of service attacks in software defined networks," in 2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI). IEEE, 2016, pp. 2576–2581.

[3] S. Gupta and et al., "Xss-safe: a server-side approach to detect and mitigate cross-site scripting (xss) attacks in javascript code," Arabian Journal for Science and Engineering, vol. 41, no. 3, pp. 897–920, 2016.

[4] S. Gupta and et al, "Php-sensor: a prototype method to discover workflow violation and xss vulnerabilities in php web applications," in Proceedings of the 12th ACM international conference on computing frontiers, 2015, pp. 1–8.

[5] D. Sharma, J. Mishra, A. Singh, R. Govil, G. Srivastava, and J.-W. Lin, "Explainable artificial intelligence for cybersecurity," Computers and Electrical Engineering, vol. 103, 2022. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85137646132&doi=10.1016%2fj.compeleceng.2022.108356&partnerID=40&md5=2878fe72da3ec2734f83c8f227dfaef9

[6] B. B. Gupta, R. C. Joshi, and M. Misra, "Defending against distributed denial of service attacks: issues and challenges," Information Security Journal: A Global Perspective, vol. 18, no. 5, pp. 224–247, 2009.

[7] A. Mishra and et al., "A comparative study of distributed denial of service attacks, intrusion tolerance and mitigation techniques," in 2011 European Intelligence and Security Informatics Conference. IEEE, 2011, pp. 286–289.

[8] A. Gaurav and et al, "A comprehensive survey on ddos attacks on various intelligent systems and it's defense techniques," International Journal of Intelligent Systems, 2022. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85137212104&doi=10.1002%2fint.23048&partnerID=40&md5=7dfb2771d72c8248007f9990f22a6fba

[9] O. Wahab, J. Bentahar, H. Otrok, and A. Mourad, "Optimal load distribution for the detection of vm-based ddos attacks in the cloud," IEEE Transactions on Services Computing, vol. 13, no. 1, pp. 114–129, 2020. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85054704295&doi=10.1109%2fTSC.2017.2694426&partnerID=40&md5=ac396dc103d7e693e2cf6e0da8533d59

[10] B. B. Gupta and A. Gupta, "Assessment of honeypots: Issues, challenges and future directions," International Journal of Cloud Applications and Computing (IJCAC), vol. 8, no. 1, pp. 21–54, 2018.

[11] S. Tripathi and et al., "Hadoop based defense solution to handle distributed denial of service (ddos) attacks," 2013.

[12] L. Wang and et al., "Compressive sensing of medical images with confidentially homomorphic aggregations," IEEE Internet of Things Journal, vol. 6, no. 2, pp. 1402–1409, 2018.

[13] S. Gupta and et al., "Detection, avoidance, and attack pattern mechanisms in modern web application vulnerabilities: present and future challenges," International Journal of Cloud Applications and Computing (IJCAC), vol. 7, no. 3, pp. 1–43, 2017.

[14] K. Bhushan and et al., "Security challenges in cloud computing: state-of-art," International Journal of Big Data Intelligence, vol. 4, no. 2, pp. 81–107, 2017.

[15] E. Ahmed and et al., "Recent advances in fog and mobile edge computing," Transactions on Emerging Telecommunications Technologies, vol. 29, no. 4, p. e3307, 2018.

[16] B. B. Gupta, D. P. Agrawal, S. Yamaguchi, and M. Sheng, "Advances in applying soft computing techniques for big data and cloud computing," pp. 7679–7683, 2018.

[17] B. B. Gupta and et al, "Soft computing techniques for big data and cloud computing," Soft Computing, vol. 24, no. 8, pp. 5483–5484, 2020.

[18] B. B. Gupta, S. Gupta, and P. Chaudhary, "Enhancing the browser-side context-aware sanitization of suspicious html5 code for halting the dom-based xss vulnerabilities in cloud," International Journal of Cloud Applications and Computing (IJCAC), vol. 7, no. 1, pp. 1–31, 2017.

[19] A. M. e. a. Manasrah, "An optimized service broker routing policy based on differential evolution algorithm in fog/cloud environment," Cluster Computing, vol. 22, no. 1, pp. 1639–1653, 2019.

[20] C. L. Stergiou and et al., "Secure machine learning scenario from big data in cloud computing via internet of things network," in Handbook of computer networks and cyber security. Springer, 2020, pp. 525–554.

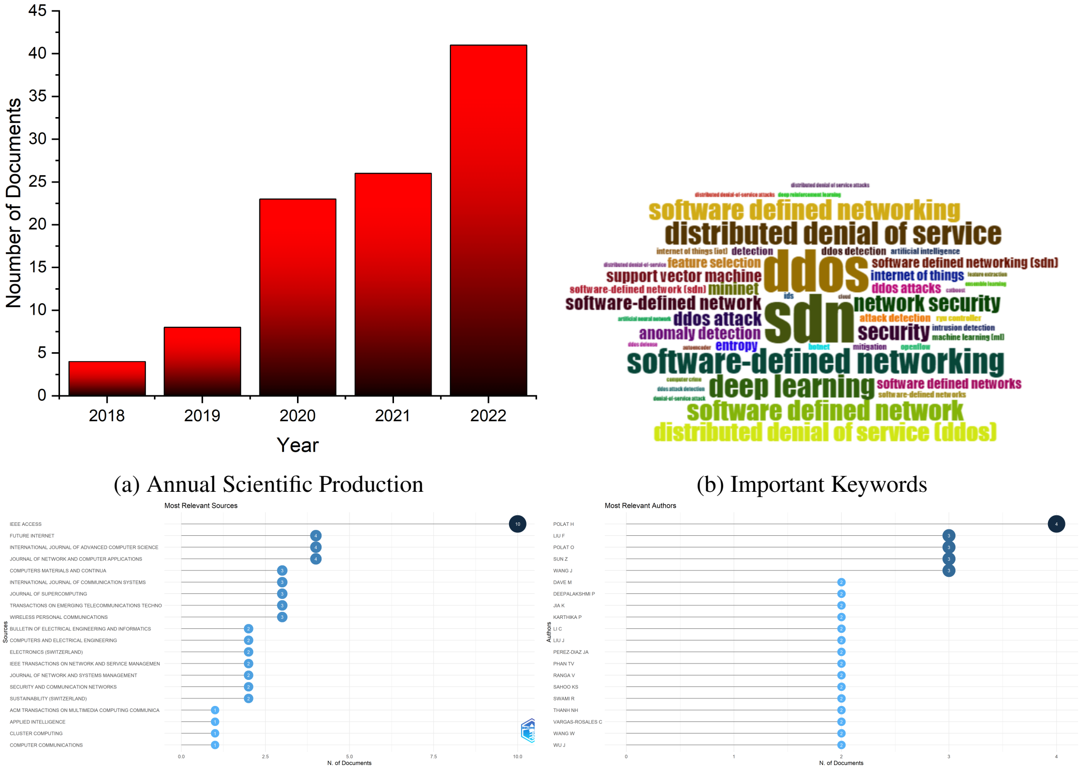
[21] A. Tewari and et al., "A mutual authentication protocol for iot devices using elliptic curve cryptography," in 2018 8th International Conference on Cloud Computing, Data Science & Engineering (Confluence). IEEE, 2018, pp. 716–720.

[22] J. Lu and et al., "Blockchain-based secure data storage protocol for sensors in the industrial internet of things," IEEE Transactions on Industrial Informatics, vol. 18, no. 8, pp. 5422–5431, 2021.

[23] B. B. Gupta and A. Tewari, A Beginner's Guide to Internet of Things Security: Attacks, Applications, Authentication, and Fundamentals. CRC Press, 2020.

[24] B. B. Gupta and M. Quamara, "Decentralised control-based interaction framework for secure data transmission in internet of automated vehicles," International Journal of Embedded Systems, vol. 12, no. 4, pp. 414–423, 2020.

[25] F. Mirsadeghi and et al., "A trust infrastructure based authentication method for clustered vehicular ad hoc networks," Peer-to-Peer Networking and Applications, vol. 14, no. 4, pp. 2537–2553, 2021.



(a) Annual Scientific Production

(b) Important Keywords

(c) Important Sources

(d) Popular Authors

FIGURE 3: Analysis of Topic

[26] A. Gaurav and et al., "Ddos attack detection in vehicular ad-hoc network (vanet) for 5g networks," in Security and Privacy Preserving for IoT and 5G Networks. Springer, 2022, pp. 263–278.

[27] M. Hammad and et al., "Myocardial infarction detection based on deep neural network on imbalanced data," Multimedia Systems, vol. 28, no. 4, pp. 1373–1385, 2022.

[28] K. T. Chui and et al., "An mri scans-based alzheimer's disease detection via convolutional neural network and transfer learning," Diagnostics, vol. 12, no. 7, p. 1531, 2022.

[29] S. Kaddoura, R. Haraty, K. Al Kontar, and O. Alfandi, "A parallelized database damage assessment approach after cyberattack for healthcare systems," Future Internet, vol. 13, no. 4, 2021. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85104388583&doi=10.3390%2ffi13040090&partnerID=40&md5=88bbf399623149df3ec0c24993fe109d

[30] M. Yunis, C. Markarian, and A.-N. El-Kassar, "A conceptual model for sustainable adoption of ehealth: Role of digital transformation culture and healthcare provider's readiness," L. N. L. B. P. P. Callaos N.C., Hashimoto S., Ed., vol. 2, 2020, pp. 179–184. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85086464783&partnerID=40&md5=d4f98fbbb38b0c82ed8c04adb297a27a

[31] R. Haraty, S. Kaddoura, and A. Zekri, "Recovery of business intelligence systems: Towards guaranteed continuity of patient centric healthcare systems through a matrix-based recovery approach," Telematics and Informatics, vol. 35, no. 4, pp. 801–814, 2018. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85039443283&doi=10.1016%2fj.tele.2017.12.010&partnerID=40&md5=ecd7e3a2a1f1494d17784c23f8d20b3b

[32] A. Dahiya and et al., "A reputation score policy and bayesian game theory based incentivized mechanism for ddos attacks mitigation and cyber defense," Future Generation Computer Systems, vol. 117, pp. 193–204, 2021.

[33] S. Gupta and et al., "Hunting for dom-based xss vulnerabilities in mobile cloud-based online social network," Future Generation Computer Systems, vol. 79, pp. 319–336, 2018.

[34] K. Alieyan and et al., "Dns rule-based schema to botnet detection," Enterprise Information Systems, vol. 15, no. 4, pp. 545–564, 2021.

[35] S. R. Sahoo and et al., "Security issues and challenges in online social networks (osns) based on user perspective," Computer and cyber security, pp. 591–606, 2018.

[36] B. B. Gupta and S. T. Ali, "Dynamic policy attribute based encryption and its application in generic construction of multi-keyword search," International Journal of E-Services and Mobile Applications (IJESMA), vol. 11, no. 4, pp. 16–38, 2019.

[37] I. Damaj and S. Kasbah, "An analysis framework for hardware and software implementations with applications from cryptography," Computers and Electrical Engineering, vol. 69, pp. 572–584, 2018. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85020661275&doi=10.1016%2fj.compeleceng.2017.06.008&partnerID=40&md5=abbc5bd1a626e1c61c025143b1a77974

[38] A. Gaurav and et al., "A novel approach for ddos attacks detection in covid-19 scenario for small entrepreneurs," Technological Forecasting and Social Change, vol. 177, p. 121554, 2022.

[39] A. Tewari and et al., "An analysis of provable security frameworks for rfid security," in Handbook of computer networks and cyber security. Springer, 2020, pp. 635–651.

[40] M. Hamad and C. Abou-Rjeily, "Fso cooperative all-active and selective relaying schemes with backup rf antennas," 2018, pp. 1–6. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85049172326&doi=10.1109%2fMENACOMM.2018.8371039&partnerID=40&md5=46f983b0943ce7d774968f28d176688f

[41] M. Chhabra and et al., "A novel solution to handle ddos attack in manet," 2013.

[42] M. Al-Ayyoub and et al., "Accelerating 3d medical volume segmentation using gpus," Multimedia Tools and Applications, vol. 77, no. 4, pp. 4939–4958, 2018.

[43] P. Negi and et al., "Enhanced cbf packet filtering method to detect ddos attack in cloud computing environment," arXiv preprint arXiv:1304.7073, 2013.

[44] B. B. Gupta, M. Misra, and R. C. Joshi, "An isp level solution to combat

TABLE 2: Highely Cited Papers

Paper	**DOI**	**Total Citations**	**TC per Year**	**Normalized TC**
LI C, 2018, INT J COMMUN SYST [62]	10.1002/dac.3497	119	23.8	2.6011
RAVI N, 2020, IEEE INTERNET THINGS J [63]	10.1109/JIOT.2020.2973176	81	27	3.4564
PHAN TV, 2019, IEEE ACCESS [64]	10.1109/ACCESS.2019.2896783	67	16.75	4.5424
POLAT H, 2020, SUSTAINABILITY [65]	10.3390/su12031035	66	22	2.8163
SAHOO KS, 2020, IEEE ACCESS [66]	10.1109/ACCESS.2020.3009733	62	20.667	2.6456
PEREZ-DIAZ JA, 2020, IEEE ACCESS [67]	10.1109/ACCESS.2020.3019330	57	19	2.4323
HAN B, 2018, SECUR COMMUN NETWORKS [68]	10.1155/2018/9649643	52	10.4	1.1366
DONG S, 2020, IEEE ACCESS [69]	10.1109/ACCESS.2019.2963077	46	15.333	1.9629
BANITALEBI DEHKORDI A, 2021, J SUPERCOMPUT [70]	10.1007/s11227-020-03323-w	44	22	5.2
ALZAHRANI AO, 2021, FUTURE INTERNET [71]	10.3390/fi13050111	39	19.5	4.6091
ZHIJUN W, 2020, IEEE ACCESS [72]	10.1109/ACCESS.2020.2967478	34	11.333	1.4508
TAN L, 2020, IEEE ACCESS [73]	10.1109/ACCESS.2020.3021435	32	10.667	1.3655
KRISHNAN P, 2019, COMPUT COMMUN [74]	10.1016/j.comcom.2019.09.014	28	7	1.8983
TUAN NN, 2020, ELECTRONICS (SWITZERLAND) [75]	10.3390/electronics9030413	25	8.333	1.0668
ASSIS MVO, 2021, J NETWORK COMPUT APPL [76]	10.1016/j.jnca.2020.102942	22	11	2.6
ABOU EL HOUDA Z, 2020, IEEE TRANS NETW SERV MANAGE [77]	10.1109/TNSM.2020.3014870	21	7	0.8961
KACI A, 2020, J NETWORK SYST MANAGE [78]	10.1007/s10922-020-09532-1	19	6.333	0.8108
AHUJA N, 2021, J NETWORK COMPUT APPL [79]	10.1016/j.jnca.2021.103108	19	9.5	2.2455
PHAN TV, 2020, IEEE TRANS NETW SERV MANAGE [80]	10.1109/TNSM.2020.3004415	17	5.667	0.7254
ALJUHANI A, 2021, IEEE ACCESS [81]	10.1109/ACCESS.2021.3062909	16	8	1.8909

ddos attacks using combined statistical based approach," arXiv preprint arXiv:1203.2400, 2012.

[45] B. Gupta, S. Gupta, S. Gangwar, M. Kumar, and P. Meena, "Cross-site scripting (xss) abuse and defense: exploitation on several testing bed environments and its defense," Journal of Information Privacy and Security, vol. 11, no. 2, pp. 118–136, 2015.

[46] A. K. Jain and et al., "Phish-safe: Url features-based phishing detection system using machine learning," in Cyber Security. Springer, 2018, pp. 467–474.

[47] N. Kumar and et al., "A novel framework for risk assessment and resilience of critical infrastructure towards climate change," Technological Forecasting and Social Change, vol. 165, p. 120532, 2021.

[48] P. Gulihar and et al, "Cooperative mechanisms for defending distributed denial of service (ddos) attacks," in Handbook of Computer Networks and Cyber Security. Springer, 2020, pp. 421–443.

[49] Z. Zhou and et al., "A statistical approach to secure health care services from ddos attacks during covid-19 pandemic," Neural Computing and Applications, pp. 1–14, 2021.

[50] B. B. Gupta, A. Gaurav, C.-H. Hsu, and B. Jiao, "Identity-based authentication mechanism for secure information sharing in the maritime transport system," IEEE Transactions on Intelligent Transportation Systems, 2021.

[51] A. K. Jain and et al., "Comparative analysis of features based machine learning approaches for phishing detection," in 2016 3rd international conference on computing for sustainable global development (INDIACom). IEEE, 2016, pp. 2125–2130.

[52] A. Almomani and et al., "Phishing dynamic evolving neural fuzzy framework for online detection zero-day phishing email," arXiv preprint arXiv:1302.0629, 2013.

[53] I. Cvitić and et al., "Ensemble machine learning approach for classification of iot devices in smart home," International Journal of Machine Learning and Cybernetics, vol. 12, no. 11, pp. 3179–3202, 2021.

[54] I. A. Elgendy and et al., "Joint computation offloading and task caching for multi-user and multi-task mec systems: reinforcement learning-based algorithms," Wireless Networks, vol. 27, no. 3, pp. 2023–2038, 2021.

[55] B. B. Gupta and A. K. Jain, "Phishing attack detection using a search engine and heuristics-based technique," Journal of Information Technology Research (JITR), vol. 13, no. 2, pp. 94–109, 2020.

[56] B. B. Gupta and M. Quamara, Smart Card Security: Applications, Attacks, and Countermeasures. CRC Press, 2019.

[57] R. Kumar and et al., "Stepping stone detection techniques: Classification and state-of-the-art," in Proceedings of the international conference on recent cognizance in wireless communication & image processing. Springer, 2016, pp. 523–533.

[58] J. Peng and et al., "A biometric cryptosystem scheme based on random projection and neural network," Soft Computing, vol. 25, no. 11, pp. 7657–7670, 2021.

[59] A. Mishra and et al., "Intelligent phishing detection system using similarity matching algorithms," International Journal of Information and Communication Technology, vol. 12, no. 1-2, pp. 51–73, 2018.

[60] A. P. Pljonkin and et al., "Features of detection of a single-photon pulse at synchronisation in quantum key distribution systems," in 2017 6th International Conference on Informatics, Electronics and Vision & 2017 7th International Symposium in Computational Medical and Health Technology (ICIEV-ISCMHT). IEEE, 2017, pp. 1–5.

[61] Z. Zhou and et al., "Coverless information hiding based on probability

graph learning for secure communication in iot environment," IEEE Internet of Things Journal, 2021.

[62] C. Li, Y. Wu, X. Yuan, Z. Sun, W. Wang, X. Li, and L. Gong, "Detection and defense of ddos attack–based on deep learning in openflow-based sdn," International Journal of Communication Systems, vol. 31, no. 5, 2018.

[63] N. Ravi and S. Shalinie, "Learning-driven detection and mitigation of ddos attack in iot via sdn-cloud architecture," IEEE Internet of Things Journal, vol. 7, no. 4, pp. 3559–3570, 2020.

[64] T. Phan and M. Park, "Efficient distributed denial-of-service attack defense in sdn-based cloud," IEEE Access, vol. 7, pp. 18 701–18 714, 2019.

[65] H. Polat, O. Polat, and A. Cetin, "Detecting ddos attacks in software-defined networks through feature selection methods and machine learning models," Sustainability (Switzerland), vol. 12, no. 3, 2020.

[66] K. Sahoo, B. Tripathy, K. Naik, S. Ramasubbareddy, B. Balusamy, M. Khari, and D. Burgos, "An evolutionary svm model for ddos attack detection in software defined networks," IEEE Access, vol. 8, pp. 132 502–132 513, 2020.

[67] J. Perez-Diaz, I. Valdovinos, K.-K. Choo, and D. Zhu, "A flexible sdn-based architecture for identifying and mitigating low-rate ddos attacks using machine learning," IEEE Access, vol. 8, pp. 155 859–155 872, 2020.

[68] B. Han, X. Yang, Z. Sun, J. Huang, and J. Su, "Overwatch: A cross-plane ddos attack defense framework with collaborative intelligence in sdn," Security and Communication Networks, vol. 2018, 2018.

[69] S. Dong and M. Sarem, "Ddos attack detection method based on improved knn with the degree of ddos attack in software-defined networks," IEEE Access, vol. 8, pp. 5039–5048, 2020.

[70] A. Banitalebi Dehkordi, M. Soltanaghaei, and F. Boroujeni, "The ddos attacks detection through machine learning and statistical methods in sdn," Journal of Supercomputing, vol. 77, no. 3, pp. 2383–2415, 2021.

[71] A. Alzahrani and M. Alenazi, "Designing a network intrusion detection system based on machine learning for software defined networks," Future Internet, vol. 13, no. 5, 2021.

[72] W. Zhijun, X. Qing, W. Jingjie, Y. Meng, and L. Liang, "Low-rate ddos attack detection based on factorization machine in software defined network," IEEE Access, vol. 8, pp. 17 404–17 418, 2020.

[73] L. Tan, Y. Pan, J. Wu, J. Zhou, H. Jiang, and Y. Deng, "A new framework for ddos attack detection and defense in sdn environment," IEEE Access, vol. 8, pp. 161 908–161 919, 2020.

[74] P. Krishnan, S. Duttagupta, and K. Achuthan, "Varman: Multi-plane security framework for software defined networks," Computer Communications, vol. 148, pp. 215–239, 2019.

[75] N. Tuan, P. Hung, N. Nghia, N. Van Tho, T. Van Phan, and N. Thanh, "A ddos attack mitigation scheme in isp networks using machine learning based on sdn," Electronics (Switzerland), vol. 9, no. 3, 2020.

[76] M. Assis, L. Carvalho, J. Lloret, and J. Proença, M.L., "A gru deep learning system against attacks in software defined networks," Journal of Network and Computer Applications, vol. 177, 2021.

[77] Z. Abou El Houda, L. Khoukhi, and A. Senhaji Hafid, "Bringing intelligence to software defined networks: Mitigating ddos attacks," IEEE Transactions on Network and Service Management, vol. 17, no. 4, pp. 2523–2535, 2020.

[78] A. Kaci and A. Rachedi, "Toward a machine learning and software defined network approaches to manage miners' reputation in blockchain," Journal of Network and Systems Management, vol. 28, no. 3, pp. 478–501, 2020.

[79] N. Ahuja, G. Singal, D. Mukhopadhyay, and N. Kumar, "Automated ddos attack detection in software defined networking," Journal of Network and Computer Applications, vol. 187, 2021.

[80] T. Phan, T. Nguyen, N.-N. Dao, T. Huong, N. Thanh, and T. Bauschert, "Deepguard: Efficient anomaly detection in sdn with fine-grained traffic flow monitoring," IEEE Transactions on Network and Service Management, vol. 17, no. 3, pp. 1349–1362, 2020.

[81] A. Aljuhani, "Machine learning approaches for combating distributed denial of service attacks in modern networking environments," IEEE Access, vol. 9, pp. 42 236–42 264, 2021.