Deep Science Publishing
https://doi.org/10.70593/978-93-49307-78-0_5

DeepScience
Open Access Books

Chapter 5

Strategic recommendations for enhancing DDoS defense mechanisms in cloud environments

5.0 Conclusion and Future work

As presented and motivated in the introduction of this project study, a DDoS detection system for a cloud environment aided by a machine learning modem technique was implemented and a comparative analysis modem was conducted. The CICFlowMeter was used to extract the new dataset to CSV format which includes obtaining the proper flow features for the model building. Furthermore, feature selection using person correlation coefficient improved the accuracy performance of the ML models training with Random Forest, Support Vector Machine, Decision Tree, and K-Nearest Neighbors achieving a rate of 100% accuracy, precision, recall and F1 score except for Naive Bayes with a 98% accuracy, 97% precision, 99% recall and 98% F1 score. Also, the open-source dataset performs very well with RF, DT and KNN achieving an accuracy of 100%, SVM 95% and NB 99%. Overall, the new dataset outperforms the open-source dataset with an accuracy score of 99.6% while the benchmark achieved 98.8%. Based on the results achieved, all the models selected, the new datasets and the open-source dataset used for this study are ideal models and datasets for intrusion detection.

The comprehensive study in Chapter 2 was conducted, where the fundamentals of an overview and the history of DDoS attacks, DDoS classification and attack tools. Discussion of some resources used to solve this type of problem. Summary of existing work, use of machine learning in this research and research gaps were further presented.

The implemented experimental setup was presented in Chapter 3, which included the system setup and supervised ML flow process used to solve this problem. The system set-up comprised of the initial set up of the systems which involved the generation of the

attack using the slowloris tool and how benign traffic was generated. The next is the supervised ML flow process starting from how the raw data was generated, processed, trained, tested and validated using ML models. Finally, the results were evaluated.

In conclusion, theoretical, and mathematical performance analysis in Chapter 4 was presented. The outcome of the ML models was evaluated using tables and charts and documented in this section which includes results on performance metrics like accuracy, precision, recall, F1-score, and computation time. In addition, the confusion matrix and validation results were explained.

5.1 Recommendation for Future Work

Further numerous studies can arise from this project study, considering both the theoretical simulation and practical implementation. The practical implementation can be modified such that an automation system is implemented and evaluated as a holistic study. Furthermore, several types of mitigating DDoS attacks using machine learning can be introduced into the system.

In terms of theoretical and mathematical performance analysis, further parameters can be investigated and derived, such as different types of machine learning and real-time dataset will be investigated.

References

ABDULRAHMAN, A.A. and IBRAHEM, M.K., (2019). Evaluation of DDoS attacks detection in a new intrusion dataset based on classification algorithms. Iraqi Journal of Information & Communications Technology, 1(3), pp. 49–55. Available from: http://dx.doi.org/10.31987/ijict.1.3.40.

ALDUAILIJ, M. et al., (2022). Machine-learning-based DDoS attack detection using Mutual Information and Random Forest Feature Importance method. *Symmetry*, 14(6), p. 1095. Available from: http://dx.doi.org/10.3390/sym14061095.

ABUBAKAR, R. et al., (2020). An effective mechanism to mitigate real-time DDoS attack. IEEE Access: Practical Innovations, Open Solutions, 8, pp. 126215–126227. Available from: http://dx.doi.org/10.1109/access.2020.2995820.

ACHBAROU, O. et al., (2017). Cloud security: A multi agent approach-based intrusion detection system. Indian Journal of Science and Technology, 10(18), pp. 1–6. Available from: http://dx.doi.org/10.17485/ijst/2017/v10i18/109044.

A. H. Lashkari, Y. Zang, G. Owhuo, M. S. I. Mamun, and G. D. Gil, "CICFlowMeter,"Github. 2017.

ALANAZI, S.T. et al., (2019). Detection techniques for DDoS attacks in cloud environment: Review paper. In: Intelligent and Interactive Computing. Singapore: Springer Singapore. pp. 337–354.

ALARQAN, M.A., ZAABA, Z.F. and ALMOMANI, A., (2020). Detection mechanisms of DDoS attack in cloud computing environment: A survey. In: Communications in Computer and Information Science. Singapore: Springer Singapore. pp. 138–152.

ALGHOSON, E.S. and ABBASS, O., (2021). Detecting distributed denial of service attacks using machine learning models. International Journal of Advanced Computer Science and Applications : IJACSA, 12(12). [online]. Available from: http://dx.doi.org/10.14569/ijacsa.2021.0121277.

ALLOGHANI, M. et al., (2020). A systematic review on supervised and unsupervised machine learning algorithms for data science. In: Unsupervised and Semi-Supervised Learning. Cham: Springer International Publishing. pp. 3–21.

ALZAHRANI, R.J. and ALZAHRANI, A., (2021). Security analysis of DDoS attacks using Machine Learning algorithms in networks traffic. Electronics, 10(23), p. 2919. Available from: http://dx.doi.org/10.3390/electronics10232919.

AMAIZU, G.C. et al., (2021). Composite and efficient DDoS attack detection framework for B5G networks. *Computer Networks*, 188(107871), p. 107871. Available from: http://dx.doi.org/10.1016/j.comnet.2021.107871.

AMMA, N. and SUBRAMANIAN, S., (2019). VCDeepFL: Vector Convolutional Deep Feature Learning approach for identification of known and unknown Denial of Service Attacks. In: IEEE Region 10 Annual International Conference,

Proceedings/TENCON. Institute of Electrical and Electronics Engineers Inc. pp. 640–645.

AYTAC, T. et al., (2020). Detection DDOS attacks using machine learning methods. Istanbul University - Journal of Electrical & Electronics Engineering, 20(2), pp. 159–167. Available from: http://dx.doi.org/10.5152/electrica.2020.20049.

BALAREZO, J.F. et al., (2022). A survey on DoS/DDoS attacks mathematical modelling for traditional, SDN and virtual networks. Engineering Science and Technology an International Journal, 31(101065), p. 101065. Available from: http://dx.doi.org/10.1016/j.jestch.2021.09.011.

BAMASAG, O. et al., (2022). Real-time DDoS flood attack monitoring and detection (RT-AMD) model for cloud computing. PeerJ. *Computer Science*, 7, p. e814. Available from: http://dx.doi.org/10.7717/peerj-cs.814.

BATCHU, R.K. and SEETHA, H., (2022). On improving the performance of DDoS attack detection system. Microprocessors and Microsystems, 93(104571), p. 104571. Available from: http://dx.doi.org/10.1016/j.micpro.2022.104571.

BENSALAH, F., KAMOUN, N.E. and EL HOUSSAINI, M.-A., (2019). Inline detection of Denial of Service Attacks in Software Defined Networking using the Hotelling Chart. *Procedia Computer Science*, 160, pp. 785–790. Available from: http://dx.doi.org/10.1016/j.procs.2019.11.010.

BHANDARI, A., (2020). *Everything you should know about confusion matrix for machine learning*. [online]. Analytics Vidhya. Available from: https://www.analyticsvidhya.com/blog/2020/04/confusion-matrix-machine-learning/ [Accessed 6 Aug 2022].

BIGELOW, S.J., (2020). Microsoft Azure. [online]. SearchCloudComputing. TechTarget. Available from: https://www.techtarget.com/searchcloudcomputing/definition/Windows-Azure [Accessed 1 Jul 2022].

BLOKDYK, G., (2019). Black box testing A complete guide - 2020 edition. 5starcooks.

BOLODURINA, I. et al., (2020). Investigation of the problem of classifying unbalanced datasets in identifying distributed denial of service attacks. Journal of Physics. Conference *Series*, 1679(4), p. 042020. Available from: http://dx.doi.org/10.1088/1742-6596/1679/4/042020.

BROOKS, R.R. et al., (2022). Distributed denial of service (DDoS): A history. IEEE Annals of the History of Computing, 44(2), pp. 44–54. Available from: http://dx.doi.org/10.1109/mahc.2021.3072582.

BROWNLEE, J., (2020). Train-test split for evaluating machine learning algorithms. [online]. Machine Learning Mastery. Available from: https://machinelearningmastery.com/train-test-split-for-evaluating-machine-learning-algorithms/ [Accessed 11 Jul 2022].

CAO, Y. et al., (2018). Understanding internet DDoS mitigation from academic and industrial perspectives. IEEE Access: Practical Innovations, Open Solutions, 6, pp.6664166648.Availablefrom:http://dx.doi.org/10.1109/access.2018.2877710.

CATAK, F.O. and MUSTACOGLU, A.F., (2019). Distributed denial of service attack detection using autoencoder and deep neural networks. *Journal of Intelligent &* Fuzzy Systems, 37(3), pp. 3969–3979. Available from: http://dx.doi.org/10.3233/jifs-190159.

CHEEMA, A. et al., (2022). Prevention techniques against Distributed Denial of service attacks in heterogeneous networks: A systematic review. *Security and Communication Networks*, 2022, pp. 1–15. Available from: http://dx.doi.org/10.1155/2022/8379532.

CHEN, W. et al., (2020). A DDoS attacks traceback scheme for SDN-based smart city. Computers & Electrical Engineering: An International Journal, 81(106503), p.106503. Availablefrom: http://dx.doi.org/10.1016/j.compeleceng.2019.106503.

CIL, A.E., YILDIZ, K. and BULDU, A., (2020). Detection of DDoS attacks with feed-forward based deep neural network model. Expert Systems with Applications, 169.

CIL, A.E., YILDIZ, K. and BULDU, A., (2021). Detection of DDoS attacks with feed forward based deep neural network model. Expert Systems with Applications, 169(114520),p.114520.Availablefrom:http://dx.doi.org/10.1016/j.eswa.2020.114520.

DAS, R., MENON, V. and MORRIS, T.H., (2018). On the edge realtime intrusion prevention system for DoS attack. BCS Learning & Development.

DAVIS, R., (2021). The history and future of DDoS attacks. [online]. Cybersecurity Magazine. Available from: https://cybersecurity-magazine.com/the-history-and-future-of-ddos-attacks/ [Accessed 20 Jul 2022].

DE DONNO, M. et al., (2018). AntibIoTic: Protecting IoT devices against DDoS attacks. In: Advances in Intelligent Systems and Computing. Cham: Springer International Publishing. pp. 59–72.

DOBBELAERE, M.R. et al., (2021). Machine learning in chemical engineering: Strengths, weaknesses, opportunities, and threats. Engineering (Beijing, China), 7(9), pp. 1201–1211.

DRIDI, S., (2022). Supervised learning - A systematic literature review. Available from: http://dx.doi.org/10.31219/osf.io/tysr4.

EFE, A., (2018). DDoS attacks and impacts on various cloud computing components. International Journal of Information Security Science, 7(1), pp. 26–48. Available from: https://www.ijiss.org/ijiss/index.php/ijiss/article/view/248 [Accessed 20 Jul 2022].

ELSAYED, M.S. et al., (2020). DDoSNet: A Deep-Learning model for detecting network attacks. ArXiv [Cs.CR*]*. Available from: http://arxiv.org/abs/2006.13981.

Einfochips.com. Available from: https://www.einfochips.com/blog/methodology-for-application-porting-on-gpus/ [Accessed 21 Jul 2022].

FEMI, A.G. and SAMUEL, I.O., (2022). The needs to embrace R programming language in every organizations that deals with statistical research and data analysis. [online]. Irejournals.com. Available from: https://irejournals.com/formatedpaper/1703170.pdf [Accessed 17 Jul 2022].

FREDRIK, J., ÅGREN, N. and BENDTSEN, M., (2022). A study of slow denial of service mitigation tools and solutions deployed in the cloud. [online]. Diva-portal.org. Available from: http://www.diva portal.org/smash/get/diva2:1327569/FULLTEXT01.pdf [Accessed 24 Jul 2022].

FREET, D. and AGRAWAL, R., (2017). A virtual machine platform and methodology for network data analysis with IDS and security visualization. In: SoutheastCon 2017. IEEE.

FURNELL, S. et al., (2020). Understanding the full cost of cyber security breaches. Computer Fraud & Security, 2020(12), pp. 6–12. Available from: http://dx.doi.org/10.1016/s1361-3723(20)30127-5.

FURNELL, S. and SHAH, J.N., (2020). Home working and cyber security – an outbreak of unpreparedness? Computer Fraud & Security, 2020(8), pp. 6–12. Available from: http://dx.doi.org/10.1016/s1361-3723(20)30084-1.

GAURAV, A., GUPTA, B.B. and PANIGRAHI, P.K., (2022). A novel approach for DDoS attacks detection in COVID-19 scenario for small entrepreneurs. Technological Forecasting and Social Change, 177(121554), p. 121554. Available from: http://dx.doi.org/10.1016/j.techfore.2022.121554.

GAURAV, A. and SINGH, A.K., (2017). Super-router: A collaborative filtering technique against DDoS attacks. In: Communications in Computer and Information Science. Singapore: Springer Singapore. pp. 294–305.

GISCLARD-BIONDI, H., (2021). An overview of the MoSCoW prioritisation method. [online].appvizer.co.uk.Appvizer.Availablefrom:https://www.appvizer.co.uk/magazine/operations/project-management/moscow-prioritisation [Accessed 21 Jul 2022].

GUPTA, A., 2020. Feature selection techniques in machine learning. [online]. Analytics Vidhya. Available from:

(‘IDS2018’2022)IDS2018,2022.online].Unb.ca.Availablefrom:https://www.unb.ca/cic/datasets/ids-2018.html [Accessed 12 Aug 2022].

https://www.analyticsvidhya.com/blog/2020/10/feature-selection-techniques-in-machine-learning/ [Accessed 4 Aug 2022].

HAO, J. and HO, T.K., (2019). Machine learning made easy: A review of Scikit-learn package in Python programming language. Journal of Educational and Behavioral Statistics: A Quarterly Publication Sponsored by the American Educational Research

Association and the American Statistical Association, 44(3),pp.348361.Availablefrom:http://dx.doi.org/10.3102/1076998619832248.
HORKOFF, J., (2019). Non-functional requirements for machine learning: Challenges and new directions. In: 2019 IEEE 27th International Requirements Engineering Conference (RE). IEEE.
HOSSEINI SHIRVANI, M., RAHMANI, A.M. and SAHAFI, A., (2020). A survey study on virtual machine migration and server consolidation techniques in DVFS-enabled cloud datacenter: Taxonomy and challenges. Journal of King Saud University - Computer and Information Sciences, 32(3), pp. 267–286. Available from: http://dx.doi.org/10.1016/j.jksuci.2018.07.001.
HOSSEINI, S. and AZIZI, M., (2019). The hybrid technique for DDoS detection with supervised learning algorithms. Computer Networks, 158, pp. 35–45. Available from: http://dx.doi.org/10.1016/j.comnet.2019.04.027.
How to plot scikit learn classification report 2022. [online]. Stack Overflow. Available from: https://stackoverflow.com/questions/28200786/how-to-plot-scikit-learn-classification-report [Accessed 11 Jul 2022].
IDS 2018 Intrusion CSVs (CSE-CIC-IDS2018), 2020. Available from: https://www.kaggle.com/datasets/solarmainframe/ids-intrusion-csv
JANUARY, F. on et al., (2022). 16 Best DDOS Attack Tools in 2022. [online]. Security Boulevard. Available from: https://securityboulevard.com/2022/01/16-best-ddos-attack-tools-in-2022/ [Accessed 16 Jul 2022].
KATI, S. et al., (2022). Comprehensive overview of DDOS attack in cloud computing environment using different machine learning techniques. SSRN ElectronicJournal.[online].Availablefrom:http://dx.doi.org/10.2139/ssrn.4096388
KHODA PARAST, F. et al., (2022). Cloud computing security: A survey of service-based models. Computers & Security, 114(102580), p. 102580. Available from: http://dx.doi.org/10.1016/j.cose.2021.102580.
KIM, J. et al., (2020). CNN-based network intrusion detection against denial-of-service attacks. Electronics, 9(6), p. 916. Available from: http://dx.doi.org/10.3390/electronics9060916.
KIM, M., (2019). Supervised learning-based DDoS attacks detection: Tuning hyperparameters. ETRI Journal, 41(5), pp. 560–573. Available from: http://dx.doi.org/10.4218/etrij.2019-0156.
KIOURKOULIS, S., (2020). DDoS datasets : Use of machine learning to analyse intrusion detection performance.
KUMAR, A., (2022). Accuracy, precision, Recall & F1-score - Python examples. [online]. Data Analytics. Available from: https://vitalflux.com/accuracy-precision-recall-f1-score-python-example/ [Accessed 9 Jul 2022].
KUSHWAH, G.S. and RANGA, V., (2021). Distributed denial of service attack detection in cloud computing using hybrid extreme learning machine. TURKISH

JOURNAL OF ELECTRICAL ENGINEERING & COMPUTER SCIENCES, 29(4), pp. 1852–1870. Available from: http://dx.doi.org/10.3906/elk-1908-87.

LI, Y. and LIU, Q., (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. Energy Reports, 7, pp. 8176–8186. Available from: http://dx.doi.org/10.1016/j.egyr.2021.08.126.

LIANG, X. and ZNATI, T., (2019). On the performance of intelligent techniques for intensive and stealthy DDos detection. Computer Networks, 164(106906), p. 106906. Available from: http://dx.doi.org/10.1016/j.comnet.2019.106906.

LIMA FILHO, F.S. de et al., (2019). Smart detection: An online approach for DoS/DDoS attack detection using machine learning. Security and Communication Networks, 2019, pp. 1–15. Available from: http://dx.doi.org/10.1155/2019/1574749.

LIU, X. and HE, W., (2022). Adaptive kernel scaling support vector machine with application to a prostate cancer image study. Journal of Applied Statistics, 49(6), pp. 1465–1484. Available from: http://dx.doi.org/10.1080/02664763.2020.1870669.

LI, Y., SHI, H. and FAN, M., (2021). DDoS attack traffic identification using recurrent neural network. In: *2021 5th* SLAAI International Conference *on* Artificial Intelligence (SLAAI-ICAI). IEEE.

LOHACHAB, A. and KARAMBIR, B., (2018). Critical analysis of DDoS—an emerging security threat over IoT networks. Journal of Communications and Information Networks, 3(3), pp. 57–78. Available from: http://dx.doi.org/10.1007/s41650-018-0022-5.

LUKEHART, M., (2022). 2022 cyber attack statistics, data, and trends. [online]. Parachute | Managed IT Services in the San Francisco Bay Area and Sacramento Valley. Parachute. Available from: https://parachute.cloud/2022-cyber-attack-statistics-data-and-trends/ [Accessed 20 Jul 2022].

MafiaBoy against the internet: this was the first big DDoS attack in history, 2022.[online].CyberLayman.Availablefrom:https://www.cyberlayman.com/technology/internet/18212/ [Accessed 20 Jul 2022].

MAHJABIN, T. et al., (2017). A survey of distributed denial-of-service attack, prevention, and mitigation techniques. International Journal of Distributed Sensor Networks, 13(12), p. 155014771774146. Available from: http://dx.doi.org/10.1177/1550147717741463.

MBAABU, O., (2022). Introduction to random forest in machine learning. [online]. Engineering Education (EngEd) Program | Section. Available from: https://www.section.io/engineering-education/introduction-to-random-forest-in-machine-learning/ [Accessed 21 Jul 2022].

METHOD KARAMAGI, R., SAID, A. and KARAMAGI, R.M., (2020_. Implementation of inter-networking with host internet in oracle ® VirtualBox guest virtual machines. Archivos de Medicina. [online]. Available from:

https://www.primescholars.com/articles/implementation-of-internetworking-with-host-internet-in-oracle-virtualbox-guest-virtual-machines.pdf.

MISRA, S. and LI, H., (2020). Noninvasive fracture characterization based on the classification of sonic wave travel times. In: Machine Learning for Subsurface Characterization. Elsevier. pp. 243–287.

MITTAL, M., KUMAR, K. and BEHAL, S., (2022). Deep learning approaches for detecting DDoS attacks: a systematic review. Soft Computing, pp. 1–37. Available from: http://dx.doi.org/10.1007/s00500-021-06608-1.

MOTSCH, W. et al., (2020). Approach for dynamic price-based demand side management in cyber-physical production systems. Procedia Manufacturing, 51, pp.1748–1754.Available from: http://dx.doi.org/10.1016/j.promfg.2020.10.243.

MUSUMECI, F. et al., (2022). Machine-Learning-enabled DDoS Attacks Detection in P4 programmable networks. Journal of Network and Systems Management, 30(1). [online]. Available from: http://dx.doi.org/10.1007/s10922-021-09633-5.

NASSIF, A.B. et al., (2021). Machine learning for cloud security: A systematic review. IEEE Access: Practical Innovations, Open Solutions, 9, pp. 20717–20735. Available from: http://dx.doi.org/10.1109/access.2021.3054129.

OBAID, H.S. and ABEED, E.H., (2020). DoS and DDoS attacks at OSI layers. *International* Journal of Multidisciplinary Research and Publications, 2(8). [online]. Available from: https://zenodo.org/record/3610833#.YtiCxHbMJn.

ORTET LOPES, I. et al., (2021). Towards effective detection of recent DDoS attacks: A deep learning approach. Security and Communication Networks, 2021, pp. 1–14. Available from: http://dx.doi.org/10.1155/2021/5710028.

PANDIT, P.D., (2021). A study of packet sniffer tools. Unpublished.

PAPADIE, R. and APOSTOL, I., (2017). Analyzing websites protection mechanisms against DDoS attacks. In: *2017 9th International Conference on Electronics*, Computers and Artificial Intelligence (ECAI). IEEE.

PEI, J., CHEN, Y. and JI, W., (2019). A DDoS attack detection method based on machine learning. Journal of Physics. Conference Series, 1237(3), p. 032040. Available from: http://dx.doi.org/10.1088/1742-6596/1237/3/032040.

PRASEED, A. and THILAGAM, P.S., (2021). Fuzzy request set modelling for detecting multiplexed asymmetric DDoS attacks on HTTP/2 servers. Expert Systems with Applications, 186(115697), p. 115697. Available from: http://dx.doi.org/10.1016/j.eswa.2021.115697.

PATIL, N.V., KRISHNA, C.R. and KUMAR, K., (2022). KS-DDoS: Kafka streams-based classification approach for DDoS attacks. *The Journal of Supercomputing*, 78(6), pp. 8946–8976. Available from: http://dx.doi.org/10.1007/s11227-021-04241-1.

PROFUMO, S., (2020). Dark matter indirect detection. EPJ Web of Conferences, 234,p.01014. Available from: http://dx.doi.org/10.1051/epjconf/202023401014.

python plot .mat Code Example, 2022. [online]. Codegrepper.com. Available from: https://www.codegrepper.com/code-examples/python/python+plot+.mat [Accessed 11 Jul 2022].

REHMAN, S. ur et al., (2021). DIDDOS: An approach for detection and identification of Distributed Denial of Service (DDoS) cyberattacks using Gated Recurrent Units (GRU). Future Generations Computer Systems: FGCS, 118, pp. 453–466. Available from: http://dx.doi.org/10.1016/j.future.2021.01.022.

RING, M. et al., (2019). A survey of network-based intrusion detection data sets. ArXiv [Cs.CR]. Available from: http://arxiv.org/abs/1903.02460.

RINKEWITZ, J., (2022). OwnCloud at the Univention Summit 2022. [online]. ownCloud.OwnCloudGmbH.Availablefrom:https://owncloud.com/events/owncloud-at-the-univention-summit-2022 [Accessed 20 Jul 2022].

RAHMAN, M.A. and associate professor of computer science, department of mathematics, jahangirnagar university, savar, dhaka, bangladesh, 2020. Detection of distributed denial of service attacks based on machine learning algorithms. International Journal of Smart Home, 14(2), pp. 15–24. Available from: http://dx.doi.org/10.21742/ijsh.2020.14.2.02.

SABEEL, U. et al., (2019). Evaluation of deep learning in detecting unknown network attacks. In: 2019 International Conference on Smart Applications, Communications and Networking (SmartNets). IEEE.

SAGHEZCHI, F.B. et al., (2022). Machine Learning for DDoS attack detection in Industry4.0CPPSs.Electronics,11(4),p.602.Availablefrom:http://dx.doi.org/10.3390/electronics11040602.

SAMBANGI, S. and GONDI, L., (2020). A machine learning approach for DDoS (Distributed Denial of Service) attack detection using multiple linear regression. Proceeding(MPDI),63(1),p.51.Availablefrom:http://dx.doi.org/10.3390/proceedings2020063051.

SAMBANGI, S., GONDI, L. and ALJAWARNEH, S., (2022. A feature similarity machine learning model for DDoS attack detection in modern network environments for industry 4.0. Computers & Electrical Engineering: An InternationaJournal,100(107955),p.107955.Availablefrom:http://dx.doi.org/10.1016/j.compeleceng.2022.107955.

SARKER, I.H., (2021). Deep learning: A comprehensive overview on techniques, taxonomy, applications and research directions. *Preprints*. Available from: http://dx.doi.org/10.20944/preprints202108.0060.v1.

SARRAF, S., (2022). Analysis and detection of DDoS attacks using machine learningtechniques.[online].Core.ac.uk.Availablefrom:https://core.ac.uk/download/pdf/288188017.pdf [Accessed 21 Jul 2022].

SHAABAN, A.R., ABD-ELWANIS, E. and HUSSEIN, M., (2019). DDoS attack detection and classification via Convolutional Neural Network (CNN). In: 2019

Ninth International Conference on Intelligent Computing and Information Systems (ICICIS). IEEE.

SHARMA, V., VERMA, V. and SHARMA, A., (2019). Detection of DDoS attacks using machine learning in cloud computing. In: Communications in Computer and Information Science. Singapore: Springer Singapore. pp. 260–273.

SHOREY, T. et al., (2018). Performance Comparison and Analysis of Slowloris, GoldenEye and Xerxes DDoS Attack Tools". In: *2018 International Conference on* Advances in Computing, Communications and Informatics (ICACCI). IEEE. pp. 318–322.

SIKORA, M. et al., (2021). Generator of slow denial-of-service cyber attacks. Sensors (Basel, Switzerland*)*, 21(16), p. 5473. Available from: http://dx.doi.org/10.3390/s21165473.

SILVA, F.S.D. et al., (2020). A taxonomy of DDoS attack mitigation approaches featured by SDN technologies in IoT scenarios. *Sensors* (Basel, Switzerland*)*, 20(11), p. 3078. Available from: http://dx.doi.org/10.3390/s20113078.

Scikit-learn, "KNeighborsClassier," *scikit-learn.org*, 2019. [Online]. Available: https://scikitlearn.org/stable/modules/generated/sklearn.neighbors.KNeighborsClassifier.html.

Scikit-learn, "LinearSVC," *scikit-learn.org*, 2019. [Online]. Available: https://scikitlearn. org/stable/modules/generated/sklearn.svm.LinearSVC.html.

Scikit-learn, "GaussianNB," *scikit-learn.org*, 2019. [Online]. Available: https://scikit63 learn.org/stable/modules/generated/sklearn.naive_bayes.GaussianNB.html.

Scikit-learn, "DecisionTreeClassifier," *scikit-learn.org*, 2019. [Online]. Available: https://scikitlearn.org/stable/modules/generated/sklearn.tree.DecisionTreeClassifier.html.

Scikit-learn,"RandomForestClassifier," *scikit-learn.org*, 2019. [Online]. Available: https://scikitlearn.org/stable/modules/generated/sklearn.ensemble.RandomForestClassifier.html.

Scikit-learn, "StratifiedKFold," *Scikit-learn 0.22.2 Documentation*, 2019.

Slowloris DDOS attack tool in Kali Linux, 2021. [online]. GeeksforGeeks. Available from: https://www.geeksforgeeks.org/slowloris-ddos-attack-tool-in-kali-linux/ [Accessed 30 Jun 2022].

Available from: https://owncloud.com/download-server/[Accessed 30 Jun 2022].

Available from: https://doc.owncloud.com/server/next/admin_manual/[Accessed 30 Jun 2022].

SOMANI, G. et al., (2017). DDoS victim service containment to minimize the internal collateral damages in cloud computing. Computers & Electrical Engineering: An International Journal, 59, pp. 165–179. Available from: http://dx.doi.org/10.1016/j.compeleceng.2016.12.004.

SRIAVASTAVA, S.K., SHARMA, Y.K. and KUMAR, S., (2020). Using of WEKA tool in machine learning: A review. International Journal of Advanced Science and Technology, 29(08), pp. 4456–4466. Available from: http://sersc.org/journals/index.php/IJAST/article/view/26579 [Accessed 17 Jul 2022].

Stephen J. bigelow, (2022). [online]. Techtarget.com. Available from: https://www.techtarget.com/contributor/Stephen-J-Bigelow [Accessed 20 Jul 2022].

TRIPATHI, N. and HUBBALLI, N., (2018). Slow rate denial of service attacks against HTTP/2 and detection. Computers & Security, 72, pp. 255–272. Available from: http://dx.doi.org/10.1016/j.cose.2017.09.009.

TRIPATHI, N. and HUBBALLI, N., (2022). Application layer Denial-of-Service attacks and defense mechanisms: A survey. *ACM Computing Surveys*, 54(4), pp. 1–33. Available from: http://dx.doi.org/10.1145/3448291.

TUAN, T.A. et al., (2020). Performance evaluation of Botnet DDoS attack detection using *machine learning. Evolutionary Intelligence*, 13(2), pp. 283–294. Available from: http://dx.doi.org/10.1007/s12065-019-00310-w.

SUMMER TRAINING FOR DEVELOPERS, 2019. 11 Visualising Correlations with a Heatmap. [online]. Youtube. Available from: https://www.youtube.com/watch?v=HoD9Fs7CTNw [Accessed 27 Jul 2022].

SWAPNILBOBE, (2021). Feature selection — machine learning. [online]. Analytics Vidhya. Available from: https://medium.com/analytics-vidhya/feature-selection-in-machine-learning-ec1f5d053007 [Accessed 2 Aug 2022].

TYCOONFURY, 2022. Detection of DDoS attack using machine learning algorithm. [online]. Youtube. Available from: https://www.youtube.com/watch?v=mNLiAW29QeA [Accessed 10 Jul 2022].

University of New Brunswick, "DDoS Evaluation Dataset (CICDDoS2019)," unb.ca, 2019.[Online]. Available: https://www.unb.ca/cic/datasets/ddos-2019.html

University of New Brunswick, "CSE-CIC-IDS2018 on AWS," 2018. [Online]. Available: https://www.unb.ca/cic/datasets/ids-2018.html.

WAN, D., n.d. icmp_attack.ipynb at master · DrakenWan/DDOS_Detection.

WANI, A.R. et al., (2019). Analysis and detection of DDoS attacks on cloud computing environment using machine learning techniques. In: 2019 Amity International Conference on Artificial Intelligence (AICAI). IEEE.

WEI, Y., YE, R. and CHEN, X., (2019). Oracle RAC performance analysis on VMware Virtual SAN. In: 2019 IEEE/ACIS 18th International Conference on Computer and Information Science (ICIS). IEEE.

Welcome to,2022.[online]. Python.org. Available from: https://www.python.org/ [Accessed 1 Jul 2022].

YEVSIEIEVA, O. and HELALAT, S.M., (2017). Analysis of the impact of the slow HTTP DOS and DDOS attacks on the cloud environment. In: 2017 4th International

Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T). IEEE.

ZACH and ZACH, V.A.P., (2021). How to Handle R Error: $ operator is invalid for atomicvectors.[online].Statology.org.Availablefrom:https://www.statology.org/r-error-operator-is-invalid-for-atomic-vectors/ [Accessed 23 Nov 2021].

ZEEBAREE, S.R.M., SHARIF, K.H. and MOHAMMED AMIN, R.M., (2018). Application layer distributed denial of service attacks defense techniques : A review. Academic Journal of Nawroz University, 7(4), p. 113. Available from: http://dx.doi.org/10.25007/ajnu.v7n4a279.

ZHOU, L. et al., (2017). Low-rate DDoS attack detection using expectation of packet size. Security and Communication Networks, 2017, pp. 1–14. Available from: http://dx.doi.org/10.1155/2017/3691629.

ZHOU, L. et al., (2022). A novel feature-based framework enabling multi-type DDoS attacks detection. WorldWide Web. [online]. Available from: http://dx.doi.org/10.1007/s11280-022-01040-3.

Appendix

Python ML codes used for for model building can be assessed in these links below

DDOS_Detection/icmp_attack.ipynb at master · DrakenWan/DDOS_Detection · GitHub