Springer Link

Assessing Deep Neural Network and Shallow for Network Intrusion Detection Systems in Cyber Security

Computer Networks and Inventive Communication Technologies pp 703-713 | Cite as

- Deena Babu Mandru (1)
- M. Aruna Safali (2)
- N. Raghavendra Sai (3)
- G. Sai Chaitanya Kumar (4)

1. Department of CSE, Malla Reddy Engineering College, , Hyderabad, India
2. Department of CSE, Dhanekula Institute of Engineering and Technology, , Gangur, India
3. Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, , Vaddeswaram, India
4. Department of CSE, MIC College of Technology, , Kanchikacherla, India

Conference paper
First Online: 14 September 2021

Part of the Lecture Notes on Data Engineering and Communications Technologies book series (LNDECT, volume 75)

Abstract

Intrusion detection system [IDS] has become a central layer that unites everything inside the most recent ICT structure on account of the consideration for advanced prosperity inside the ordinary world. Motivations to recall the weakness to search out the sorts of assaults and grow the intricacy of bleeding edge computerized assaults; IDS requires the need to hitch deep neural networks (DNN). During this report, DNNs will not foresee assaults on the N-IDS. A DNN with a learning pace of 0.1 is applied and runs for the assortment of 1000 years, and subsequently, the informational index KDDCup-'99' was utilized for readiness and site meaning association. For assessment purpose, the arrangement is finished on the comparable dataset with another obsolete AI figuring and DNN of levels begin from 1 to 5. The outcomes were broke down, and it had been accepted that a DNN of three levels would be advised for execution.

Keywords

Intrusion identification Deep neural organization Deep learning Machine learning

References

1. Lippmann, R., Haines, J., Fried, D., Korba, J., Das, K.: The 1999 DARPA off-line intrusion detection evaluation. Comput. Netw. **34**(4), 579–595 (2000). https://doi.org/10.1016/S1389-1286(00)00139-0 (https://doi.org/10.1016/S1389-1286(00)00139-0)

2. Lee, W., Stolfo, S.: A framework for constructing features and models for intrusion detection systems. ACM Trans. Inf. Syst. Secur. **3**(4), 227261 (2000). https://doi.org/10.1145/382912.382914 (https://doi.org/10.1145/382912.382914)

3. Pfahringer, B.: Winning the KDD99 classification cup: Bagged boosting. SIGKDD Explor. Newsl. **1**, 6566 (2000). https://doi.org/10.1145/846183.846200 (https://doi.org/10.1145/846183.846200)

4. Vladimir, M., Alexei, V., Ivan, S.: The MP13 approach to the KDD'99 classifier learning contest. SIGKDD Explor. Newsl. **1**, 76–77 (2000). https://doi.org/10.1145/846183.846202 (https://doi.org/10.1145/846183.846202)

5. Agarwal, R., Joshi, M.: PNrule: A new framework for learning classier models in data mining. Tech. Rep. 00-015. Department of Computer Science, University of Minnesota (2000)
Google Scholar (https://scholar.google.com/scholar?q=Agarwal%2C%20R.%2C%20Joshi%2C%20M.%3A%20PNrule%3A%20A%20new%20framework%20for%20learning%20classier%20models%20in%20data%20mining.%20Tech.%20Rep.%2000-015.%20Department%20of%20Computer%20Science%2C%20University%20of%20Minnesota%20%282000%29)

6. Elkan, C.: Results of the KDD'99 classifier learning. SIGKDD Explor. Newsl. **1**, 63–64 (2000). https://doi.org/10.1145/846183.846199 (https://doi.org/10.1145/846183.846199)

7. Sung, S., Mukkamala, A.H.: Identifying important features for intrusion detection using support vector machines and neural networks. In: Proceedings of the Symposium on Applications and the Internet (SAINT), pp. 209216. IEEE Computer Society (2003). https://doi.org/10.1109/saint.2003.1183050 (https://doi.org/10.1109/saint.2003.1183050)

8. Kayacik, H., Zincir-Heywood, A., Heywood, M.: Selecting features for intrusion detection: A feature relevance analysis on KDD 99 intrusion detection datasets. In: Proceedings of the Third Annual Conference on Privacy, Security and Trust (PST) (2005)
Google Scholar (https://scholar.google.com/scholar?q=Kayacik%2C%20H.%2C%20Zincir-Heywood%2C%20A.%2C%20Heywood%2C%20M.%3A%20Selecting%20features%20for%20intrusion%20detection%3A%20A%20feature%20relevance%20analysis%20on%20KDD%2099%20intrusion%20detection%20datasets.%20In%3A%20

Proceedings%20of%20the%20Third%20Annual%20Conference%20on%20Privacy%2C%20Security%20and%20Trust%20%28PST%29%20%282005%29)

9. Krishna Katakam, M.S., Devineni, K., Kanagala, P., Raghavendra Sai, N.: Analysis of artificial neural networks based intrusion detection system. Int. J. Adv. Sci. Technol. **29**(5s), 928–935 (2020). Retrieved from http://sersc.org/journals/index.php/IJAST/article/view/7832 (http://sersc.org/journals/index.php/IJAST/article/view/7832)

10. Raghavendra, S.N., Jogendra, K.M., Smitha, C.Ch.: A secured and effective load monitoring and scheduling migration VM in cloud computing. In: IOP Conference Series: Materials Science and Engineering ISSN-1757-899X, Vol. 981 (2020) Google Scholar (https://scholar.google.com/scholar?q=Raghavendra%2C%20S.N.%2C%20Jogendra%2C%20K.M.%2C%20Smitha%2C%20C.Ch.%3A%20A%20secured%20and%20effective%20load%20monitoring%20and%20scheduling%20migration%20VM%20in%20cloud%20computing.%20In%3A%20IOP%20Conference%20Series%3A%20Materials%20Science%20and%20Engineering%20ISSN-1757-899X%2C%20Vol.%20981%20%282020%29)

11. Chebrolu, S., Abraham, A., Thomas, J.: Feature deduction and ensemble design of intrusion detection systems. Comput. Secur. **24**(4), 295307 (2005). https://doi.org/10.1016/j.Cose.2004.09.008 (https://doi.org/10.1016/j.Cose.2004.09.008) CrossRef (https://doi.org/10.1016/j.Cose.2004.09.008) Google Scholar (http://scholar.google.com/scholar_lookup?title=Feature%20deduction%20and%20ensemble%20design%20of%20intrusion%20detection%20systems&author=S.%20Chebrolu&author=A.%20Abraham&author=J.%20Thomas&journal=Comput.%20Secur.&volume=24&issue=4&pages=295307&publication_year=2005&doi=10.1016%2Fj.Cose.2004.09.008)

12. Raghavendra Sai, N., Satya Rajesh, K.: A novel based approach for Liaison analysis in data summarization and deep web interface data extraction. Int. J. Control Theor. Appl. (IJCTA) 9(4) (2016). ISSN: 0974-5572 Google Scholar (https://scholar.google.com/scholar?q=Raghavendra%20Sai%2C%20N.%2C%20Satya%20Rajesh%2C%20K.%3A%20A%20novel%20based%20approach%20for%20Liaison%20analysis%20in%20data%20summarization%20and%20deep%20web%20interface%20data%20extraction.%20Int.%20J.%20Control%20Theor.%20Appl.%20%28IJCTA%29%209%284%29%20%282016%29.%20ISSN%3A%200974-5572)

13. Smys, S., Abul, B., Haoxiang, W.: Hybrid intrusion detection system for internet of things (IoT). J. ISMAC **2**(04), 190–199 (2020) CrossRef (https://doi.org/10.36548/jismac.2020.4.002) Google Scholar (http://scholar.google.com/scholar_lookup?title=Hybrid%20intrusion%20detection%20system%20for%20internet%20of%20things%20%28IoT%29&author=S.%20Smys&author=B.%20Abul&author=W.%20Haoxiang&journal=J.%20ISMAC&volume=2&issue=04&pages=190-199&publication_year=2020)

14. Karunakaran, P.: Deep learning approach to DGA classification for effective cyber security. J. Ubiquit. Comput. Commun. Technol. (UCCT) **2**(04), 203–213 (2020) Google Scholar (https://scholar.google.com/scholar?q=Karunakaran%2C%20P.%3A%20Deep%20learning%20approach%20to%20DGA%20classification%20for%20effective%20cyber%20security.%20J.%20Ubiquit.

%20Comput.%20Commun.%20Technol.%20%28UCCT%29%202%2804%29%2C%20203%E2%80%93213%20%282020%29)

15. Cannady, J.: Artificial neural networks for misuse detection. In: Proceedings of the 1998 National Information Systems Security Conference (NISSC), pp. 443456. Citeseer (1998)
Google Scholar (https://scholar.google.com/scholar?q=Cannady%2C%20J.%3A%20Artificial%20neural%20networks%20for%20misuse%20detection.%20In%3A%20Proceedings%20of%20the%201998%20National%20Information%20Systems%20Security%20Conference%20%28NISSC%29%2C%20pp.%20443456.%20Citeseer%20%281998%29)

16. Debar, H., Dorizzi, B.: An application of a recurrent network to an intrusion detection system. In: International Joint Conference on Neural Networks. IJCNN, vol. 2, pp. 478 483 (1992). https://doi.org/10.1109/ijcnn.1992.226942 (https://doi.org/10.1109/ijcnn.1992.226942)

17. Raghavendra Sai, N., Jogendra Kumar, M., Hussain Basha, P., Sai Chaitanya Kumar, G.: Effective intrusion detection system by using LOS classifier. Int. J. Innov. Technol. Explor. Eng. (IJITEE) 9(2) (2019). ISSN: 2278-3075
Google Scholar (https://scholar.google.com/scholar?q=Raghavendra%20Sai%2C%20N.%2C%20Jogendra%20Kumar%2C%20M.%2C%20Hussain%20Basha%2C%20P.%2C%20Sai%20Chaitanya%20Kumar%2C%20G.%3A%20Effective%20intrusion%20detection%20system%20by%20using%20LOS%20classifier.%20Int.%20J.%20Innov.%20Technol.%20Explor.%20Eng.%20%28IJITEE%29%209%282%29%20%282019%29.%20ISSN%3A%202278-3075)

18. Raghavendra Sai, N., Satya Rajesh, K.: An efficient los scheme for network data analysis. J. Adv. Res. Dyn. Control Syst. (JARDCS). **10**(9) (2018). ISSN: 1943-023X
Google Scholar (https://scholar.google.com/scholar?q=Raghavendra%20Sai%2C%20N.%2C%20Satya%20Rajesh%2C%20K.%3A%20An%20efficient%20los%20scheme%20for%20network%20data%20analysis.%20J.%20Adv.%20Res.%20Dyn.%20Control%20Syst.%20%28JARDCS%29.%2010%289%29%20%282018%29.%20ISSN%3A%201943-023X)

Copyright information

About this paper

Cite this paper as:

Mandru D.B., Aruna Safali M., Raghavendra Sai N., Sai Chaitanya Kumar G. (2022) Assessing Deep Neural Network and Shallow for Network Intrusion Detection Systems in Cyber Security. In: Smys S., Bestak R., Palanisamy R., Kotuliak I. (eds) Computer Networks and Inventive Communication Technologies. Lecture Notes on Data Engineering and Communications Technologies, vol 75. Springer, Singapore. https://doi.org/10.1007/978-981-16-3728-5_52

- First Online 14 September 2021

- DOI https://doi.org/10.1007/978-981-16-3728-5_52
- Publisher Name Springer, Singapore
- Print ISBN 978-981-16-3727-8
- Online ISBN 978-981-16-3728-5
- eBook Packages Engineering Engineering (Ro)

Personalised recommendations