LIST OF REFERENCES

[1] M. Sewak, S. K. Sahay, and H. Rathore, ‘‘Comparison of deep learning and the classical machine learning algorithm for the malware detection,’’ *2018 19th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD)*, Jun 2018. [Online]. Available: http://dx.doi.org/10.1109/SNPD.2018.8441123

[2] B. Cakir and E. Dogdu, ‘‘Malware classification using deep learning methods,’’ in *Proceedings of the ACMSE 2018 Conference*, ser. ACMSE ’18. New York, NY, USA: ACM, 2018, pp. 10:1--10:5. [Online]. Available: http://doi.acm.org/10.1145/3190645.3190692

[3] E. Raff, R. Zak, R. J. Cox, J. Sylvester, P. Yacci, R. Ward, A. Tracy, M. McLean, and C. Nicholas, ‘‘An investigation of byte n-gram features for malware classification,’’ *Journal of Computer Virology and Hacking Techniques*, vol. 14, pp. 1--20, 2016.

[4] X. Meng, Z. Shan, F. Liu, B. Zhao, J. Han, H. Wang, and J. Wang, ‘‘Mcsmgs: Malware classification model based on deep learning,’’ in *2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*, Oct 2017, pp. 272--275.

[5] Kaggle, ‘‘Deep learning vs machine learning efficiency over size of data,’’ https://ibb.co/m2bxcc, Mar 2018, (Accessed on 10/01/2018).