**REFERENCES**

[1] S. Naseer, Y. Saleem, S. Khalid, M. K. Bashir, J. Han, M. M. Iqbal, K. Han, "Enhanced Network Anomaly Detection Based on Deep Neural Networks," *IEEE Access*, vol. 6, pp. 48231-48246, 2018.

[2] B. Zhang, G. Hu, Z. Zhou, Y. Zhang, P. Qiao, L. Chang, "Network Intrusion Detection Based on Directed Acyclic Graph and Belief Rule Base", *ETRI Journal*, vol. 39, no. 4, pp. 592-604, Aug. 2017

[3] W. Wang, Y. Sheng and J. Wang, "HAST-IDS: Learning hierarchical spatial-temporal features using deep neural networks to improve intrusion detection," *IEEE Access*, vol. 6, no. 99, pp. 1792-1806, 2018.

[4] M. K. Hussein, N. Bin Zainal and A. N. Jaber, "Data security analysis for DDoS defense of cloud based networks," *2015 IEEE Student* *Conference on Research and Development (SCOReD)*, Kuala Lumpur, 2015, pp. 305-310.

[5] S. Sandeep Sekharan, K. Kandasamy, "Profiling SIEM tools and correlation engines for security analytics," *In Proc. Int. Conf.* *Wireless Com., Signal Proce. and Net.(WiSPNET)*, 2017, pp. 717-721.

[6] N.Hubballiand V.Suryanarayanan,‘‘False alarm minimization techniques in signature-based intrusion detection systems: A survey,’’ *Comput. Commun.*, vol. 49, pp. 1-17, Aug. 2014.

[7] A. Naser, M. A. Majid, M. F. Zolkipli and S. Anwar, "Trusting cloud computing for personal files," *2014 International Conference on* *Information and Communication Technology Convergence (ICTC)*, Busan, 2014, pp. 488-489.

[8] Y. Shen, E. Mariconti, P. Vervier, and Gianluca Stringhini, "Tiresias: Predicting Security Events Through Deep Learning," *In Proc. ACM* *CCS 18*, Toronto, Canada, 2018, pp. 592-605.

[9] Kyle Soska and Nicolas Christin, "Automatically detecting vulnerable websites before they turn malicious,", *In Proc. USENIX* *Security Symposium.*, San Diego, CA, USA, 2014, pp.625-640.

[10] K. Veeramachaneni, I. Arnaldo, V. Korrapati, C. Bassias, K. Li, "AI2: training a big data machine to defend," *In Proc. IEEE* *BigDataSecurity HPSC IDS*, New York, NY, USA, 2016, pp. 49-54

[11] Mahbod Tavallaee, Ebrahim Bagheri, Wei Lu and Ali A. Ghorbani, "A detailed analysis of the kdd cup 99 data set," *In Proc. of the Second IEEE Int. Conf. Comp. Int. for Sec. and Def. App*., pp. 53-58,

2009.

[12] I. Sharafaldin, A. H. Lashkari, A. A. Ghorbani, "Toward generating a new intrusion detection dataset and intrusion traffic characterization", *Proc. Int. Conf. Inf. Syst. Secur. Privacy*, pp. 108- 116, 2018.

[13] [online] Available: http://www.takakura.com/Kyoto\_data/

[14] N. Shone, T. N. Ngoc, V. D. Phai and Q. Shi, "A deep learning approach to network intrusion detection," *IEEE Trans. Emerg. Topics* *Comput. Intell.*, vol. 2, pp. 41-50, Feb. 2018

[15] R. Vinayakumar, Mamoun Alazab, K. P. Soman, P. Poornachandran, Ameer Al-Nemrat and Sitalakshmi Venkatraman, "Deep Learning Approach for Intelligent Intrusion Detection System," *IEEE Access*, vol. 7, pp. 41525-41550, Apr. 2019.

[16] W. Hu, W. Hu, S. Maybank, "Adaboost-based algorithm for network intrusion detection," *IEEE Trans. Syst. Man B Cybern.,* vol. 38, no. 2, pp. 577-583, Feb. 2008.

[17] T.-F. Yen et al., "Beehive: Large-scale log analysis for detecting suspicious activity in enterprise networks", *Proc. 29th Annu.* *Comput. Security Appl. Conf*., New York, NY, USA, 2013, pp. 199- 208.

[18] K.-O. Detken, T Rix, C Kleiner, B Hellmann, L. Renners, "Siem approach for a higher level of it security in enterprise networks", *In* *Proc. IDAACS*, Warsaw, Poland, 2015, pp. 322-327.

[19] en.wikipedia.org,“Security information and event management,” 2016 [Online] Available: <https://en.wikipedia.org/wiki/Security-> \_information\_and\_event\_management.

[20] Y. LeCun, L. Bottou, Y. Bengio, and P. Haffner, "Gradient-based learning applied to document recognition," *Proc. IEEE*, vol. 86, no. 11, pp. 2278-2324, Nov. 1998.

[21] C. Dong, C. C. Loy, K. He and X. Tang, "Image Super-Resolution Using Deep Convolutional Networks," in *IEEE Transactions on* *Pattern Analysis and Machine Intelligence*, vol. 38, no. 2, pp. 295- 307, 1 Feb. 2016.

[22] A. Karpathy, "Connecting images and natural language," P*h.D. dissertation, Fac. Comput. Sci., Stanford Univ., Stanford*, CA, USA,2016.

[23] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "Imagenet classificationwith deep convolutional neural networks," *In Proc. Of* *the 25th Int. Conf.on Neural Inf. Proc. Systems -Volume 1*, ser. NIPS’12, 2012, pp. 1097-1105.

[24] Q. Zhu, X. Li, A. Conesa, and C. Pereira, “Gram-cnn: a deep learning approach with local context for named entity recognition in biomedical text,” *Bioinformatics*, vol. 34, no. 9, pp. 1547–1554, 2017.

[25] W.Wang, M. Zhu, X. Zeng, X. Ye, and Y. Sheng, “Malware traffic classification using convolutional neural network for representation learning,” *In Proc. Int. Conf. on Infor. Net. (ICOIN)*, Da Nang, Vietnam, Jan. 2017, pp. 712–717.

[26] Z. Li, Z. Qin, K. Huang, X. Yang, and S. Ye, “Intrusion detection using convolutional neural networks for representation learning,” *In* *Proc. Int. Conf. Neural Information Springer*, 2017, pp. 858–866.

[27] M. Alazab, S. Venkatraman, P. Watters, and M. Alazab, “Zero-day malware detection based on supervised learning algorithms of API call signatures,” *In Proc. 9th Australas. Data Mining Conf.*, vol. 121. Ballarat, Australia, Dec. 2011, pp. 171-182.

[28] E. Raff, J. Sylvester, and C. Nicholas, “Learning the PE header, malware detection with minimal domain knowledge,'' *In Proc. 10th* *ACMWorkshop Artif. Intell. Secur*. New York, NY, USA, Nov. 2017, pp. 121-132.

[29] J. Gu et al., "Recent advances in convolutional neural networks", CoRR, pp. 187-332, Dec. 2017

[30] Kehe Wu, Zuge Chen, Wei Li, "A Novel Intrusion Detection Model for a Massive Network Using Convolutional Neural Networks", *Access IEEE*, vol. 6, pp. 50850-50859, 2018

[31] Taejoon Kim, Sang C. Suh, Hyunjoo Kim, Jonghyun Kim and Jinoh Kim, "An Encoding Technique for CNN-based Network Anomaly Detection," *In Proc. IEEE International Conference on Big Data* *(IEEE BigData)*, Seattle, WA, USA, Jan. 2019, pp. 2960-2965.

[32] R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran and S. Venkatraman "Robust Intelligent Malware Detection Using Deep Learning," *IEEE Access*, vol. 7, pp. 46717-46738, Apr. 2019

[33] Y. LeCun, Y. Bengio, and G. Hinton, “Deep learning,” *Nature*, vol. 521, no. 7553, pp. 436-444, 2015.

[34] S. Hochreiter, Y. Bengio, P. Frasconi, and J. Schmidhuber, “Gradient flow in recurrent nets: the difficulty of learning long-term dependencies,” 2001.

[35] D. Sisiaridis and Olivier Markowitch, "Reducing Data Complexity in Feature Extraction and Feature Selection for Big Data Security Analytics", *In Proc. Int. Conf. Data Intel. and Sec. (ICDIS)*, South Padre Island, TX, USA, May 2018, pp. 43-48.

[36] V. N. Inukollu, S. Arsi, S. R. Ravuri, "Security issues associated with big data in cloud computing", *International Journal of Network* *Security & Its Applications*, vol. 6, no. 3, pp. 45, 2014.