**REFERENCES**

**[1] Z.-K. Zhang, M. C. Y. Cho, C.-W. Wang, C.-W. Hsu, C.-K. Chen, and**

**S. Shieh, “Iot security: ongoing challenges and research opportunities,”**

**in 2014 IEEE 7th international conference on service-oriented computing**

**and applications. IEEE, 2014, pp. 230–234.**

**[2] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, “Blockchain for**

**iot security and privacy: The case study of a smart home,” in 2017 IEEE**

**international conference on pervasive computing and communications**

**workshops (PerCom workshops). IEEE, 2017, pp. 618–623.**

**[3] E. Bertino and N. Islam, “Botnets and internet of things security,”**

**Computer, no. 2, pp. 76–79, 2017.**

**[4] C. Zhang and R. Green, “Communication security in internet of thing:**

**preventive measure and avoid ddos attack over iot network,” in Proceedings**

**of the 18th Symposium on Communications & Networking. Society**

**for Computer Simulation International, 2015, pp. 8–15.**

**[5] W. Kim, O.-R. Jeong, C. Kim, and J. So, “The dark side of the internet:**

**Attacks, costs and responses,” Information systems, vol. 36, no. 3, pp.**

**675–705, 2011.**

**[6] H. Eun, H. Lee, and H. Oh, “Conditional privacy preserving security**

**protocol for nfc applications,” IEEE Transactions on Consumer Electronics,**

**vol. 59, no. 1, pp. 153–160, 2013.**

**[7] R. V. Kulkarni and G. K. Venayagamoorthy, “Neural network based**

**secure media access control protocol for wireless sensor networks,” in**

**2009 International Joint Conference on Neural Networks. IEEE, 2009,**

**pp. 1680–1687.**

**[8] M. A. Alsheikh, S. Lin, D. Niyato, and H.-P. Tan, “Machine learning**

**in wireless sensor networks: Algorithms, strategies, and applications,”**

**IEEE Communications Surveys & Tutorials, vol. 16, no. 4, pp. 1996–**

**2018, 2014.**

**[9] A. L. Buczak and E. Guven, “A survey of data mining and machine**

**learning methods for cyber security intrusion detection,” IEEE Communications**

**Surveys & Tutorials, vol. 18, no. 2, pp. 1153–1176, 2015.**

**[10] F. A. Narudin, A. Feizollah, N. B. Anuar, and A. Gani, “Evaluation**

**of machine learning classifiers for mobile malware detection,” Soft**

**Computing, vol. 20, no. 1, pp. 343–357, 2016.**

**[11] Z. Tan, A. Jamdagni, X. He, P. Nanda, and R. P. Liu, “A system**

**for denial-of-service attack detection based on multivariate correlation**

**analysis,” IEEE transactions on parallel and distributed systems, vol. 25,**

**no. 2, pp. 447–456, 2013.**

**[12] Y. Li, D. E. Quevedo, S. Dey, and L. Shi, “Sinr-based dos attack on**

**remote state estimation: A game-theoretic approach,” IEEE Transactions**

**on Control of Network Systems, vol. 4, no. 3, pp. 632–642, 2016.**

**[13] L. Xiao, Y. Li, X. Huang, and X. Du, “Cloud-based malware detection**

**game for mobile devices with offloading,” IEEE Transactions on Mobile**

**Computing, vol. 16, no. 10, pp. 2742–2750, 2017.**

**[14] J. W. Branch, C. Giannella, B. Szymanski, R. Wolff, and H. Kargupta,**

**“In-network outlier detection in wireless sensor networks,” Knowledge**

**and information systems, vol. 34, no. 1, pp. 23–54, 2013.**

**[15] I. Jolliffe, Principal component analysis. Springer, 2011.**

**[16] I. Guyon and A. Elisseeff, “An introduction to variable and feature**

**selection,” Journal of machine learning research, vol. 3, no. Mar, pp.**

**1157–1182, 2003.**

**[17] L. Yu and H. Liu, “Feature selection for high-dimensional data: A fast**

**correlation-based filter solution,” in Proceedings of the 20th international**

**conference on machine learning (ICML-03), 2003, pp. 856–863.**

**[18] A. H. Sodhro, S. Pirbhulal, and V. H. C. de Albuquerque, “Artificial**

**intelligence driven mechanism for edge computing based industrial**

**applications,” IEEE Transactions on Industrial Informatics, 2019.**

**[19] A. H. Sodhro, Z. Luo, G. H. Sodhro, M. Muzamal, J. J. Rodrigues, and**

**V. H. C. de Albuquerque, “Artificial intelligence based qos optimization**

**for multimedia communication in iov systems,” Future Generation**

**Computer Systems, vol. 95, pp. 667–680, 2019.**

**[20] L. University, “Refit smart home dataset,” https://repository.lboro.ac.uk/**

**articles/REFIT Smart Home dataset/2070091, 2019 (accessed April 26,**

**2019).**

**[21]** **R, “Rstudio,” 2019 (accessed October 23, 2019).**