

REFERENCES

- [1] “What is IoT Security?” [Online.] Available: <https://greenwavesystems.com/what-is-iot-security/>. [Accessed: 28-Sep-2019].
- [2] U. Andra, “Network Security in the Age of Hyperconnectivity_ Pervasive, Proactive, and Persistent Protection is Essential to Thwart Cyberattacks.” [Online.] Available: <https://blogs.cisco.com/sp/network-security-in-the-age-of-hyperconnectivity-pervasive-proactive-and-persistent-protection-is-essential-to-thwart-cyberattacks>. [Accessed: 17-Jan-2019]
- [3] G. Blaine, “Encrypted Attacks, IoT Malware Surge as Global Malware Volume Dips.” Available: <https://blog.sonicwall.com/en-us/2019/10/sonicwall-encrypted-attacks-iot-malware-surge-as-global-malware-volume-dips/>. [Accessed: 16-Dec-2019]
- [4] USTELECOM, “International Botnet and IoT Security Guide,” pp. 1- 54, 2020.
- [5] McAfee Labs, “Threats Report,” pp. 1–49, 2017.
- [6] P. Aggarwal and S. K. Sharma, “An empirical comparison of classifiers to analyze intrusion detection,” *Int. Conf. Adv. Comput. Commun. Technol. ACCT*, vol. 2015-April, pp. 446–450, 2015.
- [7] S. Samdani and S. Shukla, “A novel technique for converting nominal attributes to numeric attributes for intrusion detection,” *8th Int. Conf. Comput. Commun. Netw. Technol. ICCCNT 2017*, no. 1, pp. 1–5, 2017.
- [8] Z. Anming, “An intrusion fetection algorithm based on NFPA,” vol. 33, no. 1, pp. 491–497, 2012.
- [9] P. Kushwaha, H. Buckchash, and R. Balasubramanin, “Anomaly based intrusion detection using filter based feature selection on KDD-CUP 99,” *Proc. 2017 IEEE Reg. 10 Conf. (TENCON), Malaysia*, pp. 839–844, 2017.
- [10] K. Ibrahimi and M. Ouaddane, “Management of intrusion detection systems based-KDD99: Analysis with LDA and PCA,” *Proc. - 2017 Int. Conf. Wirel.*

- Networks Mob. Commun. WINCOM 2017*, 2017.
- [11] I. E. L. Farissi, M. Saber, S. Chadli, M. Emharraf, and M. Ghaouth, “The analysis performance of an Intrusion Detection Systems based on Neural Network,” pp. 145–151, 2016.
 - [12] K. Ghanem, F. J. Aparicio-Navarro, K. G. Kyriakopoulos, S. Lambbotharan, and J. A. Chambers, “Support Vector Machine for Network Intrusion and Cyber-Attack Detection,” *Def. Conf. SSPD Sens. Signal Process. 2017*, vol. 2017-Janua, pp. 1–5, 2017.
 - [13] J. Zhu, J. Mu, D. Wei, B. Feng, Y. Wang, and K. Yin, “A spatial correlation-based hybrid method for intrusion detection,” *Int. Conf. Commun. Softw. Networks*, pp. 0–5, 2017.
 - [14] C. Cervantes, D. Poplade, M. Nogueira, and A. Santos, “Detection of sinkhole attacks for supporting secure routing on 6LoWPAN for Internet of Things,” *Proc. 2015 IFIP/IEEE Int. Symp. Integr. Netw. Manag. IM 2015*, pp. 606–611, 2015.
 - [15] Z. Guo, I. G. Harris, Y. Jiang, and L. F. Tsaur, “An efficient approach to prevent battery exhaustion attack on BLE-based mesh networks,” *2017 Int. Conf. Comput. Netw. Commun. ICNC 2017*, pp. 1–5, 2017.
 - [16] Y. Fu, Z. Yan, J. Cao, O. Koné, and X. Cao, “An Automata Based Intrusion Detection Method for Internet of Things,” *Mob. Inf. Syst.*, vol. 2017, pp. 6–10, 2017.
 - [17] A. K. Kyaw, Y. Chen, and J. Joseph, “Pi-IDS: Evaluation of open-source intrusion detection systems on Raspberry Pi 2,” *2015 2nd Int. Conf. Inf. Secur. Cyber Forensics, InfoSec 2015*, pp. 165–170, 2016.
 - [18] A. Sforzin, F. G. Marmol, M. Conti, and J. M. Bohli, “RPiDS: Raspberry Pi IDS - A Fruitful Intrusion Detection System for IoT,” *Proc. - 13th IEEE Int. Conf. Ubiquitous Intell. Comput. 13th IEEE Int. Conf. Adv. Trust. Comput. 16th IEEE Int. Conf. Scalable Comput. Commun. IEEE Int.*, pp. 440–448, 2017.
 - [19] A. M. Da Silva Cardoso, R. F. Lopes, A. S. Teles, and F. B. V. Magalhaes, “Real-

- time DDoS detection based on complex event processing for IoT,” *Proc. - ACM/IEEE Int. Conf. Internet Things Des. Implementation, IoTDI 2018*, pp. 273–274, 2018.
- [20] T. L. von Sperling, F. L. de Caldas Filho, R. T. de Sousa, L. M. C. e Martins, and R. L. Rocha, “Tracking intruders in IoT networks by means of DNS traffic analysis,” *2017 Work. Commun. Networks Power Syst.*, pp. 1–4, 2017.
- [21] T. Zitta, M. Neruda, and L. Vojtech, “The security of RFID readers with IDS/IPS solution using Raspberry Pi,” *2017 18th Int. Carpathian Control Conf. ICC3 2017*, pp. 316–320, 2017.
- [22] A. Aspernäs and T. Simonsson, “IDS on Raspberry Pi: A Performance Evaluation,” Linnaeus University, Sweden, 2015.
- [23] B. S. Khater *et al.*, “A Lightweight Perceptron-Based Intrusion Detection System for Fog Computing,” *Appl. Sci.*, 9. 178, 2019.
- [24] A. R. Baker and J. Esler, *Snort IDS, IPS Toolkit*. Syngress Publishing, Inc. Elsevier, Inc. 30 Corporate Dr. Burlington, MA 01803, 2007.
- [25] OISF, “Suricata User Guide,” *Open Information Security Foundation: Boston, MA, USA*, 2019.
- [26] S. S. Tirumala, H. Sathu, and A. Sarrafzadeh, “Free and open source intrusion detection systems: A study,” *Proc. - Int. Conf. Mach. Learn. Cybern.*, vol. 1, pp. 205–210, 2015.
- [27] A. Sforzin and M. Conti, “RPiDS : Raspberry Pi IDS A Fruitful Intrusion Detection System for IoT,” pp. 440–448, 2016.
- [28] S. A. R. Shah and B. Issac, “Performance comparison of intrusion detection systems and application of machine learning to Snort system,” *Futur. Gener. Comput. Syst.*, vol. 80, no. March, pp. 157–170, 2018.
- [29] A. Blanter and M. Holman, “Internet of Things 2020: A Glimpse into the Future,” [Online.] Available: https://www.atkearney.com/documents/4634214/6398631/AT+Kearney_Interne

- t+of+Things. [Accessed: 17-Mar-2010]
- [30] R. Kohavi and G. H. John, “Wrappers for Feature Subset Selection,” *Artif. Intell.*, pp. 273–324, 1997.
 - [31] R. Kohavi and D. Sommerfield, “Feature Subset Selection Using the Wrapper Method: Overfitting and Dynamic Search Space Topology,” in *First International Conference on Knowledge Discovery and Data Mining (KDD’95)*, 1995, pp. 192–197.
 - [32] Y. Feng, H. Akiyama, L. Lu, and K. Sakurai, “Feature Selection for Machine Learning-Based Early Detection of Distributed Cyber Attacks,” *IEEE Cyber Sci. Technol. Congr. (CyberSciTech)*, *CyberSciTech2018*, pp. 173–180, 2018.
 - [33] G. Chandrashekar and F. Sahin, “A survey on feature selection methods,” *Comput. Electr. Eng.*, vol. 40, no. 1, pp. 16–28, 2014.
 - [34] I. Guyon and A. Elisseeff, “An Introduction to Variable and Feature Selection,” *J. Mach. Learn. Res.*, no. 3, pp. 1157–1182, 2003.
 - [35] R. Battiti, “Using mutual information for selecting features in supervised neural net learning,” *IEEE Trans. Neural Networks*, vol. 5(4), no. 4, pp. 537–550, 1994.
 - [36] A. G. Karegowda, A. S. Manjunath, G. Ratio, and C. F. Evaluation, “Comparative study of Attribute Selection Using Gain Ratio,” *Int. J. Inf. Technol. Knowl. Knowl. Manag.*, vol. 2, no. 2, pp. 271–277, 2010.
 - [37] R. Margaret, “Lightweight.” [Online.] Available: <https://whatis.techtarget.com/definition/lightweight> [Accessed: 1-Jul-2010]
 - [38] Tutorialspoint, “Internet of Things,” *Tutorials Point (I) Pvt. Ltd.* pp. 1–13, 2019.
 - [39] M. G. Samaila, M. Neto, D. A. B. Fernandes, M. M. Freire, and P. R. M. Inácio, “Challenges of securing Internet of Things devices: A survey,” *Secur. Priv.*, vol. 1, no. 2, p. e20, 2018.
 - [40] P. Sethi and S. R. Sarangi, “Internet of Things: Architectures, Protocols, and Applications,” *J. Electr. Comput. Eng.*, vol. 2017, 2017.
 - [41] J. E. Gómez, F. R. Marcillo, F. L. Triana, V. T. Gallo, B. W. Oviedo, and V. L.

- Hernández, “IoT for ENVIRONMENTAL VARIABLES in URBAN AREAS,” *Procedia Comput. Sci.*, vol. 109, no. 2016, pp. 67–74, 2017.
- [42] D. Mocrii, Y. Chen, and P. Musilek, “IoT-based smart homes: A review of system architecture, software, communications, privacy and security,” *Internet of Things*, vol. 1–2, pp. 81–98, 2018.
- [43] “Raspberry Pi Projects.” [Online.] Available: <https://nevonprojects.com/raspberry-pi-projects/> [Accessed: 3-Jan-2020].
- [44] R. van Kranenburg and A. Bassi, “IoT Challenges,” *Commun. Mob. Comput.*, vol. 1, no. 1, pp. 1–5, 2012.
- [45] A. Harper, “10 Biggest security challenges for IoT,” *Peerbits*, 2019. [Online.] Available: <https://www.peerbits.com/blog/biggest-iot-security-challenges.html>. [Accessed: 13-Aug-2020].
- [46] K. Lewis, “IoT Security vs. IT Security: What’s the difference?” [Online.] <https://www.ibm.com/blogs/internet-of-things/security-iot/> [Accessed: 31-Jan-2020].
- [47] Devry Jane, “Mirai Botnet Infects Devices in 164 Countries - Cybersecurity Insiders,” *Cybersecurity Insiders*, 2019. [Online.] Available: <https://www.cybersecurity-insiders.com/mirai-botnet-infects-devices-in-164-countries/>. [Accessed: 06-Nov-2020].
- [48] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, “DDoS in the IoT: Mirai and other botnets,” *Computer (Long. Beach. Calif.)*, vol. 50, no. 7, pp. 80–84, 2017.
- [49] M. Antonakakis *et al.*, “Understanding the Mirai Botnet,” *USENIX Secur.*, pp. 1093–1110, 2017.
- [50] A. Marzano *et al.*, “The Evolution of Bashlite and Mirai IoT Botnets,” *Proc. - IEEE Symp. Comput. Commun.*, vol. 2018-June, pp. 813–818, 2018.
- [51] M. Nieves, K. Dempsey, and V. Y. Pillitteri, *An Introduction to Computer Security: the NIST Handbook*, vol. 1. 2017.
- [52] S. William and W. Stallings, “Cryptography and Network Security,” *Prentice Hall*

Press, 5th Edition, USA. 2010.

- [53] R. Margaret, "What is intrusion detection (ID)?," [Online.] Available: <https://searchsecurity.techtarget.com/definition/intrusion-detection-system>. [Accessed: 12-Feb-2019].
- [54] T. Bradley, "Introduction to Intrusion Detection Systems (IDS)," *Lifewire*, 2020. [Online.] Available: <https://www.lifewire.com/introduction-to-intrusion-detection-systems-ids-2486799>. [Accessed: 15-Apr-2020].
- [55] B. Subba, S. Biswas, and S. Karmakar, "Host based intrusion detection system using frequency analysis of n-gram terms," *IEEE Reg. 10 Annu. Int. Conf. Proceedings/TENCON*, vol. 2017-Decem, pp. 2006–2011, 2017.
- [56] P. Innella and O. McMillan, "An Introduction to IDS | Symantec Connect Community," *Tetrad Digital Integrity, LLC*, 2001.
- [57] Y. Maleh et al., "A hybrid intrusion detection system," *Procedia Computer Science*, vol. 52, pp. 1047-1052, 2015.
- [58] A. Garg and P. Maheshwari, "Identifying anomalies in network traffic using hybrid Intrusion Detection System," in *2016 3rd Int. Conf on Advanced Computing and Communication Systems (ICACCS)*, Coimbatore, 2016, pp. 1-6, 2016.
- [59] F. L. Bello, K. Ravulakollu, and Amrita, "Analysis and evaluation of hybrid intrusion detection system models," *2015 Int. Conf. Comput. Commun. Syst.*, pp. 93–97, 2015.
- [60] V. Kumar, J. Srivastava, and A. Lazarevic, "Managing cyber threats: issues, approaches, and challenges," *New York: Springer-Verlag*, pp. 247-266, 2005.
- [61] P. García-Teodoro, J. Díaz-Verdejo, G. Maciá-Fernández, and E. Vázquez, "Anomaly-based network intrusion detection: Techniques, systems and challenges," *Comput. Secur.*, vol. 28, no. 1–2, pp. 18–28, 2009.
- [62] A. R. KARTIT, A.SAIDI, F.BEZZAZI, M.EL MARRAKI, "a New Approach To Intrusion Detection System," *J. Theor. Appl. Inf. Technol.* © 2005 - 2012, vol. 36,

no. 2, 2012.

- [63] T. M. Mitchell, "Machine Learning," *New York: McGraw-Hill*, 2009.
- [64] A. Ashari, I. Paryudi, and A. Min, "Performance Comparison between Naïve Bayes, Decision Tree and k-Nearest Neighbor in Searching Alternative Design in an Energy Simulation Tool," *Int. J. Adv. Comput. Sci. Appl.*, vol. 4, no. 11, pp. 33–39, 2013.
- [65] P. Domingos and G. Hulten, "Mining high-speed data streams," *Proceeding Sixth ACM SIGKDD Int. Conf. Knowl. Discov. Data Min.*, pp. 71–80, 2000.
- [66] G. Hulten and L. Spencer, "Mining Time-Chaning Data Streams," *Association for Computing Machinery*, New York, NY, USA, pp. 97–106, 2001.
- [67] V. G. T. da Costa, A. C. P. de L. F. de Carvalho, and S. Barbon Junior, "Strict Very Fast Decision Tree: A memory conservative algorithm for data stream mining," *Pattern Recognit. Lett.*, vol. 116, pp. 22–28, 2018.
- [68] N. Landwehr, M. Hall, and E. Frank, "Logistic model trees," *Lect. Notes Artif. Intell. (Subseries Lect. Notes Comput. Sci.)*, vol. 2837, pp. 241–252, 2005.
- [69] J. Friedman, T. Hastie, and R. Tibshirani, "Additive Logistic Regression: A Statisticl View of Boosting," *Ann. Stat.*, vol. 28, no. 2, pp. 337–407, 2000.
- [70] L. Breiman, "Random forests," pp. 1–33, 2001.
- [71] T. M. Oshiro, P. S. Perez, and J. A. Baranauskas, "How Many Trees in a Random Forest?," in *Machine Learning and Data Mining in Pattern Recognition*, vol. 3587, no. June, 2012, pp. 154–168.
- [72] S. Haykin, "Neural Networks and Learning Machines," *Pearson Education: 3rd Edition, Upper Saddle River, NJ*, 2009.
- [73] R. Rojas, "Neural Networks," *Springer, Berlin Heidelberg NewYork*, pp. 1-509, 1996.
- [74] B. Ding, H. Qian, and J. Zhou, "Activation functions and their characteristics in deep neural networks," *Proc. 30th Chinese Control Decis. Conf. CCDC 2018*, pp. 1836–1841, 2018.

- [75] C. E. Nwankpa, W. Ijomah, A. Gachagan, and S. Marshall, “Activation Functions : Comparison of Trends in Practice and Research for Deep Learning,” pp. 1–20.
- [76] M. Hall, “Correlation-based Feature Selection for Machine Learning,” *Methodology*, vol. 21i195-i20, no. April, pp. 1–5, 1999.
- [77] I. H. Witten and E. Frank, *Datamining. Practical Machine Learning Tools and Technicals with Java Implementations.*, 2nd ed. Morgan Kaufmann series in data management systems, 2005.
- [78] Cisco, “Cisco visual networking index (VNI) global mobile data traffic forecast update, 2017-2022 white paper,” [Online.] Available: <https://s3.amazonaws.com/media.mediapost.com/uploads/CiscoForecast.pdf>. [Accessed: 14-Aug-2019].
- [79] Spamhaus Malware Labs, “Spamhaus Botnet Threat Report 2019,” [Online.] Available: <https://www.spamhaus.org/news/article/793/spamhaus-botnet-threatreport-2019>. [Accessed: 3-Mar-2010].
- [80] W. Haider, G. Creech, Y. Xie, and J. Hu, “Windows based data sets for evaluation of robustness of Host based Intrusion Detection Systems (IDS) to zero-day and stealth attacks,” *Futur. Internet*, vol. 8, no. 3, 2016.
- [81] Check Point Research, “Cyber Attack Trends Analysis Report,” [Online.] Available: http://snt.hr/boxcontent/CheckPointSecurityReport2019_vol01.pdf. [Accessed: 20-Jun-2019].
- [82] V. K. Mikhail Kuzin, Yaroslav Shmelev, “New trends in the world of IoT threats - Securelist,” *Kaspersky Lab*. 2018.
- [83] S. A. R. Shah and B. Issac, “Performance comparison of intrusion detection systems and application of machine learning to Snort system,” *Futur. Gener. Comput. Syst.*, vol. 80, no. November 2017, pp. 157–170, 2018.
- [84] D. Evans, “The Internet of Things: How the Next Evolution of the Internet is Changing Everything.”, Cisco Internet Business Solutions Group (IBSG), pp.1-

- 11, 2011.
- [85] N. Koroniotis, N. Moustafa, E. Sitnikova, and B. Turnbull, “Towards the Development of Realistic Botnet Dataset in the Internet of Things for Network Forensic Analytics: Bot-IoT Dataset,” 2018.
 - [86] W. Tylman, “Misuse-Based Intrusion Detection Using Bayesian Networks,” *2008 Third Int. Conf. Dependability Comput. Syst. DepCoS-RELCOMEX*, pp. 211–218, 2008.
 - [87] A. Ahmed, A. Lisitsa, and C. Dixon, “A Misuse-Based Network Intrusion Detection System Using Temporal Logic and Stream Processing,” pp. 1–8, 2011.
 - [88] Z. Vi, Z. Li-jun, and N. Network, “A Rule Generation Model Using S-PSO for Misuse Intrusion Detection,” *Evol. Comput.*, no. Iccasm, pp. 418–423, 2010.
 - [89] M. K. Goyal, A. Aggarwal, and N. Jain, “Effect of change in rate of genetic algorithm operator on composition of signatures for misuse intrusion detection system,” *Proc. 2012 2nd IEEE Int. Conf. Parallel, Distrib. Grid Comput. PDGC 2012*, pp. 669–672, 2012.
 - [90] C. G. Cordero, S. Hauke, M. Muhlhauser, and M. Fischer, “Analyzing flow-based anomaly intrusion detection using Replicator Neural Networks,” *2016 14th Annu. Conf. Privacy, Secur. Trust. PST 2016*, pp. 317–324, 2016.
 - [91] N. Neupane, “Comparative Analysis of Backpropagation Algorithm Variants for Network Intrusion Detection,” pp. 726–729, 2017.
 - [92] A.-C. Enache and V. Sgarciu, “Anomaly Intrusions Detection Based on Support Vector Machines with an Improved Bat Algorithm,” *2015 20th Int. Conf. Control Syst. Comput. Sci.*, pp. 317–321, 2015.
 - [93] M. E. Aminanto, R. Choi, H. C. Tanuwidjaja, P. D. Yoo, and K. Kim, “Deep abstraction and weighted feature selection for Wi-Fi impersonation detection,” *IEEE Trans. Inf. Forensics Secur.*, vol. 13, no. 3, pp. 621–636, 2017.
 - [94] C. Cervantes, D. Poplade, M. Nogueira, and A. Santos, “Detection of sinkhole attacks for supporting secure routing on 6LoWPAN for Internet of Things,” *Proc.*

- 2015 IFIP/IEEE Int. Symp. Integr. Netw. Manag. IM 2015, pp. 606–611, 2015.
- [95] P. Kasinathan, C. Pastrone, M. A. Spirito, and M. Vinkovits, “Denial-of-Service detection in 6LoWPAN based Internet of Things,” *Int. Conf. Wirel. Mob. Comput. Netw. Commun.*, pp. 600–607, 2013.
 - [96] I. Ghafir, V. Prenosil, J. Svoboda and M. Hammoudeh, "A Survey on Network Security Monitoring Systems," *2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)*, Vienna, 2016, pp. 77-82, doi: 10.1109/W-FiCloud.2016.30.
 - [97] E. Anthi, L. Williams, and P. Burnap, “Pulse: an adaptive intrusion detection for the internet of things,” in *Living in the Internet of Things: Cybersecurity of the IoT - 2018* pp. 1-4, 2018.
 - [98] M. Nobakht, V. Sivaraman, and R. Boreli, “A host-based intrusion detection and mitigation framework for smart home IoT using OpenFlow,” *Proc. - 2016 11th Int. Conf. Availability, Reliab. Secur. ARES 2016*, pp. 147–156, 2016.
 - [99] M. Coşar and H. E. Kiram, “Performance Comparison of Open Source IDSs via Raspberry Pi,” in *2018 International Conference on Artificial Intelligence and Data Processing (IDAP)*, 2018.
 - [100] S. Tripathi, “Raspberry Pi as an Intrusion Detection System , a Honeypot and a Packet Analyzer,” *2018 Int. Conf. Comput. Tech. Electron. Mech. Syst.*, pp. 80–85, 2018.
 - [101] G. Creech and J. Hu, “Generation of a new IDS test dataset: Time to retire the KDD collection,” *IEEE Wirel. Commun. Netw. Conf. WCNC*, pp. 4487–4492, 2013.
 - [102] B. Subba, S. Biswas, and S. Karmakar, “A Neural Network based system for Intrusion Detection and attack classification,” *2016 Twenty Second Natl. Conf. Commun.*, pp. 1–6, 2016.
 - [103] N. Neupane and S. Shakya, “Comparative analysis of backpropagation algorithm variants for network intrusion detection,” *Proceeding - IEEE Int. Conf. Comput.*

- Commun. Autom. ICCCA 2017*, vol. 2017-Janua, pp. 726–729, 2017.
- [104] M. Anbar, R. Abdullah, I. H. Hasbullah, Y.-W. Chong, and O. E. Elejla, “Comparative performance analysis of classification algorithms for intrusion detection system,” *2016 14th Annu. Conf. Privacy, Secur. Trust*, pp. 282–288, 2016.
- [105] Z. A. Foroushani and Y. Li, "Intrusion Detection System by Using Hybrid Algorithm of Data Mining Technique", in *ICSCA 2018: Proceedings of the 2018 7th International Conference on Software and Computer Applications*, pp. 119–123, 2018.
- [106] P. S. Sarawagi, “Intrusion Detection Using Data Mining,” *Management*, vol. 3, no. 04329022, pp. 93–101, 2017.
- [107] “Power Consumption Benchmarks | Raspberry Pi Dramble.” [Online]. Available: <https://www.pidramble.com/wiki/benchmarks/power-consumption>. [Accessed: 23-Jul-2020].
- [108] S. D. Bay, D. Kibler, M. J. Pazzani, and P. Smyth, “The UCI KDD archive of large data sets for data mining research and experimentation,” *ACM SIGKDD Explor. Newsl.*, vol. 2, no. 2, pp. 81–85, 2000.
- [109] J. Song, H. Takakura, and Y. Okabe, “Description of Kyoto University Benchmark Data,” pp. 10–12, 2010.
- [110] N. Moustafa and J. Slay, “UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set),” *2015 Mil. Commun. Inf. Syst. Conf. MilCIS 2015 - Proc.*, no. December, 2015.
- [111] Y. Meidan *et al.*, “N-BaIoT: Network-based Detection of IoT Botnet Attacks Using Deep Autoencoders,” vol. 13, no. 9, pp. 1–8, 2018.
- [112] N. Moustafa and J. Slay, “The significant features of the UNSW-NB15 and the KDD99 data sets for Network Intrusion Detection Systems,” *Proc. - 2015 4th Int. Work. Build. Anal. Datasets Gather. Exp. Returns Secur. BADGERS 2015*, no. March 2016, pp. 25–31, 2017.

- [113] Y. Mirsky, T. Doitshman, Y. Elovici, and A. Shabtai, “Kitsune: An Ensemble of Autoencoders for Online Network Intrusion Detection,” no. February, pp. 18–21, 2018.
- [114] M. Kuhn and K. Johnson, “An Introduction to Feature Selection,” *Applied Predictive Modeling*, pp. 487–519, 2013.
- [115] Y. N. Soe, Y. Feng, P. I. Santosa, R. Hartanto, and K. Sakurai, “Implementing Lightweight IoT-IDS on Raspberry Pi Using Correlation-Based Feature Selection and Its Performance Evaluation,” in *Advanced Information Networking and Applications - Proceedings of the 33rd International Conference on Advanced Information Networking and Applications AINA-2019*, 2019, pp. 458–469.
- [116] P. Amini, M. A. Araghizadeh, and R. Azmi, “A survey on Botnet: Classification, detection and defense,” *Proc. - 2015 Int. Electron. Symp. Emerg. Technol. Electron. Information, IES 2015*, no. January 2016, pp. 233–238, 2016.
- [117] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, “A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures,” *IEEE Access*, vol. 7, pp. 82721–82743, 2019.
- [118] A. Glória, F. Cercas, and N. Souto, “Design and implementation of an IoT gateway to create smart environments,” *Procedia Comput. Sci.*, vol. 109, pp. 568–575, 2017.
- [119] S. Esquembri, “IoT with the Raspberry-Pi3,” 2018. [Online.] Available: http://oa.upm.es/53066/1/IoT_with_the_raspberrypi_v1_2.pdf. [Accessed: 10-Mar-2020].
- [120] Y. N. Soe, Y. Feng, P. I. Santosa, R. Hartanto, and K. Sakurai, “A sequential scheme for detecting cyber attacks in IoT environment,” in *Proceedings - IEEE 17th International Conference on Dependable, Autonomic and Secure Computing, IEEE 17th International Conference on Pervasive Intelligence and Computing, IEEE 5th International Conference on Cloud and Big Data Computing, 4th Cyber Scienc*, 2019, vol. 324, pp. 238–244.

- [121] Hisham, “Htop - an interactive process viewer for Unix.” [Online]. Available: <http://hisham.hm/htop/>. [Accessed: 15-Jul-2019].
- [122] M. Shafiq, Z. Tian, A. K. Bashir, X. Du, and M. Guizani, “IoT malicious traffic identification using wrapper-based feature selection mechanisms,” *Comput. Secur.*, vol. 94, p. 101863, 2020.
- [123] A. V. Aho and M. J. Corasick, “Efficient String Matching: An Aid to Bibliographic Search,” *Commun. ACM*, vol. 18, no. 6, pp. 333–340, 1975.
- [124] H. Zhao, Y. Feng, and H. Koide, “A Sequential Detection Method for Intrusion Detection System Based on Artificial Neural Networks,” *J. Chem. Inf. Model.*, vol. 53, no. 9, pp. 1689–1699, 2019.
- [125] F. E. Heba, E. H. Aboul, K. Tai-hoon, and B. Soumya, “Linear Correlation-Based Feature Selection for Network Intrusion Detection Model,” *Adv. Secur. Inf. Commun. Networks*, vol. 381, pp. 240–248, 2013.
- [126] M. Tavallaei, E. Bagheri, W. Lu, and A. A. Ghorbani, “A Detailed Analysis of the KDD CUP 99 Data Set,” in *Proceedings of the Second IEEE International Conference on Computational Intelligence for Security and Defense Applications*, 2009, pp. 53–58.
- [127] F. Amiri, M. Rezaei Yousefi, C. Lucas, A. Shakery, and N. Yazdani, “Mutual information-based feature selection for intrusion detection systems,” *J. Netw. Comput. Appl.*, vol. 34, no. 4, pp. 1184–1199, 2011.
- [128] M. A. Hall, “Correlation-based Feature Selection for Machine Learning,” *Ph.D. Thesis, University of Waikato*, Hamilton, New Zealand, 1999.
- [129] Y. N. Soe, Y. Feng, P. I. Santosa, R. Hartanto, and K. Sakurai, “Machine learning-based IoT-botnet attack detection with sequential architecture,” *Sensors (Switzerland)*, vol. 20, no. 16, pp. 1–15, 2020.
- [130] C. Zhang and S. Zhang, *Association Rule Mining: Models and Algorithms*, vol. 53, no. 9. Springer-Verlag, Berlin, Heidelberg, New York, 2002.