REFERENCE LIST

[1] V. Chandola, A. Banerjee and V. Kumar, "Anomaly detection: A survey," *ACM computing surveys (CSUR),* vol. 41, no. 3, pp. 1-58, 2009.

[2] A. Lakhina, M. Crovella and C. Diot, "Diagnosing network-wide traffic anomalies," *ACM SIGCOMM computer communication review,* vol. 34, no. 4, pp. 219-230, 2004.

[3] N. Hoque, M. H. Bhuyan, R. C. Baishya, D. K. Bhattacharyya and J. K. Kalita, "Network attacks: Taxonomy, tools and systems," *Journal of Network and Computer Applications,* vol. 40, pp. 307-324, 2014.

[4] G. Fernandes, J. J. Rodrigues, L. F. Carvalho, J. F. Al-Muhtadi and M. L. Proena, "A comprehensive survey on network anomaly detection," *Telecommunication Systems,* vol. 70, no. 3, pp. 447-489, 2019.

[5] M. M. Ogonji, G. Okeyo and J. M. Wafula, "A survey on privacy and security of Internet of Things," *Computer Science Review,* vol. 38, 2020.

[6] S. Eggers, "A novel approach for analyzing the nuclear supply chain cyber-attack surface," *Nuclear Engineering and Technology,* 2020.

[7] M. Nieles, K. Dempsey and V. Pillitteri, "An introduction to information security," National Institute of Standards and Technology, 2017.

[8] M. Z. Gunduz and R. Das, "Cyber-security on smart grid: Threats and potential solutions," *Computer Networks,* vol. 169, 2020.

[9] F. Mouton, M. M. Malan and H. S. Venter, "Social engineering from a normative ethics perspective," in *2013 Information Security for South Africa*, 2013.

[10] R. A. Maxion and T. N. Townsend, "Masquerade detection using truncated command lines," in *Proceedings international conference on dependable systems and networks*, 2002.

[11] J. M. Vidal, A. L. S. Orozco and L. J. G. Villalba, "Online masquerade detection resistant to mimicry," *Expert Systems with Applications,* pp. 162-180, 2016.

[12] M. Feng and R. Gupta, "Detecting virus mutations via dynamic matching," in *2009 IEEE International Conference on Software Maintenance*, 2009.

[13] P. C. Van Oorschot, "Intrusion Detection and Network-Based Attacks," in *Computer Security and the Internet: Tools and Jewels*, Springer Nature, 2020, pp. 310-334.

[14] D. E. Denning, "An intrusion-detection model," *IEEE Transactions on software engineering,* no. 2, pp. 222-232, 1987.

[15] W. T. Yue and M. Cakanyildirim, "Intrusion prevention in information systems: Reactive and proactive responses," *Journal of Management Information Systems,* vol. 24, no. 1, pp. 329-353, 2007.

[16] A. Khraisat, I. Gondal, P. Vamplew and J. Kamruzzaman, "Survey of intrusion detection systems: techniques, datasets and challenges," *Cybersecurity,* vol. 2, no. 1, p. 20, 2019.

[17] M. M. Hassan, "Current studies on intrusion detection system, genetic algorithm and fuzzy logic," *International Journal of Distributed and Parallel Systems (IJDPS),* vol. 4, no. 2, 2013.

[18] H. Bostani and M. Sheikhan, "Hybrid of anomaly-based and specification-based IDS for Internet of Things using unsupervised OPF based on MapReduce approach," *Computer Communications,* pp. 52-71, 2017.

[19] C.-I. Fan, H.-W. Hsiao, C.-H. Chou and Y.-F. Tseng, "Malware detection systems based on API log data mining," in *2015 IEEE 39th annual computer software and applications conference*, 2015.

[20] P. Wang and Y.-S. Wang, "Malware behavioural detection and vaccine development by using a support vector model classifier," *Journal of Computer and System Sciences,* vol. 81, no. 6, pp. 1012-1026, 2015.

[21] J. B. Fraley and M. Figueroa, "Polymorphic malware detection using topological feature extraction with data mining," in *SoutheastCon 2016*, 2016.

[22] S. Gamage and J. Samarabandu, "Deep learning methods in network intrusion detection: A survey and an objective comparison," in *Journal of Network and Computer Applications*, 2020.

[23] K. Scarfone and P. Mell, "Guide to intrusion detection and prevention systems (idps)," National Institute of Standards and Technology, 2012.

[24] R. Sekar, A. Gupta, J. Frullo, T. Shanbhag, A. Tiwari, H. Yang and S. Zhou, "Specification-based anomaly detection: a new approach for detecting network intrusions," in *Proceedings of the 9th ACM conference on Computer and communications security,* 2002.

[25] M. V. de Assis, J. J. Rodrigues and M. L. Proenca Jr, "A seven-dimensional flow analysis to help autonomous network management," *Information Sciences,* vol. 278, pp. 900-913, 2014.

[26] P. Garcia-Teodoro, J. Diaz-Verdejo, G. Macia-Fernandez and E. Vazquez, "Anomaly-based network intrusion detection: Techniques, systems and challenges," *computers & security,* vol. 28, no. 1-2, pp. 18-28, 2009.

[27] S. Axelsson, “The base-rate fallacy and its implications for the difficulty of intrusion detection,” in *Proceedings of the 6th ACM Conference on Computer and Communications Security*, 1999.

[28] C. Kruegel, D. Mutz, W. Robertson and F. Valeur, “Bayesian event classification for intrusion detection,” in *19th Annual Computer Security Applications Conference, 2003. Proceedings*, 2003.

[29] S. Solani and N. K. Jadav, “A Novel Approach to Reduce False-Negative Alarm Rate in Network-Based Intrusion Detection System Using Linear Discriminant Analysis,” in *Inventive Communication and Computational Technologies*, 2020.

[30] C. Kruegel, F. Valeur, G. Vigna and R. Kemmerer, “Stateful intrusion detection for high-speed network's,” in *Proceedings 2002 IEEE Symposium on Security and Privacy*, 2002.

[31] J. E. Gaffney and J. W. Ulvila, “Evaluation of intrusion detectors: A decision theory approach,” in *Proceedings 2001 IEEE Symposium on Security and Privacy. S&P 2001*, 2000.

[32] S. J. Stolfo, W. Fan, W. Lee, A. Prodromidis and P. K. Chan, “Cost-based modeling for fraud and intrusion detection: Results from the JAM project,” in *Proceedings DARPA Information Survivability Conference and Exposition. DISCEX'00*, 2000.

[33] O. Bouziani, H. Benaboud, A. S. Chamkar and S. Lazaar, “A Comparative study of Open Source IDSs according to their Ability to Detect Attacks,” in *Proceedings of the 2nd International Conference on Networking, Information Systems & Security*, 2019.

[34] F. Siemons, “Open Source IDS: Snort or Suricata? [Updated 2021],” Infosec Institute, 27 January 2021. [Online]. Available: https://resources.infosecinstitute.com/topic/open-source-ids-snort-suricata/. [Accessed 21 May 2021].

[35] M. Schrotter, T. Scheffler and B. Schnor, “Evaluation of Intrusion Detection Systems in IPv6 Networks,” in *Proceedings of the 16th International Joint Conference on e-Business and Telecommunications (ICETE 2019)*, 2019.

[36] V. Paxson, “Bro: a system for detecting network intruders in real-time,” *Computer networks*, vol. 31, no. 23-24, pp. 2435-2463, 1999.

[37] S. Talukder, “Tools and techniques for malware detection and analysis,” 2020.

[38] M. Amrollahi, S. Hadayeghparast, H. Karimipour, F. Derakhshan and G. Srivastava, “Enhancing network security via machine learning: opportunities and challenges,” in *Handbook of Big Data Privacy*, Springer, 2020, pp. 165-189.

[39] R. J. Boyle and R. R. Panko, Corporate computer security, Pearson Upper Saddle River, 2013.

[40] . M. H. Bhuyan, D. K. Bhattacharyya and J. K. Kalita, “Networks and Network Traffic Anomalies,” in *Network traffic anomaly detection and prevention: concepts, techniques, and tools*, Springer, 2017, pp. 27-32.

[41] A. S. Ashoor and S. Gore, “Difference between intrusion detection system (IDS) and intrusion prevention system (IPS),” in *International Conference on Network Security and Applications*, 2011.

[42] R. Boutaba, M. A. Salahuddin, N. Limam, S. Ayoubi, N. Shahriar, F. Estrada-Solano and O. M. Caicedo, “A comprehensive survey on machine learning for networking: evolution, applications and research opportunities,” *Journal of Internet Services and Applications*, vol. 9, no. 1, p. 16, 2018.

[43] S. Iqbal, M. L. M. Kiah, B. Dhaghighi, M. Hussain, S. Khan, M. K. Khan and K.-K. R. Choo, “On cloud security attacks: A taxonomy and intrusion detection and prevention as a service,” *Journal of Network and Computer Applications*, vol. 74, pp. 98-120, 2016.

[44] W. T. Yue and M. Cakanyildirim, “Intrusion prevention in information systems: Reactive and proactive responses,” *Journal of Management Information Systems*, vol. 24, no. 1, pp. 329-353, 2007.

[45] J. W. d. G. Stênico and L. L. Ling, “Network Traffic Monitoring,” in *The State of the Art in Intrusion Prevention and Detection*, Auerbach Publications, 2014, pp. 23-46.

[46] S. Bhatt, P. K. Manadhata and L. Zomlot, “The operational role of security information and event management systems,” *IEEE security & Privacy*, vol. 12, no. 5, pp. 35-41, 2014.

[47] O. Akinrolabu, I. Agrafiotis and A. Erola, “The challenge of detecting sophisticated attacks: Insights from SOC Analysts,” in *Proceedings of the 13th International Conference on Availability, Reliability and Security*, 2018.

[48] A. Milenkoski, M. Vieira, S. Kounev, A. Avritzer and B. D. Payne, “Evaluating computer intrusion detection systems: A survey of common practices,” *ACM Computing Surveys (CSUR)*, vol. 48, no. 1, pp. 1-41, 2015.

[49] Z. Jadidi, V. Muthukkumarasamy and E. Sithirasenan, “Artificial Intelligence-Based Intrusion Detection Techniques,” in *The State of the Art in Intrusion Prevention and Detection*, CRC Press, 2014, p. 285.

[50] C. Sekhar and K. V. Rao, “A Study: Machine Learning and Deep Learning Approaches for Intrusion Detection System,” in *International Conference on Computer Networks and Inventive Communication Technologies*, 2019.

[51] M. S. Husain, “Nature Inspired Approach for Intrusion Detection Systems,” *Design and Analysis of Security Protocol for Communication*, pp. 171-182, 2020.

[52] H. Jin, G. Xiang, F. Zhao, D. Zou, M. Li and L. Shi, “VMFence: A customized intrusion prevention system in distributed virtual computing environment,” in *3rd*

International Conference on Ubiquitous Information Management and Communication (ICUIMC'09), 2009.

[53] C. Modi and D. Patel, "A novel hybrid-network intrusion detection system (H-NIDS) in cloud computing," in *IEEE Symposium on Computational Intelligence in Cyber Security*, 2013.

[54] N. A. Azeez, T. M. Bada, S. Misra, A. Adewumi, C. V. d. Vyver and R. Ahuja, "Intrusion Detection and Prevention Systems: An Updated Review," in *Data Management, Analytics and Innovation*, Springer, 2020, pp. 685-696.

[55] CyberEdge Group, "2020 Cyberthreat Defence Report," CyberEdge Group, 2020.

[56] C. M. &. S. -. U. Department for Digital, "Cyber Security Breaches Survey 2020," *Computer Fraud & Security,* vol. 2020, no. 1361-3723, p. 4, 2020.

[57] C. M. &. S. Department for Digital, "Official Statistics Cyber Security Breaches Survey 2020," Department for Digital, Culture, Media & Sport, 26 March 2020. [Online]. Available: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2020/cyber-security-breaches-survey-2020#fn:1. [Accessed 10 February 2021].

[58] Sri Lanka Computer Emergency Readiness Team, "Sri Lanka Computer Emergency Readiness Team Annual Activity Report 2019," Sri Lanka Computer Emergency Readiness Team, 2019. [Online]. Available: https://www.cert.gov.lk/Downloads/General/Sri_Lanka_CERT_Annual_Activity_Report_2019.pdf. [Accessed 10 February 2021].

[59] A. H. Sung and S. Mukkamala, "Identifying important features for intrusion detection using support vector machines and neural networks," in *2003 Symposium on Applications and the Internet*, 2003.

[60] W. Lee and S. J. Stolfo, "A framework for constructing features and models for intrusion detection systems," *ACM transactions on Information and system security (TiSSEC),* vol. 3, no. 4, pp. 227-261, 2000.

[61] R. Sommer and V. Paxson, "Outside the closed world: On using machine learning for network intrusion detection," in *2010 IEEE symposium on security and privacy*, 2010.

[62] Z. Ahmad, A. S. Khan, C. Wai Shaiang, J. Abdullah and F. Ahmad, "Network intrusion detection system: A systematic study of machine learning and deep learning approaches," *Transactions on Emerging Telecommunications Technologies,* vol. 32, no. 1, p. 4150, 2020.

[63] Y. Meng, Y. Xiang and L.-F. Kwok, "Applications of Machine Learning in Intrusion Detection," in *The state of the art in intrusion prevention and detection*, CRC Press, 2014, pp. 311-332.

[64] H. Liu and B. Lang, “Machine learning and deep learning methods for intrusion detection systems: A survey,” *applied sciences*, vol. 9, no. 20, 2019.

[65] The Zeek Project, “Zeek Documentation current (v3.2.3),” The Zeek Project, 2019. [Online]. Available: https://docs.zeek.org/en/current/. [Accessed 11 February 2021].

[66] S. M. Sohi, J.-P. Seifert and F. Ganji, “RNNIDS: Enhancing network intrusion detection systems through deep learning,” *Computers & Security*, vol. 102, 2021.

[67] J. Grashöfer, C. Titze and H. Hartenstein, “Attacks on Dynamic Protocol Detection of Open Source Network Security Monitoring Tools,” in *2020 IEEE Conference on Communications and Network Security (CNS)*, 2020.

[68] C. V. Martinez, M. Sollfrank and B. Vogel-Heuser, “A Multi-Agent Approach for Hybrid Intrusion Detection in Industrial Networks: Design and Implementation,” in *2019 IEEE 17th International Conference on Industrial Informatics (INDIN)*, 2019.

[69] L. Diederichsen, K.-K. R. Choo and N.-A. Le-Khac, “A graph database-based approach to analyze network log files,” in *International Conference on Network and System Security*, 2019.

[70] N. Moustafa and J. Slay, “UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set),” in *2015 military communications and information systems conference (MilCIS)*, 2015.

[71] C.-T. Yang, W.-J. Jiang, E. Kristiani, Y.-W. Chan and J.-C. Liu, “The Implementation of a Network Log System Using RNN on Cyberattack Detection with Data Visualization,” in *International Conference on Frontier Computing*, 2019.

[72] C.-K. Tsung, C.-T. Yang and S.-W. Yang, “Visualizing potential transportation demand from ETC log analysis using ELK stack,” *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 6623-6633, 2020.

[73] E. B.V, “Filebeat overview,” Elasticsearch B.V, [Online]. Available: https://www.elastic.co/guide/en/beats/filebeat/current/filebeat-overview.html. [Accessed 18 03 2021].

[74] P. Sharma, K. Chaudhary, M. Wagner and M. G. M. Khan, “A comparative analysis of Malware anomaly detection,” in *Advances in Computer, Communication and Computational Sciences*, Springer, 2021, pp. 35-44.

[75] P. Gogoi, M. H. Bhuyan, D. Bhattacharyya and J. K. Kalita, “Packet and flow based network intrusion dataset,” in *International Conference on Contemporary Computing*, 2012.

[76] M. Ring, S. Wunderlich, D. Scheuring, D. Landes and A. Hotho, “A survey of network-based intrusion detection data sets,” *Computers & Security*, vol. 86, pp. 147-167, 2019.

[77] N. Moustafa and J. Slay, “The evaluation of Network Anomaly Detection Systems: Statistical analysis of the UNSW-NB15 data set and the comparison with the KDD99 data set,” *Information Security Journal: A Global Perspective,* vol. 25, pp. 18-31, 2016.

[78] N. Moustafa and J. Slay, “The significant features of the UNSW-NB15 and the KDD99 data sets for network intrusion detection systems,” in *2015 4th international workshop on building analysis datasets and gathering experience returns for security (BADGERS)*, 2015.

[79] Verizon Communications Inc., “Verizon: 2019 Data Breach Investigations Report,” *Computer Fraud & Security,* 2019.

[80] J. Fruhlinger, “Top cybersecurity facts, figures and statistics,” CSO, 9 March 2020. [Online]. Available: https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html. [Accessed 22 May 2021].

[81] Cisco, “Cisco Annual Internet Report (2018–2023) White Paper,” Cisco, 9 March 2020. [Online]. Available: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html. [Accessed 22 May 2021].

[82] J. R. Vacca, “Chapter 6 - Intrusion Detection in Contemporary Environments,” in *Computer and Information Security Handbook (Third Edition)},,* Morgan Kaufmann, 2017, pp. 109-130.

[83] R. J. Bates, “Chapter 1 - Introduction,” in *Securing VoIP*, Syngress, 2015, pp. 1-34.

[84] M. Hao, “Analysis of the 2020 H1 Malware Trend,” NSFOCUS Technologies Group Co Ltd, 25 September 2020. [Online]. Available: https://nsfocusglobal.com/analysis-of-the-2020-h1-malware-trend/. [Accessed 22 May 2021].

[85] V. Benson and J. Mcalaney, “Chapter 4 - The social and psychological impact of cyberattacks,” in *Emerging Cyber Threats and Cognitive Vulnerabilities*, Academic Press, 2020, pp. 73-92.

[86] R. Patgiri, H. Katari, R. Kumar and D. Sharma, “Empirical study on malicious URL detection using machine learning,” in *International Conference on Distributed Computing and Internet Technology*, 2019.