BIBLIOGRAPHY

[1] U. Ahmed, J. C.-W. Lin, and G. Srivastava. Mitigating adversarial evasion attacks of ransomware using ensemble learning. *Computers and Electrical Engineering*, 100: 107903, 2022.

[2] B. A. S. Al-Rimy, M. A. Maarof, and S. Z. M. Shaid. Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions. *Computers & Security*, 74:144–166, 2018.

[3] A. O. Almashhadani, M. Kaiiali, S. Sezer, and P. O'Kane. A multi-classifier network-based crypto ransomware detection system: A case study of locky ransomware. *IEEE access*, 7:47053–47067, 2019.

[4] A. O. Almashhadani, D. Carlin, M. Kaiiali, and S. Sezer. Mfmcns: A multi-feature and multi-classifier network-based system for ransomworm detection. *Computers & Security*, 121:102860, 2022.

[5] A. Arabo, R. Dijoux, T. Poulain, and G. Chevalier. Detecting ransomware using process behavior analysis. *Procedia Computer Science*, 168:289–296, 2020.

[6] A. Arfiani and Z. Rustam. Ovarian cancer data classification using bagging and random forest. In *AIP Conference Proceedings*, volume 2168. AIP Publishing, 2019.

[7] S. I. Bae, G. B. Lee, and E. G. Im. Ransomware detection using machine learning algorithms. *Concurrency and Computation: Practice and Experience*, 32(18):e5422, 2020.

[8] K. Cabaj, M. Gregorczyk, and W. Mazurczyk. Software-defined networking-based crypto ransomware detection using http traffic characteristics. *Computers & Electrical Engineering*, 66:353–368, 2018.

[9] Y. Chai, L. Du, J. Qiu, L. Yin, and Z. Tian. Dynamic prototype network based on sample adaptation for few-shot malware detection. *IEEE Transactions on Knowledge and Data Engineering*, 35(5):4754–4766, 2022.

[10] S. Dai, K. Li, Z. Luo, P. Zhao, B. Hong, A. Zhu, and J. Liu. Ai-based nlp section discusses the application and effect of bag-of-words models and tf-idf in nlp tasks. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, 5(1):13–21, 2024.

[11] A. DIB and G. Dabri. Ransomware/benignware system calls, 2022. URL `https://doi.org/10.17632/kbt8xt3678.1`.

[12] A. Dib and G. Dabri. Ransomware/benignware system calls, 2022.

[13] E. Eliando and Y. Purnomo. Lockbit 2.0 ransomware: Analysis of infection, persistence, prevention mechanism. *CogITo Smart Journal*, 8(1):232–243, 2022.

[14] M. García, S. Maldonado, and C. Vairetti. Efficient n-gram construction for text categorization using feature selection techniques. *Intelligent Data Analysis*, 25(3): 509–525, 2021.

[15] B. Gaye, D. Zhang, and A. Wulamu. Improvement of support vector machine algorithm in big data background. *Mathematical Problems in Engineering*, 2021(1): 5594899, 2021.

[16] J. Hwang, J. Kim, S. Lee, and K. Kim. Two-stage ransomware detection using dynamic analysis and machine learning techniques. *Wireless Personal Communications*, 112 (4):2597–2609, 2020.

[17] M. İbrahim, B. Issa, and M. B. Jasser. A method for automatic android malware detection based on static analysis and deep learning. *IEEE Access*, 10:117334–117352, 2022.

[18] M. Ijaz, M. H. Durad, and M. Ismail. Static and dynamic malware analysis using machine learning. In *2019 16th International bhurban conference on applied sciences and technology (IBCAST)*, pages 687–691. IEEE, 2019.

[19] W. A. Iwan, V. Suryani, and F. A. Yulianto. Video injection attack detection on cctv using ensemble learning with random forest classification. In *2023 11th International Conference on Information and Communication Technology (ICoICT)*, pages 23–27. IEEE, 2023.

[20] A. Kamboj, P. Kumar, A. K. Bairwa, and S. Joshi. Detection of malware in downloaded files using various machine learning models. *Egyptian Informatics Journal*, 24 (1):81–94, 2023.

[21] D. Kim and J. Lee. Blacklist vs. whitelist-based ransomware solutions. *IEEE Consumer Electronics Magazine*, 9(3):22–28, 2020.

[22] C. B. Liu, B. P. Chamberlain, D. A. Little, and Â. Cardoso. Generalising random forest parameter optimisation to include stability and cost. In *Machine Learning and Knowledge Discovery in Databases: European Conference, ECML PKDD 2017, Skopje, Macedonia, September 18–22, 2017, Proceedings, Part III 10*, pages 102–113. Springer, 2017.

[23] A. Luque, A. Carrasco, A. Martín, and A. de Las Heras. The impact of class imbalance in classification performance metrics based on the binary confusion matrix. *Pattern Recognition*, 91:216–231, 2019.

[24] R. Meenal, P. A. Michael, D. Pamela, and E. Rajasekaran. Weather prediction using random forest machine learning model. *Indonesian Journal of Electrical Engineering and Computer Science*, 22(2):1208–1215, 2021.

[25] Microsoft. What is threat detection and response (tdr)?, 2024. URL `https://www.microsoft.com/id-id/security/business/security-101/what-is-threat-detection-response-tdr`. Accessed: 2025-02-24.

[26] H. Oz, A. Aris, A. Levi, and A. S. Uluagac. A survey on ransomware: Evolution, taxonomy, and defense solutions. *ACM Computing Surveys (CSUR)*, 54(11s):1–37, 2022.

[27] G. Palaniappan, S. Sangeetha, B. Rajendran, S. Goyal, B. Bindhumadhava, et al. Malicious domain detection using machine learning on domain name features, host-based features and web-based features. *Procedia Computer Science*, 171:654–661, 2020.

[28] D. A. Pisner and D. M. Schnyer. Support vector machine. In *Machine learning*, pages 101–121. Elsevier, 2020.

[29] N. Rani, S. V. Dhavale, A. Singh, and A. Mehra. A survey on machine learning-based ransomware detection. In *Proceedings of the Seventh International Conference on Mathematics and Computing: ICMC 2021*, pages 171–186. Springer, 2022.

[30] M. Rhode, P. Burnap, and K. Jones. Early-stage malware prediction using recurrent neural networks. *computers & security*, 77:578–594, 2018.

[31] J. Ribeiro, F. B. Saghezchi, G. Mantas, J. Rodriguez, and R. A. Abd-Alhameed. Hidroid: prototyping a behavioral host-based intrusion detection and prevention system for android. *IEEE Access*, 8:23154–23168, 2020.

[32] A. Roy and S. Chakraborty. Support vector machine in structural reliability analysis: A review. *Reliability Engineering & System Safety*, 233:109126, 2023.

[33] S. Sharmeen, Y. A. Ahmed, S. Huda, B. Ş. Koçer, and M. M. Hassan. Avoiding future digital extortion through robust protection against ransomware threats using deep learning based adaptive approaches. *IEEE Access*, 8:24522–24534, 2020.

[34] P. Shijo and A. Salim. Integrated static and dynamic analysis for malware detection. *Procedia Computer Science*, 46:804–811, 2015.

[35] G. Sidorov, F. Velasquez, E. Stamatatos, A. Gelbukh, and L. Chanona-Hernández. Syntactic n-grams as machine learning features for natural language processing. *Expert Systems with Applications*, 41(3):853–860, 2014.

[36] S. Suthaharan and S. Suthaharan. Support vector machine. *Machine learning models and algorithms for big data classification: thinking with examples for effective learning*, pages 207–235, 2016.

[37] A. Vehabovic, N. Ghani, E. Bou-Harb, J. Crichigno, and A. Yayimli. Ransomware detection and classification strategies. In *2022 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom)*, pages 316–324. IEEE, 2022.

[38] H. Zhou. Research of text classification based on tf-idf and cnn-lstm. In *Journal of Physics: Conference Series*, volume 2171, page 012021. IOP Publishing, 2022.