

classifiers for identification. These samples show the ground truth of the models for comparisons. RF classifier tool shows the highest classification rate in both cases with an average classification rate 96.24%.

References

- [1] Alabadi, Montdher, and Yuksel Celik. "Anomaly Detection for Cyber-Security Based on Convolution Neural Network: A survey." In 2020 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), pp. 1-14. IEEE, 2020.
- [2] Bao, Haiyong, et al. "BLITHE: Behavior rule-based insider threat detection for smart grid." IEEE Internet of Things Journal 3.2 (2015): 190-205.
- [3] Bensaoud, Ahmed, Nawaf Abudawood, and Jugal Kalita. "Classifying Malware Images with Convolutional Neural Network Models." arXiv preprint arXiv:2010.16108 (2020).
- [4] Bujorianu, Manuela L. "CPS Dependability Framework Based on Inhomogeneous Stochastic Hybrid Systems." In Cyber Physical Systems. Model-Based Design, pp. 134-153. Springer, Cham, 2018.
- [5] Drayer, Elisabeth, and Tirza Routtenberg. "Cyber Attack Localization in Smart Grids by Graph Modulation (Brief Announcement)." In International Symposium on Cyber Security Cryptography and Machine Learning, pp. 97-100. Springer, Cham, 2019.
- [6] Drayer, Elisabeth, and Tirza Routtenberg. "Intrusion detection in smart grid measurement infrastructures based on principal component analysis." In 2019 IEEE Milan PowerTech, pp. 1-6. IEEE, 2019.
- [7] Gupta, Maanak, Sudip Mittal, and Mahmoud Abdelsalam. "AI assisted Malware Analysis: A Course for Next Generation Cybersecurity Workforce." arXiv preprint arXiv:2009.11101 (2020).
- [8] Jha, Sudan, Deepak Prashar, Hoang Viet Long, and David Taniar. "Recurrent neural network for detecting malware." Computers & Security 99 (2020): 102037.
- [9] Kumar, Nitesh, Subhasis Mukhopadhyay, Mugdha Gupta, Anand Handa, and Sandeep K. Shukla. "Malware Classification using Early Stage Behavioral Analysis." In 2019 14th Asia Joint Conference on Information Security (AsiaJCSIS), pp. 16-23. IEEE, 2019.
- [10] Kumar, Amit, Nitesh Kumar, Anand Handa, and Sandeep Kumar Shukla. "PeerClear: Peer-to-Peer Bot-net Detection." In International Symposium on Cyber Security Cryptography and Machine Learning, pp. 279-295. Springer, Cham, 2019.
- [11] Li, Xiang, Kefan Qiu, Cheng Qian, and Gang Zhao. "An Adversarial Machine Learning Method Based on OpCode N-grams Feature in Malware Detection." In 2020 IEEE Fifth International Conference on Data Science in Cyberspace (DSC), pp. 380-387. IEEE, 2020.
- [12] Mills, Alan, and Phil Legg. "Investigating anti-evasion malware triggers using automated sandbox reconfiguration techniques." Journal of Cybersecurity and Privacy 1, no. 1 (2020): 19-39.
- [13] Mirsky, Reuth, Ahmad Majadly, Kobi Gal, Rami Puzis, and Ariel Felner. "New Goal Recognition Algorithms Using Attack Graphs." In International Symposium on Cyber Security Cryptography and Machine Learning, pp. 260-278. Springer, Cham, 2019.
- [14] Pieper, Tobias. "Distributed co-simulation framework for hardware-and software-in-the-loop testing of networked embedded real-time systems." (2020).
- [15] Roy, Sohini, and Arunabha Sen. "Identification of the K-most Vulnerable Entities in a Smart Grid System." In 2020 3rd International Conference on Advanced Communication Technologies and Networking (CommNet), pp. 1-6. IEEE, 2020.
- [16] Singh, Ajay, Anand Handa, Nitesh Kumar, and Sandeep Kumar Shukla. "Malware classification using image representation." In International Symposium on Cyber Security Cryptography and Machine Learning, pp. 75-92. Springer, Cham, 2019.
- [17] Sebastián, Silvia, and Juan Caballero. "AVclass2: Massive Malware Tag Extraction from AV Labels." Annual Computer Security Applications Conference. 2020.
- [18] Schauer, Stefan, Stefan Rass, Sandra König, Klaus Steinnocher, Thomas Schaberreiter, and Gerald Quirchmayr. "Cross-Domain Risk Analysis to Strengthen City Resilience: the ODYSSEUS Approach.
- [19] Singh, Ajay, Anand Handa, Nitesh Kumar, and Sandeep Kumar Shukla. "Malware classification using image representation." In International Symposium on Cyber Security Cryptography and Machine Learning, pp. 75-92. Springer, Cham, 2019.
- [20] Wang, Wenbo, Yurong Song, Yinwei Li, and Yaqiong Jia. "Research on Cascading Failures Model of Power Grid Based on Complex Network." In 2020 Chinese Control And Decision Conference (CCDC), pp. 1367-1372. IEEE, 2020.
- [21] Wang, X., & Miikkulainen, R. (2020). MDEA: Malware Detection with Evolutionary Adversarial Learning. arXiv preprint arXiv:2002.03331.
- [22] Yang, Li, and Junlin Liu. "TuningMalconv: Malware Detection With Not Just ." IEEE Access 8 (2020): 140915-140922.
- [23] Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on cyber security for smart grid communications," IEEE Communications Surveys and tutorials, vol. 14, no. 4, pp. 998-1010, 2012.

Authors Profile



I "Manish Kumar Rai" am pursuing doctorate degree from Rashtriya Raksha University (A Institute of National Importance) under the department of Research and Publication in Cyber Security. I have completed my Post Graduation from Central University of South Bihar in Computer Science. I am currently holding the position of Junior Research fellow. My key research area is industrial security and SCADA security. I have qualified GATE, NET and JRF in computer Science of Engineering.