

## REFERENCES

- [1] L. Girish and S. K. Rao, “Anomaly detection in cloud environment using artificial intelligence techniques,” *Computing*, vol. 105, no. 3, pp. 675–688, 2023.
- [2] Z. He, P. Chen, X. Li, Y. Wang, G. Yu, C. Chen, X. Li, and Z. Zheng, “A spatiotemporal deep learning approach for unsupervised anomaly detection in cloud systems,” *IEEE Transactions on Neural Networks and Learning Systems*, vol. 34, no. 4, pp. 1705–1719, 2020.
- [3] T. Hagemann and K. Katsarou, “A systematic review on anomaly detection for cloud computing environments,” in *Proceedings of the 2020 3rd Artificial Intelligence and Cloud Computing Conference*, 2020, pp. 83–96.
- [4] S. K. Moghaddam, R. Buyya, and K. Ramamohanarao, “Performance-aware management of cloud resources: A taxonomy and future directions,” *ACM Computing Surveys (CSUR)*, vol. 52, no. 4, pp. 1–37, 2019.
- [5] C. Sauvanaud, M. Kaâniche, K. Kanoun, K. Lazri, and G. D. S. Silvestre, “Anomaly detection and diagnosis for cloud services: Practical experiments and lessons learned,” *Journal of Systems and Software*, vol. 139, pp. 84–106, 2018.
- [6] C.-W. Tien, T.-Y. Huang, C.-W. Tien, T.-C. Huang, and S.-Y. Kuo, “Kubanomaly: anomaly detection for the docker orchestration platform with neural network approaches,” *Engineering reports*, vol. 1, no. 5, p. e12080, 2019.
- [7] M. Cavalcanti, P. Inacio, and M. Freire, “Performance evaluation of container-level anomaly-based intrusion detection systems for multi-tenant applications using machine learning algorithms,” in *Proceedings of the 16th International Conference on Availability, Reliability and Security*, ser. ARES '21. New York, NY, USA: Association for Computing Machinery, 2021. [Online]. Available: <https://doi.org/10.1145/3465481.3470066>

- [8] S. Naseer, Y. Saleem, S. Khalid, M. K. Bashir, J. Han, M. M. Iqbal, and K. Han, "Enhanced network anomaly detection based on deep neural networks," *IEEE access*, vol. 6, pp. 48 231–48 246, 2018.
- [9] S.-J. Han and S.-B. Cho, "Evolutionary neural networks for anomaly detection based on the behavior of a program," *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, vol. 36, no. 3, pp. 559–570, 2006.
- [10] R. Chalapathy, A. K. Menon, and S. Chawla, "Anomaly detection using one-class neural networks," *arXiv preprint arXiv:1802.06360*, 2018.
- [11] M. S. alDosari, "Unsupervised anomaly detection in sequences using long short term memory recurrent neural networks," Ph.D. dissertation, 2016.
- [12] H. Gantikow, T. Zöhner, and C. Reich, "Container anomaly detection using neural networks analyzing system calls," in *2020 28th Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP)*. IEEE, 2020, pp. 408–412.
- [13] Y. Lin, O. Tunde-Onadele, and X. Gu, "Cdl: Classified distributed learning for detecting security attacks in containerized applications," in *Proceedings of the 36th Annual Computer Security Applications Conference*, 2020, pp. 179–188.
- [14] M. S. Islam, W. Pourmajidi, L. Zhang, J. Steinbacher, T. Erwin, and A. Miransky, "Anomaly detection in a large-scale cloud platform," in *2021 IEEE/ACM 43rd International Conference on Software Engineering: Software Engineering in Practice (ICSE-SEIP)*. IEEE, 2021, pp. 150–159.
- [15] C. Cao, A. Blaise, S. Verwer, and F. Rebecchi, "Learning state machines to monitor and detect anomalies on a kubernetes cluster," in *Proceedings of the 17th International Conference on Availability, Reliability and Security*, 2022, pp. 1–9.
- [16] R. R. Karn, P. Kudva, H. Huang, S. Suneja, and I. M. Elfadel, "Cryptomining detection in container clouds using system calls and explainable machine learning," *IEEE transactions on parallel and distributed systems*, vol. 32, no. 3, pp. 674–691, 2020.

- [17] T. Wang, W. Zhang, C. Ye, J. Wei, H. Zhong, and T. Huang, "Fd4c: Automatic fault diagnosis framework for web applications in cloud computing," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 46, no. 1, pp. 61–75, 2015.
- [18] Q. Du, T. Xie, and Y. He, "Anomaly detection and diagnosis for container-based microservices with performance monitoring," in *Algorithms and Architectures for Parallel Processing: 18th International Conference, ICA3PP 2018, Guangzhou, China, November 15-17, 2018, Proceedings, Part IV 18*. Springer, 2018, pp. 560–572.
- [19] A. Samir and C. Pahl, "Detecting and localizing anomalies in container clusters using markov models," *Electronics*, vol. 9, no. 1, p. 64, 2020.
- [20] D. Rahmawati and R. Sarno, "Anomaly detection using control flow pattern and fuzzy regression in port container handling," *Journal of King Saud University-Computer and Information Sciences*, vol. 33, no. 1, pp. 11–20, 2021.
- [21] A. Samir and C. Pahl, "Autoscaling recovery actions for container-based clusters," *Concurrency and Computation: Practice and Experience*, vol. 33, no. 23, p. e5955, 2021.
- [22] A. Samir, N. El Ioini, I. Fronza, H. R. Barzegar, V. T. Le, and C. Pahl, "Anomaly detection and analysis for reliability management clustered container architectures," *International Journal on Advances in Systems and Measurements*, vol. 12, no. 3&4, pp. 247–264, 2020.
- [23] J. Shetty, B. S. Babu, and G. Shobha, "Proactive cloud service assurance framework for fault remediation in cloud environment." *International Journal of Electrical & Computer Engineering (2088-8708)*, vol. 10, no. 1, 2020.
- [24] I. Kotenko, I. Saenko, A. Chechulin, L. Vitkova, M. Kolomeec, I. Zelichenok, M. Melnik, D. Makrushin, and N. Petrevich, "Detection of anomalies and attacks in container systems: An integrated approach based on black and white lists," in

*Proceedings of the Sixth International Scientific Conference “Intelligent Information Technologies for Industry”(IITI’22)*. Springer, 2022, pp. 107–117.

- [25] O. Mart, C. Negru, F. Pop, and A. Castiglione, “Observability in kubernetes cluster: Automatic anomalies detection using prometheus,” in *2020 IEEE 22nd International Conference on High Performance Computing and Communications; IEEE 18th International Conference on Smart City; IEEE 6th International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*. IEEE, 2020, pp. 565–570.
- [26] Y. Wang, Q. Wang, X. Chen, D. Chen, X. Fang, M. Yin, and N. Zhang, “Containerguard: A real-time attack detection system in container-based big data platform,” *IEEE Transactions on Industrial Informatics*, vol. 18, no. 5, pp. 3327–3336, 2020.
- [27] A. S. Abed, M. Azab, C. Clancy, and M. S. Kashkoush, “Resilient intrusion detection system for cloud containers,” *International Journal of Communication Networks and Distributed Systems*, vol. 24, no. 1, pp. 1–22, 2020.