REFERENCES

[1] L. De Lauretis, “From Monolithic Architecture to Microservices Architecture,” *IEEE Xplore*, Oct. 01, 2019. https://ieeexplore.ieee.org/abstract/document/8990350.

[2] V. Velepucha and P. Flores, "A survey on microservices architecture: Principles patterns and migration challenges", *IEEE Access*, vol. 11, pp. 88339-88358, 2023.

[3] Baškarada, S., Nguyen, V., & Koronios, A. (2018). Architecting Microservices: Practical Opportunities and Challenges. *Journal of Computer Information Systems*, *60*(5), 428–436. https://doi.org/10.1080/08874417.2018.1520056

[4] P. Billawa, A. B. Tukaram, N. E. D. Ferreyra, J.-P. Steghöfer, R. Scandariato, and G. Simhandl, “SOK: Security of Microservice Applications: A Practitioners’ perspective on challenges and best practices,” *Proceedings of the 17th International Conference on Availability, Reliability and Security*, pp. 1–10, Aug. 2022, doi: 10.1145/3538969.3538986.

[5] U. Zdun *et al.*, “Microservice Security Metrics for secure communication, identity management, and observability,” *ACM Transactions on Software Engineering and Methodology*, vol. 32, no. 1, pp. 1–34, May 2022, doi: 10.1145/3532183.

[6] B. Soundararajan, “Secure configuration Management for microservices architecture,” *International Journal of Multidisciplinary Research and Growth Evaluation*, vol. 1, no. 1, pp. 110–114, Jan. 2020, doi: 10.54660/.ijmrge.2020.1.1.110-114.

[7] Cerny, T.; Svacina, J.; Das, D.; Bushong, V.; Bures, M.; Tisnovsky, P.; Frajtak, K.; Shin, D.; Huang, J. “On code analysis opportunities and challenges for enterprise systems and microservices,” *IEEE Journals & Magazine | IEEE Xplore*, 2020. https://ieeexplore.ieee.org/abstract/document/9179733

[8] L. P. Kaelbling, M. L. Littman, and A. W. Moore, “Reinforcement Learning: a survey,” *Journal of Artificial Intelligence Research*, vol. 4, pp. 237–285, May 1996, doi: 10.1613/jair.301.

[9] S. H. Oh, J. Kim, J. H. Nah, and J. Park, “Employing deep reinforcement learning to Cyber-Attack simulation for enhancing cybersecurity,” *Electronics*, vol. 13, no. 3, p. 555, Jan. 2024, doi: 10.3390/electronics13030555.

[10] A. Ganje, “Microservices in organizations,” *Journal of Software Engineering and Applications*, vol. 18, no. 02, pp. 76–86, Jan. 2025, doi: 10.4236/jsea.2025.182005.

[11] A. Katal, P. Prasanna, R. Birla, and N. Kunal, “Evolution from Monolithic to Microservices Architecture: A New Era in Software Architecture,” in *Springer tracts in nature-inspired computing*, 2025, pp. 235–279. doi: 10.1007/978-981-96-0706-8_12.

[12] O. Kumar and A. Narang, “Securing Microservices: Challenges and solutions,” Jan. 26, 2025. https://ijircstjournal.org/index.php/ijircst/article/view/50

[13] E. Safeer, “Reinforcement learning approaches in cyber security,” in *Advances in information security, privacy, and ethics book series*, 2024, pp. 53–76. doi: 10.4018/979-8-3693-5415-5.ch002.

[14] J. Schulman, F. Wolski, P. Dhariwal, A. Radford, and O. Klimov, “Proximal Policy optimization Algorithms,” *arXiv.org*, Jul. 20, 2017. https://arxiv.org/abs/1707.06347

[15] C. Henríquez, J. D. R. Valencia, and G. S. Torres, “Architectural Evolution at Netflix: A Case Study on Microservices and the Transformation from Monolithic to Scalable Systems.,” *ojs.uac.edu.co*, Mar. 2025, doi: 10.15665/rp.v23i1.3683.

[16] S. Bhatnagar and R. Mahant, “Overview of microservices,” in *Apress eBooks*, 2025, pp. 53–134. doi: 10.1007/979-8-8688-1267-5_2.

[17] A. Shukla, “Exploring the integration of APIs in microservices for scalable application development,” Jan. 18, 2025. https://jrtcse.com/index.php/home/article/view/JRTCSE.2025.13.1.4

[18] D. Ordonez-Camacho, “Reduciendo la brecha de seguridad del IoT con una arquitectura de microservicios basada en TLS y OAuth2,” *Ingenius*, no. 25, pp. 94–103, Dec. 2020, doi: 10.17163/ings.n25.2021.09.

[19] G. Somashekar and A. Gandhi, “Towards optimal configuration of microservices,” in Proceedings of the 1st Workshop on Machine Learning and Systems, 2021, pp. 7–14.

[20] “A Systematic literature review of Inter-Service security threats and mitigation strategies in microservice architectures,” *IEEE Journals & Magazine | IEEE Xplore*, 2024. https://ieeexplore.ieee.org/abstract/document/10540127

[21] J. Clifton and E. Laber, “Q-Learning: Theory and applications,” *Annual Review of Statistics and Its Application*, vol. 7, no. 1, pp. 279–301, Mar. 2020, doi: 10.1146/annurev-statistics-031219-041220.

[22] J. Fan, Z. Wang, Y. Xie, and Z. Yang, “A theoretical analysis of deep Q-Learning,” *PMLR*, Jul. 31, 2020. https://proceedings.mlr.press/v120/yang20a

[23] C. Wu, W. Bi, and H. Liu, “Proximal policy optimization algorithm for dynamic pricing with online reviews,” *Expert Systems With Applications*, vol. 213, p. 119191, Nov. 2022, doi: 10.1016/j.eswa.2022.119191.

[24] M. Lopez-Martin, B. Carro, and A. Sanchez-Esguevillas, “Application of deep reinforcement learning to intrusion detection for supervised problems,” *Expert Systems With Applications*, vol. 141, p. 112963, Sep. 2019, doi: 10.1016/j.eswa.2019.112963.

[25] J. Schwartz and H. Kurniawati, “Autonomous Penetration Testing using Reinforcement Learning,” *arXiv.org*, May 15, 2019. https://arxiv.org/abs/1905.05965

[26 T. Zhang, “Information Security Challenges in FinTech: Strategies for Protecting Digital Assets,” Sep. 23, 2024. https://www.pioneerpublisher.com/jpeps/article/view/1000

[27] R. Mazzolin, A. Madni, “A survey of contemporary cyber security vulnerabilities and potential approaches to automated defence,” *IEEE Conference Publication | IEEE Xplore*, Aug. 24, 2020. https://ieeexplore.ieee.org/abstract/document/9275828

[28] S. Chugh, “Bridging the gap: industry perspectives and trends in cloud security, and opportunities for collaborative research,” *IEEE Conference Publication | IEEE Xplore*, Nov. 01, 2023. https://ieeexplore.ieee.org/abstract/document/10431562

[29] J. Schulman, S. Levine, P. Abbeel, M. Jordan, and P. Moritz, “Trust Region Policy optimization,” *PMLR*, Jun. 01, 2015. https://proceedings.mlr.press/v37/schulman15.html

[30] F. Sangoleye, J. Johnson and E. Eleni Tsiropoulou, “Intrusion detection in industrial control systems based on deep reinforcement learning,” *IEEE Journals & Magazine | IEEE Xplore*, 2024. https://ieeexplore.ieee.org/abstract/document/10713374

[31] A. d. Rio, D. Jimenez and J. Serrano, “Comparative analysis of A3C and PPO algorithms in Reinforcement Learning: A survey on general environments,” *IEEE Journals & Magazine | IEEE Xplore*, 2024. https://ieeexplore.ieee.org/abstract/document/10703056

[32] S. De Paoli and J. Johnstone, “A qualitative study of penetration testers and what they can tell us about information security in organisations,” *Information Technology and People*, vol. 38, no. 1, pp. 380–398, Oct. 2023, doi: 10.1108/itp-11-2021-0864.

[33] “Manual and automated penetration testing. Benefits and drawbacks. Modern tendency,” *IEEE Conference Publication | IEEE Xplore*, Feb. 01, 2016. https://ieeexplore.ieee.org/abstract/document/7452095

[34] M. Sewak, “Actor-Critic models and the A3C,” in *Springer eBooks*, 2019, pp. 141–152. doi: 10.1007/978-981-13-8285-7_11.

[35] V. R. Konda, J. N. Tsitsiklis, Laboratory for Information and Decision Systems, and Massachusetts Institute of Technology, “Actor-Critic algorithms,” journal-article. [Online]. Available: https://proceedings.neurips.cc/paper_files/paper/1999/file/6449f44a102fde848669bdd9eb6b76fa-Paper.pdf

[36] K. Lange, D. R. Hunter, and I. Yang, “Optimization transfer using surrogate objective functions,” *Journal of Computational and Graphical Statistics*, vol. 9, no. 1, pp. 1–20, Mar. 2000, doi: 10.1080/10618600.2000.10474858.