

Data quality problem in AI-based network intrusion detection systems studies and a solution proposal

Halisdemir, Emre; Karacan, Hacer; **Pihelgas, Mauno**; Lepik, Toomas; Cho, Sungbaek 14th International Conference on Cyber Conflict : Keep Moving 2022 / p. 367-383 https://ccdcoe.org/uploads/2022/06/CyCon_2022_book.pdf

Evaluating the robustness of ML models to out-of-distribution data through similarity analysis

Lindén, Joakim; Forsberg, Håkan; **Daneshtalab, Masoud**; Söderquist, Ingemar New Trends in Database and Information Systems; ADBIS 2023 Short Papers, Doctoral Consortium and Workshops: AIDMA, DOING, K-Gals, MADEISD, PeRS, Barcelona, Spain, September 4–7, 2023, Proceedings 2023 / p. 348 - 359 https://doi.org/10.1007/978-3-031-42941-5_30