security of internet of things. *IEEE Internet Things J*, 10(24):21309-21321.
https://doi.org/10.1109/JIOT.2023.3283408

Lu HM, Wang T, Xu X, et al., 2021. Cognitive Memory-guided AutoEncoder for effective intrusion detection in internet of things. *IEEE Trans Ind Inform*, 18(5):3358-3366.
https://doi.org/10.1109/TII.2021.3102637

Makkar A, Garg S, Kumar N, et al., 2021. An efficient spam detection technique for IoT devices using machine learning. *IEEE Trans Ind Inform*, 17(2):903-912.
https://doi.org/10.1109/TII.2020.2968927

Mehedi ST, Anwar A, Rahman Z, et al., 2022. Dependable intrusion detection system for IoT: A deep transfer learning based approach. *IEEE Trans Ind Inform*, 19(1):1006-1017.
https://doi.org/10.1109/TII.2022.3164770

Neto ECP, Dadkhah S, Ferreira R, et al., 2023. CICIOT2023: a real-time dataset and benchmark for large-scale attacks in IoT environment. *Sensors*, 23(13):5941.
https://doi.org/10.3390/s23135941

Nichol A, Achiam J, Schulman J, 2018. On first-order meta-learning algorithms, .
https://arxiv.org/abs/1803.02999

Niu ZQ, Guo WJ, Xue JF, et al., 2023. A novel anomaly detection approach based on ensemble semi-supervised active learning (ADESSA). *Comput Secur*, 129:103190.
https://doi.org/10.1016/j.cose.2023.103190

Ouyang YK, Li BB, Kong QL, et al., 2021. FS-IDS: a novel few-shot learning based intrusion detection system for SCADA networks. ICC 2021-IEEE Int Conf on Communications, p.1-6.
https://doi.org/10.1109/ICC42927.2021.9500607

Schwartz E, Karlinsky L, Shtok J, et al., 2018. Δ-encoder: an effective sample synthesis method for few-shot object recognition. 32nd Conf on Neural Information Processing Systems, p.2850-2860.
https://doi.org/10.48550/arXiv.1806.04734

Shi ZX, Xing MY, Zhang J, et al., 2023. Few-shot network intrusion detection based on model-agnostic meta-learning with L2F method. IEEE Wireless Communications and Networking Conf, p.1-6.
https://doi.org/10.1109/WCNC55385.2023.10118898

Simon C, Koniusz P, Nock R, et al., 2020. Adaptive subspaces for few-shot learning. IEEE/CVF Conf on Computer Vision and Pattern Recognition, p.4135-4144.
https://doi.org/10.1109/CVPR42600.2020.00419

Snell J, Swersky K, Zemel R, 2017. Prototypical networks for few-shot learning. Proc 31st Int Conf on Neural Information Processing Systems, p.4080-4090.

Sun HD, Wan L, Liu MY, et al., 2023. Few-shot network intrusion detection based on prototypical capsule network with attention mechanism. *PloS One*, 18(4):e0284632.
https://doi.org/10.1371/journal.pone.0284632

Sung F, Yang YX, Zhang L, et al., 2017. Learning to compare: relation network for few-shot learning. IEEE/CVF Conf on Computer Vision and Pattern Recognition, p.1199-1208.
https://doi.org/10.1109/CVPR.2018.00131

Thakkar A, Lohiya R, 2023. Attack classification of imbalanced intrusion data for IoT network using ensemble learning-based deep neural network. *IEEE Internet Things J*, 10:11888-11895.
https://doi.org/10.1109/JIOT.2023.3244810

Vinyals O, Blundell C, Lillicrap T, et al., 2016. Matching networks for one shot learning. Proc 30th Int Conf on Neural Information Processing Systems, p.3637-3645.
https://doi.org/10.48550/arXiv.1606.04080

Wang QL, Wu BG, Zhu PF, et al., 2020. ECA-Net: efficient channel attention for deep convolutional neural networks. IEEE/CVF Conf on Computer Vision and Pattern Recognition, p.11531-11539.
https://doi.org/10.1109/CVPR42600.2020.01155

Wang YH, Zhang ZY, Zhao KJ, et al., 2024. A few-shot learning based method for industrial internet intrusion detection. *Int J Inf Secur*, 23(5):3241-3252.
https://doi.org/10.1007/s10207-024-00889-x

Wang YK, Xu CM, Liu C, et al., 2020. Instance credibility inference for few-shot learning. IEEE/CVF Conf on Computer Vision and Pattern Recognition, p.12836-12845.
https://doi.org/10.1109/CVPR42600.2020.01285

Wang YX, Girshick R, Hebert M, et al., 2018. Low-shot learning from imaginary data. IEEE/CVF Conf on Computer Vision and Pattern Recognition, p.7278-7286.
https://doi.org/10.1109/CVPR.2018.00760

Wang ZM, Tian JY, Qin J, et al., 2021. A few-shot learning-based siamese capsule network for intrusion detection with imbalanced training data. *Comput Intell Neurosci*, 2021(1):7126913.
https://doi.org/10.1155/2021/7126913

Xu CY, Shen JZ, Du X, 2020. A method of few-shot network intrusion detection based on meta-learning framework. *IEEE Trans Inform Forensics Secur*, 15:3540-3552.
https://doi.org/10.1109/TIFS.2020.2991876

Xu H, Wang YJ, 2022. A continual few-shot learning method via meta-learning for intrusion detection. IEEE 4th Int Conf on Civil Aviation Safety and Information Technology, p.1188-1194.
https://doi.org/10.1109/ICCASIT55263.2022.9986665

Yan Y, Yang Y, Gu YH, et al., 2023. A few-shot intrusion detection model for the internet of things. 3rd Int Conf on Electronic Information Engineering and Computer Science, p.531-537.
https://doi.org/10.1109/EIECS59936.2023.10435498

Yan Y, Yang Y, Shen F, et al., 2024. Meta learning-based few-shot intrusion detection for 5G-enabled industrial internet. *Complex Intell Syst*, 10(3):4589-4608.
https://doi.org/10.1007/s40747-024-01388-1