

Multimodal deep learning research on adversarial attack resilience and application in building real-time IoT camera intrusion detection systems

Ly Sac San

Abstract: The research focuses on enhancing the security of IoT camera systems against cyber threats and adversarial attacks. The project proposes a multimodal deep learning solution that combines network/log data analysis with video data for intrusion detection. The author studies and compares the performance of Transformer and State Space Model (Mamba) architectures on the standard CIC-IDS-2018 dataset. The system integrates the n8n platform for automated alerting, ensuring real-time response capability and model robustness against intentional data manipulation.

Keywords: Multimodal Deep Learning, Adversarial Attack, IoT Camera IDS

References

- [1] A. Vaswani et al., "Attention is all you need," Adv. Neural Inf. Process. Syst., vol. 30, 2017.
- [2] A. Gu and T. Dao, "Mamba: Linear-Time Sequence Modeling with Selective State Spaces," arXiv:2312.00752, 2023.
- [3] I. J. Goodfellow, J. Shlens, and C. Szegedy, "Explaining and Harnessing Adversarial Examples," in Proc. Int. Conf. Learn. Represent. (ICLR), 2015.
- [4] UNB, "CIC-IDS-2018 Dataset for Intrusion Detection," Canadian Institute for Cybersecurity, 2018.