Transferable Adversarial Attacks, Data Governance, and Flood Relocation Analytics

Abstract

Transferable adversarial attacks reveal the vulnerability of intelligent systems that rely on shared representation spaces and cross-domain model generalization. These risks are relevant not only to computer security but also to recommendation, biomedical analysis, and disaster-policy analytics. Privacy-aware data governance architectures can help coordinate system design, access control, data separation, and lifelong adaptation. Sequential recommendation research contributes methods for dynamic user modeling, while biomedical injury studies provide a high-stakes evidence environment requiring reliable interpretation. Flood relocation analytics adds a public-policy setting where household heterogeneity and risk perception must be modeled carefully. This literature cluster positions adversarial robustness and data governance as foundational requirements for intelligent systems that support decision-making across personal, medical, and disaster contexts.

Keywords

pre-disaster relocation; agent-based model; flood disaster; household behavior; disaster governance; relocation planning; climate adaptation

References

Xu, B., Dai, X., Tang, D., & Zhang, K. (2025, November). One surrogate to fool them all: Universal, transferable, and targeted adversarial attacks with clip. In Proceedings of the 2025 ACM SIGSAC Conference on Computer and Communications Security (pp. 3087-3101).
Yin, J., Zeng, Z., Li, M., Yan, H., Li, C., Han, W., ... & Wang, S. (2025, April). Unleash llms potential for sequential recommendation by coordinating dual dynamic index mechanism. In Proceedings of the ACM on Web Conference 2025 (pp. 216-227).
Tao, J., Lyu, R., & Cao, X. (2026). A Scalable Data Governance Architecture for Privacy-Aware Intelligent Learning Systems in Lifelong. Future-Adaptive Intelligence and Lifelong Systems, 1(1).
Zhang, Z., Duan, Y., Gu, F., Wei, J., Huo, H., Wang, Y., ... & Gao, Z. (2026). Circulating ATP from hepatic ischemia-reperfusion drives remote cardiac injury via macrophage inflammasome activation. Pharmacological Research, 108306.
Zhou, Y. (2022). Pre-disaster relocation and agent-based model for flood disaster [Doctoral dissertation, University of Wisconsin–Madison].
Radford, A., Kim, J. W., Hallacy, C., Ramesh, A., Goh, G., Agarwal, S., ... & Sutskever, I. (2021). Learning transferable visual models from natural language supervision. In International conference on machine learning (pp. 8748-8763). PMLR.
Goodfellow, I. J., Shlens, J., & Szegedy, C. (2015). Explaining and harnessing adversarial examples. In International Conference on Learning Representations.
Dwork, C. (2006). Differential privacy. In International Colloquium on Automata, Languages, and Programming (pp. 1-12). Springer.
Kairouz, P., McMahan, H. B., Avent, B., Bellet, A., Bennis, M., Bhagoji, A. N., ... & Zhao, S. (2021).

Advances and open problems in federated learning. Foundations and Trends® in Machine Learning, 14(1-2), 1-210.
Mach, K. J., Kraan, C. M., Hino, M., Siders, A. R., Johnston, E. M., & Field, C. B. (2019). Managed retreat through voluntary buyouts of flood-prone properties. Science Advances, 5(10), eaax8995.