Taxonomy and Review: Privacy GANs

Boudaoud Arbia
Ahmed Draia University, Adrar, Algeria

Kabou Salheddine
Higher Normal School - Bechar, Algeria

Abstract

Generative Adversarial Networks (GANs) have emerged as a double-edged sword in the context of data privacy. On one hand, they enable the generation of high-fidelity synthetic data that can reduce reliance on sensitive real-world datasets; on the other hand, they introduce new privacy risks through attacks such as membership inference and model inversion. This review presents a systematic taxonomy of GAN architectures developed for privacy-preserving data generation. We categorize models from foundational designs (e.g., Vanilla GAN) to conditional and domain-specific variants (e.g., CycleGAN, TimeGAN), and further to advanced frameworks explicitly incorporating privacy mechanisms (e.g., DPGAN, FedGAN). By mapping the evolution of these models, we aim to provide a comprehensive understanding of their design principles, privacy implications, and practical applications.

Keywords

Generative adversarial networks, privacy-preserving, Synthetic data.