Differentially Private Releasing via Deep Generative Model : Résumé

Alexandre Huat
INSA Rouen Normandie
Master Science des Données

15 février 2018

Supposons des un groupe de clients et un prestateur de services informatiques collectant et analysant leurs données (*e.g.* image, texte, audio). Afin de réaliser les tâches d'analyses, le prestateur est amené à traiter des données sensibles. Soucieux et/ou contraint de respecter la vie privée des clients, le prestateur doit trouver un moyen de traiter efficacement ces données tout en conservant leur confidentialité. Pour répondre à cette problématique, Zhang, Ji et Wang [1] ont proposé l'architecture profonde dp-GAN [1], que je résumerai ici. En particulier, dp-GAN offre (i) une garantie théorique à la préservation de la confidentialité des données via le principe de « confidentialité différentielle »,

dp-GAN est une architecture dont le rôle est de générer des données synthétiques mais sémantiquement riches qui pourront être utilisées sans violer la vie privée des utilisateurs, ou « clients » (*cf.* Figure 1).

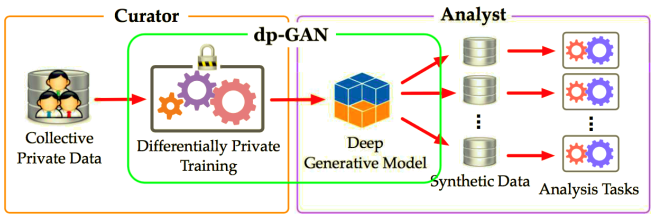

Figure 1. La place de dp-GAN dans la chaîne de traitement des données privées

Références

[1] X. Zhang, S. Ji et T. Wang, « Differentially Private Releasing via Deep Generative Model », *ArXiv e-prints*, jan. 2018. arXiv : 1801.01594 [cs.CR].

1. *Differentially Private Generative Adversarial Network*