

## Differentially Private Synthetic Time Series Data Generation with Generative Adversarial Networks (GANs)

Privacy has become a major concern in the past few years with the rise of machine learning and deep learning models being vulnerable to invasion attacks. The humongous amount of data being used to train these models is susceptible to leakage due to the model's capability of retaining training information. Attackers exploit these models by procuring training information that was private by model inversion techniques [1]. Therefore, much research effort was dedicated to exploring differential privacy (DP) [2] as a means of privacy preservation.

DP is a mathematically sound promise that ensures that the result of a differentially private analysis will essentially make the same inference about any individual's private information, independent of that individual's private information being included as an input to the analysis [3][4]. Federated learning[5], model agnostic private learning, and DP-Stochastic Gradient Descent (DP-SGD) [2] are some of the well-known methods to offer DP. In particular, DP-SGD is considered a promising line of work with many efforts in trying to generate synthetic data with attributes similar to the real data to be protected. Generative Adversarial Network (GAN) models are being extensively used to generate this DP synthetic data, giving rise to numerous types of GAN such as Differentially Private GAN (DPGAN) [6], Private Aggregate of Teacher Ensemble GAN (PATE-GAN) [7], Gradient Sanitized Wasserstein GAN (GS-WGAN)[8], and many more [9].

This project focuses on generating differentially private time series data by utilizing the capabilities of the GAN model to identify and address previously observed shortcomings [10]. To understand the features of each model, the tradeoff between data privacy and model utility is observed and plotted. With DP image generation garnering much of the attention concerning GANs, delving into DP time series data offers better insight into understanding the model's strengths and weaknesses. GAN variants are compared based on privacy and utility tradeoffs to observe the effects of different architectures. This project aims to use GAN model characteristics to produce differential private synthetic time series data and compare the performance of each model.

## References

1. Ghoshch, Ghadeer, Jin Li, and Tingting Zhu. "A review of Generative Adversarial Networks for Electronic Health Records: applications, evaluation measures and data sources." *arXiv preprint arXiv:2203.07018* (2022).
2. Abadi, Martin, Andy Chu, Ian Goodfellow, H. Brendan McMahan, Ilya Mironov, Kunal Talwar, and Li Zhang. "Deep learning with differential privacy." In Proceedings of the


- 2016 ACM SIGSAC conference on computer and communications security, pp. 308-318. 2016.
3. Dwork, Cynthia. "Differential privacy: A survey of results." In International conference on theory and applications of models of computation, pp. 1-19. Springer, Berlin, Heidelberg, 2008.
  4. Dwork, Cynthia, and Aaron Roth. "The algorithmic foundations of differential privacy." Foundations and Trends® in Theoretical Computer Science 9, no. 3-4 (2014): 211-407.
  5. Xin, Bangzhou, Yangyang Geng, Teng Hu, Sheng Chen, Wei Yang, Shaowei Wang, and Liusheng Huang. "Federated synthetic data generation with differential privacy." Neurocomputing 468 (2022): 1-10.
  6. Xie, Liyang, Kaixiang Lin, Shu Wang, Fei Wang, and Jiayu Zhou. "Differentially private generative adversarial network." arXiv preprint arXiv:1802.06739 (2018).
  7. Jordon, James, Jinsung Yoon, and Mihaela Van Der Schaar. "PATE-GAN: Generating synthetic data with differential privacy guarantees." In International conference on learning representations. 2018.
  8. Chen, Dingfan, Tribhuvanesh Orekondy, and Mario Fritz. "Gs-wgan: A gradient-sanitized approach for learning differentially private generators." Advances in Neural Information Processing Systems 33 (2020): 12673-12684.
  9. Fan, Liyue. "A survey of differentially private generative adversarial networks." In The AAAI Workshop on Privacy-Preserving Artificial Intelligence, p. 8. 2020.
  10. te Marvelde, Pepijn. "Differentially Private GAN for Time Series." (2021).
  11. Lin, Zinan, Vyas Sekar, and Giulia Fanti. "On the privacy properties of gan-generated samples." In International Conference on Artificial Intelligence and Statistics, pp. 1522-1530. PMLR, 2021.

### Team Members

- |                               |        |
|-------------------------------|--------|
| 1. KUMARESH S                 | 19Z327 |
| 2. METHUKULA S AJITH NARAYANA | 19Z331 |
| 3. MRIDULA M                  | 19Z332 |
| 4. SRAVYA VANKADARA           | 19Z348 |
| 5. CHANDRA PRAKASH J          | 20Z461 |

### Team Mentor

Dr. K. SATHIYAPRIYA



Signature

(Dr. K. Sathiyapriya)