Project proposal for big data privacy

1. **Name of the project**

Adding privacy to Generative Adversarial Networks(GAN)

1. **Team members and division for work**

Haihan Gao, student ID:, majoring in, from;

Li Zhang, student ID:SA22221064, majoring in Cyberspace Security, from USTC;

Xiaolu Chen,student ID: SA22221005, majoring in Cyberspace Security, from School of Cyber Science and Technology.

All members in the team are discussing and working for the scheme of this project together, as well as writing related documents.

1. **Purpose and significance of the research**

Generative Adversarial Network(GAN) is a generative model that has been used to generate fake data from the distribution of real data, so that it can be used as a tool to protect privacy. Yet owed to its principle, there is still some further work ought to be done to enhance its generation ability.

* 1. **Significance of research**

As a generative model, GAN can produce new data without exposing the original figure to data users, so that massive individual information sensitively related to people privacy can be converted to data fakes remaining the feature and then fully used in numerous fields like governmental, medical and so on.

As a result, using GAN in privacy protection has become one of the current focus. The research on GAN for privacy security can offer more efficient guarantee for data providers and expanding the development of privacy security. Also, it supplies a strong support for data analysis.

* 1. **Problem definition**

GAN is quite widely used as a kind of privacy-preserving techniques to generate fake data which is highly similar to the original data , so that the generated one can replace the real in practice. Despite its success, it is still limited in maintaining the same quality of generated data when protecting the original privacy for their sharing highly resemble feature distribution. The problem about GAN applied in privacy-preserving is to improve GAN to generate data with both a higher availability and better secret feature.

* 1. **Background**

Due to evolution of science, with the arrival of age of big data, massive data is created and contributes to numerous techniques.

GAN is a a generative model. The principle of its work is to map real data(such as images and texts)into latent variables which represent the information or cluster characteristic in latent space and then to create new data with these variables and target distribution. Because of the process, new data retrains features from the original one, which may result in leakage of training data, as well as contains difference.

DP

* 1. **Related work**

**DP-SGD**. Training GANs with the DP-SGD method can be effective in generating high-dimensional sanitized data. However, DP-SGD relies on the clipping bound of gradient norm, i.e., the sensitivity value. Sensitivity values vary greatly with model architecture and training dynamics, which makes the implementation of DP-SGD difficult.

**PATE**. Privatization of Teacher Aggregates (PATE) has recently been adapted to generative models. and two main approaches were studied: PATE-GAN and G-PATE. Both of these methods only train generators with DP guarantees, however, the gradients of G-PATE need to be manually selected to adapt to the PATE framework and secondly the high-dimensional nature of the PATE framework brings high privacy costs.

**Fed-Avg GAN**. Fed-Avg GAN is a solution to the decentralized case by using the DP-Fed-Avg algorithm to adapt GAN training to provide user-level DP guarantees under a trusted server. And it merely works on decentralized data.

* 1. **Preliminary scheme**

We use a new gradient-sanitized Wasserstein GAN (GS-WGAN), which is capable of generating high-dimensional data with DP guarantees, in both centralized and decentralized datasets. In the decentralized case, user-level DP security is guaranteed under an untrusted server. And we evaluate our method on various datasets against other state-of-the-art approaches.

1. **Prepared work**

At present, all members in the team have :

1. Mastered the programming language Python;
2. Reading related papers and had sufficient knowledge about the research.