Privacy in GNNs

Abhigyan Martin Ninama 19110071
Ninad Shah 19110126

What is Privacy in GNNs?

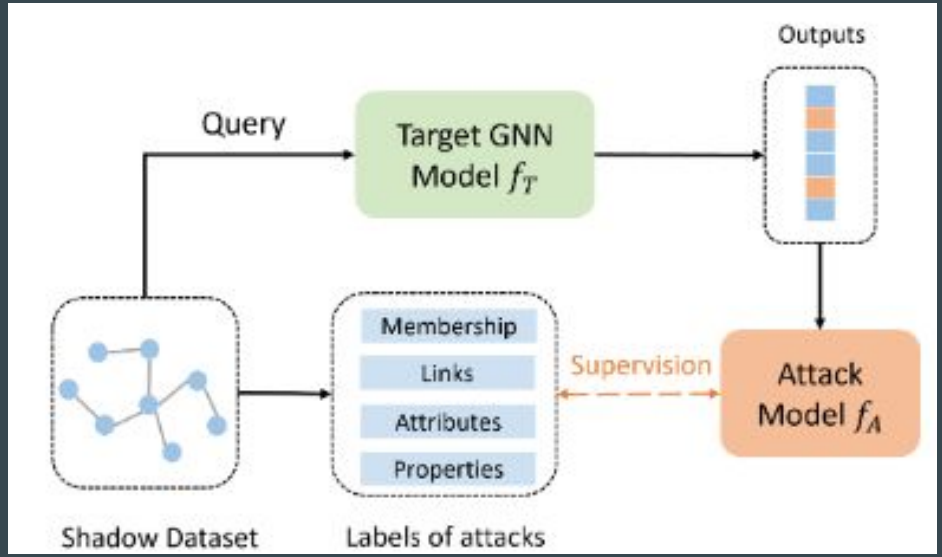
- Data Isolation
- Sensitive Information on human related variables
- Personal information

Types of Privacy Attacks

- Membership Inference Attack
- Reconstruction Attacks
- Property Inference Attack
- Model Extraction Attack

Framework for attacks

- Create Shadow dataset of samples with high confidence scores.
- Train new ensembles of model from shadow dataset which mimics appropriate task.



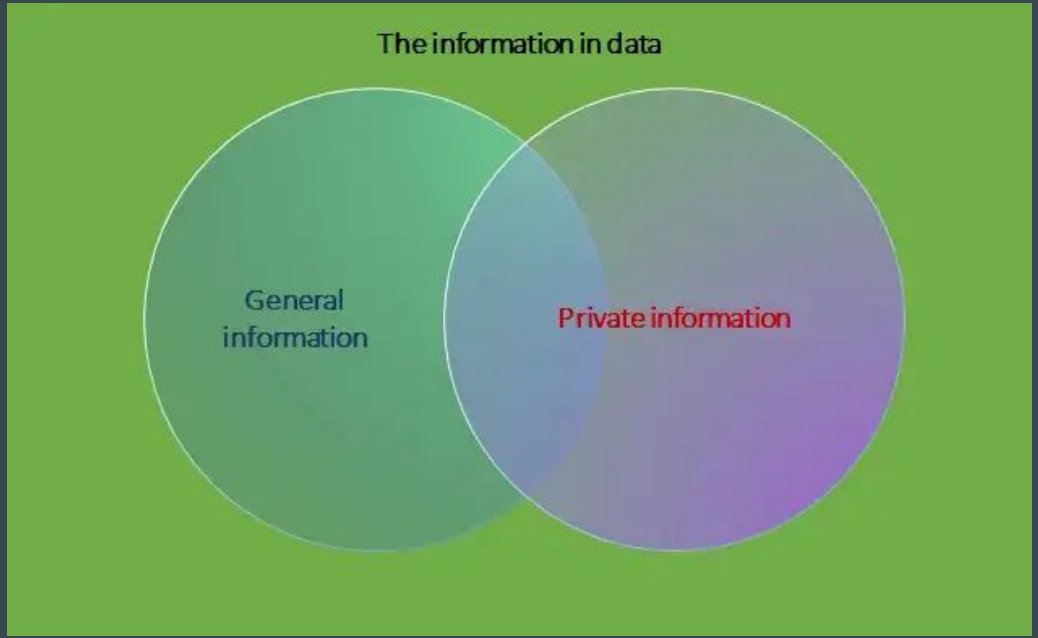
Differential Privacy

What is Differential Privacy?

What does it guarantee?

What does it not guarantee?

How does it work?



Current Research and Related Works

Locally Private Graph Neural Networks

Federated Graph Neural Network Framework for privacy-preserving personalization

Semi-Supervised Knowledge Transfer For Deep Learning from Private Training Data

Releasing Graph Neural Networks with Differential Privacy Guarantees

Our Work

Use the approaches mentioned in the following papers:

- Locally Private Graph Neural Networks
- Semi-Supervised Knowledge Transfer For Deep Learning from Private Training Data
- Releasing Graph Neural Networks with Differential Privacy Guarantees

And train them on Flickr dataset and study and the understand the Privacy vs Accuracy Trade-off

Flickr Dataset

Number of photos: 14460

Total Number of Tags: 52857

Total Number of Groups: 32450

Features based on Neighbours:

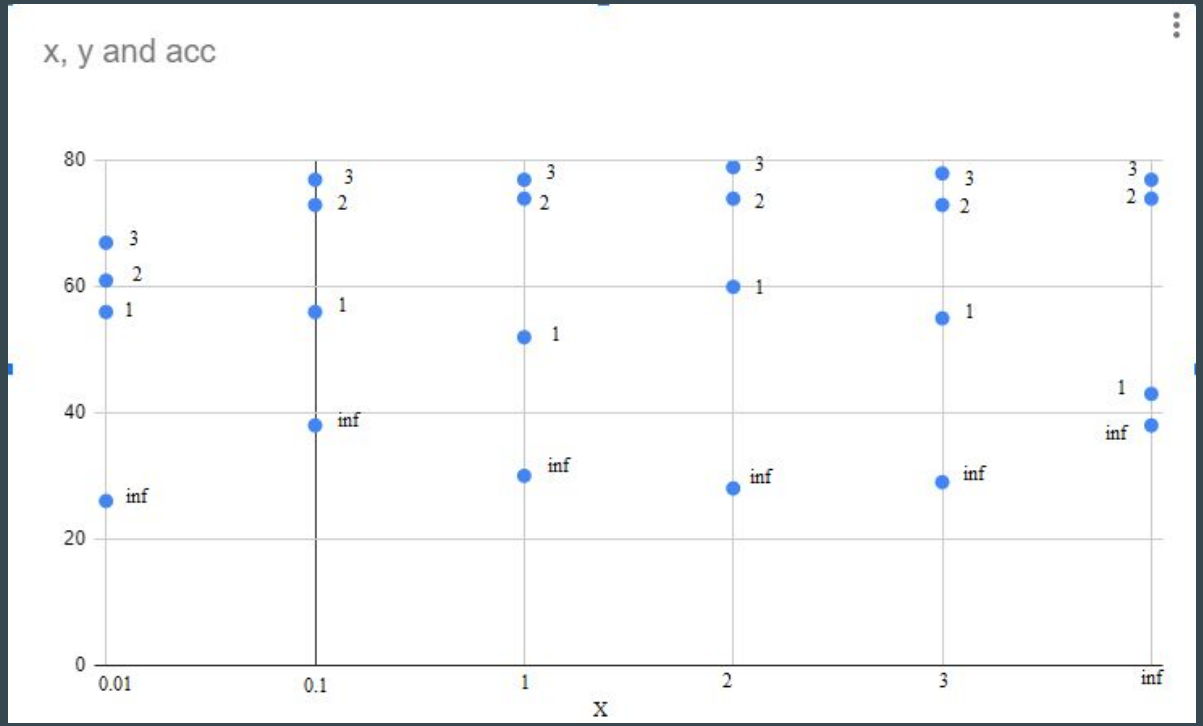
- The number of common tags, groups, collections, and galleries.
- Whether both photos were taken in the same location.
- Whether both photos were taken by same user.
- Whether both photos were taken by contacts/friends.

LPGNN

Implemented the LPGNN paper using pytorch framework.

Feature Privacy Budget

Label Privacy Budget



References

Dai, Enyan, Tianxiang Zhao, Huaisheng Zhu, Junjie Xu, Zhimeng Guo, Hui Liu, Jiliang Tang, and Suhang Wang. “A Comprehensive Survey on Trustworthy Graph Neural Networks: Privacy, Robustness, Fairness, and Explainability.” arXiv.org, April 18, 2022. https://doi.org/10.48550/arXiv.2204.08570.

Olatunji, Iyiola E., Thorben Funke, and Megha Khosla. “Releasing Graph Neural Networks with Differential Privacy Guarantees.” arXiv.org, September 18, 2021. https://doi.org/10.48550/arXiv.2109.08907.

Olatunji, Iyiola E., Wolfgang Nejdl, and Megha Khosla. “Membership Inference Attack on Graph Neural Networks.” 2021 Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA), 2021. https://doi.org/10.1109/tpsisa52974.2021.00002.

Sajadmanesh, Sina, and Daniel Gatica-Perez. “Locally Private Graph Neural Networks.” Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security, 2021. https://doi.org/10.1145/3460120.3484565.

References

Scarselli, F., M. Gori, Ah Chung Tsoi, M. Hagenbuchner, and G. Monfardini. “The Graph Neural Network Model.” IEEE Transactions on Neural Networks 20, no. 1 (2009): 61–80. https://doi.org/10.1109/tnn.2008.2005605.

Wu, Bang, Xiangwen Yang, Shirui Pan, and Xingliang Yuan. “Model Extraction Attacks on Graph Neural Networks.” Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security, 2022. https://doi.org/10.1145/3488932.3497753.

Wu, Chuhan, Fangzhao Wu, Lingjuan Lyu, Tao Qi, Yongfeng Huang, and Xing Xie. “A Federated Graph Neural Network Framework for Privacy-Preserving Personalization.” Nature Communications 13, no. 1 (2022). https://doi.org/10.1038/s41467-022-30714-9.

Wu, Zonghan, Shirui Pan, Fengwen Chen, Guodong Long, Chengqi Zhang, and Philip S. Yu. “A Comprehensive Survey on Graph Neural Networks.” IEEE Transactions on Neural Networks and Learning Systems 32, no. 1 (2021): 4–24. https://doi.org/10.1109/tnnls.2020.2978386.

Thank You