Federated Fine Tuning of Large Language Models

Atharva Joshi atharvaj@usc.edu, Pratyush Bhatnagar

Introduction

Data Protection Alert!

Knock knock - Who's at the door? - It's the GDPR
What's their request? They demand that user text data remains within the user's systems.

Aim

To showcase viability of federated fine tuning of large language models using fully homomorphic encryption functions.

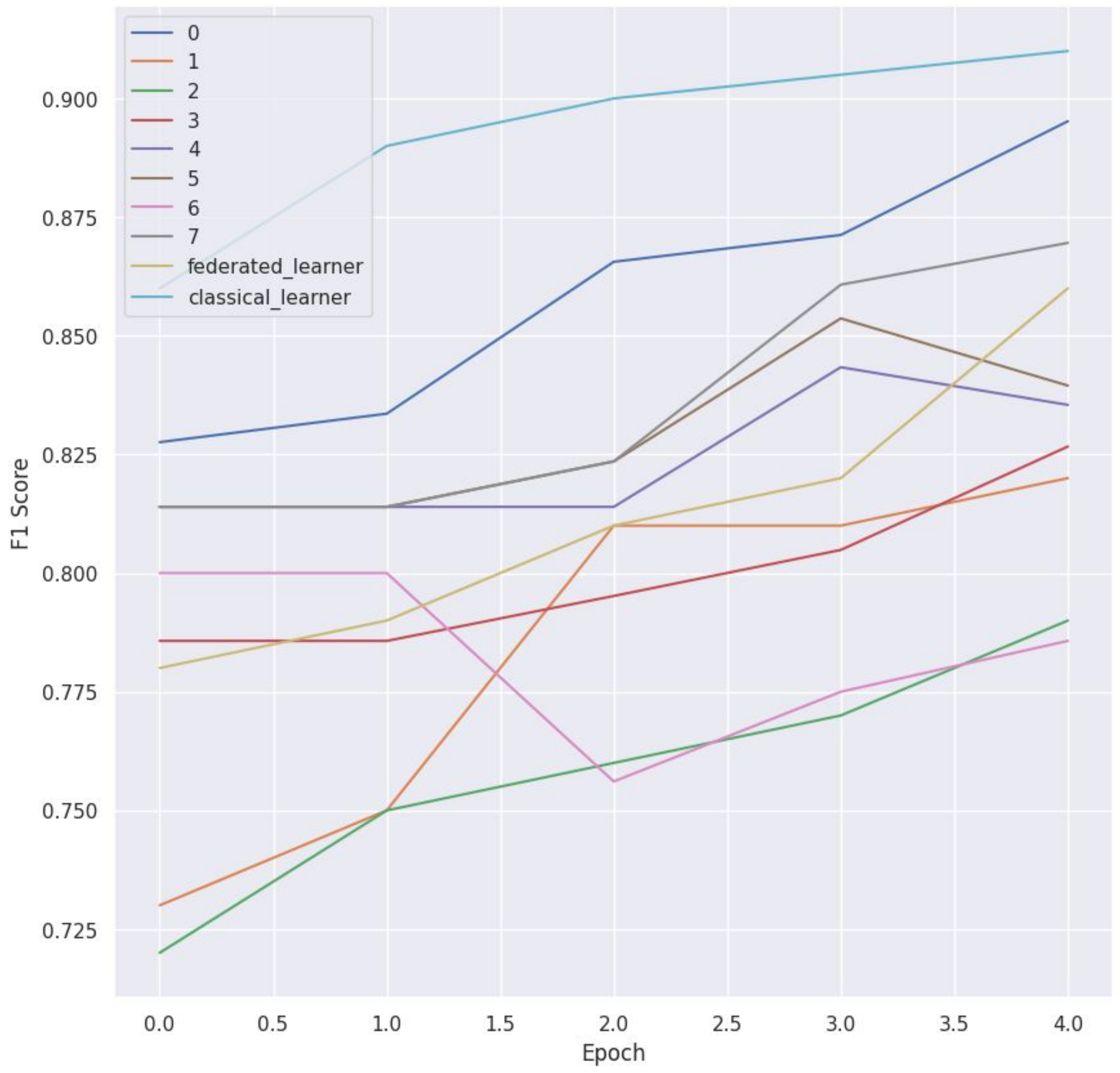
Methods

- Recreating Top-Performing Models on the GLUE MRPC Dataset: We will replicate the results of the highest-performing models on the GLUE MRPC dataset through conventional fine-tuning techniques.
- Simulating Edge-Level Datasets: To mimic edge-level scenarios, we will randomly partition the data, creating datasets that mirror real-world edge node conditions.
- Federated Fine-Tuning: We will implement federated fine-tuning on the divided datasets with the objective of achieving optimal results. This approach allows for distributed learning while keeping data localized to the edge nodes.

Conclusion

Our work demonstrates that federated fine-tuning is a viable and effective approach, offering the promise of maintaining high standards of model performance while adhering to data privacy and security concerns.

Results



Acknowledgements

- Professor Ambite for his guidance and encouragement.
- USC CARC for it’s access to computational resources.