

Peer Review

Review of: "DEeR: Deviation Eliminating and Noise Regulating for Privacy-preserving Federated Low-rank Adaptation"

Ping Zhao¹

1. Donghua University, Shanghai, China

This paper proposes a novel privacy-preserving federated finetuning framework called Deviation Eliminating and Noise Regulating (DEeR). Moreover, this paper conducts an in-depth analysis of the noise amplification effect and finds that this problem is mainly caused by the “linear relationship” between DP noise and LoRA parameters. Finally, the paper performs comprehensive ablated experiments to verify the effectiveness of the deviation eliminator and noise regulator.

The presentation of this paper is, in general, clear and easy to follow. However, there are some issues that need to be addressed.

- 1) The paragraphs in the introduction lack a certain logic, and the descriptions of problems and challenges are too redundant. It would be better if they could be simplified. In addition, too many formulas and symbols should be avoided in the introduction unless necessary.
- 2) The content of the related work section is quite redundant, and it is difficult to see the relevance between the paragraphs. It would be better if some transition sentences could be used to connect the paragraphs.
- 3) In the second paragraph of the related work section, some key words should not be marked with underscores. Instead, they can be marked with italics.
- 4) What are the attack models and design goals considered in this article?
- 5) Some symbols in the formulas are missing some definitions. For example, what is the definition of the symbol ‘d’ in Formula 5?

- 6) In the methodology section of the article, you should avoid introducing the overview section as a separate section. At the same time, each small section in the methodology looks independent, and it would be better if it is connected by some transition sentences.
- 7) The arrows in Figure 3 seem confusing, and some modules cover the arrows. It is recommended to improve them.
- 8) What do the two equations in Formula 18 mean? They seem to have the same final result.
- 9) The performance evaluation of the experimental section is inadequate. Specifically,
- a. In the data set introduction section, the introduction of each data set is too redundant, so it is a brief introduction. More importantly, why does this article not use the CIFAR-100 data set?
 - b. It would be better if some references could be added to the evaluation indicators.
 - c. The result analysis section should not only introduce the phenomenon; it would be better if the causes could be analyzed based on the phenomenon.

Declarations

Potential competing interests: No potential competing interests to declare.