Review of: "Secure and Private Machine Learning: A Survey of Techniques and Applications"

Zhiyu Xie[1]

1 Institute of Electrical and Electronics Engineers (IEEE)

Potential competing interests: No potential competing interests to declare.

This article reviews the latest methods of privacy-preserving machine learning (PPML), including secure multi-party computation, homomorphic encryption, and differential privacy, evaluates the limitations and challenges of these methods, and finally proposes future research directions and opportunities in the field of PPML. The article is satisfactory, but I think there are still some shortcomings:

1. The introduction can be further improved, including, but not limited to, adding more comparative literature to illustrate the advantages and disadvantages of this article compared to other solutions.
2. It is recommended to add a table or a picture to better explain the research of this article.
3. There are some errors in the article.
4. It is recommended that the formulas used in this article be numbered to be more rigorous.