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

Agbotiname Lucky Imoize[1]

1 University of Lagos

Potential competing interests: No potential competing interests to declare.

The survey presents Secure and Private Machine Learning techniques and applications. The work is important and relevant but there are major issues that should be addressed before processing the paper further.

1. The problem being addressed in this survey is adequately motivated. The authors should review the key papers in this domain to identify key problems or gaps. A tabular presentation of the key literature will be preferred. The Table should show the coverage of the papers, gaps and show how the gaps have been filled in the current survey.
2. The key contributions of this paper should be highlighted in bullet points toward the end of section 1.
3. The use of future tenses in the paper should be revised. The entire paper suffers from limited English. Massive revision is required to improve the readability of the paper.
4. The figures require a sharper definition. Most of them are blurred and poorly created. Revise all figures and ensure the texts in the figures are consistent and meaningful. Please, present only neat and bright figures with sufficient descriptions.
5. The style of the review of each paper is not proper. Please, refer to my earlier comment 1.
6. The equations need to be adequately explained and numbered serially throughout the paper.
7. In Figures 3 and 4, the author claimed to have proposed some algorithms and architecture. However, there is no sufficient explanation on why these were proposed and what results were achieved.
8. It would be very interesting to include a section on the lessons learned.
9. Most of the references do not have full citation information. The list is grossly inadequate for a survey paper. The authors should take time to conduct an extensive literature search in this domain.