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

Harsh Kasyap[1]

1 Indian Institute of Technology Patna

Potential competing interests: No potential competing interests to declare.

1. The abstract is well written, and now I am excited to read the whole paper. However, wondering, is privacy violation keyword justified.
2. Safe multi-party computation is more well known as Secure multi-party computation.
3. can lead to serious privacy violations. → privacy leaks/threats.
4. More suitable references should be added in Introduction for PPML, security protocols, and secure machine learning.
5. PPML approaches can be divided roughly into two groups: ? Why HE is not there? Do authors considering under SMPC?
6. Description of ML models is very naive, either make it descriptive or no requirement of it even.
7. Again, crypto techniques like HE and SMPC are too briefly covered, they should be in some detail.
8. Figures should use standard text fonts.
9. 2.3. Deferential Privacy → I think it is misspelled, and at a lot of places.
10. I don't understand the significance of Section 3.
11. 3 sections 2-5 for covering background and related works are too much.
12. 4.x should be names as the scheme's names, not like citations.
13. And, I reached to the end of the manuscript. I think authors should look at some survey papers, and rigorously revise this one.