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

Vartika Puri[1]

1 Jaypee Institute of Information Technology

Potential competing interests: No potential competing interests to declare.

This paper presents the surveys of available techniques and application of Secure and Private Machine learning. My suggestions are:

1. Inclusion of four papers are not enough, at least there are 20+ different papers should be presented.
2. No comparative analysis of different approaches are there, there should be a comparison table.
3. There are some typos like ‘thread’ instead of ‘threat’, ‘rendom’ instead of ‘random’.
4. Future work should mentioned some gaps, a generic future work is not enough.

Requires Major Revision