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

George Meghabghab[1]

1 Roane State Community College

Potential competing interests: No potential competing interests to declare.

The present review describes the problems of secure and privacy violations in Machine Learning (ML). It examines four approaches for addressing these issues, limitations, while comparing these results.

Here are my comments on the paper:

1- The paper has its own merit as such. It cannot be put aside.

2- The paper has provided a broad summary of research and yet limited the number of approaches in a topic that is highly practical, greatly sought out, and well researched, and covered.

3- I was hoping for an original classification of all these different approaches to the topic. It could have helped future authors and the common reader in understanding a topic that is highly volatile and at times with boundaries that are not clear in their approaches.

4- The paper highlights these four approaches without further addressing the reason for their selection. Had my point in 3. been addressed, it would have help strengthen the author proof of his choice and validated his choice of the four techniques.

5- Are these four techniques a good examplar of four different approaches of studying secure and privacy violations in Machine Learning. While there have been other surveys of the same topic, I do not see any serious critique of earlier surveys.

6- I would love for the author of the paper to address the issues raised in 3-, 4-, and 5-. My approval is conditional on seeing a rewrite of the paper addressing issues 3, 4-, and 5.