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

Yi Liu[1]

1 University of Massachusetts at Dartmouth

Potential competing interests: No potential competing interests to declare.

This paper presents a survey on the techniques of Privacy-Preserving Machine Learning and discusses the future direction. My suggestions are given below.

1. This study presented very limited related work, including only 4 papers. As this is a survey paper, it is recommended that the author expands the review to include a broader range of related research.
2. The related work presented in section 4.1 (Al-Rubaie, 2019) is a survey on the state-of-the-art in PPML, covering some topics that are not addressed in this study, such as federated learning. What is the novelty of this study?
3. The author should justify how and where the literature for review was found. Please explain the literature search process (such as search engines, journals, conference, and databases used for the search), selection criteria (such as inclusion/exclusion criteria), and the relevance of the selected papers to the topic.
4. Please make sure that a term is consistently used throughout the paper. For example, please use a consistent term for ‘differential privacy’, ‘deferential Privacy’, and ‘differentiated privacy,’ as well as ‘secure multi-party computation’ and ‘safe multi-part computation.’
5. The organization of the paper is not very easy to follow. Perhaps consider reorganize section 3 as section 2.3.
6. In section 4, consider giving each section a title in addition to the reference. Section 4.4 is very short. Please add more details about “their proposal includes implementation of the standard ResNet-20 model with the RNS-CKKS Fully Homomorphic Encryption (FHE) with bootstrapping.”
7. Why do you choose those 4 papers in section 4 to review? What are the pros and cons of each study?
8. Please proofread the paper to eliminate typos.