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

Yange Chen

Potential competing interests: No potential competing interests to declare.

1. Safe *multiparty* computation should be secure multiparty computing. Please check the whole paper.

2. ML in the introduction should be Machine Learning ML first since the main body and abstract both need to be described when the acronym first appeared.

3. There are many grammatical mistakes in this paper. In addition, this paper needs to be made more readable.

4. “PPML approaches can be divided roughly into two groups” should be “PPML approaches can be divided roughly into three groups”, and homomorphic encryption should be added. If you divide PPML into two groups, it can be analyzed from the perspectives of cryptography and non-cryptography.

5. “cryptographic techniques such as homomorphic encryption, safe multiparty computing, and secret sharing are used.” exists the technical description error in section 2.2. Secret sharing is a technology of secure multiparty computing, and it belongs to SMC.

6. The concept of homomorphic encryption does not embody the property of homomorphism.

7. Deferential Privacy and differentiated privacy should be “Differential privacy” in section 2.3. Please check the whole paper.

8. The abstract presented in this paper is inconsistent with the content of the main body.