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

Ahmet Cumhur Öztürk[1]

1 Adnan Menderes University

Potential competing interests: No potential competing interests to declare.

In section 2.1 authors did not well explained how unsupervised machine learning tasks are performed.

Figure 1 can be forund at https://www.spiceworks.com/it-security/data-security/articles/how-homomorphic-encryption-protects-data/

There are other methods than cryptography or differential privacy in privacy preserving machine learning, such as adding noise to the data, preserving the privacy in output data that is generated by machine learning techniques and so on. Other techniques should also be mentioned.

There are four up to date previous studies well reviewed with examples in sections;4.1,4.2,4.3 and 4.4. However for a survey paper there should have been more related articles reviewed. Also the reviewed articles can be compared in a table.