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

Maria Natália Dias Soeiro Cordeiro[1]

1 Universidade do Porto

Potential competing interests: No potential competing interests to declare.

The present review thoroughly describes the problems of secure and privacy violations in Machine Learning (ML) that society is currently facing. It also examines the commonly employed approaches for addressing these issues, highlighting their benefits and drawbacks that hinder their widespread adoption in practical applications.

The motivation for this review is well-outlined and justified, providing a clear rationale for the importance of studying and addressing these problems. Indeed, by dealing with privacy concerns and implementing security measures, organisations can ensure the responsible and ethical use of machine learning data while protecting the rights and interests of individuals.

The algorithms described and examples provided, as well as the related works, are highly relevant to the aims of the review. They are discussed systematically, presenting a comprehensive overview of the subject matter.

The manuscript is well-written and effectively falls within the scope of Qeios. It serves as an important source of information for addressing the challenges associated with maintaining privacy in sensitive data. Therefore, it can be published after coping with the following aspects:

- More details about the federated learning approach should be given, which it is somehow disregarded in the present review.
- The authors should carefully revise the whole manuscript to correct typos (e.g.: Page 5: Please correct the sentence "… For more information about "differential" privacy, …"; Figure 2: Please change "rendom" to random; , and so forth), and minor shortcomings (e.g.: including a more specific caption to Figure 3).