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

Jose Javier Garcia Aranda[1]

1 Nokia (Spain)

Potential competing interests: No potential competing interests to declare.

- **Homomorphic encryption** allows computations to be performed on encrypted data. However, there is certain impact on data training because certain properties of data change. For instance, ANNs learn better with data using whole valid range. If the original input data range belongs to [0..1] and cypher data belongs to [0.01 … 0.1], this change of magnitude affects learning process. **I miss an analysis of the impact of encryption at learning process** In fact, the article from Olzak, T. does not analyze this key point, neither other cited papers
- Regarding **deferential privacy**, there is an example of noise addition, but **I miss an analysis of the impact of noise at learning process**. Noise could produce false rules and worse training and it is not a minor problem. In fact, the paper of Dwork, C. B does not analyze this key point, neither other cited papers
- possibly encryption and noise are suitable for examples like the one described in section 4.3. however, this is a classification problem. **How does it work with a regression problem?** I'm sure there are drawbacks that haven't been mentioned.

In general terms, the area of the article is interesting but it does not enter the keys of the limitations and problems of the current proposals. Just list/describe them. An article that analyzes different methods and proposals should cover the drawbacks of all of them and show strengths and weaknesses.

I also suggest including a comparison matrix of different methods, which could be the basis of a criteria for choosing a solution based on the nature of the data and the type of problem.