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

Rupen Mitra[1]

1 University of Edinburgh

Potential competing interests: No potential competing interests to declare.

The survey paper is a nice attempt to summarize the emerging body of literature on PPML. The strengths of the survey paper are (i) providing an introduction to the subject of Differential Privacy and PPML, (ii) discussing the major contributions of four recent works in the field, and (iii) pointing the readers to possible future directions of PPML research.

However, the author might want to provide (i) a more in-depth analysis of the training methods under noisy training data sets, (ii) why those 4 papers are selected and not others, and finally (iii) what are the open research questions/challenges in this field and what are the possible approaches to address those questions.

Finally, a tabular illustration of the applications areas of PPML in the emerging fields such as mobile networking, cloud computing, and social network analysis would make the survey more interesting for a wider spectrum of audiences.