Open Science Index, Computer and Information Engineering Vol:15, No:12, 2021 publications.waset.org/abstracts/128037.pdf

A Comparison of Methods for Neural Network Aggregation

Authors : John Pomerat, Aviv Segev

Abstract : Recently, deep learning has had many theoretical breakthroughs. For deep learning to be successful in the industry, however, there need to be practical algorithms capable of handling many real-world hiccups preventing the immediate application of a learning algorithm. Although AI promises to revolutionize the healthcare industry, getting access to patient data in order to train learning algorithms has not been easy. One proposed solution to this is data- sharing. In this paper, we propose an alternative protocol, based on multi-party computation, to train deep learning models while maintaining both the privacy and security of training data. We examine three methods of training neural networks in this way: Transfer learning, average ensemble learning, and series network learning. We compare these methods to the equivalent model obtained through data-sharing across two different experiments. Additionally, we address the security concerns of this protocol. While the motivating example is healthcare, our findings regarding multi-party computation of neural network training are purely theoretical and have use-cases outside the domain of healthcare.

Keywords : neural network aggregation, multi-party computation, transfer learning, average ensemble learning
Conference Title : ICLR 2021 : International Conference on Learning Representations
Conference Location : Sydney, Australia
Conference Dates : December 02-03, 2021