Title:	Secure machine learning
Authors:	Gopal, Bhavish Raj.
Keywords:	Secure Machine Learning
Issue Date:	28-Jul-2021
Publisher:	IISERM
Abstract:	In the last decade, there has been an increase in technologies involving applications of Ma- chine Learning. For instance, Hospitals use Machine Learning tools to predict a disease; Navigation systems predict traffic flow using machine Learning. In the heart of all this tech- nology is sensitive user data, which has led to several privacy concerns. The development of privacy-enhancing technologies enabled systems to collect and perform computations on data while preserving privacy. We can use several cryptographic tools to develop privacy-enhancing technologies. Multi- party computation(MPC) is one such cryptographic tool where non-colluding parties per- form joint computation over data. Privacy is preserved by no party having any information about the data being computed on. In our work, we focus on implementing Multi-Party Computation(MPC) techniques in Machine Learning setting. More specifically, we fo- cus on improving SecureNN, a three-party secure computation framework for Neural Net- works(NN) training, and inference. The SecureNN framework is state-of-the-art; however, it is mainly limited to Convolutional Neural Networks(CNN). In our work, we extend the SecureNN framework to other neural networks such as RNNs, GRU, and LSTMs. We also work on making SecureNN user- friendly by integrating it with TensorFlow. For this, we make significant improvements to the CrypTFlow, a framework for secure inference in TensorFlow. We implement secure training in CrypTFlow by implementing Secure Training functionalities from SecureNN. We also explore ML algorithms that are computationally less expensive and enable parallel computations to reduce the overheads of SecureNN.
URI:	http://hdl.handle.net/123456789/3812
Appears in Collections:	MS-16

Files in This Item:

File	Description	Size	Format	
MS16049.pdf		916.7 kB	Adobe PDF	View/Open

Show full item record