TF Encrypted Documentation

Release 0.5.9

The TF Encrypted Authors

Apr 17, 2020

API

TF Encrypted is a framework for encrypted machine learning in TensorFlow. It looks and feels like TensorFlow, taking advantage of the ease-of-use of the Keras API while enabling training and prediction over encrypted data. Under the hood, TF Encrypted integrates state-of-the-art cryptography like secure multi-party computation, and homomorphic encryption. TF Encrypted aims to make privacy-preserving machine learning readily available, without requiring expertise in cryptography, distributed systems, or high performance computing.

TF Encrypted focuses on:

- **Usability**: The API and its underlying design philosophy make it easy to get started, use, and integrate privacy-preserving technology into pre-existing machine learning processes.
- **Extensibility**: The architecture supports and encourages experimentation and benchmarking of new cryptographic protocols and machine learning algorithms.
- **Performance**: Optimizing for tensor-based applications and relying on TensorFlow's backend means runtime performance comparable to that of specialized stand-alone frameworks.
- **Community**: With a primary goal of pushing the technology forward the project encourages collaboration and open source over proprietary and closed solutions.
- **Security**: Cryptographic protocols are evaluated against strong notions of security and known limitations are highlighted.

This page only contains API documentation. Checkout the examples on github to learn how to get up and running with private machine learning.

You can view the project source, contribute, and asks questions on GitHub.

CHAPTER

ONE

LICENSE

This project is licensed under the Apache License, Version 2.0 (see License). Copyright as specified in the NOTICE contained in the code base.