Dissertation

The Relation between Neural Networks and Homomorphic Encryption

Project Overview:

Applying machine learning techniques to an industry problem which involves medical, financial or other types of sensitive data, not only requires accurate predictions but also careful attention to maintaining data privacy and security. Legal and ethical requirements may prevent the use of cloud-based machine learning solutions for such tasks. This project will explore elements linking learned neural networks to homomorphic encryption. How can neural networks help to ensure that data remains confidential and allows the data owner to send their data in an encrypted form?

This thesis will aim to explore the development of machine learning on encrypted data. This includes discussing methods used prior to neural networks and discussing potential solutions for the future. I will attempt to use current solutions on my own set of example data and explore the benefits and pitfalls.

Standards:

- 60 – 80 Pages
- Due date: 24th August

Objectives:

- Identify how neural networks and machine learning can be used in a Cryptographic scenario.
- Identify and analyze what is being done within the industry to develop this topic currently.
- Explore the timeline for machine learning and Encryption.

Requirements/Task(s):

Introduction
Literature Review
System Design
Implementation
Test and Evaluation
Discussion and Future work (Conclusion)

Outline the steps/plan for your project:

Firstly, I intend to define some core concepts such as Homomorphic Encryption and Neural Networks. Next, I will explore the timeline of machine learning and encryption discuss how methods improved and developed upon previous techniques and models. Concluding this I will present some present-day concepts such as Cryptonets, SageMaker and Discretized Neural Networks and show a simple technique to build these models. Building upon some of these current concepts I will try to apply them to dataset of my choice and draw some conclusions and comparisons. Finally, I will discuss future aspects of the topic and conclude my findings.

Useful Links:

- http://proceedings.mlr.press/v48/gilad-bachrach16.pdf
- https://github.com/microsoft/CryptoNets
- https://eprint.iacr.org/2017/1114.pdf
- https://www.amazon.science/blog/machine-learning-models-that-act-on-encrypted-data