Discussion Leader Papers

HAORAN GENG

ACM Reference Format:
Haoran Geng. 2022. Discussion Leader Papers. 1, 1 (March 2022), 2 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 INTRODUCTION

Machine learning have driven increasing deployment of neural network inference in popular application like voice recognition and image classification. However, the use of the inference in many such applications raises a lot of privacy concerns. Privacy-preserving frameworks, in which functions are computed directly on encrypted data, is one of most powerful solution for providing both security and privacy in neural network inference. A huge amount of studies work on using privacy-preserving frameworks to deploy security neural network inference protocol in real life. In this presentation, I would like to discuss two state-of-art implementation of cryptographic inference service, which use privacy-preserving frameworks, for neural network.

2 GAZELLE: A LOW LATENCY FRAMEWORK FOR SECURE NEURAL NETWORK INFERENCE [1]

This paper is from MIT and accepted at USENIX 2018. This paper presents GAZELLE, a scalable and low latency system for secure neural network inference. GAZELLE use Homomorphic encryption for linear algebra kernels and Garbled Circuit for non-linear kernels. The authors also give a complete study of choose between Homomorphic encryption and Garbled Circuit in the neural network computation. They evaluate GAZELLE protocols on neural network trained on the MNIST and CIFAR-10 datasets. GAZELLE can outperforms the best existing systems by 20-30x in online run time. Compare with the fully Homomorphic encryption approach, GAZELLE performs three times faster in online phase.

3 DELPHI: A CRYPTOGRAPHIC INFERENCE SERVICE FOR NEURAL NETWORKS[2]

This paper is from UCB and accepted at USENIX 2020. This paper presents Delphi, a cryptographic prediction system which has same usage as GAZELLE, but has better performance. Delphi has a hybrid cryptographic protocol that improves upon the communication and computation costs over prior work. It also has a planner that automatically generates the performance-accuracy trade-offs. Delphi's architecture is based on the GAZELLE, but they use an off-line phase to precalculate the Homomorphic cryptographic operations. GAZELLE compute these operations in the off-line phase make the communication and computation cost relatively high. Delphi can gain 22x performance improvements in online predictions compare to GAZELLE.

REFERENCES

[1] Chiraag Juvekar, Vinod Vaikuntanathan, and Anantha Chandrakasan. "{GAZELLE}: A low latency framework for secure neural network inference". In: *27th USENIX Security Symposium (USENIX Security 18)*. 2018, pp. 1651–1669.

Author's address: Haoran Geng.

XXXX-XXXX/2022/3-ART $15.00
https://doi.org/10.1145/nnnnnnn.nnnnnnn

[2] Pratyush Mishra et al. “Delphi: A cryptographic inference service for neural networks”. In: *29th USENIX Security Symposium (USENIX Security 20)*. 2020, pp. 2505–2522.