New Ensemble Method for Convolutional Neural Networks on Encrypted Images

Christopher Sasso

Department of Computer Science, Cal Poly Pomona

Faculty Advisor: Dr. Tingting Chen, Cal Poly Pomona

Motivation

- Cloud computing provides a solution to scale the demanding workloads of machine learning.
- Concerns of data vulnerability exist in cloud computing since ML algorithms are typically developed without rigorous security or privacy protection [1].
- Works including CryptoNets [2], using homomorphic encryption to solve the data privacy issue, have been proposed towards enabling inference as a service.
- If we can upload encrypted data and obtain the same classification results as on clear-text data, we can preserve the privacy of sensitive information.
- Challenges include computationally intensive activation function evaluation and training data distributions.

Project Objective

The project objective is to design and implement a privacy preserving prediction system through an ensemble of convolutional neural networks (CNN).

Comparison with existing literature:

- The work enables more general activation functions on ciphertext
- Prove that ensemble CNN is a viable approach

Based on CryptoNets [2], we implemented a CNN on ciphertexts (encrypted images) and computed the accuracy of the predictions after decryption by the user. (Fig 1.)

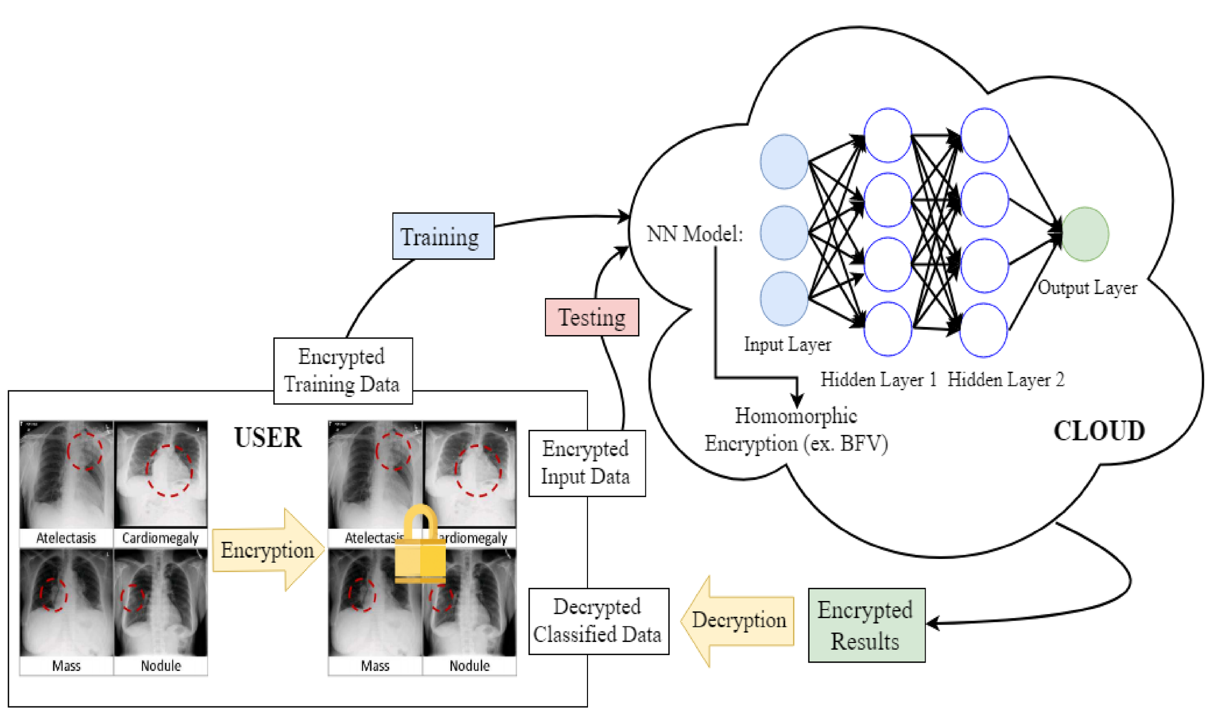

Fig 1. Architecture of Privacy Preserving Neural Network in a cloud setting

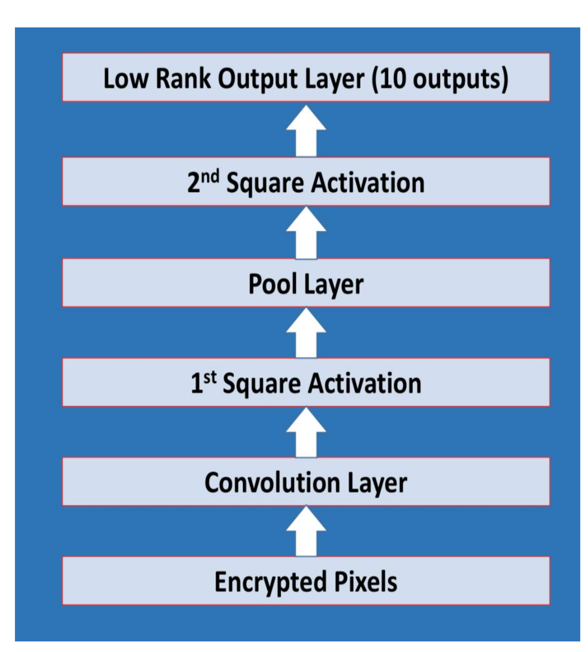

Fig 2. CryptoNets Structure (credit: Microsoft)

CNN Ensemble on Ciphertext

Fully Homomorphic Encryption

- To enable inference using the CNN ensemble, we utilize fully homomorphic encryption.
- Fully homomorphic encryption supports additive and multiplicative computations on ciphertext while preserving the computations on plaintext.
- We used the Brakerski/Fan-Vercauteren (BFV) scheme, a lattice-based cryptographic scheme dependent on the Ring Learning With Errors problem [3], provided by the SEAL library [4].

Approximated ReLU Activation Function

- We implemented the approximate ReLU activation function, a more comprehensive activation function than the previous square activation function, in CryptoNets [2].
- Approx. ReLU has a polynomial estimate allowing for more faster and more effective training of a neural network.

CNN Ensemble

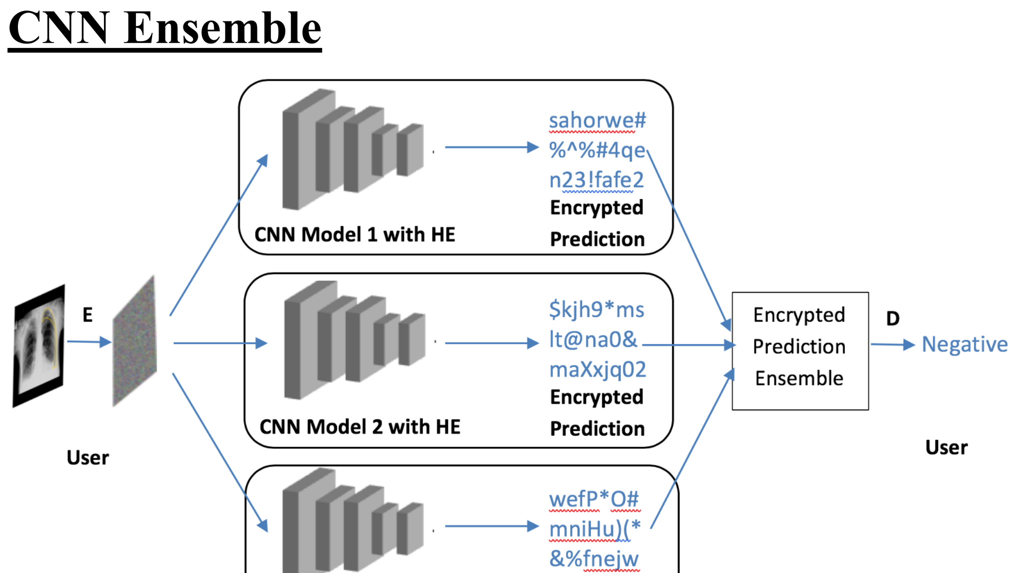

Fig. 3. Encrypted CNN Ensemble Diagram.

1. End user encrypts their sensitive data and sends it to multiple model holders (service providers).
2. Each model holder runs predictions on ciphertexts and outputs the encrypted local prediction results.
3. Ensemble step on encrypted predictions can be performed by a service coordinator and generates the final encrypted prediction.
4. End user decrypts the result.

This is the first work to enable an encrypted CNN ensemble to leverage more diverse training datasets to push the performance of homomorphic encryption based deep learning.

Testing Different Ensemble Calculations

The accuracy of ensembles were tested using different dataset distributions and different ensemble calculations. From the results as shown in Fig. 4, the less restricted datasets provided the more accurate results. And from testing the different ensemble calculations, they provide similar results.

All experiments were performed on a workstation with Intel Core i9-9900K CPU @3.60GHz, and 32 GB RAM and a NVIDIA GeForce RTX 2080 TI.

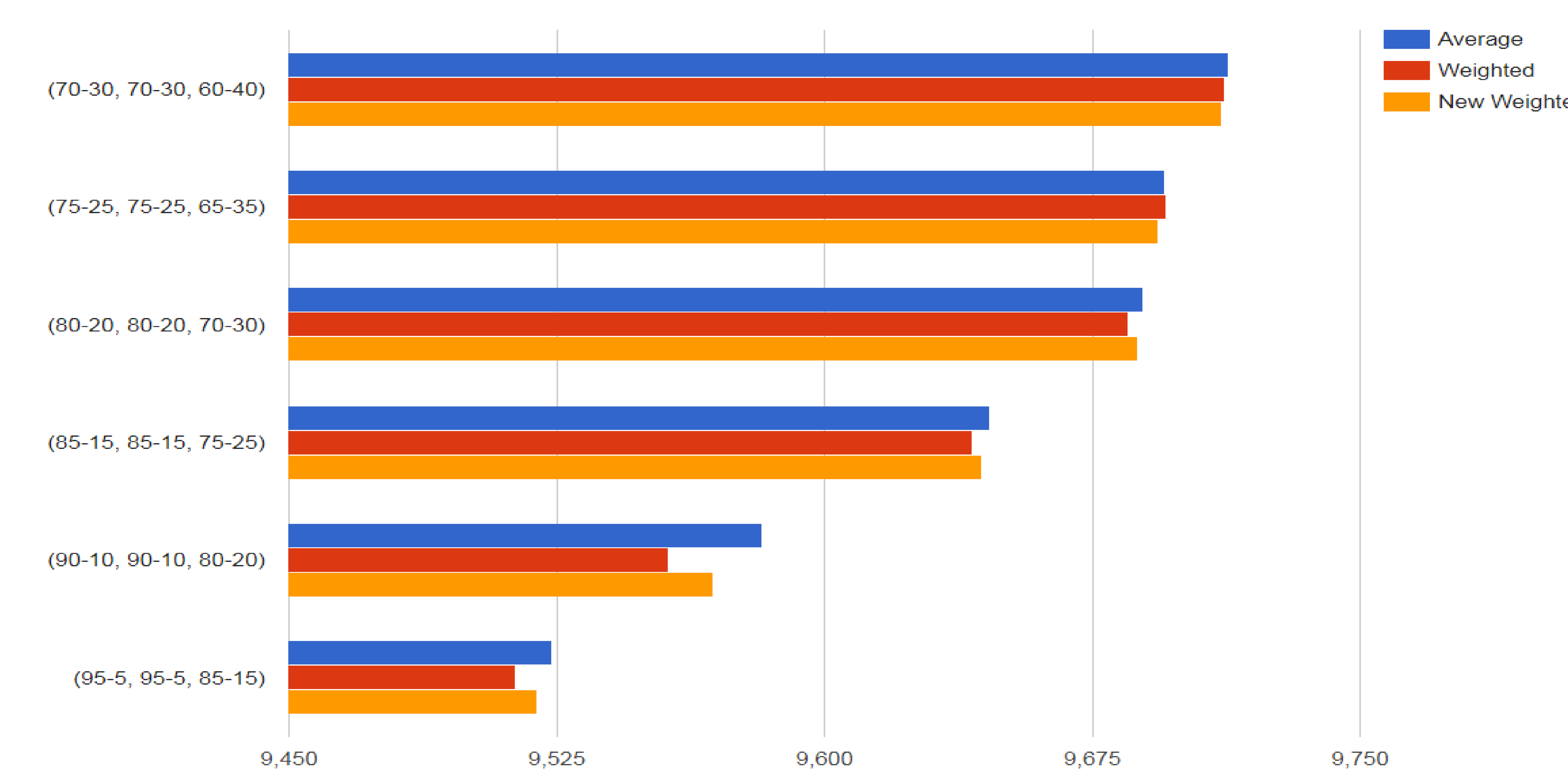

Fig 4. Accuracy of Ensemble Calculations per Split

Observations:

- Accuracy for the average ensemble is greater than that of any model individually.

Current & Future Work

To enhance the accuracy of the Convolutional Neural Network Ensemble, different ensemble calculation methods could improve the accuracy. Different types of average calculations produce similar results. Future work would have to continue to explore calculus-based algorithms for determining the overall accuracy of a Convolutional Neural Network Ensemble.

- **Combine Homomorphic Encryption with Differential Privacy**
  - Differential privacy is the standard quantitative data privacy definition. In the future, we would like to extend our work to mitigate the computational intensity of homomorphic encryption through differential privacy [8].

References

1. Ping Li, Jin Li, Zhengan Huang, Tong Li, Chong-Zhi Gao, Siu-Ming Yiu, Kai Chen, "Multi-key privacy-preserving deep learning in cloud computing," Future Generation Computer Systems, Volume 74, 2017, Pages 76-85, Accessed:https://doi.org/10.1016/j.future.2017.02.006..
2. Nathan Dowlin, Ran Gilad-Bachrach, Kim Laine, Kristin Lauter, Michael Naehrig, and John Wernsing.,"CryptoNets: applying neural networks to encrypted data with high throughput and accuracy," ICML'16 -, Volume 48) Pages 201-210, Accessed: https://www.microsoft.com/en-us/research/publication/cryptonets-applying-neural-networks-to-encrypted-data-with-high-throughput-and-accuracy/.
3. Fan, J., & Vercauteren, F. (2012). Somewhat Practical Fully Homomorphic Encryption. IACR Cryptology ePrint Archive, 2012, 144., Accessed: https://eprint.iacr.org/2012/144.
4. Microsoft SEAL, Release 3.2, Feb. 2019, Microsoft Research, Redmond, WA., SEAL, Accessed: https://github.com/Microsoft/SEAL.
5. Edward Chou, Josh Beal, Daniel Levy, Serena Yeung, Albert Haque, Li Fei-Fei, "Faster CryptoNets: Leveraging Sparsity for Real-World Encrypted Inference," CoRR 2018, 1811.09953, Accessed: http://arxiv.org/abs/1811.09953.
6. LeCun, Yann and Cortes, Corinna. "MNIST handwritten digit database." (2010): http://yann.lecun.com/exdb/mnist/.
7. Ma Z, Wang P, Gao Z, Wang R, Khalighi K (2018), "Ensemble of machine learning algorithms using the stacked generalization approach to estimate the warfarin dose." PLOS ONE 13, Accessed: https://doi.org/10.1371/journal.pone.0205872.
8. Xiangyun Tang, Liehuang Zhu, Meng Shen, Xiaojiang Du, "When Homomorphic Cryptosystem Meets Differential Privacy: Training Machine Learning Classifier with Privacy Protection", CoRR, 2018, Accessed: http://arxiv.org/abs/1812.02292.