JAINTH CHAUDHARY
STUDENT, INFORMATION TECHNOLOGY

SAFE AI: PRIVACY PRESERVING MACHINE LEARNING ALGORITHMS FOR TRUST SENSITIVE ENVIRONMENTS

Objectives: Despite the breakthrough success of Machine Learning (ML) algorithms - especially Deep Learning - in a broad spectrum of big data applications, cyberspace threats and vulnerabilities to ML systems raise major concerns in security- and trust- sensitive environments such as healthcare, defense, finance, government organization, and social network. A novel combination of ML techniques and privacy mechanisms is of the utmost importance for enabling secure privacy-preserving ML algorithms by making a trade-off between security and performance in ML systems.

Research Approaches: Homomorphic encryption (HE) allows computations over encrypted data and thus preserves privacy in a cloud computing environment. HE could be categorized into two main categories; partially homomorphic encryption (PHE), and fully homomorphic encryption (FHE). FHE can help solve privacy issues completely, but it introduces high performance overhead. To avoid such overhead, PHE can be used. In this research we evaluated the performance of different ML algorithms such as regression, neural network, and deep learning over both PHE and FHE and an extensive comparative studies have been conducted in a broad range of privacy sensitive environments such as employee salary prediction, sentiment analysis from reviews data, email spam classification, handwritten digit recognition, and credit card screening.

Novelty and expected significance: This research provides a far insight on the trade-off between performance and security for a wide number of combinations of cryptographic and ML algorithms for constructing a secure PPDML system which have been tested on a number of trust sensitive applications. This research envisages moving one step towards bridging the knowledge gap between the ML and cryptography communities, which is the paramount requirement for addressing privacy concerns adequately in ML systems.

Research Advisor: Dr. Baidya Nath Saha