Clement Fung - Statement of Purpose for Northeastern University Computer Science PhD Application

I want to pursue a PhD in computer science, specifically in the field of computer security. I have a particular interest in securing and democratizing interactions with distributed machine learning systems. Given the increasing popularity of decentralized architectures like Google's federated learning and the recent discoveries of attacks on models such as backdooring and attacks on data providers such as property inference, I consider this area to be both incredibly interesting and of paramount importance.

Throughout my masters degree at the University of British Columbia (UBC), I was supervised by Professor Ivan Beschastnikh. Together, we completed three different projects in the area of secure and private multi-party machine learning: (1) Biscotti[1]: A private and secure distributed ledger for peer to peer machine learning, (2) FoolsGold[2]: A protocol for detecting and mitigating sybil-based poisoning attacks on federated learning, and (3) TorMentor[3]: A system and protocol for private, secure machine learning over an anonymous network. For each of these projects, the central theme was: how can we modify distributed multi-party machine learning systems in ways that protect the privacy of their users while maintaining the integrity of the learned model?

One solution to providing more privacy and security to distributed multi-party machine learning is to eliminate the centralization present in modern architectures such as federated learning. I worked on developing an alternative peer-to-peer ledger-based solution to coordinate the training process, called Biscotti.

In FoolsGold, I developed a mechanism for protecting federated learning systems from sybil-based targeted poisoning attacks, using the similarity of gradients between clients as a penalization function for thwarting targeted poisoning attacks. Unlike prior defenses, this mechanism does not rely on observation of client training data, which makes it suitable for federated learning systems. This work is currently in submission at the 2019 IEEE European Symposium on Security and Privacy.

In TorMentor, I augmented stronger defenses onto federated learning by using anonymous onion routers as the communication medium in distributed learning. Through anonymous communication, I defined a new learning paradigm called brokered learning, in which data providers and model curators do not need to directly communicate with each other. TorMentor gives more control to clients and performs secure and anonymous machine learning in a democratic fashion.

In addition to the systems I have built at UBC, I have experience building large scale systems over 2 internships spanning 8 months at LinkedIn. Following the conclusion of my Masters degree in December, I will be furthering my industry experience by spending 6 months working at Oasis Labs[4], an early stage privacy-preserving blockchain research startup founded by Professor Dawn Song from UC Berkeley.

While my work so far is a first step towards securing distributed multi-party machine learning, there are still several unanswered questions left. One particular idea that I would like to pursue builds upon my work in Biscotti to allow retraining of machine learning models after poisoning attacks are detected and their data sources are identified. This idea would leverage ideas from data provenance and auditing on the blockchain to allow model providers to apply security patches to models, ideally without requiring the original datasets or the associated clients.

At Northeastern University, I am particularly intrigued by the work of the Network and Distributed Systems Security (NDS2) group, led by Professors Christina Nitu-Rotaru and Alina Oprea. Their recent work investigates methods for detecting and preventing poisoning attacks on distributed systems, including the internet of things, distributed ledgers and cloud computing. This group's work in securing systems against machine learning attacks is in an area of great interest to me. Additionally, I am also interested in collaborating with Long Lu, who has also done significant relevant work in systems security.

Thank you for your time in considering me as an applicant of the PhD program at Northeastern University.

[1] ArXiv, November 2018. `https://arxiv.org/abs/1808.04866`
[2] ArXiv, August 2018. `https://arxiv.org/abs/1808.04866`
[3] ArXiv, November 2018. `https://arxiv.org/abs/1808.04866`
[4] `https://www.oasislabs.com/`