CAREER: Blockchain-Assisted Secure Cloud Storage

Outsourcing data storage to a remote platform has become a popular computing paradigm due to the advent of cloud computing. With emerging applications in security-sensitive domains (e.g. IoT clouds as in Google [1], healthcare clouds such as in Amazon [2] and IBM [3]), the continued success of cloud storage in the near future relies heavily on increasing cloud security and trustworthiness, especially in the presence of the man-in-the-middle attacks which are constantly found on the news. On the other hand, the Blockchain technology, through its recent successful applications to BitCoin alike cryptocurrency, has shown its great potential to behave as the first practical trusted third-party (TTP).

Intellectual Merits: In this career proposal, the PI will study Blockchain-assisted Secure Cloud Storage. The objective is to enable stronger security of cloud services against existing and emerging man-in-the-middle attacks and to build functional prototype systems with low and practical overhead. The key research question to answer is whether it is possible to reduce the security of complex cloud-client interaction to the Blockchain (as a TTP). The proposed research will be consistent with the PI's long-term career goal of building secure and trustworthy distributed systems. Towards the proposal objective, the PI identifies a series of new research problems that no existing research tackle. The PI propose a series of research tasks to tackle these problems:

Task 1: Secure weakly-consistent cloud storage by semantic-aware Blockchain logging. Weak consistency (e.g., eventual consistency) has become the standard storage model for geo-distributed clouds and web services. Violating storage consistency and forking attacks (cloud sending different results to different clients) are fundamental and important forms of man-in-the-middle attacks in the untrusted cloud model. This research task addresses a new research problem --- preventing forking attacks in the context of weakly-consistent cloud storage. The proposed technique is Blockchain transaction logging schemes that map weak-consistency specification to a Blockchain transaction layout, such that violating weak consistency will be as hard as violating the no-double-spending security of Blockchain. The proposed technique will have the potential to secure other cloud-storage applications, such as Git.

Task 2: Update-efficient authenticated cloud storage by trusted smart-contracts. In the untrusted cloud model, an open research problem is designing update-efficient authenticated data structures (ADS). Update efficiency in untrusted cloud storage is particularly important for big-data applications and key-transparency schemes. In this research task, the PI proposes a new approach by including Blockchain as a trusted program-execution platform and to design the first ADS protocol with theoretically-optimal update-efficiency. Based on the proposed new protocol, the PI will build practical cloud systems for big-data applications on low-end devices (e.g., IoT devices) and public-key directory services with minimal key-revocation delay.

Broader Impacts: 1) The proposed research advocates a new trustworthy-system building paradigm and will create impacts on the follow-up research work in systems and cybersecurity community. 2) For impacts in industry, the outcome of proposed research will increase the adoption of public clouds in emerging security-sensitive applications (e.g., IoT clouds, smart-home clouds, health clouds, etc.). 3) For educational impacts, the PI will develop Blockchain-centric lab modules to address the imminent workforce shortage in Blockchain application development. The targeted audience will be students in computer science and in business. Accordingly, the proposed labs will feature two areas of focus: information-security (InfoSec) applications and financial applications. The PI, through cross-disciplinary

collaboration, will develop Blockchain-based financial labs and will co-teach a cross-listed course to evaluate the labs. In addition to impacts to on-campus curriculum, the proposed labs will be integrated into the SEED education platform for nation-wide dissemination. The project will create research opportunities for undergraduate students and under-represented groups.

Key Words: Cloud security, blockchain, trusted third-party, cloud storage, consistency, cloud outsourcing, data authentication.