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 security-sensitive applications (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 enhancing cloud security and trustworthiness, especially in the presence of the man-in-the-middle attacks. 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).

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 proposed research will be consistent with the PI's long-term career goal of building secure and trustworthy distributed systems.

Intellectual Merits: The motivating insight is to repurpose Blockchain as a TTP for cloud security. The research questions to be answered involve what cloud applications can benefit from the presence of a Blockchain, which Blockchain security property can be (ab)used to harden the cloud security, how to bridge performance and cost gap between cloud and Blockchain. Towards the proposal objective, the PI identifies a series of new research problems that no existing research tackles. To address these problems, the PI propose the following research tasks:

Task 1: Lightweight cloud consistency verification with Blockchain. Verifying the cloud storage consistency is an important security measure against a malicious cloud that gives data control back to cloud clients. In this research task, the PI proposes a new consistency-verification approach by leveraging Blockchain. The motivating insight is that one can map consistency specification to Blockchain transactions in such a way that concealing consistency violation will be as hard as sending double-spending transactions. Instantiating the insight, the key research problem to explore is whether Blockchain's transaction model is expressive enough for various consistency models adopted by the clouds. The PI proposes new Blockchain logging techniques and systematically tailors them for cloud-consistency models, including storage consistency such as strong consistency and weak consistency, and transactional database consistency, such as snapshot isolation and serializability. Additional new techniques will be proposed for applications-specific consistency models such as Git. This research task will results in security protocols and system prototypes for practical consistency verification against malicious man-in-the-middle cloud and with performance efficiency for large-scale cloud applications.

Task 2: Update-efficient authenticated cloud storage by 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 secure big-data applications and key-transparency schemes[4]. In this research task, the PI proposes a new approach of designing ADS with optimal update efficiency by including Blockchain as a trusted platform for truthful program execution (namely smart contract). Based on the new protocol, the PI will propose performance optimization schemes to reduce the cost of running smart contract. The research outcome will be 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 based on Blockchain 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.

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

[1] "Google Cloud IoT - Fully managed IoT services from Google | Google Cloud," *Google Cloud*. [Online]. Available: https://cloud.google.com/solutions/iot/. [Accessed: 05-Apr-2018].
[2] "Amazon Healthcare Clouds." [Online]. Available: https://aws.amazon.com/health/.
[3] "IBM Cloud Solutions for Healthcare | IBM Cloud." [Online]. Available: https://www.ibm.com/cloud/healthcare. [Accessed: 05-Apr-2018].
[4] M. S. Melara, A. Blankstein, J. Bonneau, E. W. Felten, and M. J. Freedman, "CONIKS: Bringing Key Transparency to End Users," in *USENIX Security Symposium*, 2015, vol. 2015, pp. 383–398.