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.

CAREER: Blockchain-Assisted Cloud Security

Hosting data applications on a third-party platform has become a popular computing paradigm due to the advent of cloud computing. With emerging security-sensitive applications (in domains like healthcare, smart-homes, etc.), the continued success of cloud computing in the near future heavily relies on hardening cloud security and increasing cloud trustworthiness, especially in the presence of the constant data breaches and man-in-the-middle attacks on the news. On the other hand, the Blockchain technology, through its recent successful applications to BitCoin alike cryptocurrency, has shown the great potential to behave as the first practical trusted third-party (TTP).

Intellectual Merits: In this career proposal, the PI proposes the study of Blockchain-assisted Cloud Security. The proposal objective is to enable stronger security of cloud services against existing and emerging attacks and to build functional prototype systems with low practical overhead. The key research question to answer is whether it is possible to build trustworthy and complex cloud systems by reducing the security to the Blockchain (as a TTP). The proposed research will be consistent with the PI's long-term career goal, that is, building secure and trustworthy distributed systems. Towards the proposal objective, the PI will initiate a series of research tasks:

Task 1: Secure weakly-consistent cloud storage by semantic-aware Blockchain logging. Weakly consistent data storage becomes the standard model for geo-distributed clouds and web services. Forking views to different cloud clients is a fundamental and important man-in-the-middle attack 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 and co-PI Su (in the business college) will develop the Blockchain 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 disseminated, through Co-PI Du's SEED platform, to nation-wide audiences. 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.

Task 3: ZeroCash-based Confidential Cloud Storage

Task 4: Verified Remote Program Execution with Blockchain

Task 5: Side-channel Confidential Program Execution with Blockchain

Outline/Key points

My identity:

My area is secure distributed systems.

Long-term goal: Secure and trustworthy remote storage systems.

Short-term goal: Secure and trustworthy remote storage systems by blockchain.

My past research focused on designing efficient and secure data storage on the cloud [TechRep17,WTSC18,ACSAC14] and P2P networks [CCGrid15, ICDCS08/09,TKDE10,TPDS11].

Privacy-preserving directory [TKDE,CIKM,etc.]

My preliminary work [WTSC18] uses Blockchain as trusted computation platform to design end-device friendly cloud storage.

Intellectual merits (New knowledge):

New settings and problem

Blockchain and strongly consistent storage (e.g. certificate/public-key directory): the key challenge is to prevent forking attack in a SUNDR alike formation. The key problem is how to map operational history to transactions such that statement verification can be made with efficiency.

Blockchain and weakly consistent cloud storage: How to map weak consistent operation history to transactions such that valid application transcript can be validated by miners while invalid transcript can be invalidated.

Blockchain and write-intensive key-value stores for IoT devices: How to map the write-intensive storage workflow to Blockchain in such a way that is friendly to power-limited end devices?

Blockchain and git workflow: How to map git graph to transactions such that valid git graph can be validated by miners while invalid git graph can be invalidated.

Blockchain and end-to-end encrypted storage/Signal: How to conduct computation on encrypted data using Blockchain.

New approach

Blockchain as a highly-available TTP presents a candidate solution for open problems.

Blockchain as trusted computation can be used to design a dynamic ADS with optimal client efficiency.

Blockchain as no-double-spend storage can be used to prevent forking attacks with efficiency (Catena is not efficient).

New results

Forking-secure and efficient trusted storage

Forging secure and update-efficient trusted storage.

Educational impacts

Design labs based on Blockchain applications in IT, finance, laws, etc.

Business students: financial applications

CS students, future IT professionals: Blockchain cloud storage, Blockchain web applications

Broader impacts

Cloud is widely used in domains ranging from personal cloud, IoT cloud, military applications, to others. The proposed research will result in an impact on these application domains.

Summary

[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].