CAREER: Blockchain-Assisted Cloud Security

With the adoption of BitCoin-alike cryptocurrency, the Blockchain technology has shown the great potential of positioning itself as the first trustworthy and highly available third party (TTP) used in practice. This new abstraction is promising to solve many open security problems and to revolutionize our society overall. On another front, the cloud computing technology, while having been successful in many aspects in the last decade, has stumbled in security-sensitive emerging applications such as personal clouds, IoT clouds, etc; this can be seen by constant data breaches on the news. The root cause is the lack of trust to cloud service providers.

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 overhead. The key question to answer is whether it is possible to build a trustworthy and complex cloud system by reducing its security to the Blockchain (as a TTP). The proposed research is consistent with the PI's long-term career goal, that is, building secure and trustworthy distributed systems.

Towards the 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 is the standard model for geo-distributed clouds and web services. Forking views to different cloud clients are a fundamental attack in the untrusted cloud model. This research task addresses an unstudied research problem, namely, preventing forking attacks in the context of weak consistency. The proposed technique is Blockchain transaction logging schemes that map weak-consistency specification to a Blockchain transaction layout, such that the violation of weak consistency can be made equivalent to a violation of no double-spending transactions in Blockchain. The proposed technique will have 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 emerging big-data applications where data updates are generated continuously. In this research task, the PI proposes a new approach by including Blockchain as a trusted program-execution platform to achieve optimal update-efficiency in the ADS design. The PI will study the design of mapping write-intensive storage workflow to Blockchain and propose techniques friendly to intensive updates and low-end devices (e.g. IoT devices).

Task 3: Blockchain-based secure cloud program execution:

Broader Impacts: 1) The research could create impacts and influence follow-up research work in systems and cybersecurity community. 2) For impacts in industry, the project outcome 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.

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