Department of Computer Science

COMPUTER SCIENCE SEMINAR SERIES

Searching an Encrypted Cloud Meets Blockchain: A Decentralized, Reliable and Fair Realization

SPEAKER **Mr Chengjun CAI**

PhD Student
Department of Computer Science
City University of Hong Kong
Hong Kong

DATE 2 May 2018 (Wednesday)
TIME 10:30 am - 11:00 am
VENUE CS Seminar Room, Y6405
6th Floor, Yellow Zone
Yeung Kin Man Academic Building
City University of Hong Kong
83 Tat Chee Avenue
Kowloon Tong

ABSTRACT

Enabling search directly over encrypted data is a desirable technique to allow users to effectively utilize encrypted data outsourced to a remote server like cloud service provider. So far, most existing solutions focus on an honest-but-curious server, while security designs against a malicious server have not drawn enough attention. It is not until recently that a few works address the issue of verifiable designs that enable the data owner to verify the integrity of search results. Unfortunately, these verification mechanisms are highly dependent on the specific encrypted search index structures, and fail to support complex queries. There is a lack of a general verification mechanism that can be applied to all search schemes. Moreover, no effective countermeasures (e.g., punishing the cheater) are available when an unfaithful server is detected.

In this work, we explore the potential of smart contract in Ethereum, an emerging blockchain-based decentralized technology that provides a new paradigm for trusted and transparent computing. By replacing the central server with a carefully designed smart contract, we construct a decentralized privacy preserving search scheme where the data owner can receive correct search results with assurance and without worrying about potential wrongdoings of a malicious server. To better support practical applications, we introduce fairness to our scheme by designing a new smart contract for a financially-fair search construction, in which every participant (especially in the multiuser setting) is treated equally and incentivized to conform to correct computations. In this way, an honest party can always gain what he deserves while a malicious one gets nothing. Finally, we implement a prototype of our construction and deploy it to a locally simulated network and an official Ethereum test network, respectively. The extensive experiments and evaluations demonstrate the practicability of our decentralized search scheme over encrypted data.

This paper was presented at the IEEE International Conference on Computer Communications (INFOCOM), April 15-19, 2018, Honolulu, HI, USA.

Supervisor: Dr Cong WANG

Research Interests: Distributed Application; Secure Search; Blockchain

All are welcome!

In case of questions, please contact Dr WANG Cong at Tel: 3442 2010, E-mail: congwang@cityu.edu.hk, or visit the CS Departmental Seminar Web at http://www.cs.cityu.edu.hk/news/seminars/seminars.html.