EncKV: An Encrypted Key-value Store with Rich Queries

SPEAKER **Mr GUO Yu**
Mr WANG Xinyu

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

DATE 15 June 2017 (Thursday)

TIME 3:00 pm - 4:00 pm

VENUE G7315, 7th Floor, Green Zone
Yeung Kin Man Academic Building
City University of Hong Kong
83 Tat Chee Avenue
Kowloon Tong

ABSTRACT

Distributed data stores are fast evolved to serve the needs of large-scale applications such as online gaming and real-time targeting. Among others, key-value stores are widely adopted because of their superior performance. However, these systems do not ensure strong protection on data confidentiality, thereby falling short of addressing serious privacy concerns raised from massive data breaches.

In this paper, we introduce EncKV, an encrypted key-value store with secure rich query support. First, EncKV stores encrypted data records with multiple secondary attributes in the form of encrypted key-value pairs. Second, EncKV leverages the latest practical primitives for search over encrypted data, i.e., searchable symmetric encryption and order-revealing encryption, and provides encrypted indexes with guaranteed security respectively to enable exact-match and range-match queries via secondary attributes of data records. Third, EncKV carefully integrates the above indexes into a distributed index framework to facilitate secure query processing in parallel. To mitigate recent inference attacks on encrypted database systems, EncKV protects the order information during range queries, and presents an interactive batch query mechanism to further hide the associations across data values on different attributes. We implement the EncKV prototype on a Redis cluster, and conduct performance evaluation on Amazon Cloud. The results show that EncKV preserves the efficiency and scalability of plaintext distributed key-value stores.

This paper was presented at the ACM Asia Conference on Computer and Communications Security (ASIACCS) 2017, April 2-6, Abu Dhabi, UAE.

Supervisors: Prof JIA Xiaohua, Dr WANG Cong

Research interests: Security, Database and Distributed System.

All are welcome!

In case of questions, please contact Prof JIA Xiaohua / Dr Cong WANG at Tel: 3442 9670 / 3442 2010, E-mail: csjia@cityu.edu.hk / congwang@cityu.edu.hk, or visit the CS Departmental Seminar Web at http://www.cs.cityu.edu.hk/news/seminars/seminars.html.