TECHNOLOGY

Dynamic Searchable Encryption with Minimal Data Leakage

OVERVIEW

Background
Dynamic Searchable Symmetric Encryption (DSSE) methods are used to perform searches on encrypted data without decryption. This allows for the secure storage of data on remote or third-party storage while maintaining the ability for the user to access data as needed. However, current DSSE schemes have drawbacks that make practical implementations of DSSE difficult. Some methods produce data leakage, where information about what is being stored can be learned by the storage server via access patterns, hashes of encrypted search keywords, keywords shared among different documents, access to deleted documents, total number of documents stored, and other information. Other implementations provide stronger security against data leakage but are impractical because of search time, additional storage space required, or a chance of false positive occurring from a search.

Innovative Technology
Researchers at the University of Maryland's Maryland Cybersecurity Center (MC2) and the University of California Berkeley have developed a dynamic searchable encryption method that minimizes the amount of data leaked when performing a search query. The method allows for a sublinear search time in the worst case while guaranteeing that the only information that can be leaked to the server is the access and search patterns and deleted documents that match the searched keyword. The server requires a roughly linear amount of storage, and the client requires only a small amount of storage at any time (in the hundreds of megabytes). Adding or deleting a keyword to search requires a minimal amount of bandwidth (kilobytes). This method has been implemented in a cloud storage environment (Amazon EC2) and been shown to be practical with a variety of database sizes, network latencies, and results per query.

APPLICATIONS

· Secured cloud storage

ADVANTAGES

· Minimizes the amount of information that can be leaked while maintaining a sublinear search time
· Requires minimal storage by the client device
· Method can be run asynchronously, i.e. searches and additions to storage can run simultaneously

CONTACT INFO

UM Ventures
0134 Lee Building
7809 Regents Drive
College Park, MD 20742
Email: umdtechtransfer@umd.edu
Phone: (301) 405-3947 | Fax: (301) 314-9502

Additional Information

INSTITUTION

University of Maryland, College Park

PATENT STATUS

Pending

LICENSE STATUS

Available for exclusive or non-exclusive license

CATEGORIES

- Information Technology

EXTERNAL RESOURCES

IS-2014-035