The key to private and efficient data storage

May 1 2017

Research sponsored by a multinational IT service provider in 2010 suggested that up to 75% of all produced data is duplicated. Credit: Wavebreak Media Ltd/ 123rf

Cloud storage services, like Dropbox and Gmail, may soon be able to better manage your content, giving you more storage capacity while still being unable to 'read' your data.

People and businesses are more often than ever storing large amounts of private data in 'the cloud' with storage service providers. To protect their clients' private information, this stored data is encrypted so that no one, including the service providers, can read it. But this makes it impossible for cloud storage providers to efficiently manage that data and provide their clients with better storage capacity. Research sponsored by a multinational IT service provider in 2010 suggested that up to 75% of all produced data is duplicated. Owners of an open source 'deduplication' solution suggest that reducing duplicate data could clear up to 95% of storage space.

For cloud storage providers to remove, or 'deduplicate', data, they need to be able to recognize it without infringing on their clients' privacy. Now, researchers at the Agency for Science, Technology and Research (A*STAR) Data Storage Institute in Singapore have developed a system that allows cloud storage providers to do just that.

The system, called HEDup, involves the use of a separate 'key server', which assigns a secure key to the data that will be encrypted and then uploaded for storage on the cloud's server. The service provider, such as Dropbox or Gmail, can then employ 'homomorphic encryption', which involves carrying out computations on the encrypted text, to detect information from the data's secure key. This allows the provider to determine, without actually reading the original data, whether it is a duplicate. Duplicate data will have the same key, which can only be accessed for encryption and decryption purposes by data owners.

The team tested its system and found that it increased the uploading time of a 16-megabyte file, which normally takes an average of 5.22 seconds, by 1.4 seconds. It also increased the downloading time by only 0.4 seconds.

The team next plans to improve the security of the key server and to develop a method for clients to upload and download data from multiple devices without the need for manually providing their private key for its encryption and decryption.

Provided by Agency for Science, Technology and Research (A*STAR), Singapore

Citation: The key to private and efficient data storage (2017, May 1) retrieved 27 April 2024 from https://phys.org/news/2017-05-key-private-efficient-storage.html