Credit for lock image: tuulijumala / 123rf

TAKING CONTROL BACK FROM THE CLOUD

A user-controlled file security scheme makes it possible to instantly revoke access to files hosted on Internet cloud servers.

By securing data files with a 'need-to-know' decryption key, researchers at Singapore's Agency for Science, Technology and Research (A*STAR) have developed a way to control access to cloud-hosted data in real time, adding an extra layer of security for data sharing via the Internet.

Cloud-based file storage has rapidly become one of the most popular uses of the Internet, allowing files to be safely saved in a virtual drive that is often replicated on numerous servers around the world. Cloud storage theoretically provides near-seamless backup and data redundancy, preventing data loss and also enabling files to be shared among users almost anywhere. However, proper treatment of sensitive or confidential information stored on the cloud cannot be taken for granted: the security of the cloud environment is not immune to hacker attacks or misuse by a cloud provider.

"Cloud storage services make data storage and sharing more efficient and cost-effective, but their use requires trust in the cloud's security," explains Jianying Zhou from the A*STAR Institute for Infocomm Research. "We wanted to find a way to ease the security concerns by creating a system that does not require the data owner to trust the cloud service or assume perfect protection against hacking."

The scheme Zhou and his team developed allows access to an individual file hosted on a cloud service to be issued or revoked in real time, and eliminates the possibility that files can be taken offline and accessed without authorization.

Zhou explains the process. "The file owner, Alice, generates the proxy keys, which define who can decrypt the file, for example Bob, and gives them to the cloud server. When Bob wants to access the encrypted file in the cloud, the cloud server needs to first decrypt the file for Bob using the proxy key as well as the cloud server's private key. This results in an intermediate decryption that the cloud server passes to Bob. He then uses his private key to decrypt the file to get the plaintext file. If Alice wants to revoke Bob's access, she simply informs the cloud server to remove his proxy key."

The scheme allows the data owner to retain control over file access while making use of all the other benefits of cloud hosting. Importantly, it is applicable at the per-file and per-user level, and has 'lightweight' user decryption, meaning that files can be opened quickly even on mobile devices such as smart phones.

"Our technology could be used to provide scalable and fine-grained access control to various bodies of data collected by different organizations and shared via the cloud, with applications in areas such as healthcare, finance and data-centric cloud applications," says Zhou.

Jianying Zhou | E-mail: jyzhou@i2r.a-star.edu.sg
Institute for Infocomm Research
Agency for Science, Technology and Research

Further information