User-controlled system makes it possible to instantly revoke access to files hosted on internet cloud servers

13 July 2016

By securing data files with a 'need-to-know' decryption key, A*STAR researchers 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.

"We achieved this by depositing what we call a proxy key for each authorized user on the cloud," says Zhou. "This is a partial key that also requires another revocable private key lodged with the cloud service provider to safeguard against collusion at the provider level. By requiring files to be decrypted using the two keys every time they are accessed, we can revoke a user's access instantly simply by deleting the proxy key from the cloud."

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 natural applications in areas such as healthcare, finance, and data-centric cloud applications," says Zhou.

More information: Yang, Y., Liu, J. K., Liang, K., Choo, K.-K. R. & Zhou, J. Extended proxy-assisted approach: Achieving revocable fine-grained encryption of cloud data, Computer Security ESORICS 2015, in *Lecture Notes in Computer Science* 9327, 146–166 (2015). dx.doi.org/10.1007/978-3-319-24177-7_8

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