Technology Review
PUBLISHED BY MIT

Thursday, November 12, 2009

Searching an Encrypted Cloud

Researchers are working on ways to make encrypted data easier to find.

By David Talbot

Recent advances in cryptography could mean that future cloud computing services will not only be able to encrypt documents to keep them safe in the cloud--but also make it possible to search and retrieve this information without first decrypting it, researchers say.

"This will be a challenging endeavor," says Dawn Song (http://www.cs.berkeley.edu/~dawnsong/) , a computer scientist at the University of California, Berkeley, who has made fundamental research contributions to using encrypted search strings to find encrypted documents. "However, some of these recent advances are very powerful and, if cleverly engineered and deployed, could lead to significant advances," in adding security and privacy to cloud computing over the next few years.

At the ACM Cloud Computing Security Workshop (http://crypto.cs.stonybrook.edu/ccsw09/) in Chicago tomorrow, Microsoft Research will propose a theoretical architecture (http://research.microsoft.com/en-us/people/klauter/cryptostoragerlcps.pdf) that would stitch together several cryptographic technologies in various stages of development to make the encrypted cloud more searchable. The basic idea is that cloud users could download software that would encrypt their data before it's sent into the cloud. In addition, the software would issue encrypted strings, called tokens, which can be used to check that documents are intact and--crucially--to search their contents without first having to decrypt them.

While the underlying technologies weren't developed by Microsoft, "we want to show how existing and emerging cryptographic techniques can be combined to make data in the cloud more secure," says Kristin Lauter (http://research.microsoft.com/en-us/people/klauter/) , head of the Cryptography Group at Microsoft Research, who will describe the proposal tomorrow.

While cloud computing has exploded in popularity in recent years thanks to the potential efficiency and cost savings of outsourcing the management of data and applications, a few high-profile glitches and hacks have left many potential users worried, and prompted experts to suggest that new technologies may be needed.

For example, early this year, a hacker who guessed the correct answer to a Twitter employee's security question was able to extract all of the documents stored in Twitter's "Google Apps" account. And, in March this year, a software bug led to a foul-up in the sharing privileges of Google Docs. As a result, for a small number of users (a fraction of 1 percent), choosing to share a single document instantly gave that contact access to all other shared documents, too.

Encrypted search architectures and tools have been developed by groups at several universities and companies. Though there are a variety of different approaches, most technologies encrypt data in a file--as well as tags called metadata that describe the contents of those files--and issue a master key to the user. The token used to search through encrypted data contains functions that are able to find matches to metadata attached to certain files, and then return the encrypted files to the user. Once the user has the file, he can use his master decryption "key" to decrypt it.

While some parts of these encryption processes are already mature, the technologies needed to execute encrypted search are still painfully slow because of the heavy computation involved. Unless limits are imposed on the extent of the search, conducting a general search even with a single word could take "tens of seconds" to complete, says Radu Sion (http://www.cs.sunysb.edu/~sion/) , a computer scientist at Stony Brook University in New York, who is co-chairing the cloud security workshop tomorrow. Performing searches with two or more words, if possible at all, could increase the needed computation exponentially, he adds.

Microsoft's report is an architecture proposal, and does not describe a new advance in the underlying encryption technologies. But, along with other research groups, the company's research team is working on next-generation search using more computationally efficient versions of cryptography.

"Cryptographic storage and key management are interesting areas, and we are exploring some of the technologies that are discussed on a theoretical basis in this [Microsoft] report," says Eran Feigenbaum, director of security for Google Apps. But Feigenbaum notes that it's not clear how such techniques could be used while still allowing cloud users to collaborate on documents in real-time. "There are significant implementation challenges that would need to be addressed," he added.

Still, Sion says that the new technologies and architecture proposals are badly needed. "This would be a first step to providing technologies that address the new liabilities the cloud brings," he says. "You don't want the cloud having access to your data, number one, and being subpoenaed for your data, number two. The cloud hosts all your stuff--but you don't want to shift all your liability to a lawyer in the cloud."

Boston, MA
Tuesday, November 17, 2009
www.mitxawards.org/interactive (www.mitxawards.org/interactive)

The Tough Get Growing: How to Succeed in a Down Economy (http://enterpriseforum.mit.edu/network/broadcasts/200911/index.html)
MIT Campus, Cambridge, MA
Monday, November 16, 2009
http://enterpriseforum.mit.edu/network/broadcasts/200911/index.html (http://enterpriseforum.mit.edu/network/broadcasts/200911/index.html)