# How secure is your data when it’s stored in the cloud?

As cloud storage becomes more common, data security is an increasing concern. Companies and schools have been increasing their use of services like Google Drive for some time, and lots of individual users also store files on Dropbox, Box, Amazon Drive, Microsoft OneDrive and the like. They’re no doubt concerned about keeping their information private – and millions more users might store data online if they were more certain of its security.

Data stored in the cloud is nearly always stored in an encrypted form that would need to be cracked before an intruder could read the information. But as a scholar of cloud computing and cloud security, I’ve seen that where the keys to that encryption are held varies among cloud storage services. In addition, there are relatively simple ways users can boost their own data’s security beyond what’s built into systems they use.

**Who holds the keys?**

Commercial cloud storage systems encode each user’s data with a specific encryption key. Without it, the files look like gibberish – rather than meaningful data.

But who has the key? It can be stored either by the service itself, or by individual users. Most services keep the key themselves, letting their systems see and process user data, such as indexing data for future searches. These services also access the key when a user logs in with a password, unlocking the data so the person can use it. This is much more convenient than having users keep the keys themselves.

But it is also less secure: Just like regular keys, if someone else has them, they might be stolen or misused without the data owner knowing. And some services might have flaws in their security practices that leave users’ data vulnerable.

**Letting users keep control**

A few less popular cloud services, including Mega and SpiderOak, require users to upload and download files through service-specific client applications that include encryption functions. That extra step lets users keep the encryption keys themselves. For that additional security, users forgo some functions, such as being able to search among their cloud-stored files.

These services aren’t perfect – there’s still a possibility that their own apps might be compromised or hacked, allowing an intruder to read your files either before they’re encrypted for uploading or after being downloaded and decrypted. An encrypted cloud service provider could even embed functions in its specific app that could leave data vulnerable. And, of course, if a user loses the password, the data is irretrievable.

One new mobile app says it can keep phone photos encrypted from the moment they’re taken, through transmission and storage in the cloud. Other new services may arise offering similar protection for other types of data, though users should still be on guard against the potential for information to be hijacked in the few moments after the picture is taken, before it’s encrypted and stored.

Article written by Haibin Zhang, Associate Professor of Computer Science and Electrical Engineering, University of Maryland
RSW Publishing has an agreement to republish this author’s content.
This article was originally published on The Conversation.

## Protecting yourself

To maximize cloud storage security, it’s best to combine the features of these various approaches. Before uploading data to the cloud, first encrypt it using your own encryption software. Then upload the encoded file to the cloud. To get access to the file again, log in to the service, download it and decrypt it yourself.

This, of course, prevents users from taking advantage of many cloud services, like live editing of shared documents and searching cloud-stored files. And the company providing the cloud services could still modify the data, by altering the encrypted file before you download it.

The best way to protect against that is to use authenticated encryption. This method stores not only an encrypted file, but additional metadata that lets a user detect whether the file has been modified since it was created.

Ultimately, for people who don’t want to learn how to program their own tools, there are two basic choices: Find a cloud storage service with trustworthy upload and download software that is open-source and has been validated by independent security researchers. Or use trusted open-source encryption software to encrypt your data before uploading it to the cloud; these are available for all operating systems and are generally free or very low-cost.

*Haibin Zhang does not work for, consult, own shares in or receive funding from any company or organization that would benefit from this article, and has disclosed no relevant affiliations beyond his academic appointment.*

Article written by Haibin Zhang, Associate Professor of Computer Science and Electrical Engineering, University of Maryland

RSW Publishing has an agreement to republish this author’s content.
This article was originally published on The Conversation.

Article written by Haibin Zhang, Associate Professor of Computer Science
and Electrical Engineering, University of Maryland
RSW Publishing has an agreement to republish this author’s content.
This article was originally published on The Conversation.