Cloud, backup and storage devices—how best to protect your data

March 31 2017, by Adnene Guabtni

Credit: AI-generated image (disclaimer)

We are producing more data than ever before, with more than 2.5 quintillion bytes produced every day, according to computer giant IBM. That's a staggering 2,500,000,000,000 gigabytes of data and it's growing fast.

We have never been so connected through smart phones, smart watches, laptops and all sorts of wearable technologies inundating today's marketplace. There were an estimated 6.4 billion connected "things" in 2016, up 30% from the previous year.

We are also continuously sending and receiving data over our networks. This unstoppable growth is unsustainable without some kind of smartness in the way we all produce, store, share and backup data now and in the future.

In the cloud

Cloud services play an essential role in achieving sustainable data management by easing the strain on bandwidth, storage and backup solutions.

But is the cloud paving the way to better backup services or is it rendering backup itself obsolete? And what's the trade-off in terms of data safety, and how can it be mitigated so you can safely store your data in the cloud?

The cloud is often thought of as an online backup solution that works in the background on your devices to keep your photos and documents, whether personal or work related, backed up on remote servers.

In reality, the cloud has a lot more to offer. It connects people together, helping them store and share data online and even work together online to create data collaboratively.

It also makes your data ubiquitous, so that if you lose your phone or your device fails you simply buy a new one, sign in to your cloud account and voila! – all your data are on your new device in a matter of minutes.

Do you *really* back up your data?

An important advantage of cloud-based backup services is also the automation and ease of use. With traditional backup solutions, such as using a separate drive, people often discover, a little too late, that they did not back up certain files.

Relying on the user to do backups is risky, so automating it is exactly where cloud backup is making a difference.

Cloud solutions have begun to evolve from online backup services to primary storage services. People are increasingly moving from storing their data on their device's internal storage (hard drives) to storing them directly in cloud-based repositories such as DropBox, Google Drive and Microsoft's OneDrive.

Devices such as Google's Chromebook do not use much local storage to store your data. Instead, they are part of a new trend in which everything you produce or consume on the internet, at work or at home, would come from the cloud and be stored there too.

Recently announced cloud technologies such as Google's Drive File Stream or Dropbox's Smart Sync are excellent examples of how cloud storage services are heading in a new direction with less data on the device and a bigger primary storage role for the cloud.

Here is how it works. Instead of keeping local files on your device, placeholder files (sort of empty files) are used, and the actual data are kept in the cloud and downloaded back onto the device only when needed.

Edits to the files are pushed to the cloud so that no local copy is kept on your device. This drastically reduces the risk of data leaks when a device

is lost or stolen.

So if your entire workspace is in the cloud, is backup no longer needed?

No. In fact, backup is more relevant than ever, as disasters can strike cloud providers themselves, with hacking and ransomware affecting cloud storage too.

Backup has always had the purpose of reducing risks using redundancy, by duplicating data across multiple locations. The same can apply to cloud storage which can be duplicated across multiple cloud locations or multiple cloud service providers.

Privacy matters

Yet beyond the disruption of the backup market, the number-one concern about the use of cloud services for storing user data is privacy.

Data privacy is strategically important, particularly when customer data are involved. Many privacy-related problems can happen when using the cloud.

There are concerns about the processes used by cloud providers for privacy management, which often trade privacy for convenience. There are also concerns about the technologies put in place by cloud providers to overcome privacy related issues, which are often not effective.

When it comes to technology, encryption tools protecting your sensitive data have actually been around for a long time.

Encryption works by scrambling your data with a very large digital number (called a key) that you keep secret so that only you can decrypt the data. Nobody else can decode your data without that key.

Using encryption tools to encrypt your data with your own key before transferring it into the cloud is a sensible thing to do. Some cloud service providers are now offering this option and letting you choose your own key.

Share vs encryption

But if you store data in the cloud for the purpose of sharing it with others – and that's often the precise reason that users choose to use cloud storage – then you might require a process to distribute encryption keys to multiple participants.

This is where the hassle can start. People you share data with would need to get the key too, in some way or another. Once you share that key, how would you revoke it later on? How would you prevent it from being re-shared without your consent?

More importantly, how would you keep using the collaboration features offered by cloud providers, such as Google Docs, while working on encrypted files?

These are the key challenges ahead for cloud users and providers. Solutions to those challenges would truly be game-changing.

This article was originally published on The Conversation. Read the original article.

Provided by The Conversation