Why Use MyS3

Encrypt your files on the fly and sync with Amazon cloud

Ove Bakken

Revision 2
September 7th, 2020
Norway, Innlandet

Why Use MyS3

Ove Bakken

"Even if you're not doing anything wrong, you're being watched and recorded."

- Edward Snowden
(NSA whistleblower)

Are You Too Trusting?

Are you using services like Dropbox, Google Drive, Microsoft OneDrive, etc? Do you trust them *not* to look at your personal photos, read your documents, etc? If so, why? **Don't you know that surveillance is big business, and that *your* data is the currency?**

Nobody knows what the future brings: What kind of society will we be living in? What kind of government will we have to endure? Is it (still) going to be a free country? What kind of new criminal laws will be passed? ….. So what is *your* data going to tell about you, in the future, if everything is turned upside down? Are you suddenly a suspicious person that needs to be watched 24/7? Are you even fit to be left alone, drive a car, own a gun or raise children? Can you be trusted not to do something stupid when flying? …. Anything can be cherry picked out of context, twisted around, and used against you. Race, religion, political affiliation, you name it.

Remember, **everything you upload is very likely to stay in the cloud forever. And if you think you're in control, it's only imaginary**. Legal mumbo jumbo in a terms of service (ToS) agreement, or something like GDPR, does nothing to make your data unreadable. You should instead put your trust in technical implementations that make it impossible!

Only Trust Yourself

A lot of data gathered by big corporations as well as small companies is not only acquired and accessed by civil authorities, if you peak their interest. Every time there is a data breach your data may be spread by criminals all around the world.

By the time of this writing haveibeenpwned.com has personal data from 10 194 766 818 different accounts (that's 10 billion!), gathered from 478 breached web companies.

Some companies even sell your information despite their own ToS, because they just don't give a shit. **Trying to earn profit will always impact users' privacy.** Anybody claiming otherwise is clueless, stupid or simply lying to you.

A general rule of thumb that everyone should learn to live by:

> ***"You can trust almost no one with your data if you want that same data to remain private for the rest of time, with a 0% chance of breach. You should take control yourself and make sure your data is safe."***

File Hosting Services Table

Comparison of some popular file hosting services:

Name	Client-side encryption *	Open source **	Server locations	Reputation/trustworthiness
Dropbox	No	No	USA, Germany, Australia, Japan	Good
Microsoft OneDrive	No	No	USA	Good
Google Drive	No	No	America, EU, Asia	Good
iCloud	No	No	US, Denmark, Asia	Good
MEGA	Yes	Yes	EU	Mediocre (example)
Tresorit	Yes	No	Ireland, The Netherlands	Good
Jottacloud	No	No	Norway	Good

** "Client-side encryption is the cryptographic technique of encrypting data on the sender's side, before it is transmitted to a server such as a cloud storage service."*
-https://en.wikipedia.org/wiki/Client-side_encryption

*** Open source to that extent that you can review all the relevant source code yourself.*

Take Control

Ove Bakken

One way to secure your data yourself in the cloud is by using MyS3. MyS3 is a newly developed software which makes is possible to encrypt file data on the fly and upload the output to Simple Storage Service (S3), which is part of Amazon Web Services (AWS).

Anyone can register an AWS account and create S3 buckets for file uploads. But enabling hassle free and secure file encryption is an entirely different matter. Which is why I started this project a few months ago.

AWS do of course offer cryptography for S3, but you can't trust it 100%. **Only the data owner himself should possess all the necessary pieces of information to recover his own data.** Meaning all file data has be encrypted locally *before* coming into contact with the upload API. This is basic client-side encryption which most file hosting services still lack, despite Edward Snowden exposing massive world cyber surveillance back in 2013.

To solve this MyS3 uses symmetric encryption (AES-128 GCM) before uploading anything to the AWS cloud. And the encryption key never leaves the computer.

Transparency

I'm not a cryptography expert by any means ("only" a computer engineer), but I did follow best practices regarding AES cryptography. So I trust MyS3 enough to use it myself on a daily basis, uploading all kinds of files, despite being paranoid by nature.

MyS3 is a NET Core app, so it can run on Windows, Linux, and Mac OS. And since it's open source and free for all, anyone can review and improve it. At the time of this writing I'm running MyS3 on Windows 10, CentOS 8 and Debian 10, and I love it. I've already replaced Dropbox and MEGA with it.

A few words about cost: When you use MyS3 you pay for the S3 resources that MyS3 is consuming. But not to worry, S3 has very competitive pricing. New AWS customers also get a lot for free the first year.

Open Source

If you're curious to see how MyS3 is put together go to github.com/flaskevann/MyS3.

The only code classes in MyS3 with some real action is `MyS3Runner` and `S3Wrapper`. All the rest is just boiler plate for plumbing and packaging that gives the user usability.

MyS3 is really just a simple tool that strings *other* more powerful tools together. So the source code is only a few thousand lines of code, and it's made to be easy to read.
(I prefer to write simple-stupid code; it makes it easier to get back into and to debug.)

I welcome all and any code feedback, no matter the size of the contribution. MyS3 has an MIT license so anyone can improve on it or make it their own.

Thank You

I appreciate your interest and welcome questions and feedback!

post(a)ovebakken.no