# Distributed Cloud File Storage

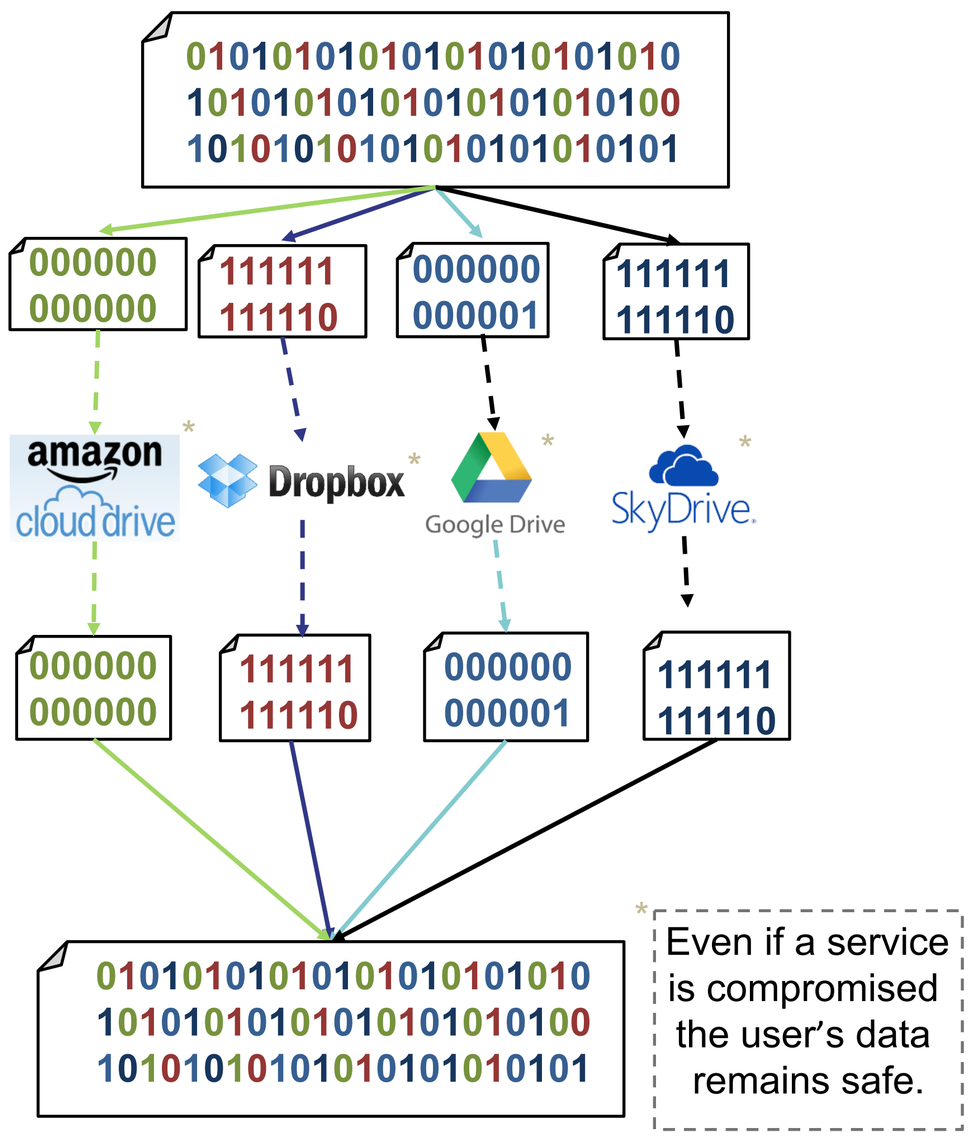
Chris Seltzer

Abstract

Gartner estimates that nearly 36% of consumer data will be stored in the cloud by the year 2016. This represents a massive increase from the 7% currently stored there. This increase in use will almost certainly come with added scrutiny. In numerous surveys consumers list security followed by storage limitations, then missing / inaccessible files as their primary concerns. These concerns can be significantly mitigated through a distributed approach. Specifically we can ensure improved security, more reliable access, and guard against failures.

## Security

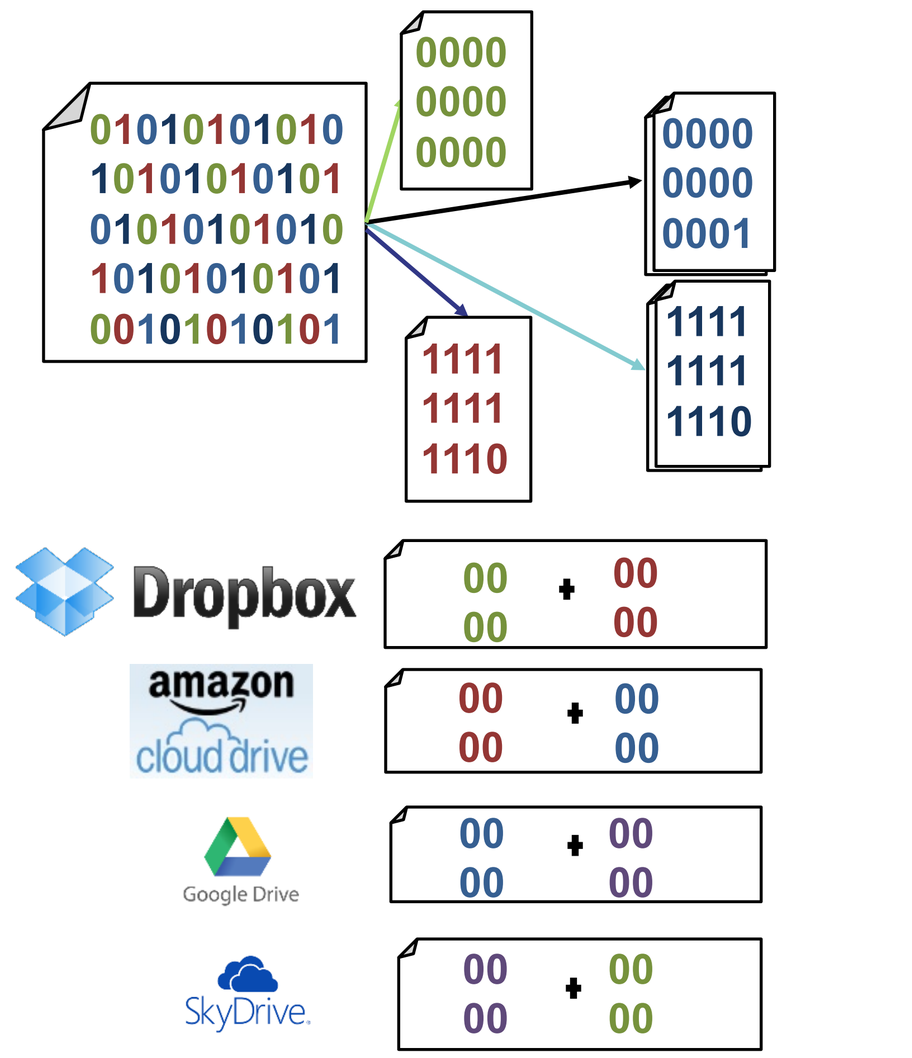
By uploading these files to different cloud storage services we can ensure that even if individual service is compromised the attacker will be unable to read the users data. The process can however still be reversed allowing the user to read their data as normal.




Even if a service is compromised the user's data remains safe.

## Loss and Inaccessibility

Consider a system (depicted below) where after breaking the original file down into 4 constituent parts; the parts are then "mixed" together, two at a time, in order to form the files which will be uploaded to the cloud services.




In this example, because we have encoded redundantly, any 3 out of the 4 pieces (and services), can be used to construct the original file. This also means protection against catastrophe and corruption. Because any 3 of the 4 services are sufficient to reconstruct the original file we also have strong error checking abilities to find the exact spot corruption occurred, and fix it.

## Related Publications

Zeng, Wenying, et al. "Research on cloud storage architecture and key technologies." *Proceedings of the 2nd International Conference on Interaction Sciences: Information Technology, Culture and Human*. ACM, 2009.

Sponsored By Cisco