CS293B - Cloud Computing
Spring 2016

Multi-Cloud Secure File Store

Secure cloud based file storage leveraging multiple cloud providers

Aviral Takkar
Darshan Maiya
Wei-Tsung Lin

Vision

File storage on the cloud is gaining momentum with almost all the big tech players having products that let you store files on the cloud. The question of security of these products is still under scrutiny and it's not uncommon to hear of successful attacks on cloud providers that resulted in a data breach.

To tackle this we propose a new secure file storage system that leverages multiple cloud providers to distribute the data in such a way that compromising of data in one of the cloud providers will not result in exposure of user data.

We will use Adi Shamir's secret sharing algorithm[1] to encrypt and split the data across multiple cloud providers and use replication to provide high availability in the face of site failures. We take into account the fact that a site may spawn a data center, a city, an entire region or a cloud provider itself.

Description

This project aims to provide "Storage as a Service" to the user. The core idea of the project is to encrypt the user data using a key generated based on user provided parameters and store the encrypted data on multiple cloud providers. The generated key is then split using the secret sharing algorithm with parts of the key being stored on different data stores in multiple cloud providers. To provide high availability not all parts of the key are required to retrieve the original key but only a predecided number of quorums would be required.

The user facing application would be hosted on a cluster running on multiple cloud providers which would together act as a controller for the entire application.

References

[1] Adi Shamir. 1979. How to share a secret. Commun. ACM 22, 11 (November 1979), 612-613. DOI=http://dx.doi.org/10.1145/359168.359176