Cryptology ePrint Archive: Report 2011/585

Iris: A Scalable Cloud File System with Efficient Integrity Checks

Emil Stefanov and Marten van Dijk and Alina Oprea and Ari Juels

Abstract: We present Iris, a practical, authenticated file system designed to support workloads from large enterprises storing data in the cloud and be resilient against potentially untrustworthy service providers. As a transparent layer enforcing strong integrity guarantees, Iris lets an enterprise tenant maintain a large file system in the cloud. In Iris, tenants obtain strong assurance not just on data integrity, but also on data freshness, as well as data retrievability in case of accidental or adversarial cloud failures.

Iris offers an architecture scalable to many clients (on the order of hundreds or even thousands) issuing operations on the file system in parallel. Iris includes new optimization and enterprise-side caching techniques specifically designed to overcome the high network latency typically experienced when accessing cloud storage. Iris also includes novel erasure coding techniques for efficient support of dynamic Proofs of Retrievability (PoR) protocols over the file system.

We describe our architecture and experimental results on a prototype version of Iris. Iris achieves end-to-end throughput of up to 260MB per second for 100 clients issuing simultaneous requests on the file system. (This limit is dictated by the available network bandwidth and maximum hard drive throughput.) We demonstrate that strong integrity protection in the cloud can be achieved with minimal performance degradation.

Category / Keywords: cloud computing, file systems, proofs of retrievability

Date: received 28 Oct 2011, last revised 14 Mar 2012

Contact author: aoprea at rsa com