

Do You Have My Data? Prove It!
(Provable Data Possession at Untrusted Stores)

Reza Curtmola
Ph.D Johns Hopkins University

Date: Feb 22nd, 2008
Time: 3:00 PM
Venue: 256 Coates Hall

ABSTRACT

Faced with cost and regulatory considerations, many companies are outsourcing the storage of their data to third parties. Outsourcing data storage achieves economies of scale for the management of storage and avoids the large initial investment to set up data centers. Recently, many such online archival systems have emerged from within the research and industrial communities.

In storage outsourcing, a client sends data to a server, which is required by contract to provide persistent archival of the data. Since the server is not trusted and may misbehave, the client typically retains a small piece of metadata which is used to verify the authenticity of the data upon its retrieval. The problem is that by the time data is retrieved, it might be already too late to recover lost or damaged data. Current systems lack a basic guarantee: Proving data possession upon a user's request (usually before data retrieval).

In this presentation we introduce a model for provable data possession (PDP) which allows a client that has stored data at an untrusted server to verify that the server possesses the original data. We present provably-secure PDP schemes that have low (or even constant) overhead at the server and minimize network communication by transmitting a small, constant, amount of data for every challenge/response. The constructs use novel homomorphic verification tags, which allow checking data possession without retrieving the data from the server and without having the server access the entire data. This revolutionizes the ability of users to outsource large data sets by providing a previously-unattainable degree of performance and scalability in verifying the health of external data repositories.

Bio

Reza Curtmola is a post doctoral researcher in the Department of Computer Science at Purdue University. He received a PhD degree in Computer Science in 2007 and a MS degree in Security Informatics in 2003, both from The Johns Hopkins University. His research focuses on applied cryptography and security aspects of wireless networks. He has previously worked as a research intern at Bell Labs Research. More information can be found at <http://www.cs.purdue.edu/homes/crix>