# Secret Sharing and Reliable Cloud Computing

Yvo Desmedt
Department of Computer Science
University College London, UK
y.desmedt@cs.ucl.ac.uk

Abstract

Today several organization, including the US Government use clouds to store important data. Indeed, the US Government now has a "cloud-first" policy (Washington Post, November 22, 2010 and April 17, 2011).

We argue that the decision to move to cloud storage does not take reliability into account. Indeed, the deliberate disconnection in Egypt (January 2011) of the internet, the accidental destruction of the cell phone network in the Fukushima area, Japan (March 2011), demonstrate the risk of using clouds for such storage. Moreover, there is no guarantee that companies involved in this storage will still exist in a few years. Indeed, DEC used to be the 2nd largest computer manufacturer in the world, but vanished after being bought by Compaq, which merged with HP.

Secret sharing is a technology that could be used to reduce the risk of aforementioned failures, while at the same time achieving privacy. The usual model assumes at most $t$ failures occur. However, this model is not realistic. Indeed, similar platforms often fail at the same time. Indeed, botnets exploit the weakness of a particular platform. Moreover, the 2006 Hengchun earthquake destroyed several international submarine communications cables at roughly the same time. Color-based color adversary structures allow to deal with this problem.

Secret sharing is also the foundation of secure multiparty computation, which is much more promising to achieve reliable cloud computing compared to homomorphic encryption. The state of the art of homomorphic encryption does not allow to use it in any reasonable application. Another application of secret sharing is Perfectly Secure Message Transmission.

Standards are definitely needed for secret sharing and verifiable secret sharing both for the case of a threshold and general adversary structure. Secure multiparty computation could be considered at a later stage.