In Clouds Shall We Trust?

The idea of cloud computing isn’t new. Viewing computing as a utility, similar to that of providing water or electricity on a for-fee basis via a shared grid-like infrastructure, dates back to at least the 1960s, with the Project on Mathematics and Computation (MAC) at MIT and the invention of timesharing. What has changed since then—those things that have enabled the dream of utility computing to come true—is the advancement of underlying technology, including cheap, fast CPUs, low-cost RAM, inexpensive storage, and the high-bandwidth standardized communication needed to efficiently move data from one point to another. In addition, considerations such as the economies of scale involved in building very large data centers nudged organizations toward cloud computing.

A recent technical report states that there is no commonly agreed upon definition of cloud computing (www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf). Instead, a definition is emerging as the various organizations that are developing cloud services evolve their offerings. In addition, there are many shades of cloud computing, each of which can be mapped into a multidimensional space with the dimensions being characteristics, service models, and deployment models (http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc).

We can argue that it isn’t a matter of whether cloud computing will become ubiquitous—because the economic forces are inescapable—but rather what we can do to improve our ability to provide direct users (for example, an insurance company that maintains client records) and indirect users (such as the insurance company’s policy holders) of cloud computing with trust in the software services and infrastructure that make up the cloud. Cloud computing providers should supply their customers with transparency into the providers’ operations to alleviate customers’ reservations about the security and privacy the cloud afforded, but how much transparency is enough? Where does customer data reside (in which cloud or clouds) and how are customer requests for services processed? Is there a tipping point at which additional levels of transparency would only serve to help malefactors compromise the services and datacenters?

In addition, as users and developers find new ways of applying cloud technologies, there will be new expectations about security and privacy. For instance, Twisted Pair Solutions of Seattle proposes to provide cloud computing resources for state and local agencies to link up disparate public safety radio systems—a novel but difficult-to-predict usage of cloud computing but also one that makes the cloud part of mission-and safety-critical systems (www.fcw.com/Articles/2009/04/16/Cloud-computing-moving-into-public-safety-realm.aspx). The expectations for security, privacy, reliability, and so on will be different in some respects for voice-over-IP (VoIP) radio systems than for social networking aspects of the cloud. This raises the question: how do we manage risk when we don’t fully understand what we’re trying to protect or guard against?

Cloud computing’s fluid nature makes it a moving target when even trying to determine what questions we should be asking regarding trust. However, we can ask fundamental questions like: are the architectures we have adequate for building trusted clouds, and, if not, what types of software system architectures do we need? Consider, for instance, the possibility that an organization might opt to fully outsource its computing infrastructure and datacenter to the cloud, retaining only thin clients within the organization. How do we make the thin client user terminals secure?

The growing importance of cloud computing makes it increasingly imperative that we grapple with the meaning of trust in the cloud and how the customer, provider, and society in general establish that trust. Look for the themed issue of IEEE Security & Privacy on cloud computing to appear in November/December 2010.