# Dependability in the Cloud: Challenges and Opportunities

**Moderator:**
Kaustubh R. Joshi
*Senior Member of Technical Staff, A&T Labs – Research,*
*180 Park Ave, Florham Park, NJ, 07932, USA*
*kaustubh@research.att.com*

**Panelists:**
Guy Bunker
*Chief Scientist and Distinguished Engineer, Symantec Corporation,*
*350 Brook Dr., Green Park, Reading Berkshire, RG2 6UH, UK*
*guy_bunker@symantec.com*

Farnam Jahanian
*Prof. and Chair for CSE, Dept. of EECS, Univ. of Michigan, and Founder, Arbor Networks*
*CSE Bldg., Rm. 3713, 2260 Hayward St., Ann Arbor, MI 48109-2121, USA*
*farnam@umich.edu*

Aad van Moorsel
*Reader, School of Computing Sci., Newcastle University,*
*Newcastle upon Tyne, NE1 7RU, UK*
*aad.vanmoorsel@ncl.ac.uk*

Joseph Weinman
*Executive Director, AT&T Business Solutions,*
*One AT&T Way, Rm. 4D128, Bedminster, NJ 07921, USA*
*jbweinman@att.com*

## Synopsis

Cloud based infrastructures are rapidly becoming a destination of choice to host a variety of applications ranging from high availability enterprise services and online TV stations, to batch oriented scientific computations. With investments of billions of dollars, the fortunes of dozens of companies, and major research initiatives staked on its success, it is clear that cloud computing is here to stay. However, it is not yet clear whether cloud services can be a dependable alternative to dedicated infrastructure. On one hand, availability and privacy are serious challenges for applications hosted on cloud infrastructure. On the other hand, a cloud provider's economies of scale allow levels of investment in redundancy and dependability that are difficult to match for smaller operators. Furthermore, the ability to monitor large numbers of applications can enable "wisdom of crowds" approaches to provide enhanced security much in the same way that network providers have been able to do with worms and DDoS attacks. The panel will discuss new dependability related challenges and opportunities that arise in the context of cloud computing, some examples of which are as follows.

## 1. Challenges

• An environment with a few large cloud infrastructure providers not only increases the risk of

common mode outages affecting a large number of applications, but also provides highly visible targets for attackers. Community driven sites such as [1] track outages in major cloud providers and have documented a number of outages and security vulnerabilities over the last two years affecting hundreds of Internet sites.

• Sharing of cloud resources by entities that engage in a wide range of behaviors and employ best practices to varying degrees can expose cloud applications to increased risk levels. For example, on April 26 2008, Amazon's Elastic Cloud (EC2) had an outage [2] across several instances due to a single customer applying a very large set of unusual firewall rules and instantiating a large number of instances at the same time, thereby triggering a performance degradation bug in Amazon's distributed firewall.

• Multiple administrative domains between the application and infrastructure operators reduces end-to-end system visibility and error propagation information, thus making problem detection and diagnosis very difficult. Additionally, for competitive reasons, cloud infrastructure providers may not provide full disclosure regarding the cause of outages or other detailed infrastructure design information, raising the question of the verifiability of claims regarding dependability.

• The hosting of data on outsourced and shared infrastructure that may be in a different legal jurisdiction than the owner of the data has serious legal and privacy implications. Corporate accountability legislation such as the Sarbanes-Oxley Act (SOX) of 2002 and privacy clauses included in legislation such as the Health Insurance Portability and Accountability Act (HIPAA) of 1996 and the Telecommunications Act of 1996 create obstacles to the applicability of cloud solutions in the financial, healthcare, and telecom industries. For example, BusinessWeek reported in Aug 2008 [3] that ITricity, a European provider of cloud computing capacity, couldn't offer services to such companies until it began offering owner hosted private cloud services. The recently formed industrial consortium called the Cloud Security Alliance [4] includes in its charter several issues regarding the interplay of cloud computing and legal requirements.

## 2. Opportunities

• Cloud computing enables economies of scale leading to large redundancy levels and wide geographical footprints. For example, Amazon's EC2 currently supports two regions in the US and Europe, each split into independent "availability zones", while AT&T's Synaptic cloud computing offering provides five "super IDCs" located across the world. These can be leveraged through techniques such as virtual machine migration and cloning to provide better fault tolerance and disaster recovery, especially for operators of smaller applications that may not have been able to afford such capabilities.

• New security and reliability services can be enabled or strengthened by virtue of being located in the cloud. For example, popular cloud-based email services such as Gmail amplify manual feedback from some users to provide automatic spam filtering for all users. Oberheide et. al. describe in [5] a cloud-based antivirus solution that can not only utilize multiple vendors to provide better coverage, but also compares data blocks across users to improve efficiency and provides an archival service for forensic analysis.

• Managed cloud services that include OS level support can result in improved reliability and security due to consistent centralized administration and timely application of patches and upgrades.

## 3. References


[1] Cloud Computing Incidents Database. *World Wide Web,* http://wiki.cloudcommunity.org/wiki/CloudComputing:Incidents_Database.

[2] Amazon Web Services Discussion Forums. *World Wide Web,* http://developer.amazonwebservices.com/connect/thread.jspa?threadID=21401&tstart=15.

[3] Rachael King. How Cloud Computing Is Changing the World. *In Businessweek on the World Wide Web,* http://www.businessweek.com/technology/content/aug2008/tc2008082_445669.htm. Aug 4, 2008.

[4] Cloud Security Alliance. *World Wide Web,* http://www.cloudsecurityalliance.org.

[5] J. Oberheide, E. Cooke, and F. Jahanian. CloudAV: N-Version Antivirus in the Network Cloud. *In the Proc. of the 17th USENIX Security Symposium.* July 2008.