ARINC

White Paper

Cyber Clouds and Cloud Computing 101

Exactly what is a cyber "cloud?" The term "cloud" is as nebulous as the term "cyber" for many people.

However, much like savvy marketing professionals use the term ***cyber*** to mean almost any service, infrastructure or system that touches or runs over the internet, there has also been an effort by industry professionals to change the vernacular of their managed services under the umbrella of ***cloud***-computing.

Some industry experts believe the term "cloud" is an over-used descriptor. Some industry leaders say that the over-hyped term refers to nothing more than computers attached to "networks" while others disagree. Regardless, as technology matures, whatever it is called, the more prevalent term—cloud—seems to be the future for computing in the 21st century.

The National Institute for Standards and Technology (NIST) believes that cloud computing is still an evolving term and that it will continue to be debated and defined by those in both public and private sectors. NIST admits that the cloud computing industry represents a large ecosystem of many different models, vendors, and market niches. To try to bring about a common understanding, NIST developed a cloud computing definition to encompass all of the various cloud approaches, as follows:

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.[i]

Thus, a computing cloud model promotes availability and is composed of essential characteristics, service and deployment models. To illustrate how one may better be able to relate to cloud computing at a basic level, I offer an analogy of how we use electricity in our homes today.

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources.

Most people do not have the equipment, knowledge or ability to produce electricity at home. We do not have diesel turbines, gas generators, fuel storage or the "know how" to power our electronic devices, heat/cool our homes, or keep the lights on. Why? Because, our power company provides a "cloud service" for us.

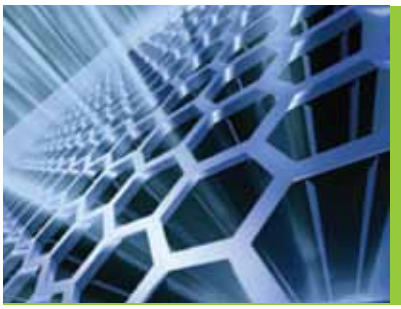
We rely on our electricity provider to build the infrastructure necessary to produce energy, maintain a supply of fuel to keep the generators producing, and supply the resulting energy to our homes for our use whenever we need it. It's a service model with which we simply plug our devices in and use the energy we need. The electric company tracks our usage and then bills us for the exact amount we use from month to month.

In a similar fashion, cloud computing providers build and maintain the infrastructure (servers, storage, applications, etc.) that allows us to plug our computers into the cloud to use various services via the internet. Cloud computing, therefore, alleviates the need for us to buy the hardware necessary to run certain applications, store large amounts of data, or even concern ourselves with the software upgrades necessary to manipulate and protect our information. We can access the "cloud" whenever we want and do not need to know the complexities of how our information is moved, stored or protected.

Cloud computing providers, like the electric company, pool together resources, offer something "on demand," and provide broad, measured access to its users. In this regard, the term "cloud" is just a metaphor to describe complex system processes about which the typical user does not need to understand in order to use it.

However, while the typical person may not need to understand how an electric grid may work, when it comes to your own personal, private and/or proprietary data, future cloud computing users should be aware of the inherent risks associated with relying on others to manage their systems and handle their data. Individuals, companies or government organizations considering cyber cloud computing need to gauge their willingness to accept the risk of their data being compromised, lost or stolen.

Chief among security concerns in the cloud environment are the human factors. A cloud administrator has privileged insider access to your data. As technology develops and more people join the cloud computing environment, a smaller number of people are likely to have access to a greater amount of hosted data



and systems. As evidenced with the WikiLeaks case, this would make the security risk of insider attacks more devastating.

Another area not discussed in great detail, concerns the current laws regarding the protection and use of data. In an ever-shrinking virtual world, the laws that protect private data in one country may not be the same in another, where data could be stored or manipulated. A largely unexplored area of the law concerns liability aspects of cyber security and who is responsible for lost or stolen data in the cloud computing environment.

So, what does the future hold? Most experts agree that, even with these security unknowns, that a shift will take place within the next decade with most people migrating away from PC-based applications to those hosted in cloud environments. A sign of this is the explosion of cloud-based social networking sites like *Facebook* (over 500 million users globally) and webmail services like *Hotmail* and *Yahoo* mail.

Due to concerns about security and data control, some larger corporations might be slower in becoming totally reliant on cloud computing. However, the shift will continue because the real "driver" in the move to cloud computing is in the numbers. The cost savings realized in moving towards cloud computing will motivate increasing numbers of CEO's and Government leaders alike, to move to cloud environments.

ARINC
2551 Riva Road | Annapolis, MD 21401 USA
Tel: +1 800.633.6882

© 2011 ARINC Incorporated. All rights reserved. 03/11

Attachment—
NIST-defined Cloud Computing Characteristics and Models[ii]

Characteristics:

- **On-demand self-service**—A consumer can access data time and storage whenever they want by themselves.
- **Broad network access**—Capabilities are available over the network and accessed through standard mechanisms that promote use by mobile phones, laptops, PDAs, etc.
- **Resource pooling**—The provider's computing resources are pooled to serve multiple consumers according to each consumer's demand.
- **Rapid elasticity**—Capabilities can be rapidly and automatically scaled to fit their needs in any quantity and at any time.
- **Measured Service**—Cloud systems automatically controlled and optimized. Resource usage can be monitored, controlled, and reported providing transparency for both the provider and consumer of the utilized service.

Service Models:

- **Cloud Software as a Service (SaaS)**—The consumer uses a provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure.
- **Cloud Platform as a Service (PaaS)**—The consumer can deploy their own applications onto the cloud infrastructure. The consumer does not manage or control the underlying cloud infrastructure, but has control over the applications they deploy.
- **Cloud Infrastructure as a Service (IaaS)**—The consumer can provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over everything else.

Deployment Models:

- **Private cloud**—The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.
- **Community cloud**—The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements,

policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.

- **Public cloud**—The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.

- **Hybrid cloud**—The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).

---

[i] Peter Mell and Timothy Grance; Special Publication 800-145 (Draft) titled The NIST Definition of Cloud Computing (Draft), National Institute of Standards and Technology (U.S. Department of Commerce); January, 2011.

[ii] Ibid.