A Futuristic Look at Cloud Computing Security

E. Eugene Schultz, Ph.D., CISSP, CISM

Abstract

The term "cloud computing" means different things to different individuals, and cloud computing is by no means new. Despite confusion and misconceptions related to cloud computing, this type of computing is currently immensely popular and is being used to substantially reduce the financial cost and complexity of computing, as well as for other reasons. Cloud service providers (CSPs) offer three basic types of services: Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS). Although cloud services offer many benefits, they are also beset with security risks, the most serious of which currently are inadequate security for data stored in the cloud, restricted ability to conduct adequate audits in cloud environment, and unavailability of cloud services. Because of deficiencies both in cloud and Internet security, costly cloud-related security incidents will start to occur increasingly, and when they do, they will not only greatly diminish the popularity of cloud services, but will also prompt extensive security-related changes in cloud processes and mechanisms that are described in this paper. Ultimately, the greatest risk to be addressed in cloud computing is the fact that cloud services are delivered over the Internet, which is becoming increasingly vulnerable to denial of service (DoS) attacks.

Introduction

There is no general agreement concerning exactly what the term "cloud computing" means. Wikipedia provides a somewhat suitable definition by defining cloud computing as:

> "…the provision of dynamically scalable and often virtualized resources as a service over the Internet on a utility basis. Users need not have knowledge of, expertise in, or control over the technology infrastructure in the 'cloud' that supports them" (WIKI09).

According to Mather, Kumaraswamy and Latif (MATH09), common characteristics of cloud computing include:

- Shared resources—at various levels (e.g., application, host, network, and so on)
- Massive scalability—in use of systems, network bandwidth and storage space
- Elasticity—cloud users can obtain more or fewer resources at will
- "Pay as you go"—users have to pay for only what they use
- Self-provisioning of resources—users can select what they need

Some people compare cloud computing to the way people and organizations obtain electricity. They could in theory have their facilities connected to a specific source of electricity, but there are many limitations in doing so. A much better alternative is connecting to the electrical grid. No one who does so knows exactly where the electricity that is delivered comes from, but the origin does not really matter anyway.

Although cloud computing is currently riding a wave of immense popularity, the notion of cloud computing (and in particular, the name "cloud computing") is at the same time being severely criticized by leading thinkers in the computing and IT arenas. For example, Larry Ellison, the CEO of Oracle, has stated that cloud computing is simply "everything that we currently do." There is much truth to what Ellison says—widely used Internet services such as Google searches and Yahoo email are in reality cloud services that have existed years before anyone coined the termed "cloud computing." In fact, cloud

computing services have actually existed for decades, with the widespread use of grid computing in high energy physics research being one of the best examples. Additionally, thinking about cloud computing is too often characterized by a kind of vagueness that is not usually tolerated in the otherwise precision- and detail-oriented computer science arena.

Benefits of Cloud Computing

Regardless of pitfalls associated with the meaning of "cloud computing," this form of computing is likely to be around for a long time. Too many benefits associated with cloud computing exist for it to fall by the wayside. Major benefits of cloud computing include:

- Financial cost savings (often substantial) resulting from paying only for resources that are actually used,
- Improved computing and network performance as the result of cloud providers delivering the needed performance,
- Scalability of services and operations because customers have the ability to select how much of what they need at each particular point in time,
- On demand services—cloud customers can get what they want when they want it (usually),
- Simplification of IT solutions—details and complexities of IT solutions can be handled by cloud providers, not cloud users, and
- Others.

Types of Cloud Computing

Three types of cloud computing currently exist. They are:

- Software-as-a-Service (SaaS). In this type of cloud computing a complete software application is provided to end users over the Web. Software is hosted on the provider's platform(s) or downloaded to client's platform(s). This typically involves a subscription fee or per-usage pricing model. Examples include Salesforce.com and Zoho.

- Infrastructure-as-a-Service (IaaS). IaaS involves providing fundamental IT resources (i.e., power, storage and memory) via a network (e.g., the Internet). It is based on virtualization and "virtualized infrastructure stacks," and usually involves a subscription or per-usage (based on resources used) pricing scheme. Examples include Amazon Web Services, Flexiscale and GoGrid.

- Platform-as-a-Service (PaaS) (sometimes also called "cloudware"). This includes Web-based development tools such as Integrated Development Environment (IDE), a run-time application platform that allows applications to run in the cloud (normally on top of IaaS and provided as SaaS). PaaS precludes the need to buy and manage necessary software and hardware throughout the Software Development Life Cycle (SDLC).

Cloud-related Security Risks

As attractive as cloud services might seem, organizations are impetuously "rushing to the cloud" without carefully considering the range and magnitude of the potential costs involved. Among the most serious of the costs are security-related risks. Cloud service customers too often assume that if they subscribe to a cloud service, a suitable level of security will somehow be provided. Nothing is farther from the truth. Numerous potentially serious security risks are typically present in cloud computing. Lamentably, once an organization is "in the cloud," the organization is for the most part at the mercy of CSPs when it comes

to security risk management. (The best analogy is valet parking at a fancy restaurant or hotel—once you hand over the keys to the attendant, you lose control of your car, although you may be able to persuade the attendant to be especially careful with your car by tipping this person.) All agreements are subject to negotiation; cloud services are no exception. Cloud contract negotiations can thus include as much security (or possibly also the ability for the customer to take direct control of cloud services) for which the customer is willing to pay.

Of all of the cloud-related security risks, the three currently most critical ones are:

- Inadequate security for data stored in the cloud. Cloud customers can obtain low cost data storage services through IaaS. At the same time, however, customers usually lose direct control over data security. For example, are data protected by stringent access controls and strong encryption? And if encryption is in place, does an effective key management process exist, and if it does, is it secure? Additionally, exactly where do cloud providers store an organization's data? Are the data are co-mingled with other organizations' data wherever they are stored? Are the virtualized environments, databases, and storage area networks (SANs) in which data are stored up to date with respect to patches for vulnerabilities? The same applies to data that are entered, stored and processed in SaaS. The privacy implications in connection with data about individuals being entered, stored and processed in the cloud are also very serious.[1] Wright asserts that privacy of data is at risk not only because a number of CSP employees may be able to gain access to cloud-stored and -processed customer data, but also because of the fact that data must be sent to the CSP, introducing the risk that someone else may gain access to the data while they are in transit (WRIG10). He suggests the principle of data minimization, that is, only the minimum amount of data needed for a cloud services should be gathered, stored, accessed, and/or shared, as the best control against cloud-related privacy risks.

- Unavailability of cloud services due to denial of service attacks. Perpetrators are perpetually creating and building up botnets designed not only to make money for the botnet owners by releasing volumes of spam messages, but also by launching massive distributed denial of service (DDoS) attacks. Examples include the Bredolab botnet that caused DoS for well over 700,000 Facebook users last October, the DDoS attacks against Estonia and Georgia that brought computing in both countries to a standstill, the persistent attacks ostensibly from North Korea against South Korea and the United States, "Mafia Boy's" DDoS attacks against eBay, eTrade, ZDnet, Amazon, and others, and many others. Some perpetrators have even targeted the Internet infrastructure; on three occasions, they targeted root Domain Name System (DNS) servers and came frightfully close to cause the Internet itself to slow down to a crawl. Additionally, perpetrators are constantly exploring new ways to cause reduced availability of computing resources such as Web-based services and to crash target hosts. The recent round of attacks in which perpetrators flooded Web servers in several countries with SSL, not HTML connections, to consume more Web server resources provides an excellent example of the use of new types of attacks of this nature.

- Restricted ability to conduct adequate audits in cloud environments. In traditional computing settings, auditors randomly sample servers, workstations, and network and storage devices that they will examine during the audit. They then interview owners and system and network administrators and inspect settings on these systems and devices by asking administrators to

[1] Privacy-related risks in cloud data storage also create many serious obstacles to achieving compliance with regulations such as the EU Data Privacy Act and the PCI-DSS standard.

display configuration settings and logs. The cloud virtually makes following traditional auditing procedures impossible. Auditors may be able to ask questions of CSP staff members and may even be able to have them remotely show certain settings and log entries, but not much more. Whatever staff members do must to cooperate with an audit must be pre-negotiated in a service contract. Additionally, there is no guarantee that auditors' observations and findings will be valid. It is, after all, generally much easier to deceive and mislead auditors in cloud environments than in conventional ones.

Cloud Computing in the Future

Experts predict that cloud service offerings will in the future substantially expand and that subscribership to these services will grow accordingly (GEEL09). Among the many predictions are the following:

1. Entry of an increasing number of large vendors into the cloud computing arena,
2. Major IDE providers will soon make their services available in the cloud,
3. The entry cost of cloud services will continue to diminish, leading to an accelerating increase in the number of new cloud service customers,
4. PaaS will greatly increase in popularity, and
5. Organizations will continually explore new ways to use cloud computing to reduce IT costs.

Sadly, however, most predictions concerning cloud computing in the future do not include any consideration whatsoever for security. Cloud computing enthusiasts continue to get wrapped up in the cloud frenzy without concern for the potential for and consequences of compromises of confidentiality and integrity as well as loss of availability of services in the cloud environment.

Cloud Security in the Future

As stated previously, cloud computing gives rise to many security risks, most of which are currently overlooked by cloud enthusiasts. As such, cloud computing is likely to continue to greatly expand, at least to a point, without suitable security controls. Consequently, cloud-related security incidents will also proliferate. The two most likely types of incidents will be data security breaches and unavailability of services. The latter is currently not too large of a risk, but it will greatly grow in magnitude because *the weakest link by far with respect to availability of cloud services is the Internet*. But the Internet is rapidly spinning out of control. With little or no intrinsic security built into many Internet mechanisms and protocols, the Internet has become an efficient and convenient conduit for computer criminals and espionage agents to launch highly productive and often financially profitable attacks. Many attacks have at the same time become much more stealthy and effective over time (SCHU09). Perpetrators are constantly exploring new ways to cause reduced availability of computing resources such as Web-based services and to crash target hosts. The recent round of attacks in which perpetrators flooded Web servers in different countries with SSL, not HTML connections, to consume more Web server resources provides an excellent example of the use of new types of attacks of this nature.

Although the cloud community has largely overlooked security considerations in cloud computing, several security-positive cloud-related developments are progressing well. The Cloud Security Alliance (CSA) is, for example, working on a set of security standards for cloud computing. Although many organizations will initially ignore whatever standards the CSA develops and approves, these standards will eventually establish a standard of due care that will leave organizations that ignore them liable to all kinds of litigation resulting from cloud data security breaches and other kinds of cloud incidents that will inevitably occur. Also, efforts to establish a level of security assurance for CSPs are well underway. The result is likely to be something similar to the WebTrust and SysTrust "seal of approval" for Web sites and systems, respectively. Once this mechanism is available, potential cloud service customers will be able to

make more informed decisions concerning which CSPs are and are not likely to provide needed levels of security and privacy in their services.

What will happen to cloud computing over time?

- Cloud customers will experience a growing number of costly data security breaches. CSPs will attempt to provide and/or improve security mechanisms for cloud data-at-rest and cloud data-in-motion, but from a security perspective, the perpetrator community is already very far ahead of CSPs, who are for the most part barely getting started when it comes to cloud security. Faced with increasing financial loss, compliance violations, and a myriad of class action and other lawsuits by individuals whose personal and financial information has been compromised, organizations will start to seriously reexamine the cost-benefit ratio of cloud computing. Cloud hysteria will greatly subside.

- The Internet will come to a standstill and will not be available for days (SCHU08). A very large number of systems infected with bots will flood the Internet with anomalous traffic such as volumes of fragmented IP packets. Internet Service Provider (ISP) networks everywhere will be affected. Gigantic pipes along some parts of the Internet will be able to move traffic, but volumes of packets to routers will overwhelm them. Consequently, links and routers that connect the infrastructure will crash or become unresponsive, and/or legitimate traffic will be disrupted such that the quality of Internet service will become intolerable. When this happens, total disruption of cloud services will occur. Loss figures will be staggering, with the amount of loss for each cloud customer depending on how effective its business continuity/disaster recovery procedures are. Many medium and small companies that rely on 24 X 7 cloud connectivity will go out of business. These events will ultimately lead to a widespread loss of trust in cloud services and a turning back to more traditional IT services. Cloud services will not disappear, however. CSPs will frantically rush to find new ways to deliver services, even if the Internet totally fails. Likely outcomes include:

  - Greater regionalization of cloud services to increase ability to shut out massive amounts of DoS traffic originating from other parts of the world.
  - Creation of new WAN pipes that are independent of the Internet, so that the most critical cloud services will be continuously available even if the Internet goes completely down for a while.
  - More integration of CSP-provided business continuity and disaster recovery capabilities with mainstream cloud services.
  - Well-funded efforts to increase the resilience of the Internet itself.

Conclusion

Cloud computing is much like outsourcing and offshoring in that both allow an organization to set up service-level agreements (SLAs) and/or statements of work (SOWs) to obtain desired services at a specified level. In reality, cloud computing and outsourcing/offshoring also involve many of the same security issues—customers do not know exactly where and how services are being provided, but cost savings are being achieved. Cloud computing (again, just like outsourcing) is becoming increasingly popular, but a proverbial time bomb is ticking. Because CSPs are hastily rollout out cloud services to cash in on the cloud frenzy, cloud services as we know them are almost certainly permeated with security vulnerabilities of which cloud service customers are for the most part unaware. Catastrophic and widespread cloud security and privacy incidents are inevitable, and when they occur, they will not only diminish the popularity of cloud computing, but they will also serve as strong catalysts for improving security in cloud services. Unfortunately, changes that are made will for the most part require retrofitting

existing cloud processes and mechanisms, because for the most part, security is not being built into them. The result will be greater than necessary financial cost and lowered effectiveness of the new or improved cloud security processes and mechanisms. But the most serious security problem to be faced is that *between every cloud service and customer is a common link—the Internet.* The Internet is more than sufficient for exchanging email among friends, social networking, obtaining information from search engines, and other casual, recreational functions, but not high-stake business functions that are critically dependent on 24 X 7 availability. Availability-related risks associated with the Internet are growing to the point that a complete outage or catastrophic, prolonged slowdown is now inevitable. Realizing this might prompt some cloud-frenzied individuals and organizations to adopt a more realistic approach to cloud computing.

REFERENCES

GEEL09 Geelan, Jeremy, "The Future of Cloud Computing." 18 January 2009. http://cloudcomputing.sys-con.com/node/771947

SCHU08 Schultz, Eugene, "July 18, 2008: The day the Internet died." Presentation at RSA Conference, San Francisco, CA, 8 April 2008.

SCHU09 Schultz, Eugene, "The new intrusion detection." Presentation at ISACA Information Security Risk Management Conference, Amsterdam, The Netherlands, 9 November 2009.

WIKI09 Wikipedia, "Cloud Computing," 2009. en.wikipedia.org/wiki/Cloud_computing

WRIG10 Wright, Joss, "On the Privacy Implications of Cloud Computing." Proceedings of the International Security Summit, May, 2010.