ASA

Annie Searle & Associates LLC

Research Note

Cloud Computing and Cyber Threats

By Andrew H. R. Hansen

Keywords: cloud computing, SaaS, IaaS, PaaS, cyber security, cyber threats

Abstract – Cloud computing is a trend which appears poised to play a prominent role in business operations in the future. The potential benefit of the cloud offers desirable features for both businesses and the standard Internet user. The primary cloud frameworks include Software-as-a-Service, Platform-as-a-Service and Infrastructure-as-a-Service. Businesses should take the time to research the cloud solution best fitted for their business strategy. Like all networked computers, cloud computing is subject to malicious behaviors. Businesses need to be educated of the types of cyber threats associated with their cloud solution and mitigate these threats with appropriate remediation.

Introduction

Renowned scholar, consultant and author Warren G. Bennis once published an article in which he quoted legendary hockey player Wayne Gretzky as saying, "It's not where the puck is, it's where the puck will be." [1] Imitating this statement, over the past two decades businesses have chased the rapidly advancing trends in technology with the hopeful intent of correctly projecting where technology – and subsequently, the profits – will be. One particular trend that has been gaining traction and appears to have staying power is cloud computing. This article will outline the basics of cloud computing, identify the major frameworks, discuss the cloud decision and describe several cyber threats associated with cloud computing.

Cloud Computing Basics

Whether they realize it or not, the majority of Internet users have already participated in cloud computing.[2] Examples of common cloud computing behaviors include accessing web-based email, participating in discussion forums or social networking, or using photo sharing websites.[3] The basic theory behind cloud computing is that alternative to storing and retrieving data on our own computers, that same data can be stored on a computer in the "cloud," making it accessible from any device with Internet access.[4] The term "cloud" originated in the

early days of network design. As network engineers started connecting to networks outside of their domain, they realized they lacked the details of these outside networks.[5] "They needed a way to indicate that there is a network, but also indicate that they weren't trying to describe it, that it was more than they know. They landed on the cloud as a symbol of this unknown domain."[6]

For the standard web user, cloud computing will offer an array of enticing possibilities. "Imagine being able to share… photos, movies, contacts, e-mails, documents etc. – with your friends, family, and coworkers in an instant." [7] In a business context, cloud computing offers different but equally intriguing opportunities. **Harvard Business Review** describes the potential business benefits in this way,

> "Rather than house your own IT servers or rent the maximum processing and storage capacity you'll ever need, why not pay only for what you use, when you use it? That's the basic idea behind cloud computing – and it's an alluring possibility for many reasons, not least the desire to contain costs and reduce energy consumption."[8]

According to the first Cisco Global Cloud Index, global cloud computing traffic is expected to rise an astonishing 1200 percent by 2015.[9] One major organization that will likely contribute to this statistic

is the United States Federal government, who recently instated a "cloud first policy… Intended to accelerate the pace at which the government will realize the value of cloud."[10] Researcher Robert L. Grossman at the University of Illinois at Chicago echoes some of the positive implications of cloud computing mentioned above by claiming the increased focus on cloud computing has been fueled by three important factors: scalability, simplicity, and pricing.[11] Each of these attributes has the potential to give an organization a competitive advantage.

Included in the discussion of basic cloud computing, concepts, the difference between private and hosted clouds should also be illuminated. A *private cloud* is "devoted to a single organization's internal use; it might be run by the organization itself or outsourced to a third party to operate." [12] Whereas a *public* or *hosted cloud* is "managed by another organization that provides cloud services to a variety of third-party clients."[13] Hybrids of these cloud frameworks can also be implemented.

Cloud Computing Frameworks

Although the precise number of cloud frameworks varies depending on the source, in their book "Cloud Security and Privacy,"

industry experts Tim Mather, Subra Kumaraswamy and Shahed Latif identify a "commonly agreed upon framework for describing cloud computing services," which goes by the acronym "SPI."[14] As illustrated in **Figure One** [15] SPI stands for Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS).[16] The services offered by each of these frameworks will be discussed below.

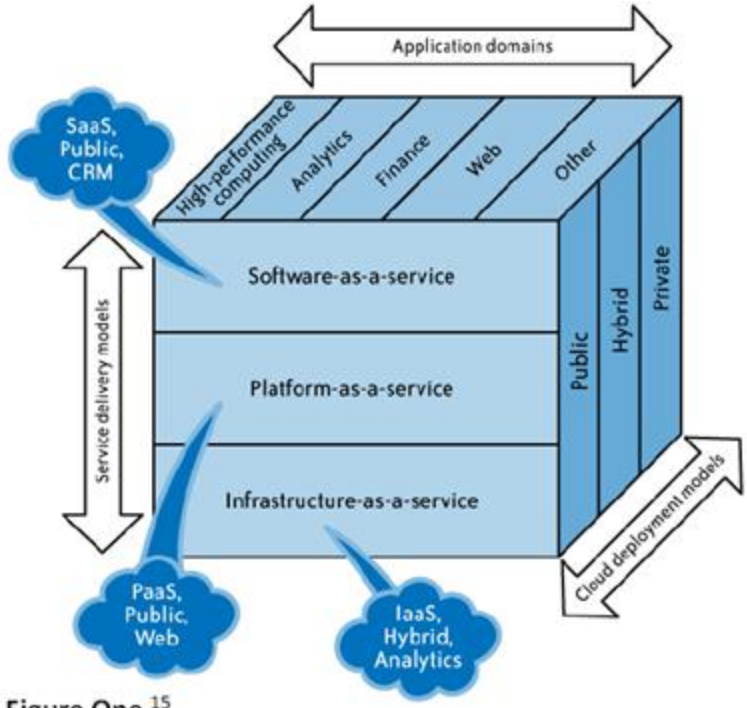

Figure One [15]

Software-as-a-Service (SaaS)

Under the SaaS model, the customer will bypass the traditional purchasing of a software license agreement, and instead they will essentially rent a subscription or get pay-per-use access to software in the cloud.[17] A Customer Relationship Management service like SalesForce is a good example of SaaS.[18] Some characteristics of SaaS include:

- A typical SaaS deployment does not require any additional hardware and can be run via a web browser

- Through outsourcing, the cost of application software licensing, servers, and other infrastructure and personnel costs are reduced
- SaaS enables software vendors to control and limit use, and prohibit the illegal copying and distribution of their software [19]

Platform-as-a-Service (PaaS)

In a PaaS model, "the vendor offers a development environment to application developers, who develop applications and offer those services through the provider's platform."[20] Windows Azure from Microsoft is a good example of the PaaS model.[21] Additional characteristics of PaaS include:

- Developers use pre-defined blocks of code and the vendor's development environment to create applications
- Offers general developers the ability to build web applications without needing specialized expertise
- Developers can often build web applications without installing any tools on their computer
- Provides a low cost entry, which greatly increases the number of applications created. [22]

Infrastructure-as-a-Service (IaaS)

IaaS has been compared to utility computing, as the service provider provides the infrastructure and the customer pays for the actual amount of processing power, disk space, etc. that they actually consume.[23] "From the IaaS provider's perspective, it can build an infrastructure that handles the peaks and troughs of its customers'

demands and add new capacity as the overall demand increases." [24]

Amazon's Elastic Compute Cloud is an example of this model.[25]

Additional characteristics of IaaS include:

- The ability to scale infrastructure needs in near-real-time based upon usage requirements
- Customers can purchase the exact amount of infrastructure required at any specific time
- In some cases the IaaS vendor will provide application support, application development, and enhancements
- Access to high quality IT talent for a fraction of the cost.[26]

The Cloud Decision

Each of the three frameworks described above have the ability to provide unique advantages to business of all sizes. But the decision to move to the cloud is not one that should be taken lightly. Business managers and others considering moving to the cloud should take the time to understand which model and which types of services would best suit their business needs. Possible good candidates for moving to the cloud might include a small-to-medium-sized business with a distributed workforce, or a business with customers that need to access their growing databases. Smaller businesses may find that the costs of supporting multiple servers and the IT expertise required to manage them is reduced by a move to the cloud. Similarly, a growing business

with a rapidly expanding sales team might be a good candidate for a cloud-based application that manages their clientele.

Companies should not be afraid to start small. "Cloud computing is a different way of working from what most people are used to, and building familiarity and trust takes time."[27] Starting small with a pilot program, before moving forward with a full implementation is likely a wise strategy. Further, organizations should not force their business strategy to fit into the cloud models. Alternatively, "consider what type of cloud would best fit your current operations and enhance your IT strategy."[28]

Security Concerns

While there are definitely benefits associated with cloud computing, there are also undeniable security concerns that need to be considered before businesses move sensitive information into the cloud. Researcher and author Michael Gregg recommends some useful questions businesses should ask when selecting a cloud service provider. The following suggested questions and explanations are taken directly from his 2010 report, "10 Security Questions for Cloud Computing." [29]

Where's the data? Different countries have different requirements and controls placed on access. Because your data is in the cloud, you may not realize that the data must reside in a physical location. Your cloud provider should agree in writing to provide the level of security required for your customers.

Who has access? Access control is a key concern, because insider attacks are a huge risk. A potential hacker is someone who has been entrusted with approved access to the cloud… Anyone considering using the cloud needs to look at who is managing their data and what types of controls are applied to these individuals.

What is the long-term viability of the provider? How long has the cloud provider been in business and what is their track record? If they go out of business, what happens to your data?

What happens if there is a security breach? If a security incident occurs, what support will you receive from the cloud provider? While many providers promote their services as being unhackable, cloud-based services are an attractive target to hackers.

What is the disaster recovery/business continuity plan? While you may not know the physical location of your services, it is physically located somewhere. All physical locations fact threats such as fire, storms, natural disasters, and loss of power. In case of any of these events, how will the cloud provider respond, and what guarantee of continued services are they promising? [30]

Cyber Threats

If the trend of businesses moving to the cloud continues as projected, expect hackers and their malicious attacks to follow. The cost of cybercrime to the global economy is estimated at $1 trillion dollars.[31] Cloud computing is not impervious to this criminal activity. Like any networked system of computers, cloud services are susceptible to things like denial of service (DoS) attacks, side channel attacks and man-in-the-middle attacks.[32] Researchers at the Cloud Computing Alliance, point out some cyber threats particularly challenging to those in the cloud computing industry. The following five threats and explanations have been taken from their report, "Top Threats to Cloud Computing."[1]

Insecure Interfaces – From authentication and access control to encryption ad activity monitoring, these interfaces must be designed to protect against both accidental and malicious attempt to circumvent policy.

Malicious Insiders – This threat is amplified for consumers of cloud services by the convergence of IT services and customers under a single management domain, combined with a general lack of transparency into provider process and procedure.

Shared Technology Issues – IaaS vendors deliver their services in a scalable way by sharing infrastructure. Often, the underlying

[1] To view the complete report, visit here: https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

components that make up this infrastructure were not designed to offer strong isolation properties for a multi-tenant architecture.

Data Loss or Leakage – There are many ways to compromise data. Deletion or alteration of records without backup of the original content is an obvious example. Unlinking a record from a larger context may render it unrecoverable, as can storage on unreliable media.

Account or Service Hijacking – Account or service hijacking is not new. Attack methods such as phishing, fraud, and exploitation of software vulnerabilities still achieve results. Credentials and passwords are often reused, which amplifies the impact of such attacks.[33]

Remediation

Fortunately, the Cloud Security Alliance has also provided a series of remediating protocols that can assist in mitigating these threats.

These recommendations include:

- Analyze the security model of cloud provider interfaces
- Ensure strong authentication in concert with encrypted transmission
- Enforce strict supply chain management and conduct a comprehensive supplier assessment
- Require transparency into overall information security and management practices, as well as compliance report
- Implement security best practices for installation/configuration
- Monitor environment for unauthorized changes/activity
- Encrypt and protect integrity of data in transit

- Implement strong key generation, storage and management, and destruction practices
- Prohibit the sharing of account credentials between users and services[34]

Businesses should seek out sufficient education related to the particular threats and remediation protocols associated with the framework and services they have selected. This begins by researching and becoming intimately familiar with the cloud service provider. Taking the time to confirm that the service provider is appropriately meeting expectations will better ensure the probability of having secure and readily accessible information in the cloud.

Conclusion

Cloud computing is going to be a particularly interesting trend to follow. If projections are correct, the future of computing is in the cloud. Businesses should take the time to research the three primary frameworks of cloud computing and move forward responsibly and in accordance with their IT strategy. Although the cloud appears to offer many enticing characteristics, like any network of computers, it is also susceptible to malicious activities that pose a potential threat to information security. Businesses should take the time to become very familiar with the threats and remediation protocols associated with the

cloud services they have selected to ensure that their business is able to continue operations safely and profitably into the future.

References

[1] Warren G. Bennis in Leadership of Change. In Michael Beer and Nitin Nohria, *Breaking the Code of Change* (Boston, MA: Harvard Business School Press).116-117.
[2] Rivka Tadjer. "What is Cloud Computing?" *PCMAG.com.* Published Nov 18, 2010. http://www.pcmag.com/article2/0,2817,2372163,00.asp
[3]Polrid, "Will Cloud Computing Feature Heavily in Forecasts for 2010?" Published Jan 2, 2010 http://www.technobuffalo.com/internet/will-cloud-feature-heavily-in-forecasts-for-2010/
[4] Stephen Alexander, "Cloud Computing to Grow 1200% by 2015." *Technorati*. Published Nov 29, 2011. http://technorati.com/technology/cloud-computing/article/cloud-computing-to-grow-1200-by/
[5] Dennis Stevenson. "Why is it Called Cloud Computing?" *Toolbox.com. Published* Mar 24, 2009. http://it.toolbox.com/blogs/original-thinking/why-is-it-called-quotcloud-computingquot-30713
[6]Stevenson, *Why is Called Cloud Computing?*
[7] Tadjer, *What is Cloud Computing?*
[8]"What we're Watching in Cloud Computing." *Harvard Business Review: The Magazine.* Published June, 2010. http://hbr.org/2010/06/what-were-watching-in-cloud-computing/ar/1
[9] Alexander, *Cloud Computing to Grow.*
[10] Vivek Kundra, "Federal Cloud Computing Strategy." *United States Federal Government.* Published Feb 8, 2011. http://www.cio.gov/documents/federal-cloud-computing-strategy.pdf
[11] Robert L. Grossman, R. "The Case for Cloud Computing." *Cloud Computing.* Published Mar, 2009. http://www.cmlab.csie.ntu.edu.tw/~freetempo/CN2011/hw/hw1/04804045.pdf
[12]Grossman, *The Case for Cloud.*
[13]Grossman, *The Case for Cloud.*
[14] Tim Mather, Subra Kumaraswamy and Shahed Latif, *Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance.* California: O'Reilly Media, Inc. 2009. pg. 11.
[15] Mather, Kumaraswamy and Latif, *Cloud Security and Privacy,* pg. 11
[16] Mather, Kumaraswamy and Latif, *Cloud Security and Privacy,* pg. 11
[17] Mather, Kumaraswamy and Latif, *Cloud Security and Privacy,* pg. 18
[18] Basant N. Singh. "SaaS Introduction with Examples – Cloud Service Model." *Cloud Computing.* Published April 26, 2010. http://www.techno-pulse.com/2010/04/saas-introduction-example-cloud-service.html
[19] Mather, Kumaraswamy and Latif, *Cloud Security and Privacy,* pg. 18
[20] Mather, Kumaraswamy and Latif, *Cloud Security and Privacy,* pg. 19
[21] Tom Henderson and Brendan Allen. "First Look at Windows Azure." *NetworkWorld*. Published June 20, 2011. http://www.networkworld.com/reviews/2011/062011-microsoft-windows-azure-test.html
[22] Mather, Kumaraswamy and Latif, *Cloud Security and Privacy,* pg. 19-20
[23] Mather, Kumaraswamy and Latif, *Cloud Security and Privacy,* pg. 22
[24] Mather, Kumaraswamy and Latif, *Cloud Security and Privacy,* pg. 22
[25] Sourya. "Cloud Computing for Dummies: SaaS, PaaS, IaaS and All That Was." *CloudTweaks.* Published Feb 15, 2011. http://www.cloudtweaks.com/2011/02/cloud-computing-for-dummies-saas-paas-iaas-and-all-that-was/
[26] Mather, Kumaraswamy and Latif, *Cloud Security and Privacy,* pg. 22
[27] James A. Martin. "Should You Move Your Small Business to the Cloud?" *PCWorld.com. Published* Jan 29, 2010.

http://www.pcworld.com/businesscenter/article/188173-2/should_you_move_your_small_business_to_the_cloud.html
[28] Sheng Liang. *SmartBusiness.* Published April 1, 2011. http://www.sbnonline.com/2011/04/sheng-liang/
[29] Michael Gregg. "10 Security Concerns for Cloud Computing." *GlobalKnowledge.com. Published* 2010. http://viewer.media.bitpipe.com/1078177630_947/1268847180_5/WP_VI_10SecurityConcernsCloudComputing.pdf
[30] Gregg, *10 Security Concerns*. http://viewer.media.bitpipe.com/1078177630_947/1268847180_5/WP_VI_10SecurityConcernsCloudComputing.pdf
[31] Henderson and Allen, *First Look.*
[32] Gregg, *10 Security Concerns, p. 5.*
[33] Cloud Security Alliance. "Top Threats to Cloud Computing." *CSA Alliance.* Published Mar, 2010. p. 8-13. https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf
[34] Cloud Security Alliance, *Top Threats,* p. 8-13