Cloud Computing: Introduction, Application and Security from Industry Perspectives

Xiangdong Li

Computer Systems Technology, NYC College of Technology, CUNY, Brooklyn, New York, USA
Computer Science, Graduate School, CUNY, New York, USA

Summary
Today, more and more industry companies and organizations recognize the value and benefit when using cloud computing services. Reducing cost and maintaining scale and high availability are essential for the business to keep its continuity. However, according to the survey, security issues exist on both customers and cloud providers. In the paper, we discuss the cloud service models and their security concerns from industry perspectives. Two case studies are analyzed to ensure the secure use of could computing services.

Key Words:
Cloud computing, Security, Application.

1. Introduction

Cloud computing is not a new concept; it came from telecommunication companies when the virtual private network (VPN) technologies and services were developed to provide security and lower cost in 1990s. The cloud symbol was first introduced to delimit the function or area between the provider and the users. Later, the cloud extends this boundary and covers the computing services and network infrastructure. On the INFORMS 1997, Chellappa first used the term "cloud computing" [1].
Cloud computing is still an evolving paradigm, the National Institute of Standards and Technology (NIST) defines cloud computing with the following five characteristics, three service models, and four deployment models [2]. In this paper, we focus on the service models.

Five Characteristics: *On-demand self-service, Broad network access, Resource pooling, Rapid elasticity, and Measured Service.* (More details are in Ref. [2]).

From an IT industry perspective, cloud computing provides a flexible benefit that the customers can request the IT services without the purchase, deployment and management as they did at their local sites before. For example, if a company needs storage next week, terabytes of storage resource can be provided immediately for the customer through cloud computing. The customer just pays the requested service of the period of time and capacity, there is no need to purchase and implement the storage and network infrastructure locally themselves, and they can access their data from different locations, such can reduce the business' IT spend and also keep the high availability and scalability.

Three Service Models:

- Infrastructure as a Service (IaaS). *The capability provided to the consumer is to 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.*

This is the most basic cloud service model, providing the on-demand resources for the IT needs. It is usually provided and paid by users on an as-needed basis. For example, the customers pay for the use of the virtual machines, storage capacity and network bandwidth, not to hold the entire physical servers, storage equipment and network devices. They share the could providers' infrastructure with other customers. The price depends on the resources and the time requested, it also depends on the deployment model, public or private, for example.

- Platform as a Service (PaaS). *The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider.*

On the top of IaaS, PaaS provides the capability to build or deploy the applications, like the Microsoft based (i.e. Windows, .NET, IIS, and SQL) or an open source based (i.e. Linux, Apache, MySQL, and PHP).

- Software as a Service (SaaS). *The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure.*

A SaaS provider offers the complete IT cloud services to the customers who do not need to install or manage the IT infrastructure. Usually the users use the interfaces to access the resources via the Internet. For example, users use a Web browser to access Gmail and Microsoft Windows Live.

Manuscript received May 5, 2011
Manuscript revised May 20, 2011

A company can choose any type of the cloud service models based on their business need.

Four Deployment Models: as the service models, cloud computing can be deployed in the following ways based on the customers' requirements.

- *Private cloud.* The entire cloud infrastructure is used only for one customer.
- *Community cloud.* Several customers share the cloud infrastructure and it supports a specific community with the same concerns (e.g., resources and security requirements, policy and compliance considerations, etc).
- *Public cloud.* The cloud infrastructure is for general public or a large industry group.
- *Hybrid cloud*. The cloud infrastructure contains different type of cloud deployments, e.g., private, community, or public.

Virtualization and high-speed Internet boost the transformation of compute environments and the compute resources into the cloud. In 2009, the number of virtual machine deployments exceeded the physical server shipments, just a couple of years after the virtualization became a standard in data center. Today, due to the wide use of VMs technology, the cloud computing quickly expands its applied fields, and it is becoming a major part of enterprise IT industry. According to an IDC report, the estimated spending in 2009 was about $3.4 billion on cloud services provided by third-party suppliers (including SaaS, IaaS, and PaaS), an expected growth of 56% in 2010 to $5.3 billion, and this figure will reach to $18.8 billion in 2014 [3].

2. Security in Cloud Computing

2.1 Can we trust cloud computing?

The cloud computing provides big benefit for the business. Should we move to the could services without a concern?

From the IT specialists' views, compared to the traditional infrastructure deployment, the pure IaaS inclines to make the secure operations more risky. One of the big concerns is that the administrators monitor the operating systems for the security concerns and often need to download the new patches. But most techniques and tools for monitoring the OSes are not perfect, and even the OSes can update themselves. The updates are not 100% reliable. If hundreds VMs are running with two or three physical servers, a small unpredicted flaw in the base image can quickly be magnified as a massive hole when it gets replicated hundreds of times [5].

Some IT specialists do worry about their use of cloud services. "The cloud is a future thing, it's a black hole right now," said Mike Myers, a lead technical analyst for Marriott International. Marriott's map sites services are hosted by a cloud provider. "This information is not sensitive; we wouldn't put anything sensitive in the cloud," added by Mike. Andy Gram, a chief platform architect at BlackRidge Technology, said "I don't know you, you don't know me. The cloud is like that, so why would I put anything sensitive there?" Peter Tam, a security engineer with NASA, said "If our systems are infected by malware; that could be a major problem. The cloud is interesting, but it does not impact my job today."

In April 2011, Sony's PlayStation Network had been down for nearly a week, the personal information of 77 million customers has been stolen by an unauthorized access. The company didn't encrypt most users' data, and the hacker obtained "profile data, including purchase history and billing address, and PlayStation Network/Qriocity password security answers." The stolen information might also include the customers' credit card numbers and expiration dates. Many users may worry more about their sensitive information in the cloud storage.

Also in April 20011, Amazon's Elastic Compute Cloud (EC2) went down and lasted several days. A number of other sites and services that rely on EC2 had been affected, like Reddit (a news site), Foursquare (a social networking site), and Quora (an online knowledge market). This kind of failure was caused by a human error which triggered a "network event". If a customer's business totally relies on the cloud service, the outage of the cloud service will suspend the customer's business.

A recent Ponemon Institute report [7] published in April 2011 shows that the cloud providers didn't put security as the No. 1 concern when providing the services. Around 74% of cloud providers in U.S. and European said their services did not strongly protect customers' sensitive data; nearly 62% of the providers are not confident that their cloud services are highly secure. About 69% of the providers do not think they have the responsibility for data security and most of them do not have dedicated personnel to exam the security of the provided services. The cloud providers believe that the high priority for the customers to use cloud services is to reduce the costs, simplify the deployment and improve the performance; but to improve the security and comply with policies are at low priorities. However, many customers do have higher priority for the cloud security. Before sending the data into the cloud, the customers should assess the security risks and exam the vendors' responsibility and the existing security policy or secure methods. If the customers feel the lack of the safety of the data and applications in cloud, they should request the vendors to implement the security technology and policy.

2.2 Cloud security analysis

The security concern should have a higher priority than the cost for storing the sensitive data in cloud. Trust is often a

big barrier for customers to adapt the cloud. The cloud providers should strengthen and test their security policy in order not to let their customers information hacked. At the RSA Conference in February 2011, Art Coviello, the executive chairman of RSA, said "… lack of trust in cloud computing is slowing broader adoption of cloud services. While cloud computing offers tremendous benefits in cost and agility, it breaks down some of the traditional means of ensuring visibility and control of infrastructure and information. Forcing enterprises to develop trusted relationships individually with each cloud service provider they wish to use is cumbersome and will not scale. New thinking in security and compliance is required to provide a future in which organizations can consume services from a wide variety of cloud-service providers' on-demand and for all their application needs."

According to the Gardber's report that more than 70% money spent in the private clouds, clearly that the businesses can spend less if using the public cloud, but they want to pay a little more to have a private cloud in order to segment their enterprise off the publicly sharing. The private cloud can give them a better control and smoothen the integration, and they can fit exactly what their businesses need.

The cloud has three level models of the cloud security alliance [4]. For the SaaS model, like salesforce.com, which is probably the first SaaS model, the business outsources its big portion of the development and design to the cloud providers, and the business relies on the providers' identity management, access management, and security design. For PaaS model, like the GoogleApp engine, force.com and Amazon API, the providers develop their own applications and deploy them on the platform as a service for the customers. The customers can build their internal application architecture and security, and run them inside containers on the cloud providers' platforms, like Tomcat container or Webcure container. The customers can build identity and access management in their security systems that meet the customers' enterprise requirement. Compared to SaaS, using PaaS the business can gain more flexibility and control. For the IaaS model, the cloud vendors only provide the bare bone services, like the Amazon Elastic Compute Cloud (EC2), the customers use the services as the OSes images, storage and other infrastructure. The customers can develop their application servers, database servers and other configuration on the platforms. It is normal for a company to have a mix type of the services. For example, the sales department may use salesforce.com, its IT department may use Amazon IaaS for its storage.

In the following, we focus on two case studies of Microsoft Active Directory integration with cloud SaaS model and could storage as IaaS model.

Case Study 1: Microsoft Active Directory (AD) integration with SaaS

A research from Goldman Sachs in February 2010 indicates that 58% of small and midsize business (SMB) will consider the adoption of SaaS. Cloud computing can allow the company employees to access the applications at any time from any location. The user access control and its authorization to the SaaS applications are challenging. For example, a temporary or fired employee's access may not be removed promptly. It is necessary for the IT department to minimize the risk when using SaaS.

Microsoft Active Directory (AD) is an authoritative user directory which uses a number of standardized protocols to manage the accesses to network and system services. Its own directory can be developed on SaaS application for the access to the application. The usernames and passwords of users are used for the access to the network and SaaS applications. As the use of SaaS application grows, a large number of user accounts with different passwords have to be created and managed. This is challenging to integrate Microsoft AD with the corresponding directory developed on the SaaS applications.

According to a white paper from Okta Inc. [8], a seamless integration with Microsoft AD should provide: User synchronization: when a user is added to or removed from AD, the change should be also made in the corresponding SaaS applications; Access provisioning and de-provisioning: when a user is added to or removed from AD, the SaaS applications should be provisioned or de-provisioned automatically; Single sign-on (SSO): when a user signs on the Windows network, he/she can gain the access to the SaaS applications as well.

The white paper discusses three different ways to integrate AD with the SaaS applications and analyzes how effectively they meet the requirements above.

- ***a.*** *Using Independent Integrations with AD.* The SaaS venders, including Google Apps, Microsoft Online Services, and Salesforce.com, offer their own AD integration tools or provide the API which allows the customers to build their own integration tools.
- ***b.*** *Using Microsoft Active Directory Federation Services (AD FS).* The AD FS is a server role in the Windows 2008 server which can be used to create a highly extensible, Internet-scalable, and secure identity access solution that can operate across multiple platforms to handle the single sign-on with applications beyond the firewall. The customer can apply the AD FS to address the single sign-on requirement of the integration, "*but it does not address user synchronization and provisioning or de-provisioning*".

c. *Using solution from third-party vendor*. Several vendors provide the solutions to meet the single sign-on and user management needs.

Case Study 2: Cloud Storage

The advanced online backup and storage techniques are cost-effective and they provide additional benefit of recovery. From a business point of view, the ability to access the data from anywhere, from any station with low cost ensure the business continuity. Every company will worry about their data safety and the vulnerabilities when using the cloud computing.

If your data is on cloud storage, you may worry about: Is there any unauthorized access to our data? Is the provider's storage device reliable and any of our data altered? Can I get our data 24 hours a day? Can I trust the environment around the cloud storage in the cases of fire, floods, and earthquakes or even wars, etc? These questions refer to the physical security, network (data transfer) security, application security, internal systems security, data management security and secure strategy, internal data access policy or procedures, third-party certification, encryption and the secure key management.

The cloud providers should ensure the customers that all these security requirements are meet. The customers' data is protected with a comprehensive physical security, the data encryption standard, a strong user authentication, and application security, as well as the latest standard-setting security practices and certifications, (including: World-class security specifications, SAS 70 Type II, SOX, ISO270011, and third-party vulnerability and SysTrust certifications1), and the secure point-to-point data replication for data backup (the backup tapes for customer data never leave the facilities).

The common technique used to protect the data in motion (during the transmission) is the SSL encryption (TLS 1.0) between the customer sites and the data storage. A public key distribution is used for the key management. When the customer connects the cloud provider site via the Internet, the server's public key and the digital certificates are sent to the customers. The customer may verify the provider's identity (i.e. through the trusted third party). After the verification, the customer sends the provider a long random number as the session key, which is used to encrypt and decrypt the data. This session key sent to cloud provider is encrypted by using the provider's public key and it only can be decrypted by using the provider's private key. Some cloud providers can support the secure virtual private network (VPN) connections, the most common technique of VPN used is the IPSec. Passwords, encryption keys, digital certificates or the verification are used for the authenticating process. On the provider site, data protection should have the highest priority than others. The common encryption standards used to encrypt the data on the storage are the Advanced Encryption Standard (AES) with 128-, 192 or 256-bit keys and 3-Data encryption Standard (3DES) (in the case that the customers do not encrypt their data themselves).

It is very important for customers to know the management policy at the cloud vendor site. All cloud providers should follow strict regulation and policy to manage the customer data. All the data should be replicated to its mirror at a different location when it reaches the storage in order to protect the data in the case of Outages or disasters happened on one location. The storage server should use well-known OS versions with Federal Information Processing Standard (FIPS) and up-to-date anti-virus software, as well as a full back-up and disaster recovery strategy. The provider should be compliant with security-oriented laws and auditing programs, including Safe Harbor, ISO 27001, and SAS70 Type II. The actual physical location of a customer's data can be very important and should satisfy some regularization or compliance, for example, the EU Data Protection Directive [6]. Most cloud providers own or lease offsite data bunkers which locate in the underground of mountains with 24x7 security guards.

3. Cloud Computing Standards

The cloud computing concept is still new and the advanced technology for cloud computing is being developed and adopted every day. As a growing number of industries, governments, and education organizations store their sensitive data on off-site servers which are managed by the third parties, congress and lawmakers should start to draft the legislation which require the business of both sides to follow in order to protect the integrity of this information, said Brad Smith, a general counsel for Microsoft Corp as a keynote speaker at the Brookings Institution in Washington, D.C. in Jan. 2010. People predict the standards and the regulations for cloud computing will be available in 2013. Several computing services providers give their own standards of the cloud computing services delivery.

The salesforce.com lists seven standards for the cloud computing service delivery [8]:

- *World-Class Security*: Provision security at all levels. It includes Physical, Network, Application, Internal system security and Secure data-backup strategy, Secure internal policies and procedures, and Third-party certification.
- *Trust and Transparency***:** Provide transparent, real-time, accurate services and timely information.
- *True Multitenancy:* Ensure maximum scalable services to customers with a true multitenant architecture.
- *Proven Scale:* Support tons of users with proven scalability
- *High Performance:* Sustain consistent, high-speed performance world-wide.

- *Complete Disaster Recovery:* Protect customer data by running the service on multiple, geographically dispersed backup centers with failover capabilities.
- *High Availability:* Equip advanced facilities to support high availability of the infrastructure and application software.

Other cloud computing providers supplement the standards with [9]: Seamless Integration On Demand; Predictable Total Cost of Ownership Model; Faster Deployment; Liberation from Non-Strategic IT Issues.

4. Conclusion

Business can significantly be benefited from using the cloud computing services. However, there is no legislation or regulation required for the could computing services today. We discuss the security issues when using the cloud computing for the sensitive data and user access control. The cloud service providers should follow a number of standards to ensure the safety of the customers' data and applications. The customers should understand the vendors' process and policy of the services provided.

Reference

[1] R. Chellappa, "Intermediaries in Cloud-Computing: A New Computing Paradigm", Proc. INFORMS Intermediaries in Electronic Markets, 1997.
[2] P. Mell, T. Grance, "The NIST Definition of Cloud Computing (Draft)", NIST, Jan. 2011.
[3] G. Nebuloni, "Accelerate Hybrid Cloud Success: Adjusting the IT Mindset", white paper, IDC, February 2011.
[4] "End-to-End Secure Client to Cloud Access", Sponsored by Intel Applications and Security and Identity Products Group, 2011.
[5] C. Brooks and J. Maitland, "Cloud security advances not yet on IT radar", Feb. 2011, searchcloudcomputing.com.
[6] "EU Data Protection Directive (Directive 95/46/EC)", Jan. 2008, http://searchsecurity.techtarget.co.uk/definition/EU-Data-Protection-Directive
[7] Ponemon Institute Research Report , "Security of Cloud Computing Providers Study ",April 2011.
[8] Salesforce Inc., whitepaper, "The Seven Standards of Cloud Computing Service Delivery", 2011.
[9] Workday Inc., whitepaper, "10 Critical Requirements for Cloud Applications", 2011.

Xiangdong Li received M.S. in Computer Information Science from CUNY Brooklyn College in 1997, and Ph.D. in physics from the CUNY Graduate School in 2000. Professor Li has five years working experience in the IT industry. He is an associate professor at the Department of Computer Systems Technology in New York City College of Technology, CUNY. He is a faculty member of both Ph.D. programs in Computer Science and Physics at the CUNY Graduate School. His research fields include information security, quantum information and nuclear physics.