Cloud Computing

A newsletter for IT Professionals

Issue 3

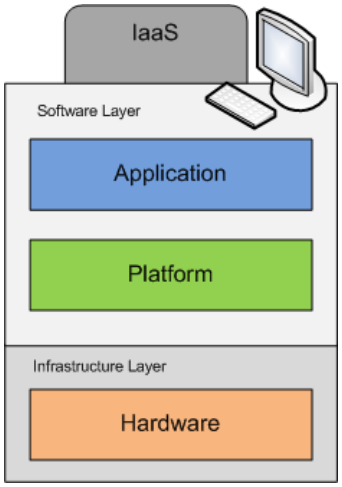
I. Background of Cloud Computing

Cloud computing is a computing style in which scalable and flexible IT functionalities are delivered as a service to external customers using Internet technologies. Cloud computing is not a revolutionary idea; Instead, it is an evolutionary concept that integrates various existing technologies to offer a useful new IT provisioning tool.

Cloud applications extend their accessibility through the Internet by using large data centres and powerful servers that host web applications and services. Anyone with a suitable Internet connection and a standard Internet browser can access a cloud application. Rapid evolution of cloud computing technologies can easily blur its definition perceived by the public. Yet, there are five key attributes to distinguish cloud computing from its conventional counterpart:

- Service-based
- Scalable and elastic
- Shared
- Metered by usage
- Uses Internet technologies

Cloud computing encompasses many aspects of computing (from hardware to software) that a single solution is not able to provide all aspects. Generally speaking, cloud computing applications incorporate the combination of the following functional service models:



1 Infrastructure as a Service (IaaS)

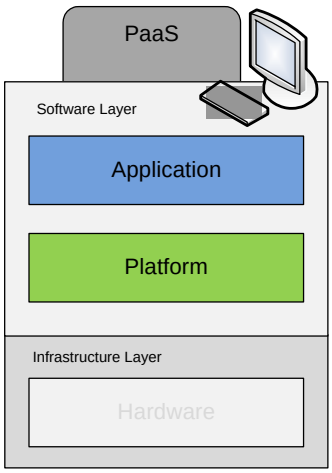
IaaS solutions provide users with physical or virtual resources that satisfy the requirements of the user applications in terms of CPU, memory, operating system and storage. Such Quality of Service (QoS) parameters are established through a Service Level Agreement (SLA) between the customer and the service provider. The end user has full controls over the virtualised computer instance, and can customise the instance accordingly. Unlike purchasing the physical servers, IaaS is usually charged on a utility basis depending on the consumption of the resources.

A big name in IaaS space is Amazon.com, which launched Elastic Compute Cloud (EC2) in 2006 to offer a pay-as-you-go hosting service for customer's computer applications. In 2008, Fujitsu also opened its "London North Data Centre" to outsource data storage and computing services with security options covering UK and International regulations, and compliance auditing according to the ISO27001 standard.

Reference:
http://www.buyya.com/papers/AnekaMagazineArticle1.pdf
http://aws.amazon.com/ec2/
http://www.fujitsu.com/uk/news/pr/fs_20080627.html

I. Background of Cloud Computing (cont'd)

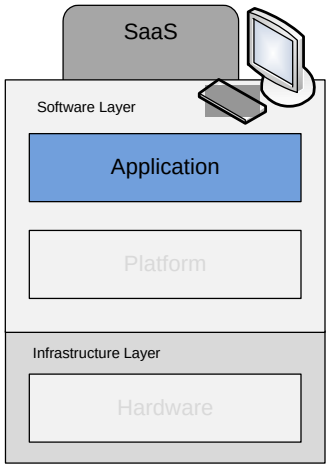
2 Platform as a Service (PaaS)



PaaS delivers cloud-based application development tools in addition to services for testing, deploying, collaborating, hosting, and maintaining applications. It hides all the complexity of managing the underlying hardware, provides all the facilities required to support the complete lifecycle of building and deploying web applications and services entirely from the Internet. With PaaS, users can develop new applications or services in the cloud that do not depend on a specific platform to run, and can make them widely available to users through the Internet. The accessibility of PaaS offerings enables any programmer to create enterprise-scale systems that integrate with other web services and databases.

Two well-known PaaS solutions, Google AppEngine and Microsoft Azure, provide users with a development platform for creating distributed applications that can automatically scale on demand. Other PaaS service providers are 3Tera, RightScale, DataSynapse, Manjrasoft, Univa UD, Elastra and Enomaly.

3 Software as a Service (SaaS)



SaaS is a model of software deployment where a provider delivers its software as a service to be used by customers on demand. Under the traditional SaaS model, an application resides at an offsite data centre where the service provider maintains data, servers and related hardware. End-users access the application remotely via an Internet browser. The SaaS model is predicated on a "one-to-many" or multi-client delivery model whereby an application is shared across clients, providing opportunities to customise the system to the needs of each customer.

Examples of SaaS are Salesforce.com and Clarizen.com, which respectively provide online Customer Relationship Management (CRM) and project management services. Google Apps provides desktop applications which are hosted in the cloud and replaces traditional desktop based Microsoft Office software. Northgatearinso offers on demand Human Resources (HR) solutions based on SAP Human Capital Management (HCM) module.

Statistical Report

New IDC Research: Through 2014 Public IT Cloud Services Will Grow at More than Five Times the Rate of Traditional IT Products

Worldwide revenue from public IT cloud services exceeded $16 billion in 2009 and is forecast to reach $55.5 billion in 2014, representing a compound annual growth rate (CAGR) of 27.4%. This rapid growth rate is over five times the projected rate of growth for traditional IT products (5%).

See the article: http://www.idc.com/getdoc.jsp?containerId=prUS22393210

Reference:
http://virtualization.sys-con.com/node/770174
http://www.buyya.com/papers/AnekaMagazineArticle1.pdf

I. Background of Cloud Computing (cont'd)

Key Benefits Achieved through Cloud Computing

- **Flexibility -** Cloud computing allows universities to expand or contract computing power as required and allows "bursts" of computing power to be utilised on an "on-demand" basis. This flexibility helps ensure resource-intensive processes will not slow down other business processes and computing services are always operating at optimal cost.

- **Scalability -** Cloud computing enables universities to quickly scale up their IT operations as provisioning of new computing resources and software applications can be delivered at a desired pace. Furthermore, constraints on pre-purchasing of resources to meet peak requirement in traditional IT no longer exist.

- **Economics -** Traditional IT has multiple fixed and variable cost elements. In order to fulfil business requirements and sustain day-to-day business operations, universities must invest a large fixed amount for initial IT infrastructure establishment and continue to spend variably for software and hardware maintenance. By outsourcing IT functions to the cloud, universities can leverage the features of a lean IT structure to reduce the overall IT expenditures involved in software licensing, infrastructure development, on-going support and upgrades.

- **Inherited Resiliency -** Cloud computing removes single points of failure since the Internet is a highly resilient computing environment. Some competitive service providers also add extra functionalities to enhance resiliency. For example, the "Availability Zones" and "Elastic IP Address" features of Amazon.com EC2 allow multi-location of application software and dynamic IP address re-mapping mechanism in an event of service interruption.

- **Highly Automated –** Cloud computing services are maintained by dedicated IT professionals of cloud service providers. As a result, universities' IT staff no longer need to worry about complex details behind the delivered computing services, such as hardware maintenance, constant software update, etc.

Related Article

Is Cloud Computing a Credible Solution for Education?

In a pilot project class focused on developing and deploying SaaS in UC Berkeley, it is found that the cloud made it easier to fulfil assignments, such as saturating large database servers. Normally that assignment would have taken 200 local servers. Instead, they were able to acquire 200 servers in a few minutes, and they could release them once the lab was over.

See the article: (http://campustechnology.com/articles/2009/11/12/is-cloud-computing-a-credible-solution-for-education.aspx)

Reference:
ftp://public.dhe.ibm.com/common/ssi/ecm/en/diw03004usen/DIW03004USEN.PDF
http://www.infoworld.com/d/cloud-computing/amazon-adds-resilience-cloud-computing-service-635

II. Risk of Cloud Computing in Universities

The benefits of cloud computing are both a friend and a foe from a security point of view. The massive concentrations of resources and shared usage pattern present a more attractive target to attackers and exposure to new security concerns. Universities should consider the risks and vulnerabilities prior to migrate to the cloud. Examples of these risks are:

1 Data and Privacy Protection

When universities store their data with programs hosted on someone else's hardware, they lose a degree of control over their sensitive information. The responsibility for protecting that information from hackers and internal data breaches then falls into the hands of the cloud service provider rather than the universities. The multi-tenancy, reuse of hardware and software resources, and resiliency through redundancy nature of cloud computing also means a higher risk of incomplete or unsecured deletion of universities' confidential data.

2 Isolation and Segregation

The multi-tenancy and shared resources are two of the defining characteristics of cloud computing environments. Computing capacity, storage, and network are shared between multiple users. Therefore, failure of mechanisms separating storage, memory, routing and even reputation between different customers of shared infrastructure (e.g. so-called guest-hopping attacks, SQL injection attacks exposing multiple customers' data stored in the same table, and side channel attacks) becomes a key risk in cloud computing.

3 Malicious Insider

The malicious activities of an insider could potentially have an impact on the confidentiality, integrity and availability of universities information asset maintained by cloud service providers. Staff of cloud service providers, such as system administrators, may be granted with privileged access to the sensitive data of all customers within their cloud environments. Any abuse of such system privileges can bring significant risks to customers' information security. On the other hand, when usage of cloud services increases, employees of cloud service providers increasingly become targets for criminal gangs.

4 Regulatory Compliance

Having data, application or processes migrated to a cloud provider, especially a public one, universities are still ultimately responsible for that data and needs to comply with relevant regulatory laws (e.g. Personal Data (Privacy) Ordinance) and information security standards (e.g. ISO27001) when handling such data. Due to the very nature of cloud computing, to know where universities' data is stored, when it is moved, who has accessed and what particular security measures are in place can be difficult. It is also questionable whether the cloud providers are willing to offer support for auditing purpose.

Reference:
http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853?page=0,1
http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport

II. Risk of Cloud Computing in Universities (cont'd)

5 Dependency to Service Provider

There is currently little to offer in the way of tools, procedures or standard data formats or services interfaces that could guarantee data, application and service portability. Universities may find it difficult to in-source their data and IT operations in the cloud or switch to another cloud service providers. This introduces a dependency on a particular cloud service provider for service provision, especially when data portability is not supported.

6 Loss of IT Governance

In using cloud infrastructures, universities necessarily outsource control to the cloud service providers on a number of issues which may affect security of universities' data and applications stored on the cloud's platform or software. At the same time, Service Level Agreement (SLA) may not offer a comprehensive commitment to provide desired IT security measures by cloud service providers, thus leaving a gap in universities IT security defences.

7 Cloud Service Termination or Failure

As in any new IT frontier, competitors'' pressure, inadequate business strategies, lack of financing, immature market, etc, could lead to some cloud providers to go out of business or at least to force them to restructure their service portfolio offering. Short or long term service termination means a loss or deterioration of service delivery performance, as well as a loss of investment. Meanwhile, Universities may be at risk to meet their own duties and obligations, and thus be exposed to contractual or legal liability to their employees, third parties, students or even the public.

8 Legal

In the event of the confiscation of physical hardware as a result of subpoena by law-enforcement agencies or civil suits, the centralisation of storage as well as shared tenancy of physical hardware means universities' sensitive information in the cloud is at risk of disclosure to unwanted parties.

On the other hand, in the absence of contractual commitment from service providers or legal enforcement, investigation of inappropriate or illegal activities may be infeasible in cloud computing as some or all universities' data may be stored with other customers and may also be spread across a set of ever-changing hosts.

Related Article

Top Cloud Computing Security Risk: One Company Gets Burned

LawLeaf, a web-based financial services company, suffered a major hit on its reputation after a SQL injection attack that compromised its cloud service provider, BlueHost. However, the argument that whether the provider or LawLeaf should be responsible for the loss still persists.

See the article: (http://www.networkworld.com/news/2010/071410-top-cloud-computing-security-risk.html)

Reference:
http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf
http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport

III. Exploitation on Cloud Computing

Cloud computing inherits security vulnerabilities from the Internet and makes them more significant when incorporating resource concentration and multi-tenancy sharing approach. Major cloud-specific vulnerabilities include: (1) Economic Denial of Service; (2) Compromise of Service Engine; (3) Interception and Leakage of Data in Transit

Major Vulnerabilities in Cloud Computing Environment

1 Economic Denial of Service (EDoS)

EDoS attempts to consume IT resources maliciously that result in economic damage to their owners. Universities' resources in the cloud can be harmed by the following kinds of EDoS attacks:

- Identity theft – an attacker hijacks the user accounts of universities' members and uses them for his personal gain or to damage universities economically.
- Resource Abuse – If effective limits on the usage of paid resources from the cloud service providers, malicious actions can be made by attackers to create unexpected consumption of such resources.
- Public Channel Attack – Cloud services delivered through public channel, such as metering per HTTP requests, are vulnerable to attacks from the public Internet, such as Disturbed Denial of Service (DDoS).

In the worst case scenario, EDoS eliminates the cost-effective benefit of cloud computing and cause serious economic damage, even bankruptcy.

2 Compromise of Service Engine

Cloud architecture relies on a highly specialised platform, the service engine that sits above the physical hardware resources and manages customer resources at different levels of abstraction.

An attacker can compromise the service engine by hacking it from inside a virtual machine (IaaS clouds), the runtime environment (PaaS clouds), the application pool (SaaS clouds), or through its Application Programming Interface (API).

3 Interception or Leakage of Data in Transit

Being a distributed architecture based on the Internet technologies, cloud computing implies more data in transit than traditional infrastructures. Data must be transferred between remote web clients of universities and cloud infrastructure to synchronise multiple distributed machine images, images distributed across multiple physical machines. Secured data transmission mechanism like Virtual Private Network (VPN) is not always followed in the cloud context.

Sniffing, spoofing, main-in-the-middle attacks, side channel and replay attacks are potential threat sources that can be used by attackers to exploit this vulnerability.

Reference:
http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport

IV. Hardening Steps to Secure Cloud Computing Environment — Infrastructure as a Service

IaaS includes the entire computing infrastructure resources stack from the facilities to the hardware platforms that reside in them. It provides limited application-like features but enormous extensibility. This generally means less integrated security capabilities and functionalities offered on the part of the cloud providers. As such, the security measures at IaaS are mainly managed and secured by the customers.

1 Data Encryption

To prevent data leakage to unauthorised parties, encryption techniques shall be implemented on:

- All network traffic using protocols such as Secure Socket Layer (SSL), Internet Protocol Security (IPSEC), Secure Shell Client (SSH) or Hypertext Transfer Protocol Secure (HTTPS)
- File systems or device drivers
- All data kept in storage areas, such as Storage Area Network (SAN), Network-attached Storage (NAS), etc.

Moreover, never store decrypting keys in the IaaS environment. Those keys shall only enter the system when decrypting.

2 Operating System

Security in the operating systems used in IaaS can be enhanced via the following approach:

- Increase the security measures of the underlying operating systems using specific security hardening tools. For example, Microsoft Baseline Security Analyzer (MBSA), Bastille Linux, etc.
- Install an Intrusion Detection System (IDS), such as Open Source Security (OSSEC) and CISCO Security Agent (CSA), at the operating system level.
- Regularly install security patches at the operating system level and update virus definition of anti-virus software.

3 Network Management

IaaS are accessed via the Internet. Hence, the following conventional network security measures can still be applied:

- Use customer RSA security tokens or client SSL certificates instead of access passwords in the console mode.
- Limit the number of network ports to the minimum. Except for public services like HTTP/HTTPS, limit the number of source IP addresses authorised to connect, especially to administrative remote accesses services.
- Perform recurring vulnerability or penetration tests to detect new undiscovered vulnerabilities.

4 Application Development

Security considerations shall be included during the Software Development Life Cycle (SDLC). Security framework such as Open Web Application Security Project (OWASP) can be used in developing programs in an IaaS environment.

Reference:
http://blogs.orange-business.com/live/2010/05/cloud-iaas-16-recommendations-for-secure-servers.html

V. Hardening Steps to Secure Cloud Computing Environment — Platform as a Service

PaaS is intended to enable developers to build their own applications on top of the platform supported by cloud service providers. As a result, it tends to be more extensible than SaaS, at the expense of customer-ready features. In the case of PaaS, it is the responsibility of the universities' system administrators to effectively manage the same level of security measures provided by the cloud providers for protecting the underlying infrastructure components to ensure basic service availability and integrity levels.

1 Logical Access

Unauthorised access to universities' data in the cloud platform should be restricted. One of the best approaches to data access control is using the least privilege rule – i.e. access to particular data shall only be granted to authorised personnel on a need-to-know basis.

Individual users shall be authenticated on their own behalf. The universities are recommended to deploy user-centric authentication method that adopts a single set of credentials at multiple sites.

2 Application Development

PaaS provides a framework of building blocks to construct customised applications based on customers' own needs. Same as IaaS, application development within PaaS environment also require consideration on security throughout the SDLC.

However, since less operational controls can be obtained by PaaS customers, application design and implementation may require additional steps to achieve the same level of security as IaaS counterparts. For example, extra data encryption mechanism shall be implemented with the application logic if secure protocols (e.g. SSL, HTTPS, etc.) cannot be utilised on PaaS platform.

3 Portability and Interoperability

When shifting from IaaS to PaaS, vendor lock-in (dependency) turns out to be a critical security issue if a university may have to change its cloud service provider in the future, portability and interoperability must be considered. With PaaS, the expectation is that certain degree of application modification will be necessary to achieve portability. The focus is minimising the amount of program re-writing while maintaining or enhancing security controls, along with achieving a successful data migration.

When possible, the university shall develop the cloud platform components with a standard syntax and open APIs. The university should also understand:

- What tools are available for secure data transfer, backup, and restore?
- How base services like monitoring, logging, and auditing would transfer over to a new cloud provider?
- What security control functions are provided by legacy cloud provider and how they would translate by the new provider?
- What is the impact on performance and availability of the application when migrating to a new PaaS platform?

Reference:
http://www.owasp.org/images/a/a6/Understanding_the_Implications_of_Cloud_Computing_on_Application_Security-Dennis_Hurst.pdf
http://www.cloudsecurityalliance.org/csaguide.pdf

VI. Hardening Steps to Secure Virtualisation Environment — Software as a Service

SaaS provides the most integrated functionality built directly into the offering, with the least customised extensibility, and a relatively high level of integrated security offered by cloud providers. From customers' perspective, implementing security in the case of SaaS means that service levels, governance, compliance, and liability expectations of the cloud services and respective providers are contractually stipulated, managed, and enforced.

1 Service Level Agreement

Universities shall assess whether security considerations are addressed in the Service Level Agreements (SLA). An adequate SLA must include a set of security standards committed by the cloud service provider, which may include the following:

- **Encryption of Sensitive Data** – ensure that the cloud providers have clear policies and sufficient technologies to achieve effective data encryption.
- **Disaster Recovery Mechanism and Testing** – ensure that the cloud providers establish proper data recovery procedures and regular drills. Universities are also recommended to specify target Recovery Time Objective (RTO) in the SLA.
- **Secure SDLC** – ensure that the cloud providers incorporate necessary security considerations and measures when developing the software used by the universities.
- **Transparency** – ensure that the statistics on cloud providers' security controls, system availabilities and performance are readily available for universities' tracking and monitoring.
- **Data Extraction** – ensure that universities data kept by the cloud providers can be retrieved back in the circumstances of SLA breaches or during service interruption.

2 Compliance and Audit

Compliance needs shall be addressed in the cloud providers' standard terms of service. It is beneficial for universities to have both legal and contracts personnel involved early to ensure that cloud services contract provisions are adequate for compliance and audit obligations. Specifically, the contract terms should allow the universities to perform security audits or reviews of the cloud computing environment.

3 Portability and Interoperability

With SaaS, universities will substitute new software applications for old ones. The focus is on preserving or enhancing the security functionalities provided by the legacy cloud provider in order to achieve a successful data migration.

In general, universities should perform regular data extractions and backups to a format that is independent from the legacy cloud provider. The ability to migrate legacy backup data by the new cloud provider must be assessed to ensure smooth transition. Consistency in security control effectiveness should be examined on the new and old cloud service providers.

Reference:
http://www.webhostingsearch.com/articles/saas-security-issues.php
http://www.cloudsecurityalliance.org/csaguide.pdf
http://dmsconsultingllc.com/blog/2009/03/24/ensuring-saas-security/

VII. Summary

The innovation of cloud computing has changed the way IT operations are deployed in various organisations around the world, including universities. Its benefits in cost saving, operational scalability and flexibility surpass the conventional platform and quickly become the center of attention for the next generation computing style.

The outsourced and resource concentration nature also shifts people's focus on the new security vulnerabilities and concerns that come with the cloud computing. It creates a dilemma for cloud customers and service providers to differentiate their responsibilities toward data privacy, malicious cyber attacks, regulatory compliance and IT governance.

As of today, cloud computing is still an emerging technology. Cloud platform cannot offer the full spectrum of certain applications architected in traditional on-premises environment, especially when the applications are highly specialised (not commonly used) or the universities require exclusive control over their IT functions.