viaccess

Cloud security for content services: thunder coming?

INTRODUCTION

As defined in NIST SP 800-145 ("NIST Cloud Computing Definition"), cloud computing is the network delivery of an elastic and on-demand “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”.

More and more companies are interested in cloud computing in order to improve their computing environment efficiency and adaptability and to reduce their costs – companies do not need to own and maintain any more dedicated servers. Cloud service providers can provide management of various tasks like mailing, collaborative tools, ERP, security, maintenance and so on. They also guarantee a large storage and computing availability.

This trend towards cloud computing is not limited to “traditional” types of applications and the use of private data centers is now also observable for other applications like Over-The-Top (OTT) applications. Indeed, OTT video content delivery through various rapidly-developing cloud-based online video platforms and digital rights locker initiatives like UltraViolet™ are fast developing.

One should however bear in mind that cloud computing is not free from security risks. This White Paper shows up security challenges than the cloud is facing and emphasizes what should be considered by Content Services Providers when it comes to developing or outsourcing content protection and rights management applications that are known to be security-critical from a business perspective for paid-for content services.

INSIDE CLOUD COMPUTING

Still looking for standardization, cloud computing is available in at least four modes of operation depending on companies requirements:

- **Public cloud**
  The cloud infrastructure is owned by an organization selling cloud services to the general public and businesses.
- **Private cloud**
  The cloud infrastructure is operated solely for an organization. It may be managed by the organization (*Internal Private Cloud*) or a third party (*External Private Cloud*).
- **Community cloud**
  The cloud infrastructure is shared by several organizations/businesses and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations).
- **Hybrid cloud**
  The cloud infrastructure in this case is a mixture of the previous modes.

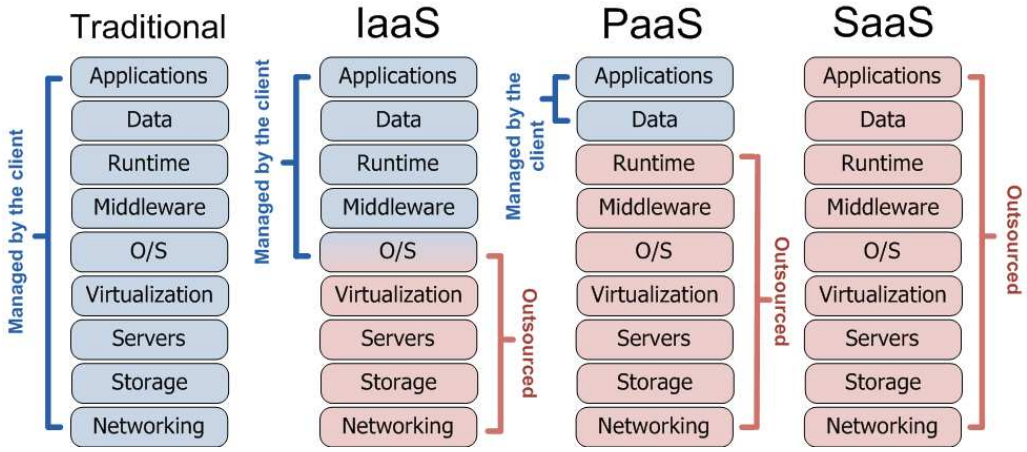
Cloud computing is designed to target quality of service and service availability requirements. Three main cloud computing delivery models are available:

- **Software as a Service** (*SaaS*);
- **Platform as a Service** (*PaaS*);
- **Infrastructure as a Service** (*IaaS*).

The following table describes the main differences between these three delivery models:

Action / Model	SaaS	PaaS	IaaS
Run	Pre-configured software Pay-per-use model (no need to buy any software license)	User applications Deployed application can be programmed by user or a cloud provider	User applications
Deliver	User service	Application platform (databases, high availability, scalability…)	Computing resources (storage, network, Virtual Machine…)
Automation	Full	Important	Limited
Cost	Very low	Low	Moderate
Operation management	All infrastructure/platform is outsourced (hardware, housing, application framework, software…)	Client is in charge of its applications and data (he rest is outsourced)	Client is in charge of its application, middleware and a part of the OS Management possibly done by a third-party
Data supervision by client	Difficult Client can supervise only few things	Moderate Roles are shared	Easy Client can supervise the complete virtual infrastructure

The next figure shows the elements which are outsourced and still managed by the client following the three delivery models of cloud computing compared to the traditional server-client mode.



Cloud computing benefits for businesses can be summarized as follows:

1. **Delivery of service**. High availability service, shorter time-to-value and time-to-market;
2. **Reduction of cost**. Businesses pay only what they use (pay-per-use), they have no capital expenditures, they can cater to varying consumer capacities as needed;
3. **IT department transformation**. Businesses can focus on innovation on their end-product instead of infrastructure maintenance.

SECURITY IN THE CLOUD

Cloud computing can provide major benefits to organizations from a cost, flexibility and scalability perspective. In addition, cloud computing also provides some security advantages:

- **Infrastructure securities**
  - *Quality of infrastructure*. Usually, providers provide quality materials (servers, networking…).
  - *Mastering*. Usually, technician's providers know their system and infrastructure and can re-construct services and infrastructures rapidly.
- **Network securities**
  - *Networking*. Usually, data centers' providers use dedicated and secure networks between other data centers.
- **Provider management**
  - *Maintenance.* Usually, providers have a dedicated team for resources management.

However, many companies and security laboratories have raised many concerns about cloud computing security. In general, cloud providers use highly secure data centers for data storage and management. But this precaution is not sufficient in most cases. The next issues must be taken into account before considering the cloud deployment of any application:

- **Data securities**
  - *Physical security.* What type of physical security measures are in place in data centers?
  - *Location of applications and data.* Cloud service providers use data centers in various countries. Knowing exactly where data are at any given time is sometimes difficult for providers. This could be a legal issue, for instance in banking or government applications.
  - *Access control.* Who can have an access to the applications and data? Access control must be properly defined and cloud provider roles properly identified.
  - *Data protection*. How is the data protected and secured from theft and damage? Are data encrypted? How are encryptions keys rotated and managed?
  - *Data segregation.* Usually companies' data share the same environment and data centers with uncontrolled third parties. How is data segregation performed?
- **Infrastructure securities**
  - *Cloud monitoring*. How is the environment monitored for OS/databases/application failures and how are clients notified?
  - *Flexibilities*. Does the system have enough customization capabilities to suit the client needs?
- **Network securities**
  - *Network protection*. Do providers guarantee data confidentiality and integrity when data enters and exits their data center? How is data protected in transit in the cloud?
- **Provider management**
  - *Responsibility*. Who is accountable if the cloud is unavailable?
  - *Recovery plan*. How do providers deal with recovery plans?
  - *End of service*. What happens if the cloud provider is out of business?
  - *Cost*. Does a cloud computing solution cost less than a traditional private infrastructure when applications are critical and have strong security requirements?

CLOUD COMPUTING FOR CONTENT SERVICES

Outsourcing or "cloudifying" content protection and rights management applications involves strong security needs and requirements that cloud service providers should be in conformance with, *i.e.*,:

- **Software compatibility**
  By default, *PaaS* and *IaaS* support a large choice of software. However, content services applications may require specific platform software and application languages for their own needs.
- **Specific hardware resource with Hardware Security Module (HSM)**

Content services applications generally require a dedicated use of HSM for cryptographic operations and data protection. Some cloud service providers are aware of, and already use, HSM in their cloud architecture.

- **Flexibility concerning data location**
  In content services applications, data location should be treated with special attention. Indeed, cloud computing elasticity is based on virtual machine migration (applications and platform) between data centers that can be located all around the world. Specific rules shall apply to personal and application data location.
- **Permanent data confidentiality and integrity**
  Content services applications' data (e.g., video content at various stages of the content management workflow, digital usage rights, authentication credentials, end-user's billing information…) are really sensitive information. Confidentiality, integrity should be considered during the complete data lifecycle. Cloud infrastructure can provide VPN based authentication, white list access or data encryption on servers' files system. Software can be deployed in the cloud to ensure data integrity.
- **Third-party application management**
  Cloud service providers do not always provide application management. But some third-party vendors can handle this. All terms should be discussed during contracting.
- **High service availability**
  Content services applications require high service availability of service even in the face of denial-of-service potential threats. Providers have to support this requirement with application replication and migration. Availability can be improved by using distant or foreign data centers and by using active-active servers principle (data/service/database are mirrored and synchronized between data centers).
- **Reducing the cost**
  Using cloud architecture should reduce application management costs. Security and high availability mechanisms should be considered in the total price.

- **Legal framework**. There is a lack of global legal framework, which could sometimes be also ineffective in some countries.

Compatible cloud computing architectures for content protection and rights management applications are only PaaS and IaaS since the SaaS model implies complete reliance upon the cloud service provider for the application framework and related data management. But PaaS and IaaS require in that context higher vigilance and a particular attention must be given to the contract with the provider since it should identify and cover a large scale of security issues.

Providing a comprehensive and global security management analysis is of paramount importance for content service application development or migration: a global security approach addressing technical, operational and legal frameworks over time is required. Moreover, security monitoring is critical for the service reliability: new attacks methods or vulnerabilities in the system must be addressed with a clear visibility into the services operations or data that could be potentially affected. Content services providers shall be able to examine the capabilities of each vendor in the chain regarding security awareness and renewability.

Among the various security topics that need to be addressed, one must pay particular attention to the following aspects:

- Application security – measures covering data integrity, data confidentiality in virtualized environments, isolation levels, physical access to data centers.
- Data management – data creation, deletion, export/import.

- Service features – application administration tools, platform management, alert management.
- Quality of Service (QoS) – service availability, connectivity requirements, resource allocation, service access, response time.
- Legal framework.

Adding a pinch of security – a lightning rod of sorts – here and there on top of cloud computing will not do to stop cloud “thunder” and “storms”. Content services in the cloud deserve a comprehensive management of security – a 360° security approach.

About Viaccess

Viaccess is a leader in solutions to protect and enhance the value of content services. Viaccess provides world class solutions for content protection, delivering conditional access and DRM-based systems for all types of content, for all networks including broadcast, broadband, fixed and mobile networks and for all categories of devices. Its subsidiary, Orca Interactive, is a leading innovative provider of IPTV middleware and applications including groundbreaking content discovery and recommendation solutions that power next-generation interactive TV. Viaccess has more than 20 years of broadcast and broadband experience and is positioned to help content service providers to monetize the content consumption revolution. Viaccess solutions are deployed worldwide in 35 countries and on more than 80 digital platforms. Viaccess S.A. is a France Telecom Group company.

For more information, please visit www.viaccess.com

viaccess