Security and Privacy in Cloud Computing

J.M.Suri, DDG(I), TEC
B.K.Nath, Dir(I), TEC

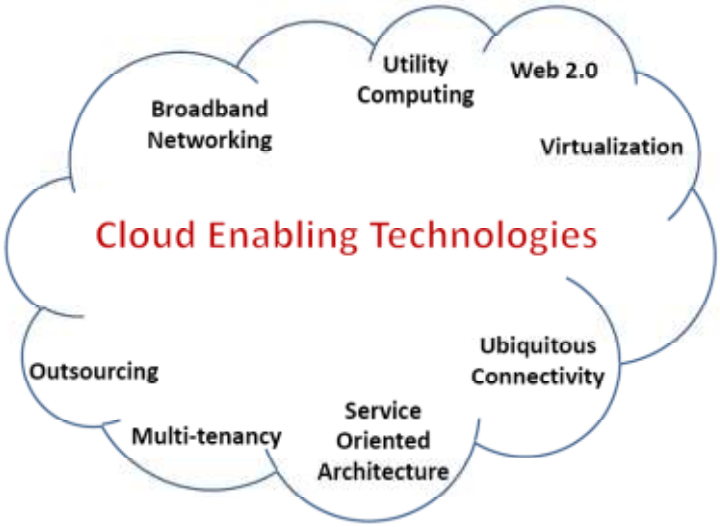
Telecommunication Engineering Centre
Khurshid Lal Bhawan
Janpath, New Delhi -1

Contents

Security and Privacy in Cloud Computing

1.0 Introduction

In recent times, cloud computing has emerged in a big way. While there is no doubt about the power of the cloud computing model and the benefits which it can give to different public and private organizations, the widespread adoption of cloud is still very far away. The cloud as a platform has been possible due to many enabling technologies which have been discovered in the recent years. Some of them are shown below.



Therefore, cloud computing environments have become a reality. However, the adoption depends on several key factors concerning the users like reliability, desired results, the amount of trust that can be imposed on the cloud, security of the data, privacy protection, intellectual property and so on. Cloud computing has some major benefits as given below, which are hard to dispute:

1. Reduced implementation and maintenance costs
2. Increased mobility for a global workforce
3. Flexible and scalable infrastructures
4. Quick time to market
5. IT department transformation (focus on innovation vs. maintenance and implementation)

6. "Greening" of the data center

7. Increased availability of high-performance applications to small/medium-sized businesses

But it will still require several years and many changes in the market before cloud computing is a mainstream IT effort. The various factors that are discouraging adoption of cloud computing are–

(i) Lack of understanding the technology,
(ii) Data ownership rights,
(iii) Performance and availability of a cloud solution as compared to in-house solutions.
(iv) Most common concern is security and privacy.

Regarding security and privacy, a finding was reported by IDC based on a study of views of 244 CIOs on cloud computing, in which 75% of respondents listed security as their number-one concern[1]. The IT infrastructure was so far designed around architectures that were built for on-premises services and secured by firewalls and threat-detection systems. Such architectures are not suitable for securing data in cloud environments. In general organizations are simply scared to move forward to cloud environment. This may be a valid concern but it is not impossible to address. The security community is also coming together through various initiatives aimed at education and guidance creation. The National Institute of Standards and Technologies (NIST) has released its first guidelines for agencies that want to use cloud computing in the second half of 2009. As with any emerging technology, there exists a learning curve with regard to security in a cloud environment but there is enough experience available to address various issues by the organizations.

2.0 Cloud Computing Deployment Models

There are primarily the following deployment models generally seen.

(i) **Public Cloud** - Public cloud computing is one of several deployment models that have been defined. A public cloud is one in which the infrastructure and other computational resources that it comprises are made available to the general public over the Internet. It is owned by a cloud provider selling cloud services and, by definition, is external to an organization.

(ii) **Private Cloud** - A private cloud is one in which the computing environment is operated exclusively for an organization. It may be managed either by the organization or a third party, and may be hosted within the organization's data center or outside of it. A private cloud gives the organization greater control over the infrastructure and computational resources than does a public cloud.

(iii) **Community Cloud** - A community cloud is somewhat similar to a private cloud, but

[1] "IT Cloud Services User Study," IDC, Inc., October 2008.

the infrastructure and computational resources are shared by several organizations that have common privacy, security, and regulatory considerations, rather than for the exclusive use of a single organization.

(iv) **Hybrid cloud -** A hybrid cloud is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables interoperability.

3.0 Cloud Computing Service Models

(i) **Software-as-a-Service -** Software-as-a-Service (SaaS) is a model of software deployment whereby one or more applications and the computational resources to run them are provided for use on demand as a turnkey service. Its main purpose is to reduce the total cost of hardware and software development, maintenance, and operations. Security provisions are carried out mainly by the cloud provider. The cloud subscriber does not manage or control the underlying cloud infrastructure or individual applications, except for preference selections and limited administrative application settings.

(ii) **Platform-as-a-Service -** Platform-as-a-Service (PaaS) is a model of software deployment whereby the computing platform is provided as an on-demand service upon which applications can be developed and deployed. Its main purpose is to reduce the cost and complexity of buying, housing, and managing the underlying hardware and software components of the platform, including any needed program and database development tools. The development environment is typically special purpose, determined by the cloud provider and tailored to the design and architecture of its platform. The cloud subscriber has control over applications and application environment settings of the platform. Security provisions are split between the cloud provider and the cloud subscriber.

(iii) **Infrastructure-as-a-Service.** Infrastructure-as-a-Service (IaaS) is a model of software deployment whereby the basic computing infrastructure of servers, software, and network equipment is provided as an on-demand service upon which a platform to develop and execute applications can be established. Its main purpose is to avoid purchasing, housing, and managing the basic hardware and software infrastructure components, and instead obtain those resources as virtualized objects controllable via a service interface. The cloud subscriber generally has broad freedom to choose the operating system and development environment to be hosted. Security provisions beyond the basic infrastructure are carried out mainly by the cloud subscriber.

(iv) **Communication-as-a-Service (CaaS) -** CaaS is an outsourced enterprise

communications solution. Providers of this type of cloud-based solution (known as CaaS vendors) are responsible for the management of hardware and software required for delivering Voice over IP (VoIP) services, Instant Messaging (IM), and video conferencing capabilities to their customers.

(v) **Monitoring-as-a-Service (MaaS) -** Monitoring-as-a-Service (MaaS) is the outsourced provisioning of security, primarily on business platforms that leverage the Internet to conduct business. It involves protecting an enterprise or government client from cyber threats. Many industry regulations require organizations to monitor their security environment, server logs, and other information assets to ensure the integrity of these systems. However, conducting effective security monitoring can be a daunting task because it requires advanced technology, skilled security experts, and scalable processes - none of which come cheap. MaaS security monitoring services offer real-time, 24/7 monitoring and nearly immediate incident response across a security infrastructure by helping to protect critical information assets of their customers.

a. The total cost of ownership (TCO) for traditional Security Operations Centre (SOCs), predominantly manual, is much higher than for a modern-technology SOC; and
b. Achieving lower security operations costs and higher security effectiveness means that modern SOC architecture must use security and IT technology to address security risks.

4.0 Building confidence in the Cloud Model

The majority of today's cloud computing infrastructure consists of timetested and highly reliable services built on servers with varying levels of virtualized technologies, which are delivered via large data centers operating under service-level agreements that require 99.99% or better uptime. Commercial offerings have evolved to meet the quality-of-service requirements of customers and typically offer such service-level agreements to their customers. From users' perspective, the cloud appears as a single point of access for all their computing needs. These cloud-based services are accessible anywhere in the world, as long as an Internet connection is available. Open standards and open-source software have also been significant factors in the growth of cloud computing.

Reliability is often enhanced in cloud computing environments because service providers utilize multiple redundant sites for disaster recovery. This is attractive to enterprises for business continuity and disaster recovery reasons. The drawback, however, is that IT managers can do very little when an outage occurs. Another benefit that makes cloud services more reliable is that scalability can vary dynamically based on changing user demands. Because the service provider manages the necessary infrastructure, security often is vastly improved. As a result of data centralization, there is an increased focus on protecting customer resources maintained by the service provider. Security has to be ensured across 3 levels - Physical, personnel and IT security. To assure customers that their data is safe, cloud providers are quick to invest in various security practices. Some of the good security certification with standards are

detailed in ISO27001[2] or PCI DSS[3] and has to be checked if these have been properly implemented in the cloud environment.

5.0 Good Security Practices in Cloud Computing Environment

1. Protection Against Internal and External Threats

Security monitoring services help to improve the effectiveness of the security infrastructure of a customer by actively analyzing logs and alerts from infrastructure devices around the clock and in real time. Monitoring teams correlate information from various security devices to provide security analysts with the data they require to eliminate false positives and respond to true threats against the enterprise. Usually the skills required to maintain the level of service of an organization is very high. The information security team can assess system performance on a periodically recurring basis and provide recommendations for improvements as needed. Typical services provided by many MaaS vendors are described below.

2. Early Detection

An early detection service detects and reports new security vulnerabilities shortly after they appear. Generally, the threats are correlated with third party sources, and an alert or report is issued to customers. Security vulnerability reports, aside from containing a detailed description of the vulnerability and the platforms affected, also include information on the impact the exploitation of this vulnerability would have on the systems or applications previously selected by the company receiving the report. Most often, the report also indicates specific actions to be taken to minimize the effect of the vulnerability, if that is known.

3. Platform, Control, and Services Monitoring

Platform, control, and services monitoring is often implemented as a dashboard interface[4] and makes it possible to know the operational status of the platform being monitored at any time. It is accessible from a web interface, making remote access possible. Each operational element that is monitored usually provides an operational status indicator, always taking into account the critical impact of each element. This service aids in determining which elements may be operating at or

---

[2] **ISO/IEC 27001**, part of the growing ISO/IEC 27000 family of standards, is an Information Security Management System (ISMS) standard published in October 2005 by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). Its full name is *ISO/IEC 27001:2005 - Information technology -- Security techniques -- Information security management systems -- Requirements*.

[3] The Payment Card Industry Data Security Standard (PCI DSS) is a widely accepted set of policies and procedures intended to optimize the security of credit, debit and cash card transactions and protect cardholders against misuse of their personal information. The PCI DSS was created jointly in 2004 by four major credit-card companies: Visa, MasterCard, Discover and American Express.

[4] A dashboard is a floating, semitransparent window that provides contextual access to commonly used tools in a software program.

near capacity or beyond the limits of established parameters. By detecting and identifying such problems, preventive measures can be taken to prevent loss of service.

4. Intelligent Log Centralization and Analysis

Intelligent log centralization and analysis is a monitoring solution based mainly on the correlation and matching of log entries. Such analysis helps to establish a baseline of operational performance and provides an index of security threat. Alarms can be raised in the event an incident moves the established baseline parameters beyond a stipulated threshold. These types of sophisticated tools are used by a team of security experts who are responsible for incident response once such a threshold has been crossed and the threat has generated an alarm or warning picked up by security analysts monitoring the systems.

5. Vulnerabilities Detection and Management

Vulnerabilities detection and management enables automated verification and management of the security level of information systems. The service periodically performs a series of automated tests for the purpose of identifying system weaknesses that may be exposed over the Internet, including the possibility of unauthorized access to administrative services, the existence of services that have not been updated, the detection of vulnerabilities such as phishing, etc. The service performs periodic follow-up of tasks performed by security professionals managing information systems security and provides reports that can be used to implement a plan for continuous improvement of the system's security level.

6. Continuous System Patching/Upgrade and Fortification

Security posture is enhanced with continuous system patching and upgrading of systems and application software. New patches, updates, and service packs for the equipment's operating system are necessary to maintain adequate security levels and support new versions of installed products. Keeping abreast of all the changes to all the software and hardware requires a committed effort to stay informed and to communicate gaps in security that can appear in installed systems and applications.

7. Intervention, Forensics, and Help Desk Services

Quick intervention when a threat is detected is crucial to mitigating the effects of a threat. This requires security engineers with ample knowledge in the various technologies and with the ability to support applications as well as infrastructures on a 24/7 basis. MaaS platforms routinely provide this service to their customers. When a detected threat is analyzed, it often requires forensic analysis to determine what it is, how much effort it will take to fix the problem, and what effects are likely to be seen. When problems are encountered, the first thing customers tend to do is pick up the phone. Help desk services provide assistance on questions or issues about the operation of running systems. This service includes assistance in writing failure reports, managing operating problems, etc.

6.0 Ensuring Privacy in Cloud Computing Environment

Privacy protection in cloud computing environment is less of a technical issue and more of a policy and legal issue. Policies are required to be framed to conform to the legal framework protecting the privacy of individual and organizations. Policies have to empower people to control the collection, use, and distribution of their personal information. A very good framework on privacy protection is given by the *Safe Harbor privacy principles*[5] developed by the U.S. Department of Commerce and the European Commission. It is based on 7 principles. These principles must provide:

- **Notice** - Individuals must be informed that their data is being collected and about how it will be used.
- **Choice** - Individuals must have the ability to opt out of the collection and forward transfer of the data to third parties.
- **Onward Transfer** - Transfers of data to third parties may only occur to other organizations that follow adequate data protection principles.
- **Security** - Reasonable efforts must be made to prevent loss of collected information.
- **Data Integrity** - Data must be relevant and reliable for the purpose it was collected for.
- **Access** - Individuals must be able to access information held about them, and correct or delete it if it is inaccurate.
- **Enforcement** - There must be effective means of enforcing these rules.

These tenets provide a framework for the development of privacy principles developed by major organizations across the world, which guide the use and management of customer and partner information. Therefore, some of the key issues while framing a suitable policy could be as given below-

(i) **Accountability –** In handling personal information by the cloud provider and with the vendors and partners

(ii) **Notice –** to individuals about how the personal information is collected, used, retained and disclosed to third parties.

(iii) **Collection –** of personal information from the individuals only for the purposes specified in the privacy notice and acceptable to the individual.

[5] **US-EU Safe Harbor** is a streamlined process for US companies to comply with the EU Directive 95/46/EC on the protection of personal data. Intended for organizations within the EU or US that store customer data, the **Safe Harbor Principles** are designed to prevent accidental information disclosure or loss. US companies can opt into the program as long as they adhere to the 7 principles outlined in the Directive. The process was developed by the US Department of Commerce in consultation with the EU.

(iv) **Choice and consent -** for individuals regarding how the cloud provider collects, uses, and discloses their personal information. The individual should be given a choice to accept or opt out.

(v) **Use and retention -** of personal information in accordance with the privacy notice and consent that individuals have provided. Individuals should be given adequate information on how the data will be used and for how long it will be retained.

(vi) **Disclosure or onward transfer –** of personal information to vendors and partners only for purposes that are identified in the privacy notice, and in a secured manner to avoid leakage in transit.

(vii) **Quality assurance -** steps to ensure that personal information in the records is accurate and relevant to the purposes for which it was collected.

(viii) **Access -** for individuals who want to inquire about and, when appropriate, review and update their personal information in the cloud provider's possession. Individuals should have the choice to correct the information in case of errors.

(ix) **Enhanced security -** of personal information to help protect against unauthorized access and use. Only authorized users to have access to the data and also to ensure that they are adequately isolated from each other.

(x) **Monitoring and enforcement –** of compliance with the privacy policies, both internally and with the vendors and partners, along with established processes to address inquiries, complaints, and disputes.

These issues are specialized and organizations may need to hire privacy professionals to adequately address the various issues and plug the loopholes in a system. They also help to ensure that the various privacy policies, Organization procedures, and technologies are applied across the cloud provider's products, services, processes, and systems.

7.0 Legal and Regulatory Challenges

Cloud services can thrive when cloud providers are able to provide services efficiently and assure customers that their data will remain private and secure. This should be the focus of cloud service providers. But then significant legal and regulatory challenges have to be overcome when the data moves out of a country.

(i) Multinational Framework on privacy and security:

As more and more data moves to the cloud, uncertainty about the legal and regulatory obligations related to that data will also increase. To ensure that cloud computing can reach its full potential different countries will have to cooperate to develop a multinational framework on privacy and security in the cloud. One particularly complicated issue is the regulation of cross-border data flows. As cloud computing evolves, traditional geographical limits on the movement of data are changing. Information might be created in India using

software hosted in UK, stored in the United States, and accessed in Singapore. It is a challenge for a cloud provider to coordinate such a situation.

(ii) Rules on Cross Border Data Transfers:

To optimize the efficiency of cloud services and deliver the fast performance and reliability customers expect, cloud providers must be able to operate datacenters in multiple locations and transfer data freely among them. Unhindered data flows allow cloud providers to optimize the efficiency of their services and deliver the performance and reliability customers expect. However, restrictions on cross-border data transfers can create uncertainty if the rules or the legal framework that applies to such transfers are not clear.

(iii) **Conflicting Legal Obligations**:

Cloud providers are put in a difficult position when different governments impose conflicting legal obligations and assert competing claims of jurisdiction over data held by cloud providers. Divergent rules on privacy, data retention, law enforcement access and other issues can lead to ambiguity and significant legal challenges. For instance, one country might insist that its rules regarding mandatory data retention or law enforcement access apply in a given context. However, those rules might be in direct conflict with the privacy laws of another country that has a strong claim of jurisdiction over the same data.

IT companies will have to face the majority of these problems first. If businesses are forced to store data locally in order to mitigate jurisdictional conflicts, the cost of investment and innovation in cloud computing will increase. As a result, the efficiency and performance benefits of cloud computing may be lost and the benefits to governments, businesses, and consumers will decline. However, for majority of the cloud providers this may be the only short-term solution till a proper global framework is evolved in consultation with different national governments. ITU, the International Telecommunication Union, can play a major role in this area by evolving a general security and privacy framework involving different countries and push them to align their national laws in this direction to facilitate cloud computing. Till such time, cloud service providers may have to build localized data centers and also ensure that the data belonging to one country stays within the limits of that country.

Large multinational Organizations, with businesses in different countries, will have to devote significant time and money to develop globally consistent policy frameworks that recognize the worldwide nature of data flows while at the same time providing strong privacy protections. On the other hand, Governments will have to clarify the rules and processes to resolve conflicting obligations in ways that protect privacy and security.

Governments around the world can enhance cloud security by increasing law enforcement resources and strengthening criminal and civil enforcement mechanisms against malicious hacking of cloud services. Although the cloud is being built with unprecedented security, the aggregation of data in cloud data centers presents new and rich targets for hackers and thieves. To combat such criminals, legislation is needed to enhance criminal enforcement of crimes targeting cloud data centers and to allow cloud service providers to sue violators directly.

Governments can also help users make informed choices by promoting transparency around cloud providers' privacy and security practices. It should not be left to the cloud providers to claim that their services are private and secure. There should be third party auditing mechanisms for cloud providers. To improve transparency, legislation should require that cloud service providers maintain comprehensive written information security programs with safeguards appropriate to the use of their services; provide summaries of those programs to potential customers, and disclose their privacy practices to any individual or customer from whom personal information is collected.

8.0 Conclusion

Cloud computing offers organizations and individuals the promise of enhanced choice, flexibility, and cost savings. To realize such benefits users must have reliable assurances from cloud providers regarding the privacy and security of their personal data. Regulators and lawmakers around the world can help fulfill the potential of cloud computing by resolving legal, jurisdictional, and public policy uncertainties surrounding cloud services. In this regard, multinational organizations, who are actually operating in many countries and have to deal with various laws and regulations can partner with industry leaders, governments and consumer organizations to develop globally consistent privacy frameworks that will maximize the economic and social benefits of cloud computing.

9.0 References

[1] Richard Chow et.al. *Controlling Data in the cloud: outsourcing Computation without outsourcing control.*

[2] Centre for the Protection of National Infrastructure, *Information Security Briefing 01/2010*

[3] Microsoft publication, *Privacy in the Cloud: A Microsoft perspective, November 2010*

[4] J.W.Rittinhouse et. al., CRC Press, 2010, *Cloud Computing Implementation, Management and Security*

[5] Jan Gabrielsson et. al., Ericsson Review.1 2010, *Cloud Computing in Telecommunications*

[6] EC Expert Group Report, *The Future of Cloud Computing: Opportunities for European Cloud Computing Beyond 2010*