Journal of Information Engineering and Applications
ISSN 2224-5782 (print) ISSN 2225-0506 (online)
Vol.5, No.1, 2015

Cloud Security Issues

Pradip Patil Rajnikant Palwe Gurudatt Kulkarni Shrikant Belsare
Lecturer in Marathwada Mitra Mandal's Polytechnic, Pune

Kundlik Koli
Lecture in Vidya Pratishtan Polytechnic, Indapur

Abstract
The emergence of cloud computing is a recent development, insights into critical aspects of security can be gleaned from reported experiences of early adopters and also from researchers analyzing and experimenting with available cloud provider platforms and associated technologies. The sections below highlight privacy and security-related issues that are believed to have long-term significance for public cloud computing and, in many cases, for other cloud computing service models. Because cloud computing has grown out of an amalgamation of technologies, including service oriented architecture, virtualization, Web 2.0, and utility computing, many of the privacy and security issues involved can be viewed as known problems cast in a new setting. The importance of their combined effect in this setting, however, should not be discounted. Public cloud computing does represent a thought-provoking paradigm shift from conventional norms to an open deperimeterized organizational infrastructure—at the extreme, displacing applications from one organization's infrastructure to the infrastructure of another organization, where the applications of potential adversaries may also operate.
Keywords: cloud security, IaaS, Privacy

1.0 Introduction

Cloud computing is not a total new concept; it is originated from the earlier large-scale distributed computing technology. However, it will be a subversion technology and cloud computing will be the third revolution in the IT industry, which represent the development trend of the IT industry from hardware to software, software to services, distributed service to centralized service. Cloud computing is also a new mode of business computing, it will be widely used in the near future. The core concept of cloud computing is reducing the processing burden on the users' terminal by constantly improving the handling ability of the "cloud", eventually simplify the users' terminal to a simple input and output devices, and busk in the powerful computing capacity of the cloud on-demand. All of this is available through a simple Internet connection using a standard browser or other Connection. Cloud architecture typically involves multiple cloud components communicating with each other over application programming interfaces, usually services. Complexity is controlled and the resulting systems are more manageable than their monolithic counterparts. The two most significant components of cloud computing architecture are known as the front end and the back end. The front end is the part seen by the client, i.e. the computer user. This includes the client's network (or computer) and the applications used to access the cloud via a user interface such as a web browser. The back end of the cloud computing architecture is the 'cloud' itself, comprising various computers, servers and data storage devices. Cloud computing is not secure by nature. Security in the Cloud is often intangible and less visible, which inevitably creates a false sense of security and anxiety about what is actually secured and controlled. The off-premises computing paradigm that comes with cloud computing has incurred great concerns on the security of data, especially the integrity and confidentiality of data, as cloud service providers may have complete control on the computing infrastructure that underpins the services This paper looks at the main security and privacy issues pertinent to cloud computing, as they relate to outsourcing portions of the organizational computing environment. It points out areas of concern with public clouds that require special attention and provides the necessary background to make informed security decisions

2.0 Service Models

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network 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. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models.[2,3]

- Cloud Software as a Service (SaaS). The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a Web browser (e.g., Web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user specific application configuration settings.

- Cloud 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. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.

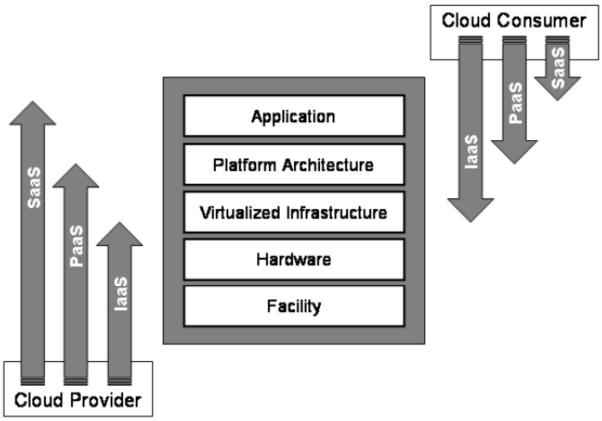

Figure 2.1 Cloud Computing Models with Implementation

- Cloud 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. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

3.0 Deployment Models: [2,3]

- Private cloud:- The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.
- Community cloud:- The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.
- Public cloud: - The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services. [2]

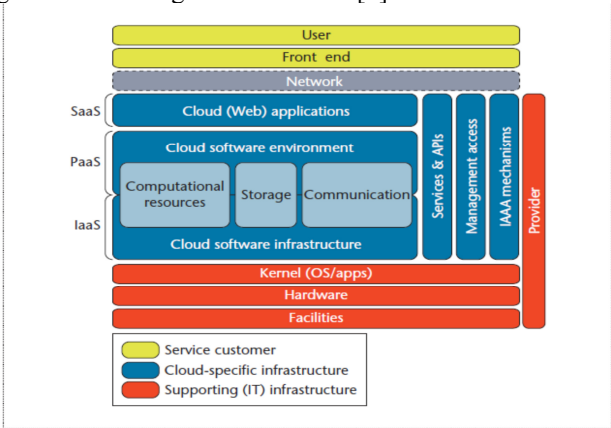

Figure 2.2 Cloud Computing Reference Architecture

- Hybrid cloud:- The cloud infrastructure 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 data and application portability (e.g., cloud bursting for load balancing between clouds).

4.0 Essential Characteristics: [3,4]

- On-demand self-service:- A consumer can unilaterally provision computing capabilities, such as server

time and network storage, as needed automatically without requiring human interaction with each service's provider.

- Broad network access:- Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and personal digital assistants [PDAs]).
- Resource pooling:- The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.
- Rapid elasticity:- Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.
- Measured Service:-Cloud systems automatically control and optimize resource use by leveraging a metering capability 3 at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

5.0 Security Issues with Cloud:-[4]

- **A user's privacy and confidentiality risks vary significantly with the terms of service and privacy policy established by the cloud provider.**
  Those risks may be magnified when the cloud provider has reserved the right to change its terms and policies at will. The secondary use of a cloud computing user's information by the cloud provider may violate laws under which the information was collected or are otherwise applicable to the original user. A cloud provider will also acquire transactional and relationship information that may itself be revealing or commercially valuable. For example, the sharing of information by two companies may signal a merger is under consideration. In some instances, only the provider's policy will limit use of that information. Many users are likely not aware of the details set out in the terms of service for cloud providers or of the consequences of sharing information with a cloud provider.
- **For some types of information and some categories of cloud computing users, privacy and confidentiality rights, obligations, and status may change when a user discloses information to a cloud provider.**
  Procedural or substantive barriers may prevent or limit the disclosure of some records to third parties, including cloud computing providers. For example, health record privacy laws may require a formal agreement before any sharing of records is lawful. Other privacy laws may flatly prohibit personal information sharing by some corporate or institutional users. Professional secrecy obligations, such as those imposed on lawyers, may not allow the sharing of client information. Sharing information with a cloud provider may undermine legally recognized evidentiary privileges. Records management and disposal laws may limit the ability of a government agency to use cloud computing for official records.
- **Disclosure and remote storage may have adverse consequences for the legal status of or protections for personal or business information.**
  For example, a trade secret shared with a cloud provider may lose some of its legal protections. When a person stores information with a third party (including a cloud computing provider), the information may have fewer or weaker privacy protections than when the information remains only in the possession of the person. Government agencies and private litigants may be able to obtain information from a third party more easily than from the original owner or creator of the content. A cloud provider might even be compelled to scan or search user records to look for fugitives, missing children, copyright violations, and other information of interest to government or private parties. Remote storage may additionally undermine security or audit requirements.
- **The location of information in the cloud may have significant effects on the privacy and confidentiality protections of information and on the privacy obligations of those who process or store the information.**
  Any information stored in the cloud eventually ends up on a physical machine owned by a particular company or person located in a specific country. That stored information may be subject to the laws of the country where the physical machine is located. For example, personal information that ends up maintained by a cloud provider in a European Union Member State could be subject permanently to European Union privacy laws.

- **Information in the cloud may have more than one legal location at the same time, with differing legal consequences.**
  A cloud provider may, without notice to a user, move the user's information from jurisdiction to jurisdiction, from provider to provider, or from machine to machine. The legal location of information placed in a cloud could be one or more places of business of the cloud provider, the location of the computer on which the information is stored, the location of a communication that transmits the information from user to provider and from provider to user, a location where the user has communicated or could communicate with the provider, and possibly other locations.
- **Laws could oblige a cloud provider to examine user records for evidence of criminal activity and other matters.**
  Some jurisdictions in the United States require computer technicians to report to police or prosecutors evidence of child pornography that they find when repairing or otherwise servicing computers. To the extent that cloud computing places a diverse collection of user and business information in a single location, it may be tempting for governments to ask or require cloud providers to report on particular types of criminal or offensive behavior or to monitor activities of particular types of users (e.g., convicted sex offenders). Other possibilities include searching for missing children and for music or software copyright violations.
- **Legal uncertainties make it difficult to assess the status of information in the cloud as well as the privacy and confidentiality protections available to users.**
  The law badly trails technology, and the application of old law to new technology can be unpredictable. For example, current laws that protect electronic communications may or may not apply to cloud computing communications or they may apply differently to different aspects of cloud computing.
- **Responses to the privacy and confidentiality risks of cloud computing include better policies and practices by cloud providers, changes to laws, and more vigilance by users.**
  If the cloud computing industry would adopt better and clearer policies and practices, users would be better able to assess the privacy and confidentiality risks they face. Users might avoid cloud computing for some classes of information and might be able to select a service that meets their privacy and confidentiality needs for other categories of information. For those risks that cannot be addressed by changes in policies and practices, changes in laws may be appropriate. Each user of a cloud provider should pay more – and indeed, close – attention to the consequences of using a cloud provider and, especially, to the provider's terms of service.

Conclusion

Determining the security of complex computer systems composed together is also a long-standing security issue that plagues large-scale computing in general, and cloud computing in particular. Attaining high-assurance qualities in system implementations has been an elusive goal of computer security researchers and practitioners and, as demonstrated in the examples given in this report, is also a work in progress for cloud computing. Nevertheless, public cloud computing is a compelling computing paradigm that agencies should consider for their information technology solution set. Accountability for security and privacy in public cloud deployments cannot be delegated to a cloud provider and remains an obligation for the organization to fulfill. Federal agencies must ensure that any selected public cloud computing solution is configured, deployed, and managed to meet the security, privacy, and other requirements of the organization. Organizational data must be protected in a manner consistent with policies, whether in the organization's computing center or the cloud. The organization must ensure that security and privacy controls are implemented correctly and operate as intended, throughout the system lifecycle.

References

1. P. Mell and T. Grance, "Draft nist working definition of cloud computing - v15," *21. Aug 2009,* 2009.
2. Tharam Dillon, Chen Wu, Elizabeth Chang, 2010 24th IEEE International Conference on Advanced Information Networking and Applications, "Cloud computing: issues and challenges".
3. Rich Maggiani, solari communication. "Cloud computing is changing how we communicate".
4. "Understanding Cloud Computing Vulnerabilities", Bernd Grobauer, Tobias Walloschek, and Elmar Stöcker, Siemens, cloud computing A digital magazine in support of the IEEE Cloud Computing Initiative

The IISTE is a pioneer in the Open-Access hosting service and academic event management. The aim of the firm is Accelerating Global Knowledge Sharing.

More information about the firm can be found on the homepage:
http://www.iiste.org

CALL FOR JOURNAL PAPERS

There are more than 30 peer-reviewed academic journals hosted under the hosting platform.

Prospective authors of journals can find the submission instruction on the following page: http://www.iiste.org/journals/ All the journals articles are available online to the readers all over the world without financial, legal, or technical barriers other than those inseparable from gaining access to the internet itself. Paper version of the journals is also available upon request of readers and authors.

MORE RESOURCES

Book publication information: http://www.iiste.org/book/

Academic conference: http://www.iiste.org/conference/upcoming-conferences-call-for-paper/

IISTE Knowledge Sharing Partners

EBSCO, Index Copernicus, Ulrich's Periodicals Directory, JournalTOCS, PKP Open Archives Harvester, Bielefeld Academic Search Engine, Elektronische Zeitschriftenbibliothek EZB, Open J-Gate, OCLC WorldCat, Universe Digtial Library , NewJour, Google Scholar