INDIAN JOURNAL OF DEVELOPMENT RESEARCH AND SOCIAL ACTION
VOLUME 11 • NUMBERS 1-2 • JANUARY-DECEMBER 2015 • PP. 23-32

Cloud Computing and Security Issues in Cloud

Razi Asgher*, Md Deedar Shamsi* and Saima Aleem*

ABSTRACT

Cloud computing has formed the conceptual and infrastructural basis for tomorrow's computing. Cloud computing is a promising technology to facilitate development of large-scale, on-demand, flexible computing infrastructures. But without security embedded into innovative technology that supports cloud computing, businesses are setting themselves up for a fall. If security is not robust and consistent, the flexibility and advantages that cloud computing has to offer will have little credibility. This paper presents a review on the cloud computing concepts as well as security issues inherent within the context of cloud computing and cloud infrastructure.

Keywords: *Cloud computing, cloud service, cloud security, computer network, distributed computing, security.*

Introduction

Cloud computing is currently one the most hyped IT innovations. Most IT companies announce to plan or (suddenly) already have IT products according to the cloud computing paradigm. Though cloud computing itself is still not yet mature enough, it is already evident that its most critical flaw in security. In a cloud based computing infrastructure, the resources are normally in someone else's premise or network and accessed remotely by the cloud users. In some cases, it might be required or at least possible for a person to store data on remote cloud servers. These gives the following three sensitive states or scenarios that are of particular concern within the operational context of cloud computing:

- The transmission of personal sensitive data to the cloud server,
- The transmission of data from the cloud server to clients' computers and
- The storage of clients' personal data in cloud servers which are remote server not owned by the clients.

All the above three states of cloud computing are severely prone to security breach that makes the research and investigation within the security

* M. Tech Scholar in Computer Science & Engineering, Al-Falah University, Faridabad

aspects of cloud computing practice an imperative one. There have been a number of different blends that are being used in cloud computing realm, but the core concept remain same – the infrastructure, or roughly speaking, the resources remain somewhere else with someone else's ownership and the users 'rent' it for the time they use the infrastructure.

In the nearest future, we can expect to see a lot of new security exploitation events around cloud computing providers and users, which will shape the cloud computing security research directions for the next decade. The study presented in this paper is organized with a view to discuss and indentify the approach to cloud computing as well as the security issues and concerns that must be taken into account in the deployment towards a cloud based computing infrastructure. Discussion on the technological concepts and approaches to cloud computing including the architectural illustration has been taken into consideration within the context of discussion in this paper.

The National Institute of Standards and Technology (NIST) Information Technology Laboratory, cloud computing is defined as follows:

> *Cloud computing is a model for enabling 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.*

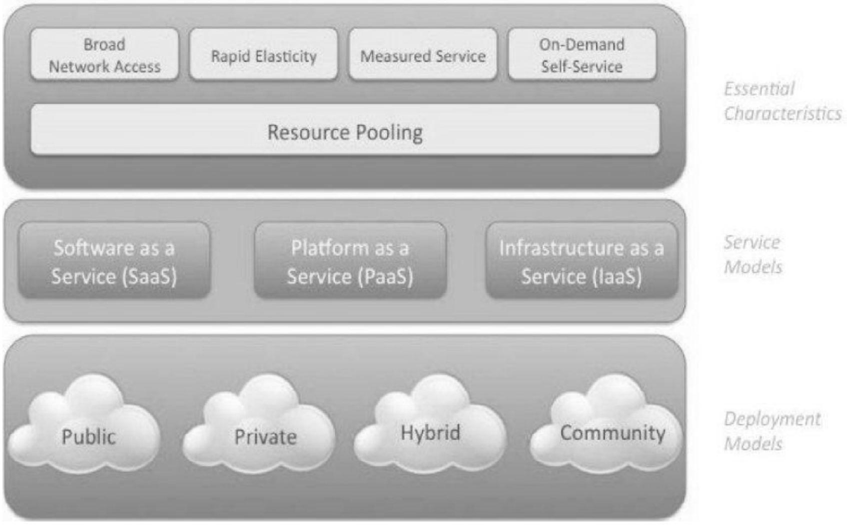
Cloud Computing Infrastructure

The term cloud computing is rather a concept which is a generalized meaning evolved from distributed and grid computing. Cloud computing is described as the offspring of distributed and grid computing by some authors. The straightforward meaning of cloud computing refers to the features and scenarios where total computing could be done by using someone else's network where ownership of hardware and soft resources are of external parties. In general practice, the dispersive nature of the resources that are considered to be the 'cloud' to the users are essentially in the form of distributed computing; though this is not apparent or by its definition of cloud computing, do not essentially have to be apparent to the user.

This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models. Essential Characteristics

- 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 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 data enter). 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 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.



Service Models

- 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.
- 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).

Deployment Models

- 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.
- 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).

Authentication In Cloud

Security is the most prioritized aspect for any form of computing, making it an obvious expectation that security issues are crucial for cloud environment as well. As the cloud computing approach could be associated with having users' sensitive data stored both at clients' end as well as in cloud servers, identity management and authentication are very crucial in cloud computing. Verification of eligible users' credentials and protecting such credentials are part of main security issues in the cloud - violation in these areas could lead to undetected security breach at least to some extent for some period. A possible authentication scenario for a cloud infrastructure is illustrated in figure.

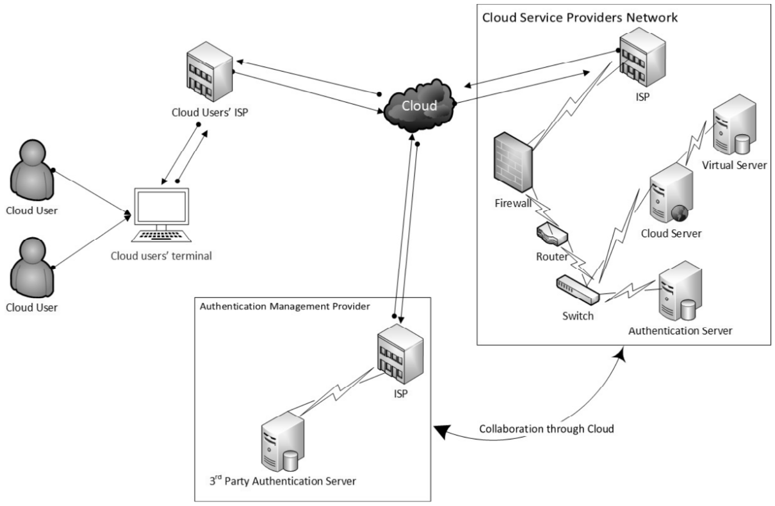


Figure: Authentication in Cloud System

The illustration presented in figure conveys that the authentication for the cloud users can be done either by the cloud service provider or the service provider can outsource the identity management and authentication service to third party specialists. In the later case, the cloud service provider is required to have collaboration with the third party authentication specialist – the collaboration between the cloud service provider and the third party authentication specialist during the authentication process of cloud users is done essentially through cloud. This feature adds performance overheads and security issues to the cloud context as the message passing between third party authentication management authority and the cloud service provider as part of collaboration might essentially be done through cloud infrastructure.

Security Issues in Cloud

Cloud computing comes with numerous possibilities and challenges simultaneously. Of the challenges, security is considered to be a critical barrier for cloud computing in its path to success. The security challenges for cloud computing approach are somewhat dynamic and vast. Data location is a crucial factor in cloud computing security. Location transparency is one of the prominent flexibilities for cloud computing, which is a security threat at the same time – without knowing the specific location of data storage, the provision of data protection act for some region might be severely affected and violated.

Some Security Concerns are Listed and Discussed Below

Concern #1: Company has violated the law (risk of data seizure by (foreign) government).

Concern #2: Storage services provided by one cloud vendor may be incompatible with another vendor's services if user decides to move from one to the other (e.g. Microsoft cloud is incompatible with Google cloud).

Concern #3: Who controls the encryption/decryption keys? Logically it should be the customer.

Concern #4: Ensuring the integrity of the data (transfer, storage, and retrieval) really means that it changes only in response to authorized transactions. A common standard to ensure data integrity does not yet exist.

Concern #5: Some government regulations have strict limits on what data about its citizens can be stored and for how long, and some banking regulators require that customer's financial data remain in their home country.

Concern #6: Customers may be able to sue cloud service providers if their privacy rights are violated, and in any case the cloud service providers may face damage to their reputation. Concerns arise when it is not clear to individuals why their personal information is requested or how it will be used or passed on to other parties.

Concern #7: With the cloud model control physical security is lost because of sharing computing resources with other companies. No knowledge or control of where the resources run.

Concern #8: The dynamic and fluid nature of virtual machines will make it difficult to maintain the consistency of security and ensure the audit ability of records.

Concern #9: In case of Payment Card Industry Data Security Standard (PCI DSS) data logs must be provided to security managers and regulators.

Concern #10: Users must keep up to date with application improvements to be sure they are protected.

Some Solution For Security Issues In Cloud Computing

Following approaches can be helpful for secure cloud computing-

- **Investigation Support:** Audit tools provided to the users to determine how their data is stored, protected, used, and verify policy enforcement. But investigation of illegal activity is quite difficult because data for multiple customers may be collocated and may also be geographically spread across set of hosts and datacenters. To solve this audit tools must be contractually committed along with the evidence.
- **Network Security**: A user can deny the access of any Internet based service by using IP Spoofing which can be a cause of security harm. To solve this we can use Digital Signature technique. SSL (Secure Socket Layer) Protocol is used for managing security of message transmission on The Internet. Which also avoid resource hacking.
- **Encryption Algorithm:** Obviously cloud service providers encrypt the user's information using strong encryption algorithm. But problem is that encryption accident can make data totally unusable and encryption also complicates the availability. To solve this problem the cloud provider must provide evidence that encryption scheme were designed and tested by experienced specialists.
- **Backup:** Natural disaster may damage the physical devices that may cause of data loss. To avoid this problem backup of information is the key of assurance of service provided by vendor
- **Customer satisfaction:** Very hard for the customer to actually verify the currently implemented security practices and initiatives of a cloud computing provided by the service provider because the customer generally has no access to the provider's facility which can be comprised of multiple facilities spread around the globe [8]. Solution for this Provider should get some standard certificate from some governing or standardized institution that ensures users that provider has established adequate internal control and these control are operating efficiently.

Conclusions

Cloud computing has enormous prospects, but the security threats embedded in cloud computing approach are directly proportional to its offered advantages. Cloud computing is the future of IT industries It helps the industries to get efficient use of their IT Hardware and Software resources at low cost. This paper totally discuss about the cloud computing security issues and Challenges. The security issues could severely affect could infrastructures. Security itself is conceptualized in cloud computing infrastructure as a distinct layer. This paper also analyze cloud computing vulnerabilities, security threats cloud computing faces and presented the security objective that need to be achieved. In this paper we discussed security issues for cloud. These issues include storage security, middleware security, data security, network security and application security. The main goal is to securely store and manage data that is not controlled by the owner of the data.

References

Open Security Architecture *http://www.opensecurityarchitecture.org/*

Nils Gruschka and Meiko Jensen, "Attack Surfaces: A Taxonomy for Attacks on Cloud Services". IEEE rd International Confrence on Cloud Computing, 2010.

http://en.wikipedia.org/wiki/Payment_Card_Industry_Data_ Security_Standard

http://en.wikipedia.org/wiki/Risk_management

http://en.wikipedia.org/wiki/Risk_assessment

https://www.pcisecuritystandards.org/index.shtml

https://cloudsecurityalliance.org/

https://cloudsecurityalliance.org/research/top-threats/

http://www.ibm.com/cloud-computing/in/en/security.html

http://www.informationweek.com/cloud/infrastructure-as-a-service/9-worst-cloud-security-threats/d/d-id/1114085

https://www.securityweek.com/security-infrastructure/cloud-security

https://www.skyhighnetworks.com/

http://challenge.semanticweb.org

Rashmi, Sahoo, G. and Mehfuz, S. (2013), Securing Software as a Service Model of Cloud Computing: Issues and Solutions.

Sharma, S. And Mittal, U. (2013). Comparative Analysis of Various Authentication Techniques in Cloud Computing. *International Journal of Innovative Research in Science, Engineering and Technology.*