Cloud Computing: Security Issues and Challenges

***Prof. Swapna.K (Kannankott)**
***Prof. Praveen Gupta**

Abstract

Today is the age of information technology. The facets of work and personal life are moving towards the concept of availability of everything online. The cloud makes it possible to access the information from anywhere at any time. Cloud computing is an internet based computing, where shared resources, software and information are provided to computers and devices on demand. In the last few years, cloud computing has grown from being a promising business concept to one of the fastest growing segments of the IT industry. Generally, cloud services are provided by a third-party supplier who possesses the arrangement. Cloud computing has completely transformed the way business organizations use IT both inside and outside of their organization. Cloud computing has many advantages like cost efficiency, convenience and continuous availability, scalability and performance, flexibility and increased storage capacity. However, Many enterprises are reluctant to move critical cloud applications out of their own data centers and into the public cloud due to security concerns. Security is a top concern for IT management because it is a most important requirement to protect the company information and to ensure system integrity. This paper mainly focuses on the security issues and challenges in cloud computing and enlightened the steps that an enterprise can take to reduce the security issues.

***Keywords**: Cloud computing, Information Security, Integrity, Challenges*

Introduction

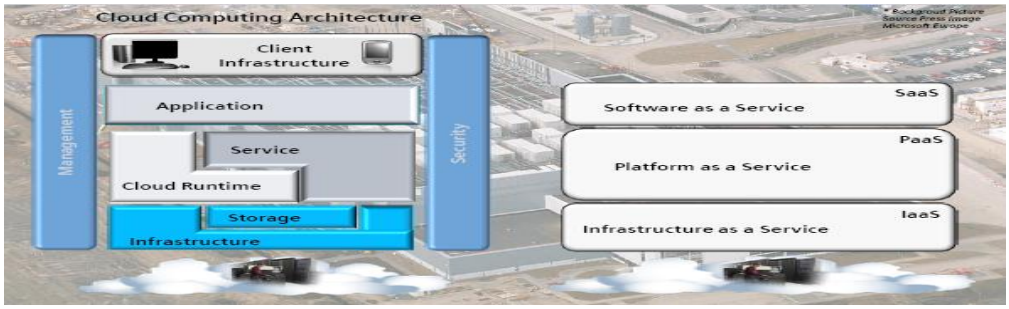
Cloud computing, in turn, refers to sharing resources, software, and information via a network. The information is stored on physical servers maintained and controlled by a cloud computing provider. The scalability and agility offered by cloud infrastructures has attracted thousands of enterprises to host their business-critical applications in public and private clouds. Cloud service providers and large enterprises are building massive data centers to host these cloud services and cloud-based resources. It's now becoming possible to use bigger applications that will leverage your business goals and functions easily in the cloud. For example, with cloud computing, you can run all your computer networks and programs as a whole without ever buying an extra piece of hardware or software. Cloud computing has received a lot of popularity in the last.Few years and market observers believe it to be the future, but not if security problems persist. In today's competitive environment, the service dynamism, elasticity, and choices offered by this highly scalable technology are too attractive for enterprises to ignore. These opportunities, how-ever, don't come without challenges. Security issues over cloud computing is definitely one of the major concerns that many companies are trying to recognize. It is very important to securely store, manage and share data in order to improve the quality and integrity. Because of the critical nature of the applications, it is important that the clouds be secure. The major security challenge with the clouds is that the owner of the data may not have control of where the data is placed.

Architecture of Cloud Computing

Cloud computing architecture refers to the components and subcomponents required for cloud computing. These components consists of a front end platform, back end platform, a cloud based delivery and a network. Combined these components makes up cloud computing architecture.

---

*Assistant Professor, YMT College of Management, Kharghar, Navimumbai,
** Associate Professor,YMT College of Management, Kharghar, Navimumbai



Service Models in Cloud Computing

- **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).

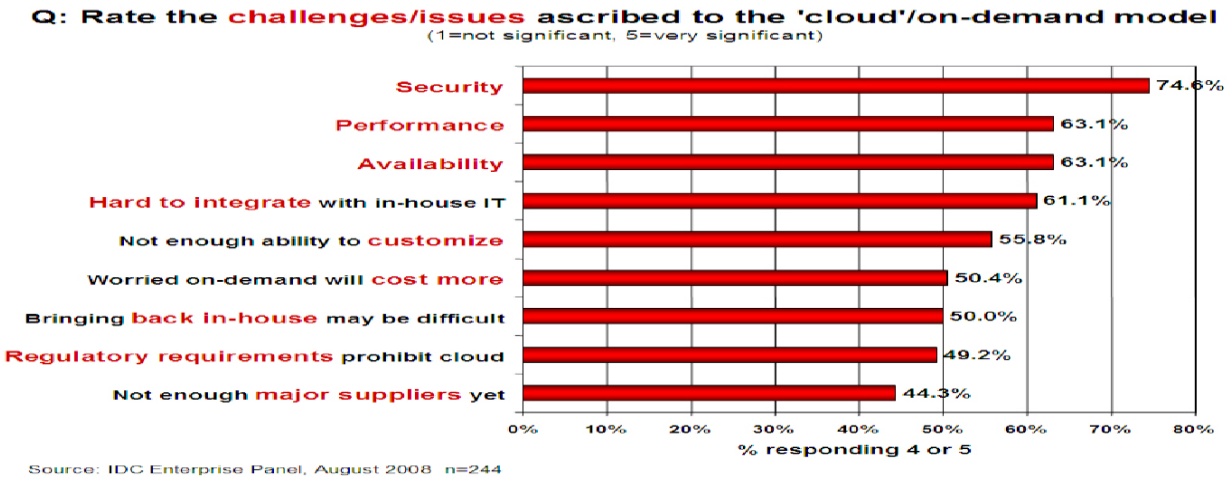
Deployment Models:

- **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).

Challenges and Concerns In Cloud Computing

With the development in technology market, cloud computing becomes an integral part of it but at the same it is important to overcome the high lightened security issues to get the full benefit from this new computing paradigm. Organizations are reluctant to use this mainly due to security concerns.



Some Security Concerns are listed and discussed below:

Loss of Physical Control: The cloud computing paradigm changes the way in which information is managed, especially where personal data processing is concerned. Storing personal data on a server somewhere in cyberspace could pose a major threat to individual privacy .Because tenants and users lose physical control over their data and applications, this gives rise to a range of concerns:

- **Data Privacy**: With public or community clouds, data may not remain in the same system, raising multiple legal concerns.
- **Data Control**: Data could be coming in to the provider in various ways with some data belonging to others. A tenant administrator has limited control scope and accountability within a public Infrastructure as a Service (IaaS) implementation, and even less with a Platform as a Service (PaaS) one. Tenants need to have confidence their provider will offer appropriate control, while recognizing the need to adapt their expectations for how much control is reasonable within these models.
- **New Risks and Vulnerabilities**: There's concern that cloud computing brings new classes of risks and vulnerabilities. There are hypothetical new risks, but the actual exploits will largely be a function of a provider's implementation. All software, hardware and networking equipment are subject to unearthing new vulnerabilities. By applying layered security and well-conceived operational processes, you can protect a cloud from common attacks, even if some of its components are inherently vulnerable.
- **Legal and Regulatory Compliance**: It may be difficult or unrealistic to use public clouds if your data is subject to legal restrictions or regulatory compliance. You can expect providers to build and certify cloud infrastructures to address the needs of

regulated markets. Achieving certification may be challenging due to the many non-technical factors, including the current state of general cloud knowledge. As best practices for cloud computing encompass greater scope, this concern should fade.

- **Disaster Recovery and Business Continuity:** Tenants and users require confidence that their operations and services will continue if the cloud provider's production environment is subject to a disaster.
- **Transparency:** When a cloud provider doesn't expose details of its own internal policy or technology, tenants or users must trust the provider's security claims. Tenants and users may still require some transparency by providers as to how they manage cloud security, privacy and security incidents.

Some solutions to cloud Security Issues

Proper implementation of security measures is mandatory in cloud computing to provide a secure infrastructure only which can ensures and builds confidence that the data stored is secured in provider's side. It can be achieved by the following ways:

Restricted Access

Restricted user access can vary from simple user name / password protection to CAPTCHA log in forms. When an employee no longer has a business need to access datacenter his privileges to access datacenter should be immediately revoked. Cloud Providers can also consider one time password authentication where the clients will get one time temporary password from SSN /mobile device which helps in data security even if password is compromised

Data Encryption

In public cloud the resources are shared by multiple cloud consumers and hence its providers responsibility to confer data separation among their clients. Data encryption is one common approach the providers follow to safe guard their clients data but the question is whether the data is getting stored in encrypted format or not. Many providers follow private/public key encryption to ensure data security. To store crucial data organizations can think of private or hybrid cloud where the data will be in secure corporate firewall. One important way to increase data protection, confidentiality and integrity is to ensure that the data is protected in transit and at rest within the cloud using file-level encryption. As the CSA Security Guidance points out, "encryption offers the benefits of minimum reliance on the cloud service provider and lack of dependence on detection of operational failure." Data-centric protection through encryption renders the data unusable to anyone that does not have the key to decrypt it. No matter whether the data is in motion or at rest, it remains protected. The owner of the decryption keys maintains the security of that data and can decide who and what to allow access to the data. Encryption procedures can be integrated into the existing workflow for cloud services. For example, an admin could encrypt all backup data before sending into the storage cloud. An executive can protect corporate IP before putting it into the private cloud. And a sales representative could encrypt a private customer contract before sending it to a collaborative worksite, like Share point, in the public cloud. Different operating systems on different computing platforms and want to share that data securely inside or outside of the private or public cloud. One of the best security solutions for cloud and virtualized environments is data-centric, file-level encryption that is portable across all computing platforms and operating systems, and works within a private, public or hybrid cloud.

Installation and Maintenance of Firewall

Firewalls are a vital cloud computing security component. Installation of firewall and its maintenance is mandatory to ensure the protection. A firewall should be present in all external interfaces. A list of necessary port and services should be maintained. Assessment of firewall policies and rule sets and reconfiguration of router should be done in regular intervals. Build and deploy a firewall that denies access from untrusted sources or applications, and adequately logs these events. Build and deploy a firewall that restricts access from systems that have direct external connection and those which contain confidential data or configuration data. To accelerate cloud based applications, we need scalable management to be effective and to maximize the benefit of modern firewall capabilities.

Backup and Recovery

In cloud computing data is stored in distributed location. The cloud customers will never be able to make out the exact storage location of their records and there comes the importance of data back up and recovery. Backup software should include public cloud APIs, enabling simple backup and recovery across major cloud storage vendors, such as Amazon S3, Nirvanix Storage Delivery Network, Rack space and others, and giving consumers flexibility in choosing a cloud storage vendor to host their data vault. Backup and recovery services ensure that we always get out data. One debatable question is whether to back up the entire data or to backup critical and vital data. If provider agrees to backup crucial data then the question arises on how to determine the priority of data. The easiest and least complicated way is to protect the entire workstation or the server. It is critical for the backup application to encrypt confidential data before sending it offsite to the cloud, protecting both data-in-transit over a WAN to a cloud storage vault and data-at-rest at the cloud storage site. Consumers need to verify that the cloud backup software they choose is certified and compliant with the Federal Information Processing Standards (FIPS) 140 requirements issued by the National Institute of Standards and Technology. FIPS 140 certification is required for government agencies as well as for regulated financial, healthcare and other industries for compliance with data retention and security regulations such as HIPAA, Sarbanes-Oxley, Gramm-Leach-Bliley and other legal requirements.

Access Control and User Profile Management

Access control and user profile management are more challenging with cloud services because the information sources may be hosted somewhere other than the cloud service that needs them. Customers need to identify trusted sources for this information and secure mechanisms for transmitting the information from the trusted source to the cloud service. It is also important to periodically reconcile the information between the cloud service and the source. Customers need to confirm that cloud providers can support their needs for adequate access control of cloud resources by checking to ensure that the cloud will:

- Control access to the cloud service's features based on policy specified by the customer, as well as the level of service purchased by either the individual user or the organization to which the user belongs.

- Control access to each user's data to protect it from other cloud service customers in multi-tenant environments. Adequately control access to both regular user functions

and privileged administrative functions. Allow collection of user profile information, and possibly access control policy, from a remote service chosen by the customer.

- Keep user profile information and access control policy accurate.

- Provide optional notification of account creation/removal and access grants to the customer, to prevent cloud employees from setting up rogue accounts or otherwise modifying access entitlements.

- Provide adequate audit logs of activity within each customer's environment, including identity management and access activity, as well as use of any resource for which quotas are enforced.

- Provide solutions for determining liability for various problems which may occur. In short, customer requirements for a cloud environment are similar to internal services, but there are several important differences.
- First, customers will want cloud services to solve the above requirements in a way that provides adequate protection in shared, multitenant environments.
- Second, the solutions must accommodate user profile and policy information from remote sources and a need for periodic reconciliation against those remote sources.
- Third, cloud services need to acknowledge that the right identity management solution(s) for a service depend on whether a user is acting on their own behalf or on behalf of some organization, and whether single sign-on is a requirement.

Conclusions

Cloud Computing brought many benefits in computing world. Along with these benefits, there are some security issues that need to be addressed to give assurance that indeed it is safe and reliable internet service. Migrating into the "Cloud" is not that easy but if carefully planned and deployed it will bring advantages in many areas like decreasing cost and resources. Security issues may still provide the biggest barrier to migrating internal applications and services to the cloud, however the industry has come a long way since the first hosted solutions hit the market. Businesses need to select a solution that can instill trust and confidence across their company and ensure they are migrating their precious assets to the most secure and reliable cloud environment. In this paper key security considerations and challenges which are currently faced in the Cloud computing are highlighted and also discussed some solutions to the security problems. Both the cloud service provider and the customer should make sure that the cloud is safe enough from all the external threats, so there will be a strong and mutual understanding between the customer and the cloud service provider. Cloud computing has the potential to become a frontrunner in promoting a secure, virtual and economically viable IT solution in the future.

References

- *M. Okuhara, et.al. "Security Architecture for Cloud Computing", FUJITSU Sci. Tech. J.vol. 46, no. 4,(2010)October pp. 397-402*
- *Sun Microsystems, Inc., "Introduction to Cloud Computing Architecture", White Paper, 1st Edition, (2009) June*.