**Available Online at www.ijcsmc.com**

**International Journal of Computer Science and Mobile Computing**

**A Monthly Journal of Computer Science and Information Technology**

**ISSN 2320–088X**
**IMPACT FACTOR: 6.017**

***IJCSMC, Vol. 6, Issue. 4, April 2017, pg.363 – 368***

# A Review Paper on Considerations and Challenges in Cloud Computing

**Khushboo Jain[1], Vinod Maan[2]**

[1]College of Engineering and Technology, Mody University, India
[2]College of Engineering and Technology, Mody University, India
[1] jainkhushboo.25@gmail.com; [2] vinodmaan.cet@modyuniversity.ac.in

***Abstract— Cloud computing provides varied capabilities to flexibly store the information in third-party information centre referred to as Cloud and utilize resources from distributed computing environments via the internet. The security of stored data, access management, data utilization and management, and data confidentiality are among the primary security aspects in cloud community.***
***This paper explores the most ideas of cloud computing along with some examples of acceptable usage of its services, deployment models, challenges and limitations involved in cloud computing. The paper concludes with a discussion on future research directions which may result in additional trustworthy cloud security and privacy***

***Keywords— Cloud, Cloud Computing, Challenges, Computing Models, Security***

## I. INTRODUCTION

Cloud computing is a form of internet-based computing model which enables omnipresent, on-demand and convenient access to a shared pool of configurable computing resources (e.g., laptop networks, servers, storage, applications and services) which can be quickly scaled up and down with marginal management effort. It has several benefits like, increasing the capability or adding capabilities without investing in a new infrastructure, to satisfy the required technological needs in a quick and automatic manner, elasticity, pay-as-you-go model, virtually eliminating the necessity to invest in costly infrastructure upfront etc. Its use has clearly grown and also the growth has been spectacular.

The foremost aspects of security, confidentiality, integrity, and accessibility should be addressed at the client front, the connection and also the server front. The key issue is that all three operate in and are a part of shared environment, thus their security and privacy needs should be combined. These problems fall under two broad categories: security problems faced by cloud providers and security problems faced by their customers. The responsibility is shared, however. The provider should make sure that their infrastructure is secure and that their clients' information and applications are protected whereas the user should take measures to fortify their application and use robust passwords and authentication measures.

 

### *A. Overview of Cloud Computing*

The cloud model consisting of front-end and back-end promotes accessibility and is composed of five essential characteristics, three delivery models, and four deployment models as outlined by the U.S. National Institute of Standards and Technology (NIST).

Cloud Computing involves multiple cloud elements interacting with one another regarding the varied data they are holding onto, therefore helping the users to get to the specified data on a faster rate as and when required.

### *B. Characteristics*

Cloud computing is comprised of three parts: application, computing and storage. Each part consists of different products and serves a different purpose for businesses and individuals. The characteristics of cloud computing, according to the U.S. National Institute of Standards and Terminology (NIST) [1] are as follows:

*1) On-Demand Self-Service:* These aspects of cloud computing mean that a consumer will use cloud services as needed, without human intervention with the cloud service provider. By using the self service interface, consumers can adopt cloud services by requesting for the required IT resources from the service catalogue. In order to be effective and acceptable to the consumer, the self-service interface should be user-friendly.

*2) Broad Network Access:* Cloud services can be accessed via the network, typically the web, from a broad range of client platforms, like desktop computer, laptop, mobile phone and thin client. Broad network accessibility eliminates the requirement for accessing a specific client platform to access the services. Thus, it permits access of service from anywhere across the world.

*3) Resource Pooling:* A Cloud must have a large and flexible resource pool to meet the consumer's needs, to provide the economies of scale and to meet service-level requirements. The resources (compute, storage, and network) from the pool are dynamically assigned to multiple consumers based on a multi-tenant model. Multi-tenancy refers to an architecture and design by which multiple independent clients/tenants are serviced using a single set of resources.

*4) Rapid Elasticity:* Resources can be both scaled up and scaled down dynamically and rapidly, to fulfil the needs without interruption of service. To the consumer, cloud appears to be infinite and they can start with minimal computing power and can expand their environment according to the requirement.

*5) Measured Service:* Measured service provides billing and chargeback information for the cloud resource used by the consumer. The metered services continuously monitor the resource usage (CPU time, bandwidth, storage capacity) and report the same to the consumer. This maintains transparency for chargeback to both cloud service provider (CSP) and consumer about the utilized service.

## II. DEPLOYMENT MODELS

These models provide a basis for how cloud infrastructures are constructed and consumed. There are three commonly-used cloud deployment models [3], namely: private, public, and hybrid. An additional model is the community cloud, which is less-commonly used. An overview of these is discussed in this section.

### *A. Public Cloud*

In a Public Cloud, resources are made accessible to the general public or organizations and are owned by the cloud service provider. The services like applications, storage capacity, or server compute cycles, are accessible to everybody via standard internet connections. This model may be thought of as an "on-demand" and as a "pay-as-you-go" environment, where there are not any on-site infrastructure or management requirements.

However, for organizations, these advantages associate with the risks: no management over the resources within the cloud, the protection of confidential data, network performance issues, and interoperability. Common examples of public clouds are Amazon's Elastic calculate Cloud (EC2), Google Apps and Salesforce.com.

 

### *B. Private Cloud*

In a Private Cloud, the cloud infrastructure is operated exclusively for one organization and is not shared with another organizations. This model offers the best level of security and control. The organizations will have to run their own hardware, storage, networking, hypervisor, and cloud software system. Several enterprises, including EMC, Cisco, IBM, Microsoft, Oracle and VMware, now offer Cloud platforms and services to build and manage a private Cloud.

### *C. Hybrid Cloud*

In Hybrid Cloud setting, the organization consumes resources from both viz. private and public Clouds. The flexibility to enhance a private Cloud with the resources of a public Cloud is utilised to keep up service levels within the face of fast workload fluctuations. Organizations use their computing resources on a private Cloud for traditional usage, however access the public Cloud for high/peak load needs.

This ensures that a boost in computing demand is handled gracefully. Ideally, the hybrid approach permits a business to take advantage of the scalability and cost-effectiveness that a public computing environment offers without exposing mission-critical applications and data to third-party vulnerabilities.

### *D. Community Cloud*

The Cloud infrastructure is shared by multiple organizations and supports a particular community that has shared considerations (E.g., mission, security requirements, policy, and compliance considerations). A community cloud may be managed by the organizations or by a third party. With the costs spread over to fewer users than a public cloud, this choice is more costly but it provides a higher level of privacy, security, and/or policy compliance. The community cloud offers organizations access to a huge pool of resources than that within the private cloud.

## III. SERVICE MODELS

Service delivery in cloud computing comprises three different basic service models[8]: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS). These are described with their common usage areas in Figure 1.

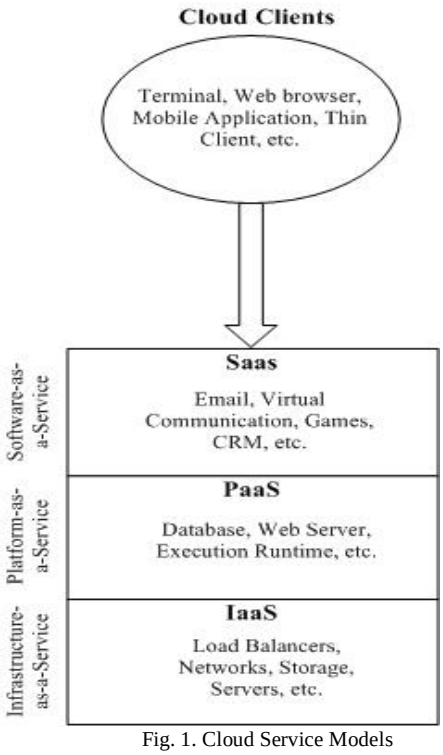


Fig. 1. Cloud Service Models

 

### *A. Infrastructure-as-a-Service (IaaS)*

Infrastructure-as-a-Service (IaaS) is base layer of the Cloud stack. It acts as foundation for the rest two layers (SaaS, PaaS) for their execution. The Cloud infrastructure like servers, routers, storage, and various networking elements are provided by the IaaS provider.

The client hires these resources as a service according to its need and pays just for the usage. The client is able to deploy and run any software, including the Operating Systems (OSs) and applications. The client does not manage or control the underlying Cloud infrastructure, however has control over the OSs and deployed applications. Here, the client has to recognize the resource requirements for the particular application to use IaaS well. Scaling and elasticity are the responsibilities of client, not the provider.

In fact, IaaS is a mini do-it-yourself data centre in which the client is able to assemble the resources (server, storage) and to get the task done. Amazon Elastic Compute Cloud (EC2), EMC Atmos online are some examples of IaaS model.

### *B. Platform-as-a-Service (PaaS)*

Platform-as-a-Service is the capability provided to client to deploy consumer-created or inherited applications on the Cloud infrastructure. PaaS can loosely be outlined as application development environments offered as a 'service' by the Cloud provider.

The consumer uses these platforms that usually have Integrated Development environment (IDE), which comprises of editor, compiler, build, and deploy capabilities to develop their applications. They then deploy the applications on the infrastructure offered by the Cloud provider. Once clients write their applications to run over the PaaS provider's software platform, elasticity and scalability is secured transparently by the PaaS platform.

Here, the consumer doesn't manage or control the underlying Cloud infrastructure, like network, servers, OSs, and storage, but it controls the deployed applications and probably the application-hosting environment configurations. For PaaS, clients pay just for the platform software elements like databases, OS instances, and middleware, which has its associated infrastructure price. Google App Engine and Microsoft Azure Platform are some examples of PaaS model.

### *C. Software-as-a-Service (SaaS)*

SaaS is at the top most layer of the Cloud Computing stack, and is directly consumed by end user. It provides the ability to the consumer, to use the service provider's applications running on a Cloud infrastructure. It can be accessed from multiple client devices through a thin client interface like web browser.

Here, the customers can use only the applications they need and pay a subscription fee for the usage. The Cloud provider can host and manage the desired infrastructure and applications to support these services. The SaaS model additionally permits for easier support for all users simultaneously, such as pushing out software package updates and fixes.

SaaS has the following advantages: Reduces the requirement for infrastructure since, storage and compute powers can be provided remotely and also reduces the need for manual updates because SaaS providers can perform those tasks automatically. EMC Mozy and Salesforce.com are some examples of SaaS model.

## IV. CLOUD COMPUTING CHALLENGES

### *A. Security*

Since the cloud is an open platform, it is susceptible to malicious attacks of continuously evolving natures. Cloud computing poses privacy concerns because the service provider can access the data that is in the cloud at any time. It could accidentally or deliberately alter or delete sensitive data. Security concerns related to managing data, applications, and interactions hamper the rapid deployment of cloud-based services on a large scale.

Well-known security issues such as data loss, phishing, etc. put an organization's data and software in serious threats. Also, the multi-tenancy model and the pooled computing resources[10] in cloud computing have introduced new security challenges that require novel techniques to tackle.

### *B. Costing Model*

Although migrating to the cloud can significantly reduce the infrastructure cost, it does raise the cost of data communication. There are some trade-offs in the computation, communication, and integration which needs to be considered by the cloud clients.

 

Thus, the cost of transferring an organization's data to and from the public and community cloud is likely to be higher. This problem is significant if the consumer uses the hybrid cloud deployment model where the organization's data is distributed among a number of public/private/community clouds. Intuitively, on demand computing makes sense only for CPU intensive jobs.

### *C. Cloud Interoperability Issue*

Currently, each cloud service is specific on how it integrates with other applications and client needs. This is referred to as the Hazy Cloud phenomenon. The integration of cloud services with an organization's own existing systems requires attention to detail and upfront discussion of system requirements to ensure seamless data transfer between cloud and the local applications.

### *D. Performance*

A majority of the obstacles for adoption and growth of cloud computing are associated with the aspects of availability, capacity or scalability. If cloud-hosted applications are to be used globally, it is necessary to monitor performance parameters like network latency across all major client locations. While selecting a cloud provider, clients should ensure that provider is able to support expected growth, and to guarantee efficient performance levels.

## V. CONCLUSION

In the recent past, cloud computing has evolved as a well-liked and universal paradigm for service oriented computing where infrastructure and solutions are delivered as a services. Cloud computing is a rising technology and can prove to be a promising one for subsequent generation of IT applications.

The barrier and hurdles toward the rise of cloud computing are data security and privacy concerns. Reducing data storage and processing cost is a necessary requirement of any organization, while analysis of data is always the most vital task of all the organizations for decision making.

With the arrival of latest utility services, giant scale data storage and utilization applications; beside infamous attacks to disrupt privacy, confidentiality, integrity and availability, additional scalable security solutions are necessary for cloud computing platforms. The paper concludes with a careful review of the terms of services, and challenges of the cloud computing.

## VI. FUTURE SCOPE

Security considerations associated with managing information, applications, and interactions hamper the speedy deployment of cloud-based services on an outsized scale. Though several solutions exist, efficiency, measurability and provable security still have problems that require to be properly addressed.

Since large amounts of data are hosted in the cloud, the providers must guarantee its authenticity and integrity to all users. Verifying the point of origin for multisource data is a challenge. It is further challenging when data are hosted with high velocity. For example, data from millions of sensors continuously.

Cryptographic solutions have been increasingly popular as viable solutions to secure data storage and access control. Some of the cryptographic techniques are attractive in terms of security, efficiency and scalability. Improving efficiency and scalability with respect to cloud deployment models and application-specific demands requires more research effort.

## ACKNOWLEDGEMENT

We take this opportunity to express our profound gratitude and deep regards to the people who have been instrumental in the successful completion of this paper.

We would also like to take this opportunity to express a deep sense of gratitude to Dr. Anil Kumar, (Head of the Dept.-CSE, Mody University) for his cordial support, valuable information and guidance which helped us in completing this task through various stages.

We are much obliged to Dr. V.K. Jain, (Dean-CET, Mody University) who has provided us with the best facilities and atmosphere for the completion and presentation of this paper.

We would also like to thank Dissertation Coordinator Mrs. Priyanka Dahiya, for giving us an opportunity to gain knowledge regarding this dissertation.

 

# REFERENCES


[1] Tari, Z.; Xun Yi; Premarathne, U.S.; Bertok, P.; Khalil, I., "Security and Privacy in Cloud Computing: Vision, Trends, and Challenges Cloud Computing", *IEEE Cloud Computing,* Issue Date: Mar.-Apr. 2015

[2] Zheng Y.; Mingjun W.; Yuxiang Li; "Encrypted Data Management with Deduplication in Cloud Computing" *IEEE Cloud Computing,* Issue Date: Mar.-Apr. 2016

[3] Walloschek T.; GroBauer B.; Elmar Stöcker; "Understanding Cloud Computing Vulnerabilities", *IEEE Security and Privacy,* Issue Date: Mar.-Apr. 2011

[4] Christian Esposito; Ben Martini; Aniello Castiglione; "Cloud Manufacturing: Security, Privacy, and Forensic Concerns", *IEEE Cloud Computing,* Issue Date: Jul.-Aug. 2016

[5] *IHS Technology*, "Cloud-Related Spending by Businesses Triple from 2011 to 2017," http://press.ihs.com/press-release/design-supply-chain/cloud-related-spending-businesses-triple-2011 -2017.

[6] V.D. Marten and A. Juels, "On the Impossibility of Cryptography Alone for Privacy-Preserving Cloud Computing," Proc. 5th USENIX Conf. Hot Topics in Security (HotSec 10), 2010; http://static.usenix.org/events/hotsec10/tech/full_papers/vanDijk.pdf.

[7] S. Yu et al., "Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing," Proc. *IEEE Conf.* Computer Comm. (INFOCOM 10), 2010, pp. 1–9; doi:10.1109/ INFCOM.2010.5462174.

[8] S. Kuyoro, and F. Ibikunle. 2011. "Cloud Computing Security Issues and Challenges". *International Journal of Computer Networks (IJCN),* Volume (3) : Issue (5).

[9] F. Giannotti et al., "Privacy-Preserving Mining of Association Rules from Outsourced Transac-tion Databases," *IEEE Systems J*., vol. 7, no. 3, 2013, pp. 385–395.

[10] X. Yi et al., "Privacy-Preserving Association Rule Mining in Cloud Computing," Proc. *ACM Symp. Information, Computer and Comm. Security* (ASIACCS), 2015, pp. 439-450.

[11] T. ElGamal, "A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," *IEEE Trans. Information Theory*, vol. 31, no. 4, 2015, pp. 469–472.

[12] K. Yang et al., "Dac-Macs: Effective Data Access Control for Multiauthority Cloud Storage Systems," *IEEE Trans. Information Forensics and Security*, vol. 8, no. 11, 2013, pp. 1790–1801.

[13] P. Jamkhedkar et al., "A Framework for Realizing Security on Demand in Cloud Computing," Proc. *IEEE Int'l Conf. Cloud Computing Technology and Science* (CloudCom 13), 2013, pp. 371–378.

[14] U. Premarathne et al., "Cloud-Based Utility Service Framework for Trust Negotiations Using Federated Identity Management," *IEEE Trans. Cloud Computing*, preprint, 2015, doi:10.1109/ TCC.2015.2404816


 