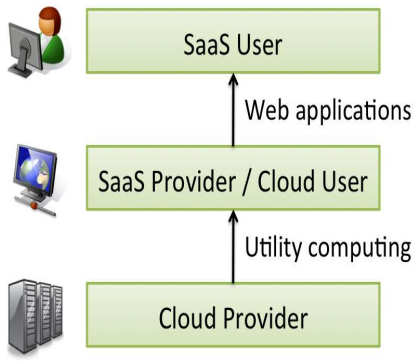
CLOUD COMPUTING: SECURITY ISSUES AND CHALLENGES

Arti Sachdeva
Assistant Professor
Sanatan Dharama College, Ambala Cantt
Email:sachdeva.arti8@gmail.com

Abstract:
Thelong-held dream of computing as a efficacy, has the prospective to renovate a large part of the IT industry, making software even more striking as a service and determining the way IT hardware is intended and purchased. Developers with inventive ideas for new Internet services no longer require the large assets outlays in hardware to arrange their service or the human expense to manage it.Despite the prospective gains achieved from the cloud computing, the organizations are slow in accommodating it due to security issues and challenges coupled with it. Security is one of the major issues as more and more information on individuals and companies is placed in the cloud, concerns are beginning to grow about just how safe an environment it is. This paper explores the concept of cloud computing and also pinpoint the challenges and issues of cloud computing.

Introduction:
Cloud computing refers to both the applications delivered as services over the Internet and the hardware and systems software in the data centers that offer those services. The services themselves have long been referred to as Software as a Service (SaaS). Some vendors use terms such as IaaS (Infrastructure as a Service) and PaaS (Platform as a Service) to illustrate their products. The data center hardware and software is what we will describe a cloud. When a cloud is made accessible in a pay-as you- go manner to the general public, we term it a public cloud; the service being sold is utility computing. We use the term private cloud to refer to internal data centers of a business or other organization, not made accessible to the general public. Other than these two, Hybrid and Community cloud are also exist.A community cloud resembles a private one to a large area; the only difference is the set of users. While a private type implies that only one company owns the server, in the case of a community one, several organizations/companies with similar backgrounds share the infrastructure and related resources. Hybrid cloud encompasses the best features of a public, private and community ones. It allows companies to mix the facets of all three types that best suit their necessities. As an example, a company can balance its load by locating mission-critical workloads on a secure private cloud and deploying less perceptive ones to a public one. Thus, cloud computing is the sum of SaaS and utility computing. but does not include small or medium sized data centers, even if these rely on virtualization for organization. People can be users or providers of SaaS, or users or providers of utility computing. We focus on SaaS providers (cloud users) and cloud providers, which have acknowledged less attention than SaaS users. Figure 1 makes provider-user relationships clear.



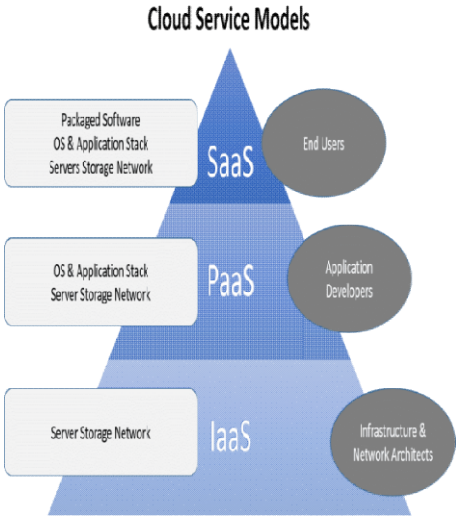
ISBN 978-93-82529-14-9

In some cases, the same artist can play multiple roles. For instance, a cloud provider might also host its own customer-facing services on cloud infrastructure. From a hardware provisioning and pricing point of sight, three aspects are new in cloud computing.

- The appearance of infinite computing resources available on demand, quickly enough to follow load surges, thereby eliminating the need for cloud computing users to plan far ahead for provisioning.
- The elimination of an up-front commitment by cloud users, thereby allowing companies to start small and increase hardware resources only when there is an increase in their needs.
- The ability to pay for use of computing resources on a short-term basis as needed (for example, processors by the hour and storage by the day) and release them as needed, thereby gratifying conservation by letting machines and storage go when they are no longer useful.

Cloud Services:

1) **Software as a Service (SaaS):** The way of shipping application as a service on the web is known as software as a service. In place of installing the software on his computer, the user can simply access it via the internet [3].It makes the user free from managing the complex software and hardware. The SaaS users do not require to buy software or hardware, maintain, and update. The only thing user must have an internet connection and then access to the particular application is very easy. Example: Microsoft Office 365, Google Apps etc.
2) **Platform as a Service (PaaS):** A development environment or platform is given to the clients as a service in PaaS, upon which user can set up their own software and coding. The customer has the liberty to construct his own applications that can run on the provider's infrastructure [3]. Platform as a service providers offers a predefined composition of operating system and application server to acquire the management capacity of the applications. For example, LAMP (Linux, Apache, MySQL, and PHP), J2EE, Ruby etc.
3) **Infrastructure as a Service (IaaS):**Infrastructure as a service is online services that provide virtualized computing resources. IaaS vendor provides clients pay-as-you-go access to storage, networking, servers and other computing resources in the cloud. IaaS users can access the services using a wide area network, such as the internet [3]. For example, a user can create virtual machines by login to the IaaS platform.



Benefits of Cloud Computing:

I. **Cost Saving**: In cloud computing users have to only pay for the services they consumed.It also reduces costs related to downtime. This means users don't have to spend time and money on setting up potential issues related to downtime. Maintenance cost is low as users do not need to purchase the infrastructure [1].

II. **Flexibility:** Cloud computing is flexible. The rapid scale up and down in the operations of any business may require quick adjustment of hardware and other resources so in order to manage these variations.

As the need of cloud computing for data storage on cloud growing, the need for security is also becoming an crucial requirement. However, the data stored in the cloud can easily be hacked due to lack of testing, backups, and proper access permissions. Heightened security threats must be overcome in order to get profit from this new computing paradigm. Some security concerns are listed and discussed below:

1) Physical security is lost because of sharing computing resources with other companies. There is no knowledge or control of where the resources run.
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). [2]
3) Who will control the encryption/decryption keys?
4) Ensuring the integrity of the data (retrieval, transfer and storage).
5) Users must stay up to date with application improvements to be sure they are protected.
6) 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.[4]
7) Customers may be able to take legal action against 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.

Challenges:

Here are six common challenges that must consider before implementing cloud computing technology.

1**. High Cost**

Cloud computing itself is reasonable, but choosing the platform according to the company's needs can be expensive. Furthermore, the cost of transferring the data to clouds can prove to be a problem for small-scale projects.

2. **Service Provider Reliability**

The capacity and capability of a technical service provider are important concern. The service provider must be accessible when we need them. The main concern should be the service provider's sustainability and reputation. Make sure you understand the techniques via which a provider observes its services and defends reliability claims.

3. **Downtime**

Downtime is a considerable shortcoming of cloud computing technology. No seller can guarantee a platform that is free of possible downtime. Cloud technology makes small companies dependent on their connectivity, so companies with an unreliable internet connection probably want to think twice before adopting cloud computing.

4. **Security**

Industrious password management plays a vital role in cloud security. However, the more people accessing your cloud account, the less secure it is. Anybody awake of your passwords will be able to access the information you store there.

Businesses should employ multi-factor verification and make sure that passwords are protected and changed regularly, particularly when staff members leave. Access rights related to passwords and usernames should only be owed to those who require them.

ISBN 978-93-82529-14-9

5. **Data privacy**
Sensitive and personal information that is kept in the cloud should be defined as being for internal use only, not to be public with third parties. Businesses must have a plan to strongly and efficiently manage the data they gather.
6. **Vendor lock-in**
Entering a distributed computing understanding is simpler than leaving it. "Merchant lock-in" happens when modifying suppliers is either too much costly or just impractical. It may be the case that the administration is nonstandard or that there is no reasonable merchant substitute.

It comes down to purchaser caution. Assurance the administrations you include are run of the mill and transportable to different suppliers, or more all, comprehend the prerequisites.

Conclusion:
We have contended that it is imperative to consider security and protection when planning and utilizing cloud administrations. In this paper security in distributed computing was explained such that spreads security issues and difficulties. Security issues show potential issues which may emerge. These are on the whole significant subjects which will be unquestionably talked about in the up and coming long periods of distributed computing.

References:
[1] Herhalt, J., Cochrane, K.: Exploring the Cloud: A Global Study of Governments‘ Adoption of Cloud (2012).

[2] M. Casassa-Mont, S. Pearson and P. Bramhall, “Towards Accountable Management of Identity and Privacy: Sticky Policies and Enforceable Tracing Services”, Proc. DEXA 2003, IEEE Computer Society, 2003, pp. 377-382.

[3] Yang, H., Tate, M.: A Descriptive Literature Review and Classification of Cloud Computing Research. Commun. Assoc. Inf. Syst. 31 (2012).

[4] Krešimir Popović, Željko Hocenski :Cloud computing security issues and challenges(2016).

[5] P. Kresimir and H. Zeljko "Cloud computing security issues and challenges." In PROC Third International Conference on Advances in Human-oriented and Personalized Mechanisms, Technologies, and Services, 2010, pp. 344-349.

[6] S. Arnold (2009, Jul.). “Cloud computing and the issue of privacy.” KM World, pp14-22. Available: www.kmworld.com [Aug. 19, 2009].

[7] Armbrust, M., et al. Above the clouds: A Berkeley view of cloud computing. Tech. Rep. UCB/EECS-2009-28, EECS Department, U.C. Berkeley, Feb 2009.

COMPARISON OF DIFFERENT SOFTWARE QUALITY MODELS – A REVIEW

Dr. Ashish Jolly [1], Ms. Shiwani [2]