Security in Cloud Computing

Sanjana Sharma, Sonika Soni, Swati Sengar

Patel institute of technology,Bhopal ,School of computer science and IT,DAVV indore,
shri ram college of Engineering and management, Gwalior

Sharmasanjana_2587@yahoo.com, sonika.soni2@gmail.com, swatisengar@yahoo.co.in,

Abstract-Cloud computing is known as one of the big next things in information technology world. Unlike other traditional computing system, cloud computing paradigm that provide unlimited infrastructure to store or execute client's data/program. Cloud computing is a long dreamed vision of computing as a utility, where data owners can remotely store their data in the cloud to enjoy on- demand highly-quality application and services from a shared pool of configurable computing resources. This paper gives a brief introduction of cloud computing its types and security issue and approaches to secure the data in the cloud environment.

Keywords- Cloud Computing, Security, SAAS, PAAS, IAAS, Public cloud, Private cloud, Hybrid cloud

I Introduction

Today's Cloud computing is a most important and reasonable technology. it is a way of computing in which dynamically scalable and often virtualized resources are provide as a services over the internet. Internet is not only a communication medium but, because of the reliable, affordable and ubiquitous broadband access, is becoming a powerful computing platform rather than running software and managing data on the desktop computer or server, user are able to execute application and access data on demand from the cloud (internet) anywhere in the world. This new computing paradigm is referred as a cloud computing. We define a general representation of cloud in which the application software and often the data itself is stored permanently not on your pc but rather a remote server that's connected to the internet.

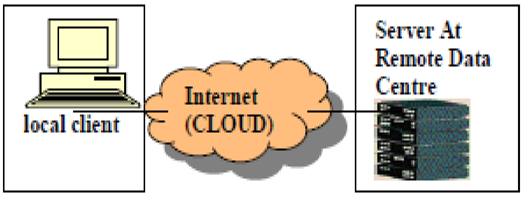


Fig.1 General Representation of cloud

We study the structure of a cloud in which the cloud uses the several application such as Amazon, Google apps for storing the data.

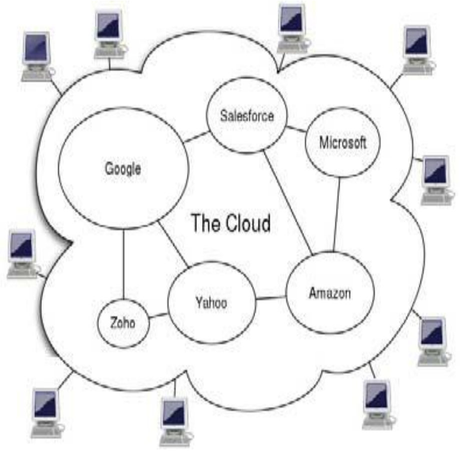


Fig.1 (a) Structure of a cloud

Now we explain the architecture of a cloud. Cloud architecture involved in the delivery of cloud computing, the two most significant component of cloud computing architecture are known as the front end and back end. The front end is the part seen by the client, like computer user. This includes the users network (computer) and the application 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.

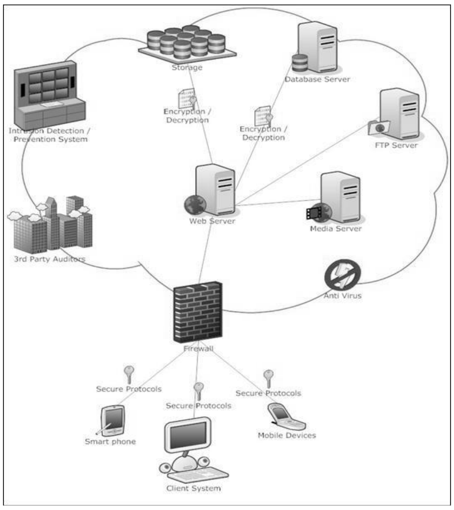


Fig.1(b) cloud storage architecture

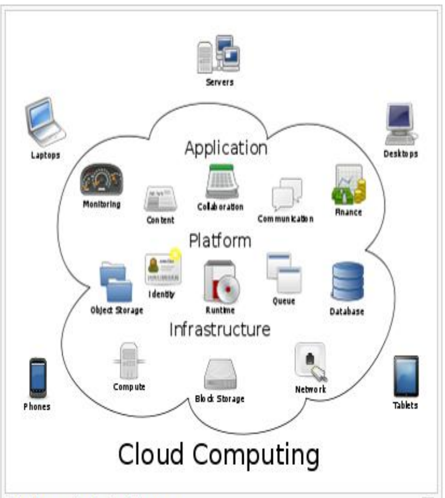
In the rest of paper organized as follows: Section II introduces the different types of cloud model that is delivery and deployment model, Section III explain the security issues and challenges, Section IV highlights the approaches of provide security and authentication in cloud computing, Section V conclusion are drawn for cloud computing.

II types of cloud model

For secure service in cloud computing there are two type of model. First is thedelivery model and another is deployment model.

Delivery model:

Delivery model in cloud computing we define by the three keys that are infrastructure as a service (IaaS), Software as a service (SaaS), Platform as a service (Paas)



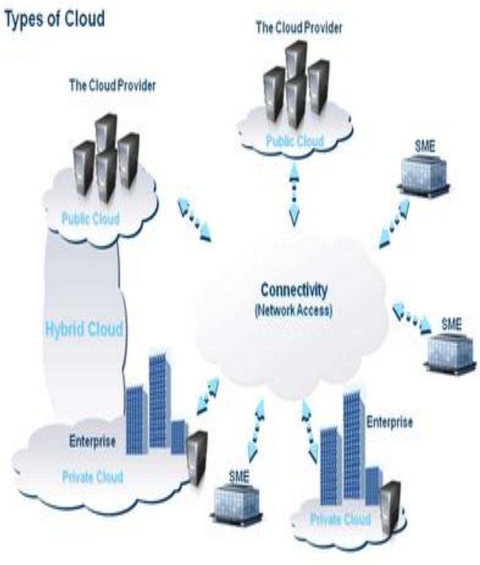
Cloud computing logical diagram

Infrastructure as a service (Iaas) is the foundation of all the cloud services (bottom layer) . It supplies a set of virtualized infrastructural component such as virtual machines.

Platform as a service (Paas) is a middle layer in cloud services. It enables programming environment to access and utilize additional application building block.

Software as a service (Saas) operates on the virtualized and pay-per-use costing model whereby software applications are leased out to contracted organization by specialized saas vendor.

Deployment model:



Cloud Computing Deployment Models

Public Clouds

In public clouds, the services and infrastructure are provided off-site over the Internet. These clouds offer the greatest level of efficiency in shared resources; however, they are less secured and more vulnerable than private clouds.

Private Clouds

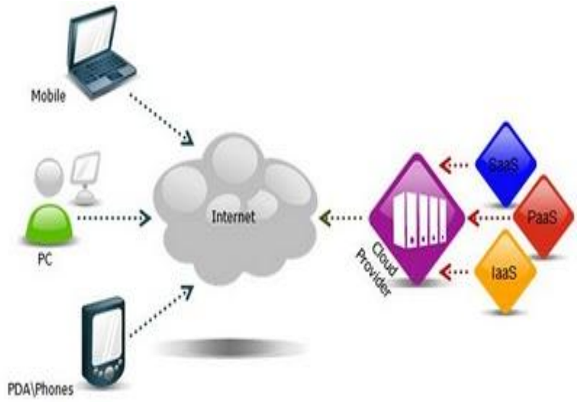
Unlike public clouds, in the Private Clouds, the services and infrastructure are maintained on a private network. These clouds offer the greatest level of security and control.

However they require the company to still purchase and maintain all the software and infrastructure.

Hybrid Clouds

A hybrid cloud includes a variety of public and private options with multiple providers.

In simple terms, when you are using cloud computing, you don't need to install the required application on your system. Instead, you use the application that runs on a remote location/datacenter which we called the 'Cloud'. You just login, customize and start using it.



Gmail is the perfect example of Cloud Computing. You don't need a software system or mail server to send/receive emails. You just login to it, customize it and start using it. Unlike other traditional email management systems like MS Exchange, Gmail doesn't requires a software system, mail server, regular upgrades or dedicated team to manage it. Instead, everything is placed in the Cloud (and Cloud have all those things) and the users get all the benefits that are provided 'as a service'

III. Security issues and challenges

The Cloud computing technology comes with many issues such as performance, resiliency, interoperability, data migration and transition from legacy systems. One of the main issues is security.
The following security issues are highlight for the cloud computing vendors.

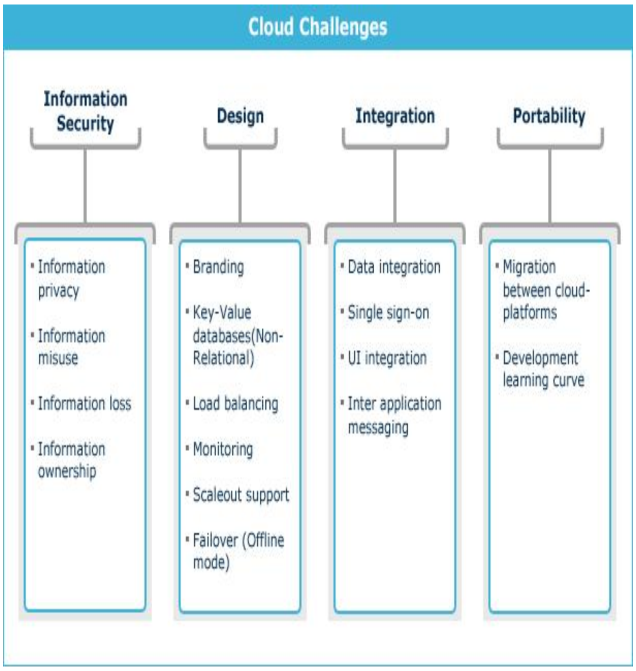
- **Privileged access:** who decides about the hiring and management of the administrator?
- **Data location:** does the cloud vender allow for any control over the location of data?
- **Recovery:** what happens to the data in the case of disaster and does the vendor offers complete restoration and if so how long does that process take?
- **Long term viability:** what happens to the data if the cloud vendor goes out of business is client’s data returns and what format?
- **Data availability:** Can the cloud vendor move all their clients’ data onto a different environment should the existing environment become compromised or unavailable?

We also describe the three another main category of issue that are

- Traditional security
- Availability
- Third party data control

Traditional security concern involves network intrusion and attacks. This category includes several issues like VM-level attack, vulnerability, phishing cloud provider, authentication and authorization, forensics in cloud, expanded network attack.
Availability: these type concern mainly on the critical application these includes such as
Uptime, single point of failure, computational integrity.
Third party data control is a legal issue in this concern lack of control and transparency.

Challenges in security in cloud computing:
Cloud computing environment are multidomain environment in which each domain can use different security, privacy and trust requirement and potentially employ various mechanism, interface and semantics. We describe some challenges in cloud computing.



Security

These security concerns are related to strong processes, service orientation, and creation of trust among users. Similar issues have been resolved earlier, probably as accepted service as banking, and Cloud Computing would also surmount these issues.

Design

Cloud Computing demands taking care of the following needs and issues of cloud computing during application design:Designing applications so that there is zero downtime during the deployment of new releases.

Integration

Any enterprise application requires a strong need to integrate with other parts of the application isolated geographically. In Cloud Computing, there is a strong possibility of integrating parts of an application that are residing in different premises. As a result, the following integration issues need to be addressed:

Portability (Lack of standardization)

Cloud Computing is an evolving paradigm and most of the industry leaders have developed platforms independently over the past few years. As of today, if an application is developed in one platform, it is a challenge to port the application to another platform of another service provider without making major code changes.

There are several more challenges in cloud

1- Cloud Migration/ Security

Foremost thing that should be tackled efficiently is the process of migrating confidential data from the internal server to one big cloud server. An exceptionally experienced and profound work force should be present to deal with and handle such issues smoothly and with ease.

2- How Reliable Cloud Environment is? Whenever a new technology is innovated or developed, next thing after security that comes to mind is whether it is reliable. Similar notions have been felt for cloud architecture as well. The recent outages ranging from **Amazon EC2** .

3- Can Cloud be Available? As per industry reports **cloud managers** assure or 100 % availability and round the clock assistance. But, is it rightly said? Providing users with **99.99% uptime** and **highly scalable** environment is possible.

4- Monitoring Measures can be Vague Once your data is migrated on the cloud, it becomes prime concern for the managed cloud providers to monitor your cloud **24 x 7**. This is only possible if your cloud provider has enough and strong infrastructure to do so, else your money invested in it can be simply in vain.

5- Lack of Communication: Communication plays a vital role in promoting anything that can bring a change. Technically, speaking, it does have importance in grooming cloud technology as well.

Now we describe the security challenges in cloud computing

Authentication and identity management: in cloud services user can easily access their personal information and make it available across the internet. Identity management can help authenticate the user.

Access control and accounting: the access control services should be flexible enough to capture dynamic, context, or attribute and to enforce the principle of least privilege.

Trust management and policy integration: a trust framework should be developed to allow for efficiently capturing a generic set of parameter required for establishing trust and to manage evolving trust and interaction requirement.

Privacy and data protection: it is the core issue in all challenges in this the need to protect identity information policy component during integration and transaction histories.

IV. Several approaches for security in cloud computing

After the brief literature survey we explain the several kind of approach for security in cloud computing such that are:

Strong authentication framework: a strong user authentication framework for cloud computing with many security features, such as identity management, mutual authentication, session key agreement between the users and the cloud server, and user friendliness (i.e., password change phase). The term, strong two factor signifies one factor in 'something you know' (password) and two factors in 'something you have' (smartcard and *OOB*).

Identity based authentication for cloud computing: Authentication is necessary in Cloud Computing. SSL Authentication Protocol is of low efficiency for Cloud services and users. we presented an identity based authentication for cloud computing, based on the identity-based hierarchical model for cloud computing (IBHMCC) and corresponding encryption and signature schemes. Being certificate-free, the authentication protocol aligned well with demands of cloud computing. Performance analysis indicated that the authentication protocol is more efficient and lightweight than SAP, especially the more lightweight user side. This aligned well with the idea of cloud computing to allow the users with an average or low-end platform to outsource their computational tasks to more powerful servers.

Privacy-preserving digital identity management: we have proposed an approach to the verification of digital identity for cloud platforms. Our approach uses efficient cryptographic protocols and matching techniques to address heterogeneous naming. We plan to extend this work in several directions. The first direction is to investigate the delegation of identity attributes from clients to CSPs. Delegation would allow a CSP, called the source CSP, to invoke the services of another CSP, called the receiving CSP, by passing to it the identity attributes of the client. However the receiving CSP must be able to verify such identity attributes in case it does not trust the source CSP. One possibility would be to allow the receiving CSP to directly interact with the client; however the source CSP may not be willing to allow the client to know the CSPs it uses for offering its services. Therefore protocols are needed able to address three requirements: confidentiality of business relations among the various CSPs, user privacy, and strength of identity verification. The second direction is the investigation of unlink ability techniques. Our approach does not require that the values of the identity attributes only used for identity verification be disclosed to the CSPs; also our approach allows the user to use pseudonyms when interacting with the CSPs, if the CSP policies allow the use of pseudonyms and the user is interested in preserving his/her anonymity.

Mutual authentication scheme: mutual authentication scheme to minimize the cloud computing security risk such as man-in-middle attack, identity theft, side channel attack and phishing attack. This scheme provides a robust and trustworthy mutual authentication between cloud user and cloud service provider communicate over the internet. It has good efficiency and suitable for cloud computing.

V. Conclusion

Cloud computing is a new way of delivery computing delivering computing resources which introduce a lot of benefits to its user. Despite its positive characteristics, it also bring in new security worries such as a data security issue, illegal data access etc. in this paper we investigate the introduction about cloud and security problems in cloud computing and several schemes to secure data in cloud. To provide a more reliable security in cloud computing is the future research goal.

VI. References

1. Amlan Jyoti Choudhury, Pardeep Kumar,Mangal Sain, Hyotaek Lim, Hoon Jae-Lee, "A Strong User Authentication Framework for Cloud Computing" 2011 IEEE Asia -Pacific Services Computing Conference
2. Ramgovind S, Eloff MM, Smith E, "The Management of Security in Cloud Computing"2010 IEEE
3. Bhagyaraj Gowrigolla, Sathyalakshmi Sivaji, M.Roberts Masillamani, "Design and
Auditing of Cloud Computing Security " 2010
4. Elisa Bertino, Federica Paci, Rodolfo Ferrini, Ning Shang, "Privacy-preserving Digital Identity Management for Cloud Computing" Bulletin of the IEEE Computer Society Technical Committee on Data Engineering ,2009
5. Richard Chow, Philippe Golle, Markus Jakobsson, Ryusuke Masuoka, Jesus Molina, Elaine Shi, Jessica Staddon Parc, " Controlling Data in the Cloud:Outsourcing Computation without Outsourcing Control" *CCSW'09,* November 13, 2009, Chicago, Illinois, USA
6. Richard Chow Parc, Markus Jakobsson FatSkunk, Ryusuke Masuoka, "Authentication in the Clouds: A Framework and its Application to Mobile Users" *CCSW'10,* October 8, 2010, Chicago, Illinois, USA
7. "Security and Privacy Challenges in Cloud Computing Environments" Copublished by the IEEE computer and reliability societies,November/December 2010
8. Hongwei Li, Yuanshun Dai1, Ling Tian, and Haomiao Yang, "Identity-Based Authentication for Cloud Computing" M.G. Jaatun, G. Zhao, and C. Rong (Eds.): CloudCom 2009, LNCS 5931, pp. 157–166, 2009.© Springer-Verlag Berlin Heidelberg 2009
9. K.Valli Madhavi, R.Tamilkodi, R.BalaDinakar, " Data Storage Security in Cloud Computing for Ensuring Effective and Flexible Distributed System", National Conference on Research Trends in Computer Science and Technology – 2012, Volume 3, Issue (1) NCRTCST, ISSN 2249 –071X
10. Kim,TaeYoug,Lee,shirly,Lee,Hoonja e, "Mutual authentication Scheme for cloud computing" Security comm. Network 2010; Available online http://mc.manuscriptcentral.com/scn