International Journal of Applied Research 2017; 3(7): 868-872

ISSN Print: 2394-7500
ISSN Online: 2394-5869
Impact Factor: 5.2
IJAR 2017; 3(7): 868-872
www.allresearchjournal.com
Received: 12-05-2017
Accepted: 14-06-2017

Sushila
Curator/Director, Dharohar Haryana Museum, Head, Department of Hindi, University College Kurukshetra University, Kurukshetra, Haryana, India

Correspondence
Sushila
Curator/Director, Dharohar Haryana Museum, Head, Department of Hindi, University College Kurukshetra University, Kurukshetra, Haryana, India

A review on cloud computing-it's security problem & solutions

Sushila

Abstract
We all know cloud computing is the most modern word in IT sector and it having huge demand in these days. So most of the IT companies like Google, IBM, Microsoft, Amazon, Yahoo and others develop cloud computing systems and products related to it for customers. But still customers are having difficulties for adopting the cloud computing technique that is only because of its security issues. Data of the customers are stored and processed in cloud, not in a local machine. Though cloud computing is considered mature for practical application, there is a need for more research. So in this paper I have discussed some of the Security Problems and also provide some solutions related to these problems.

Keywords: Cloud Computing, Models, Security Problems, Solutions

Introduction
"Cloud Computing" it is one of the most recent topics of the industry. A lot can be done on this topic. If we In the modern period of IT if we speak about the talk about the term "cloud" appears to have its origins in network diagrams that represented the internet, or various parts of it, as graphic clouds.
Cloud computing can be easily defined, there are many definitions, which share the same common denominator: the Internet. Cloud computing is a way to use the Internet in the daily life from your PC and Laptop. Cloud Computing came into action to know what happens when our data is moved to internet that is in "cloud". In the Figure 1 working of cloud is explained that how it provides various services.

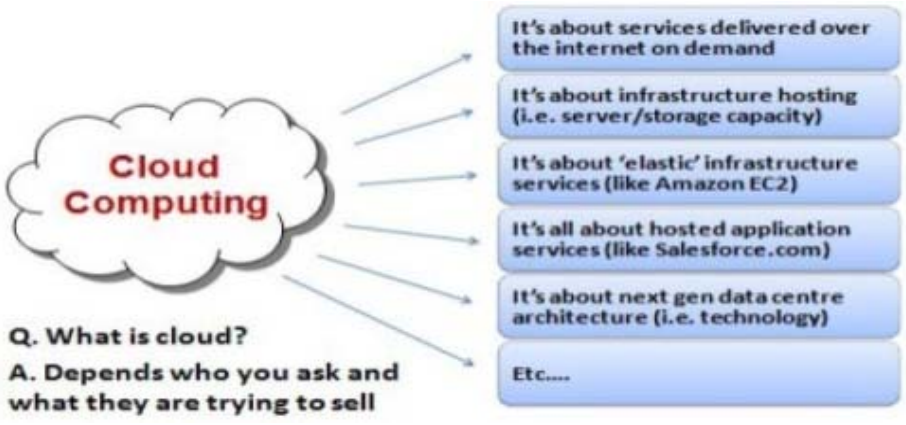

Fig 1: Cloud Computing

Cloud computing, often specified as the cloud, is the conveyance of on-demand computing resource everything from applications to data center over the internet on a pay for use basis. cloud computing is the distribution of computing services servers, storage, databases, networking, software and more over the Internet ("the cloud"). The Companies which contributes these computing services are called cloud providers. Benefits of cloud are: Less expense, speed, performance, productivity, reliability.

The things that we can do with the cloud are:

1. Create new apps and services
2. Store, back up and recover data
3. Host websites and blogs
4. Stream audio and video
5. Deliver software on demand
6. Analyze data for patterns and make prediction

Cloud: Overview

Service Models: Once a cloud is recognized, how its cloud computing services are deployed in terms of business models can differ depending on necessities. The primary service models being deployed are commonly known as:

1. Platform as a Service (PaaS): In this cloud providers deliver platforms, tools and other services that helps customers to develop, deploys, and manages their own applications, without installing any of these platforms on their local machines. The PaaS model may be hosted on top of IaaS model or on top of the cloud infrastructures directly. Example of PaaS is Google Apps and Microsoft Windows Azure.

2. Software as a Service (SaaS): In software as a Service, service providers host applications and clients access it through the World Wide Web. What actually SaaS do to see that we can also see the services provided by companies like Microsoft (Microsoft Office 365) and (Google doc). The service providers host all the programs and data in a central location, and then customers can access it through the World Wide Web. Software as a service provides the best cost savings over installed software by eliminating the need for enterprises to install and maintain hardware. Figure 2 is explaining working of SaaS.

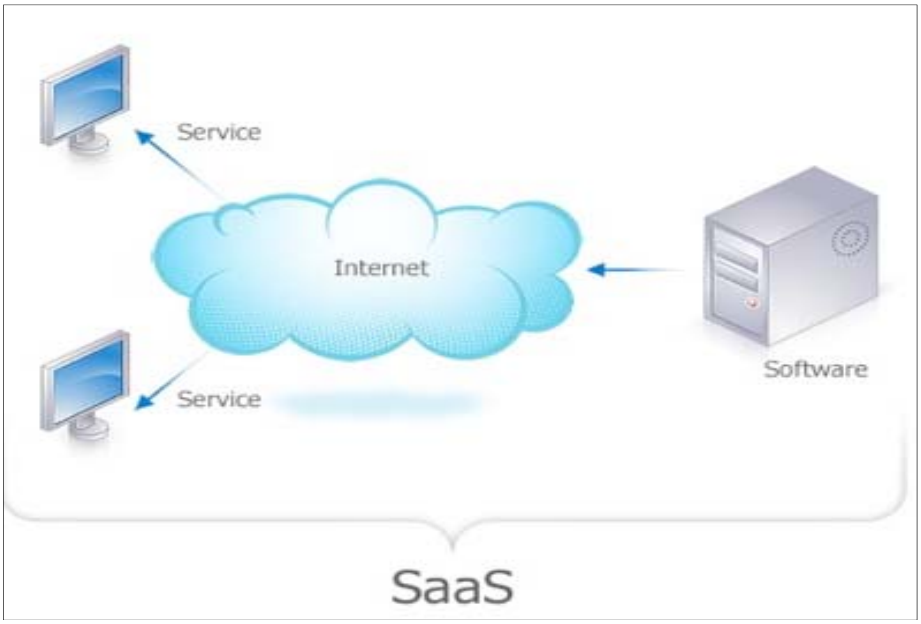

Fig 2: Software as a service

3. Infrastructure-as-a-service (IaaS): In this cloud providers provides the applications hosted on the cloud infrastructure as internet based service for customers, without any installation of the applications on the customers' computers. This model may be hosted on top of PaaS, IaaS or directly hosted on cloud infrastructure. Sales Force CRM is an example of the provider.

- Recently two more services have been provided by the Cloud Service Provider, they are:SEaaS(Security As a Service) and NEaaS(Network As a Service). SEaaS provides different security service algorithms for safeguarding the data in the cloud. Figure 1 shows the cloud environment with CSP, which has SEaaS as one of its services. In figure 1, CSP1 provides services like SaaS, PaaS, IaaS, NEaaS, and SEaaS.

Here, CSP (cloud service provider) is used only for security service, and not for storing the data. Users could store their data with other CSP's who provide storage as a service.

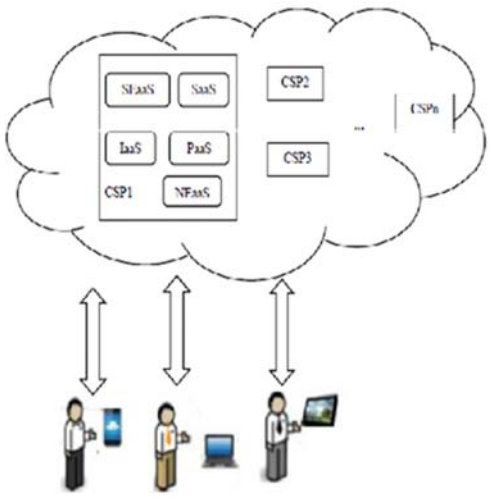

Fig 3: Cloud provider Architecture with SEaaS.

Deployment Models :- Deploying cloud computing can differ depending on requirements, and we have the following four deployment models, each with specific

characteristics that support the needs of the services and users of the clouds in particular ways:-

1) Private Cloud: The cloud that is accessible only from the inside of the any organization It means this can be accessed by the authorized person who has the access to use it only within the limited area or inside the organization.

2) Public Cloud: As the name suggests it's meaning itself i.e. the cloud that is available for all. This can be accessed from anywhere at any time by anyone. Like we have Google Drive we can store and retrieve the data from anywhere at any time free of cost.

3) Community Cloud: This type of cloud is made for those organizations that have similar requirements. This cloud is shared by number of organizations it will reduce their cost as compare to the Private Cloud but high cost than public cloud. The operation may be in-house or with a third party on the premises.

4) Hybrid Cloud: The cloud is combination of the private and public clouds. It can have no. of public and private clouds. Data of one cloud can be accessed by the other cloud. The Figure 3 is showing how hybrid cloud works.

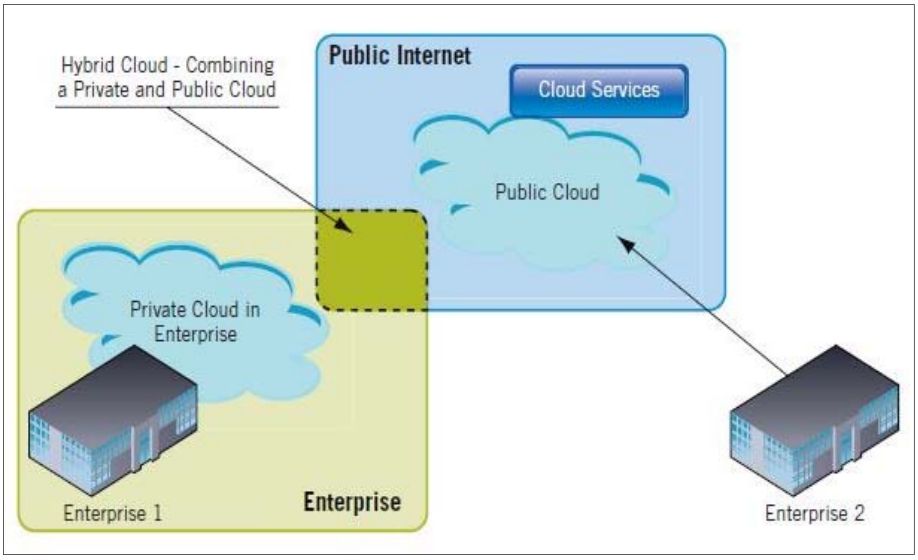

Fig 4: Example of hybrid cloud

- **Uniqueness of Cloud Computing**

1) Shared Infrastructure: In the cloud computing we are having shared resources like storage and networking. So Shared Infrastructure means we can access the resources we want from the cloud with the help of infrastructure provided to us.

2) Dynamic Provisioning: It means its having the capability to scale up his devices or we can say infrastructure. Means user need not to worry about the data.
For e.g.: Millions of people are uploading millions of pictures on Facebook but they are not just worried about it that where they are going. So Dynamic provision means the Servers of Facebook will be capable to store double of data next day. It should be scalable.

3) Network Access: It means user can access it from anywhere. User just needs an internet connection and he will be able to access it through mobile, Laptop, PC, Tab etc.

4) Managed Metering: It means user have to pay for the amount of the services he/she is using from the cloud providers. No extra charges will be there even there will be a SLA between the consumer and cloud provider.

- **Security issues in cloud**

Security of data

Cloud computing and web services as we all know run on an open network so they can be attacked by anyone on the network. In cloud computing as we all know users' data is stored and processed in cloud. Users cannot control cloud infrastructure managing their data in case of public cloud, which causes threats to the data. These security issues about users'
Data are showed as bellow:

1) Data Breach: It mainly deals with two security properties of data i.e. confidentiality and Integrity. Confidentiality allows only authorized parties or systems with the ability to access the protected data. Integrity deals with protecting data from unauthorized deletion, fabrication or modification.

2) Data lock-in: It means the customer cannot well shift from a one vendor to another. It may lose users' data, which afraid users from adapting cloud computing. Coghead is one example of a cloud platform whose shutdown left customers scrambling to rewrite their applications to run on a different platform. The solution is to standardize cloud Application Programming Interface (API), for instance GoGrid API

3) Data Remanence: - Data remanence is the residual representation of data that have been in some way nominally removed. In private cloud it gives very less security threats; however in public cloud it can cause several security issues because of the open environment, especially in an IaaS layer.

4) Data Recovery: - An incident such as a server breakdown may cause damage or loss to users' data. To avoid this kind of loss, data should be backed up should be recovered in future. Cloud users can keep a backup of critical data on a local computer.

5) Data Locality: - In a cloud environment the customer does not aware about the data where it is stored, which may be an issue. To avoid this kind of sensitive information, data privacy laws in many countries such as some Europe countries forbid some types of data to leave the country, which makes locality of data be an extremely important consideration in much enterprise architecture.

Service Provider Security Issues

1) Identity and Access Management

Identity and Access Management (lAM) features are Authorization, Authentication, and Auditing (AAA) of users accessing cloud services. In any enterprise "trust boundary" is mostly still and is monitored and controlled for applications which are deployed within the enterprise's perimeter. In a private data center, it managed the trust boundary encompasses the network, systems, and applications and it is secured with help of network security controls including intrusion prevention systems (IPSs), intrusion detection systems (IDSs), virtual private networks (VPNs), and multifactor authentication.

2) Privacy

Privacy is the one of the Security issue in cloud computing. Personal information regulations vary across the world and number of restrictions placed by number of countries whether it stored outside of the country. For a cloud service provider, in every jurisdiction a single level of service that is acceptable. Based on contractual commitments data can store within specific countries for privacy regulations, but this is difficult to verify.

3) Audit and Compliance

An organization implements the Audit and compliance to the internal and external processes that may fallow the requirements classification with which it must stand and the requirements are customer contracts, laws and regulations, driven by business objectives, internal corporate policies and check or monitor all such policies, procedures, and processes are without fail. In traditional Out sourcing relationships plays an important role for Audit and compliance. In Cloud dynamic nature, increase the importance of these functions in Platform as-a service (PaaS), Infrastructure-as-a-service (laaS), and Software-as-a- service (SaaS) environments.

Infrastructure Security Issues

1) Securing Data-Storage

In Cloud computing protecting data is one of the most important security issues. In this, it dealswith the way in which data is accessed and stored, audit requirements, compliance notification requirements, issues involving the cost of data breaches, and damage to brand value. In the cloud storage infrastructure, regulated and sensitive data needs to be properly segregated. In the service provider's datacenter, protecting data privacy and managing compliance are critical by using encrypting and managing encryption keys of data in transfer to the cloud.

2) Network and Server

Server-Side Protection: Virtual servers and applications, very like their non-virtual counterparts, have to be compelled to be secured in IaaS clouds, each physically and logically. Example, virtual firewalls are often used to isolate teams of virtual machines from different hosted teams, like production systems from development systems or development systems from different cloud-resident systems.

End User Security Issues

Browser Security

In a Cloud computing, remote servers are used for computation. The client nodes are used for input/output operations only, and for authorization and authentication of information to the Cloud. A standard Web browser is platform in-dependent client software useful for all users throughout the world. This can be categorized into different types: Software as- a-Service (SaaS), Web applications, or Web 2.0. TLS is used for data encryption and host authentication

2) Authentication

In the cloud computing, the primary basis for access control is user authentication and access control are more important than ever since the cloud and all of its data are accessible to all over the Internet. Trusted Platform Module (TPM) is a widely available and stronger authentication than username and passwords. Trusted Computing Groups (TCG's) is IF-MAP standard about authorized users and other security issue in real-time communication between the cloud provider and the customer.

- **Possible solution**

As I discussed various types of issues in cloud computing I just found a simple solution to some of the above mentioned issues. Solution is mentioned below:-

- **Strong SLA (Service Level Agreement)**

It should be able to answer the following questions:-

- How the bills are generated? What are the payment modes? How the services are affected if the customer delays in paying bills? This should contain grace period and how the customer can get the services back after the payment when the services stopped?
- What happens if the SLA is not met? How data is handled when the service contract ends, the type of data returned to the company?
- What happens if the service contract withdrawn? How data will be handled and returned to the company?
- How the service uses event logs and who actually has access to the data on the backend?
- Who will check the security of cloud providers?
- In terms of service availability, can you get your vendor to sign a service-level agreement?
- How much safe is data from Natural disaster?
- Is it possible for all of my data to be fully encrypted?
- What algorithms are used? Who holds, maintains and issues the keys?
- How much trusted is Encryption scheme of Service Provider?

- **Algorithm**

DES algorithm and RSA algorithm for providing security to cloud storage. Cyber criminals can easily cracked single

level encryption. Hence proposed system uses multilevel encryption and decryption to provide more security and Cuckoo hashing and Latent Semantic search techniques help in efficient search & retrieval of data in the Cloud Storage.

Key Generation Procedure:

1. Choose two distinct large random prime numbers p & q such that $p \neq q$.
2. Compute $n = p \times q$.
3. Calculate:a (n) = (p-1) (q-1).
4. Choose an integer e such that $1<e<a(n)$
5. Compute d to satisfy the congruence relation $d \times e = 1 \mod (n)$; d is kept as private key exponent.
6. The public key is (n, e) and the private key is (n, d).

Keep all the values d, p, q and a secret.

Encryption

Sender does the following

1. Obtains the recipient B's public key (n,e).
2. Represents the plaintext message as a positive integer m
3. Computes the cipher text $c = m^e \mod n$
4. Sends the cipher text C to B.

Decryption

Receiver does the following:-

1. Uses his private key (n, d) to compute $m = C^d \mod n$
2. Extracts the plaintext from the message representative m.

Des Algorithm

1. Fractioning of the text into 64-bit (8 octet) blocks.
2. Initial permutation of blocks.
3. Breakdown of the blocks into two parts: left and right, named L and R.
4. Permutation and substitution steps repeated 16 times called rounds.
5. Re-joining of the left and right parts then inverse initial permutation.

Conclusions and future work

In this paper, I mentioned various types of issues related to the cloud security which is showing that consumers are not adopting Cloud Computing due to lack of trust. So in this paper I mentioned a solution to make this technology trustworthy among various consumers i.e. Service Level Agreement. In future we will try to work practically on the issues.

References

1. Sunita Rani, Ambrish Gangal. Cloud Security with Encryption using Hybrid Algorithm and Secured Endpoints, International Journal of Computer Science and Information Technologies. 2012; 3:4302-4304.
2. Subhasri P, Padmapriya A. Multilevel Encryption for Ensuring Security in Public Cloud, International Journal of Advanced Research in Computer Science and Software Engineering. 2013; 3:527-532.
3. Manpreet Kaur, Rajbir Singh. Implementing Encryption Algorithms to Enhance Data Security of Cloud in Cloud Computing, International Journal of Computer Applications. 2013; 70:16-21.
4. Anshu Parashar, Rachna Arora. Secure User Data in Cloud Computing Using Encryption Algorithms, International Journal of Engineering Research and Applications. 2013; 3:1922-1926.
5. Priyanka Arora, Arun Singh, Himanshu Tiyagi. Evaluation and Comparison of Security Issues on Cloud Computing Environment", Worldof Computer Science and Information Technology Journal (WCSIT). 2012; 2(5):179-183.
6. Shashi Mehrotra Seth, Rajan Ishra. Comparative Analysis of Encryption Algorithms for Data Communication, International Journal of Computer Science and Technology. 2011; 2(2):292-294.
7. Diaa Salama Abdul, Elminaam, Hatem Mohamed Abdul Kader, Mohie Mohamed Hadhoud. Performance Evaluation of Symmetric Encryption Algorithms, IJCSNS International Journal of Computer Science and Network Security. 2008; 12:280-286.
8. Pavithra S, Ramadevi E. Performance Evaluation of Symmetric Algorithms, Journal of Global Research in Computer Science. 2012; 3(8):43-45.
9. Dr. L. Arockiam, Monikandan S. A Security Service Algorithm to Ensure the Confidentiality of Data in Cloud Storage International Journal of Engineering Research & Technology (IJERT). 2014; 3(12):1053-1058.
10. Dr. L. Arockiam, S. Monikandan. A Security Service Algorithm to Ensure the Confidentiality of Data in Cloud Storage International Journal of Engineering Research & Technology (IJERT). 2014; 3(12):1053-1058.
11. Ashok George, A. Sumathi. Efficient Data Storage and Retrieval in Cloud Environment Using Cuckoo Hashing and Latent Semantic Search Middle-East Journal of Scientific Research. 2015; 23(6):1053-1058.
12. Ashok George, Sumathi A. Efficient Data Storage and Retrieval in Cloud Environment Using Cuckoo Hashing and Latent Semantic Search Middle-East Journal of Scientific Research. 2015; 23(6):1053-1058.
13. Ajay Kulkarni Saurabh Kulkarni Ketki Haridas Aniket More Proposed Video Encryption Algorithm v/s Other Existing Engineering Research and Applications. 2013; 3:1922-1926.
14. Gurudatt Kulkarni, Jayant Gambhir, Tejswini Patil, Amruta Dongare. A Security Aspects in Cloud Computing, IEEE, 2012.
15. Pengfei You, Yuxing Peng, Weidong Liu, Shoufu Xue. Security Issues and Solutions in Cloud Computing, IEEE 32nd International Conference on Distributed Computing Systems Workshops, 2012.
16. Dale Vile, Tony Lock. Applied Cloud Computing, 2010.
17. Balachandra Reddy Kandukuri, Ramakrishna Paturi V, Dr. Atanu Rakshit. Cloud Security Issues, IEEE International Conference on Services Computing, 2009.