Vol 3 Issue 12 Jan 2014

ISSN No : 2230-7850

International Multidisciplinary Research Journal

Indian Streams Research Journal

Executive Editor
Ashok Yakkaldevi

Editor-in-Chief
H.N.Jagtap

Welcome to ISRJ

RNI MAHMUL/2011/38595 ISSN No.2230-7850

Indian Streams Research Journal is a multidisciplinary research journal, published monthly in English, Hindi & Marathi Language. All research papers submitted to the journal will be double - blind peer reviewed referred by members of the editorial board.Readers will include investigator in universities, research institutes government and industry with research interest in the general subjects.

International Advisory Board

Editorial Board

Address:-Ashok Yakkaldevi 258/34, Raviwar Peth, Solapur - 413 005 Maharashtra, India
Cell : 9595 359 435, Ph No: 02172372010 Email: ayisrj@yahoo.in Website: www.isrj.net

Indian Streams Research Journal
ISSN 2230-7850
Volume-3 | Issue-12 | Jan-2014
Available online at www.isrj.net

MULTI - CLOUD COMPUTING APPROACH

Shartaj Fatima

Lecturer, College of Business Administration King Saud University. K.S.A

Abstract:-In recent years, Cloud computing has become most needed technology for IT industry. The cloud computing has evolving rapidly due to its various features like cost effective and on demand service providing to the clients. Generally, Cloud service provider offers platform, software and infrastructure as service to the end user with respect to the pay-per-use basis. Now days, cloud is getting huge response because of its characteristics as it can be made as per requirement of an organization or end users.

As many organizations are moving to the cloud services, there is a new concept has raised name as Multi cloud where end user can use services from multiple cloud services. The paper investigates to security issues in the multi clouds environment. It explains about the onetime password use for authentication purposes from the multi-clouds at a single time. It elaborates about cloud clearly and use of multi clouds in organizations. In general, cloud works with internet. Initial step for the cloud management is about username and passwords. In same conditions, even passwords also getting hacked and accepts some malicious while working. One time passwords method introduced to work in a better way for username-password authentication.

This paper also conducted a survey that research relates to the single and multi-cloud security and deal with the possible solutions. The survey finds that multi-cloud providers should maintain security has received less interest from research community than single cloud usage. This paper also suggested multi-clouds has reduces security issues in cloud computing and also decreases affects of the security issues to the cloud user.

Keywords:multi-cloud infrastructure, security, platform, Computing, service provider.

INTRODUCTION :

Cloud computing

The term cloud computing has come with two words cloud and computing. Cloud might be thought to be identical with the internet where different resources are connected with the use of networks. One of the use of the resources is clients always should ask the simple architecture of it. The term computing refers to the processing and cloud computing is about processing on various resources over the network. In cloud computing architecture, Platform and Software/Application are the services which were provided by the service provider to the user. The cloud computing has changed the IT market where organization cannot invest in this purpose. Hence, they can hire an appropriate resource as on-demand basis or take services from the cloud. This process will decrease to the infrastructure costs to the organization. In general, cloud has three models called Infrastructure as a Service (IaaS), Software as a Service (SaaS) and Platform as a Service (PaaS). SaaS is a major model of cloud computing be positioned with the end users as place where they can save critical, real time, and important information. PaaS generally used by Application developers, this model helps to create a platform from the cloud as service to develop, test and debug or deploy their applications. It can act as a middleware to the developers.

Generally, network analysts are works with an IaaS model. In this model, services can treat as storage, networking, and also offers database management. Most of end users have attention on SaaS only because the data has devoted as well as produces by the cloud. This data can be used both cloud computing systems and with client computing systems. Basically, cloud computing doesn't has any specific definition. One of the most acceptable definitions is “It is a large scalable distributed computing model that is determined through economies of scale, in which resources can be shared among virtualized, dynamically-scalable, abstracted, managed computing power, platforms, storage, and services delivered on-demand basis to the end users over the internet. Though cloud computing is a developing technology; hence, it does not have been standard and the plenty work has been continuing regarding this.

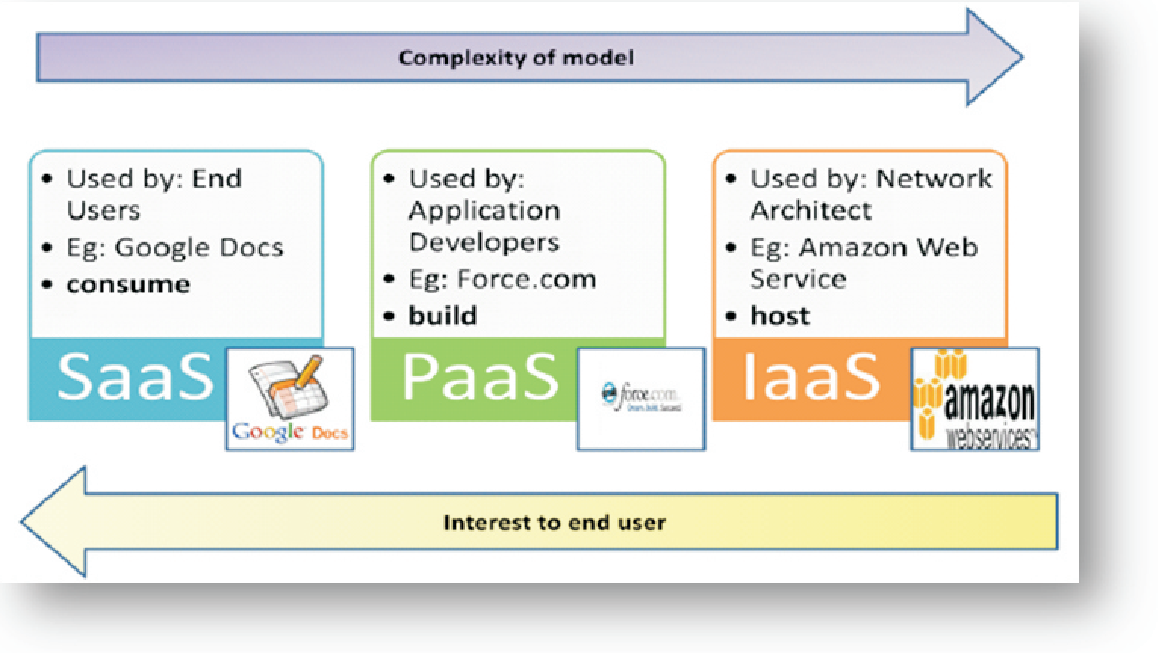

Figure - Cloud computing models

Types of cloud computing environments

1Public Clouds

Generally, public can get cloud infrastructure on a commercial basis from the provider. It makes free to the user to setting up infrastructures which is more difficult in financial aspect. Hence, user can easily use and deploy services in the cloud. Many general public can acquire these services as well as corporations and other kind of organizations. In general, third parties can involve in the public clouds to administrate over the internet and its services on Pay per use basis. This process also called as a provider clouds.

1.1.Private Clouds

The cloud infrastructure can also maintain for a particular organization. All operations could be done in the same house or third party in organizations own premises. It will close many limitations of an organization and specially made for organizations benefits.

This kind of clouds also called as internal clouds. Initially, it has been developed for IT departments within the organization who try to optimize employment of infrastructure resources in the organization. To achieve this, it needs to use concept grid and virtualizations while taking infrastructure.

1.2.Hybrid Clouds

This is a mixed cloud of both internal and external computing environments. It contains any kind of cloud, but those clouds should have ability by their interfaces to function effectively while allow data and/or applications from one cloud to another cloud.

1.3.Community Cloud

This cloud infrastructure has to distribute two different organizations with similar characteristics and requirements. It may useful to decrease capital investments costs to its establishment as the costs among both the organizations.

1.4.Multi-Cloud environment

Organizations have started working in this multi cloud environment so that they never face lack of availability of a service or a resource at any point of time and could prevent from potential loss. These days, organizations tend to rely on more than one cloud for services. The clouds could be public clouds, private clouds as well as hybrid clouds. Also trusting a single cloud is risky as there could be some malicious user or software who is spying on the data being exchanged. So, to deal with these issues multi cloud environments have gained importance. The term multi cloud as defined by Vukolicis "cloud of clouds- which says that the term cloud computing should not end up as a single cloud". The most popular is the public cloud. Here, the provider of cloud services provides the user with applications, storage, resources etc. it is majorly the responsibility of the cloud provider to provide the features of security, availability, scalability etc. The infrastructure for provided such clouds are generally shared. Consumers are either charged on a pay-per-use basis or it may also be free like first 500MB of Google App Engine are free. Other popular clouds are the private cloud within an organization. It may be connected via Internet or Intranet. It is created solely for use by an organization and its users. Hence, security concerns are less here as it also has a dedicated infrastructure for its cloud hence multi tenancy issue is also avoided. However, managing the cloud, its data, users etc all remain the responsibility of the organization providing the cloud. Users are generally not required to pay for such cloud. There may also be a condition where both these clouds and their services may be required. Such a scenario leads to hybrid cloud. Rules and protocols are to be developed to use hybrid cloud as per the need and convenience.

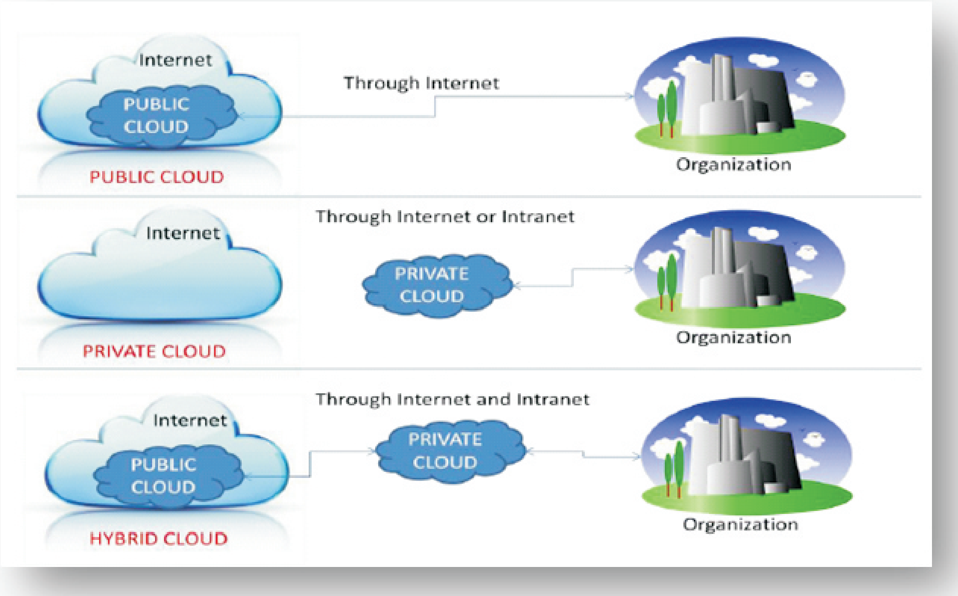

Figure - Multi cloud environment

DepSky System: Multi-Clouds Model

This section is about the multi clouds which have been covered in recent work. Bessani et al describes to the virtual storage cloud system as a DepSky which contains mixed of different clouds to build a clouds-of-clouds (multi clouds). This System supposed to the availability and secrecy of their stored data through multi service providers, combining Byzantine quorum system protocols, and cryptographic secret sharing and makes certain codes.

2.1 DepSky Architecture

The Architecture of DepSky contains four clouds and each has their own interface. This algorithm exists in the respective clients machines as software in the library to interact with each cloud. The four clouds act as storage clouds, so there is no need to update any code. But, the library of DepSky permits read/write operations along with thee storage clouds.

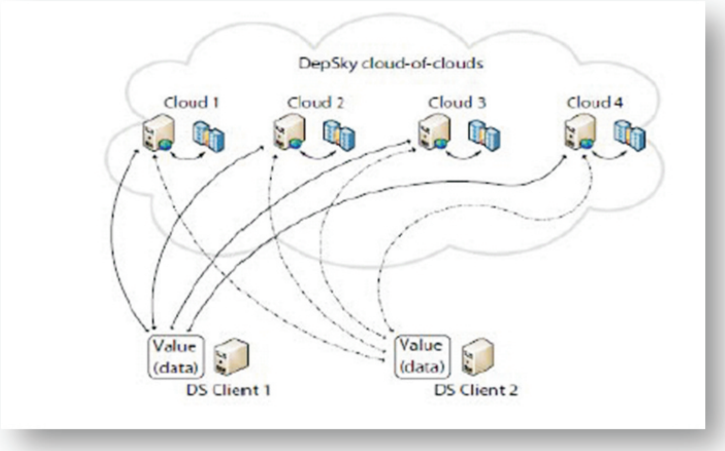

Figure - DepSky Architecture

By using different cloud providers, the DepSky library works with carious cloud interface providers and consequently and each node has to accept to the data format. The DepSky data model is having three concept levels:

1.The data unit implementation.
2.The conceptual data unit.
3.A generic data unit.

2.1 DepSky System model

The DepSky system divided into three parts such as writer, reader, and four cloud storage providers. In these storage provides readers and writers are treats as a clients tasks'. Bessani et al discussed about the differences between readers and writers in the cloud storage. For example, Readers can have chance to fail by crashing; they can fail periodically and displays any nature where writers can fail through crashing only.

2.2 Cloud storage suppliers in the DepSky system model

The Byzantine protocols engage with a collection of storage clouds (n) where n = 3 f +1, and f defined as maximum number of clouds which might be faulty. As well, any subset of (n – f) storage cloud generates byzantine quorum protocols.

LITERATURE REVIEW

In 2009, National Institute of Standards and Technology (NIST) defined multi cloud computing model. This model access and enable the appropriate network to a common pool of configurable computing resources such as servers, applications, networks, storage, applications and services which can be supply with minimal management effort or communication between service suppliers. This model utilizes and composed the three service models, four deployment models and five essential characteristics.

According to Myerson (2009), the cloud computing provides a pay per use pricing model and on demand service model, hence the customer pays for what is utilized and it based on the set service level agreement. The effective cost feature cut not only with the pricing model but also with several cost models such as salaries of IT personnel, huge cost of investing in software licensing and cost of IT maintenance. Cloud computing model has some additional incentives such as centralization of data centers, wireless transmissions, low emission, low energy consumption etc. the above mentioned models make a safe ecosystem and seems to higher priority in the computing field presently as it is encouraged by Microsoft founder Bill Gate (TED 2010).

In 2009, Vaquero stated that several others defined this cloud computing model in different ways, finally, Vaquero obtain 22 definitions of cloud computing from various authors. Before providing Cloud definition the authors encompassing it as a large pool of easily accessible, usable and virtualized resources like hardware or service development platforms. By selecting best resources researchers modifies the variable load of cloud computing. These selected resources typically effort by a pay-per-use model and which ensure offered by Infrastructure Provider by means of customized SLAs. The National Institute of Standards and Technology (NIST) stated there is no difference between encompassing definition, however, the cloud computing definition is explains about uses, features and pricing models.

According to Leyden (2009), Cloud Computing found its root in the triumph of server virtualization and run IT more efficiently through server consolidation. Day-by-day the cloud computing improves the consumption of computing services by charge up are positioned on original consumption rather than a flat rate.

In 2010, Varia stated that the Cloud Architecture and software application are designed to utilize Internet-accessible on demand services.

NIST defines five essential characteristics. They are:

1.On-demand self-service: the functioning of Cloud Computing is not depends on the human interaction this service automatically calls by the cloud users. According to Gens (2008), the definition of cloud service is business and consumers products, solutions and services are delivered and employing in real-time over the internet.
2. Broad network access: Cloud computing has more transmitted capacity through internet and this model right to use in various platforms such as laptops, phones etc.
3. Resource pooling: in the designing process of Cloud model researchers implement a multi-tenancy model in that. Therefore, several clients are serviced at the same time and which allows the computing resources to be joint together in order to satisfy the customers by providing what they want. The resources are like virtual and physical are assigned dynamically and reassigned by knowing consumers demand. However, these resources or not sited together but it need to be together to shape the entire service.

1Rapid elasticity: The resources hold the elasticity by improves the utility and the customers pay only for what they used. However, resources are available unlimited than the customer can easily scale up/down as their computing model require varies.
2Measured Service: According to consumptions of computing model the cloud services has metering capacity at various abstraction levels; based on different type of services like number of machines, bandwidth, storage and processing. These resources are controlled. Reported and monitored which supports the liability for both customer and provider services.

In 2010, Varia defines some common characteristics of cloud applications:

1.Independent Scalability: In this approach each component of the application carries out the service interfaces which will be responsible for its own scalability. Thus the total part added to overall scalability of the application.

2.Loose Coupling: the cloud application is built in a way that rigid dependencies are demoralized between components. Hence, the error event of one component of the system functions yet according to its specification.

3.Parallelization: this application has the capacity to allocate the tasks on multiple machines and aid to collect results obtained in parallel helps to attain efficiency.

OBJECTIVES OF THE STUDY

This study explores the reasons of switching IT traditional to cloud computing.
To study about cloud computing in India.
To recognize the characteristics of cloud computing.
This paper studies about different classifications and objectives of cloud computing.

METHODOLOGY:

1.Research methodology:

Research mainly refers as a search for knowledge. It can also define as a systematic and scientific explore for relevant data on a particular topic. In reality, research is a skill of scientific analysis. The function of research is to discover answers to questions via the application of scientific procedures.

2 Quantitative vs. Qualitative:

Quantitative research depends on the measurement of amount or quantity. It is applicable to processes that can be expressed in terms of quantity. Qualitative research, on the other hand, is concerned with qualitative phenomenon, i.e., processes relating to or involving quality or kind.

The research methodology for this report entails a careful blend of both primary and secondary sources available and is of qualitative approach.

Analysis

Why switch from traditional it to the cloud?

For this reasons, it is important to closely observe organization size and types of adopting model in aspect of IT sector. It could pave the way an increase in the number of capabilities without investing new infrastructure, new software license, and personal training. Ultimately, companies are considered to save huge amount of money.

i .Removal / Reduction of Capital Expenditure

In order to avoid spending huge amounts of capital on purchase and install their IT infrastructure or applications, the customers move forward to the cloud model. Capital expenses on IT reduce available to work capital for critical operations and business investments. It offers a simple operational expense and easy to get financial plan for preventing wasted money on depreciate assets. Further, a customer does not pay excess resource capacity in-house to meet the variable demand.

ii .Reduced Administration Costs

iii .The following IT solutions can be deployed
1.Maintained,
2.Extreme quick and managed,
3.Service provider patched and upgraded remotely

For reducing the burden on IT staff provides better technical support and reputable providers like Think Grid is no extra charge round the clock. They mainly focus on business tasks; can prevent obtaining excessive manpower and training costs. From IT giant IBM point of view, cloud computing allows organizations streamline procurement processes. There is a need to eliminate duplicate computer administrative skills related to configuration and support.

iv .Improved Resource Utilization There is a need to deliver and combine resources into large clouds in order to reduce costs and maximize utilization. Businesses are not concerned about over-provisioning service does not met their predictions and under-provisioning becomes suddenly unpopular. With the advancement of technology, there is a need to more and more applications, infrastructure in aspect of support into cloud relax. The concerted effort and budgets is mainly concentrate into real jobs that explores to improve better mission of the company. It drops to making out a better time and main focus of business that allows cloud providers is directly handle to manage the resources.

Multiple tenants can improve better utilization rates along with sharing computing power. As servers redundant to increase the speed of application development can reduce costs significantly. It is been known that side effect of this approach considered computer capacity rise dramatically, customers don't have engineer for peak loads.

v .Economies of scale

Cloud computing customers can socially and environmental benefit as of economies scale. The providers those who are use large scale data centers operating at multi-tenant architecture and higher efficiency levels to share some common resources among various customers. The IT model provision allows passing savings on their customers.

vi .Scalability on demand

The high valuable advantages like scalability and flexibility offer cloud computing that allows customers can quickly react changing their IT needs. For adding or subtracting users can be required and answering in reality rather than predicted requirements. The cloud-computing follows a utility model which are service based asset actual consumption. Customers are socially benefited as great elasticity of resources to pay a premium for large scale.

vii Quick and Easy implementation

There is no need to purchase hardware and software license or implementation services a company can acquire cloud-computing off the ground.

viii Helps Smaller Businesses Compete

Traditionally, there has been huge discrepancy among their IT resources towards business and enterprises. In this competitive world, cloud computing is probably for smaller companies compete and plays with competitors. Renting IT services as opposed to invest for both hardware and software make reasonably priced that leads to used for vital projects. Providers take Think Grid enterprise technology and provide better SMBs services would ensure low cost asset.

ix Quality of service

An immediate response of emergency situations is selected vendors to offered in 24/7 customer support.

x Guaranteed Uptime, SLAS

By implementing online applications and accessible services with regard to provider potential for reliability and guaranteed service levels.

xi Anywhere Access

Cloud-based IT services can be easily access your applications and secure data from various locations through internet connection. The multiple users can able to work and tie together on the similar project that is easy to collaborate with application and stored data in cloud. Further it has been point out that internet connection fails will not able to access the data. However, the nature of cloud users can simply connect a different location due to anywhere access. If your office connection fails and no redundancy can access data from home or nearest Wi-Fi enabled point. The remote working is possible to enable allows to meet innovative working regulations and customer satisfactions.

xii Technical Support

Cloud computing provider offers round clock for technical support. For instance recently, Think Grid customers are assigned one of our support pods. All subsequent contact engineers those who are available and ready to work for 24/7 is directly handles small group of skilled persons. The support model allows building better understanding of business requirements and extension of team members effectively.

xiii Disaster Recovery / Backup

The present research indicates that 90% of business does not have adequate disaster recovery or continual improvement business plans. And also its vulnerable to disruptions might be occurring. Think Grid can provide better array of disaster recovery services as of cloud backup that having ready to step in desktops , business services is to hit their problems. As per Hosted Desktops as of Think Grid, taking an example of they doesn't concern about data backup or disaster recovery as part of our service. Further it would be ensure that how long files are stored and copy available at different remote locations.

CHARACTERISTICS OF CLOUD COMPUTING

Few characteristics that have been already defined by NIST are discussed in the literature review. The additional characteristics of cloud computing are:

1 Managed Metering

Cloud computing uses metering systems to analyze and make better service and to give reports and billing details. Hence, users can pay bill for services what they exactly used during billing period.

2 High Scalability

Cloud provides services for many users as per their requirements along with high scalability.

3 Agility

In general, cloud works based on distributed background. It distributes resources among tasks and users whereas improving agility and efficiency.

4.High Availability and Reliability
There are more servers which are more reliable which are having very less chances of infrastructure failures.

5.Cost Savings

Companies can decrease capital and operational expenditures to increase their calculating abilities. It has less difficulty to start and also needs less in-house IT resources to provide system report. There are many reasons to attribute cloud computing technology with lower costs.

Multi-Sharing

A Distribution and share mode of cloud computing, pool with similar features can access both applications and multiple users easy with a cost reduction.

Shared Infrastructure

The cloud system, regardless of deployment model, requests to make the most of the available infrastructure transversely a number of users.

Dynamic Provisioning

This can work with manually by using software automation, providing the growth and reduction of service capability, as required. This dynamic grading needs to be worked out while controlling high levels of security and reliability. Cloud computing permits terms of services depending on current demand requirements.

Network Access

Deployments of services in the cloud incorporate a lot from using business applications to the latest application on the modern smart phones. Customer can access the internet from a broad range of devices such as using standards-based APIs, laptops, PCs and mobile devices.

Reliability

Services utilize multiple surplus sites, which will hold disaster recovery and business continuity.

Maintenance

Cloud service contributes to do the system maintenance, and access is through APIs that do not need application installations onto PCs, as a result further reducing maintenance requirements.

Mobile Accessible

Now days, mobile workers have increased mobile productivity to increase accessibility where it can be available.

CHALLENGES:

Security issues in cloud computing

The number or risks in cloud computing are various evolving from the fact that it includes use of various resources over the network. Primary issue of concern include authentication for which user names and passwords are used. Another issue is authorization for services for the authentic user by the cloud vendor. Another issue includes data confidentially, which should be maintained while data is transmitted over the cloud. For this various techniques like checksum, hash functions are used. Also Byzantine fault-tolerant duplication protocol surrounded by the cloud is intended to be implemented to maintain confidentiality of data over the cloud. Another major issue includes protecting the cloud from malicious attackers or data intrusion. Various encryptions schemes are used for this purpose. Lastly, service availability is also a potential risk of failure to the cloud. For this data redundancy is introduced. Also data is replicated and stored over various locations or data centre. Moreover availability of data in real time is also a risk.

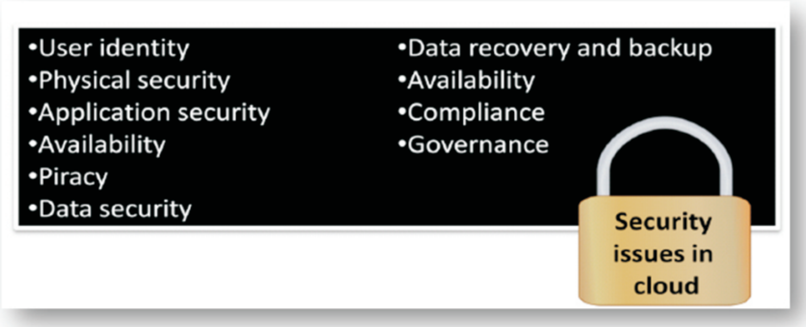

Figure - Security issues in the cloud

User Identity: Accessing resources like infrastructure, software or hardware over internet by different individuals increase the security issues. Therefore User Identity is required to authorize the person accessing the resources.

Physical Identity: Over internet sometimes the user's doesn't want to reveal their physical location. For this purpose the Physical Identity is to be kept confidential. Therefore, physical identity is also some of the concerned security issues in cloud.

Application security: As clouds provide the services and applications over internet, so there security is to be taken into consideration because user provides their information for accessing application. Hence, security of the applications is a necessity in cloud.

Data Integrity: "Protection of data stored in the cloud during transmission is known as data integrity." defined by Alzain [3]. It is an important security issue.

Availability: Availability basically defines [4] "data is continuously available in any situation either normal or disastrous". Availability is also a security issue in cloud because the data should be available to the user all the time and there should be no loss in data.

Authentication: Authentication if defined is [5] "confirmation of any data, identity being processed and accessed". The whole concept of security came into existence for this purpose.

Authorization: "The permission to access or process any data within the network", [6]. The Authorization is also one of the main and important security issues around which whole security concern lies.

Security Issues

Sharing of applications which process critical information with different tenants without sufficient proven security isolation, security SLAs or tenant control will result in "loss-of-control" and "lack of trust". Trust boundary can be moved one step further by using the proxies. Clients and CSPs have to establish trust relationships with proxies, which includes accepting a proxy's security, reliability, availability, and business continuity guarantees.

A trustworthy collaboration, which will help in management and administering proper communication, must be set between the client and Cloud service provider. In this framework different types of proxy networks will be explained. Some are on CSP's side and some are established on client side, stating the control over the assets while processing proxies. Similarly, using proxies that are within the domain of cloud service provider, exercise its control over proxy administration. Proxy network is a potential platform to develop proxy based security architecture.

Using Transport Layer Security Protocol Data, confidentiality on transmission in proxy based network can be achieved. Some other technologies that can be used to provide security are:
Warrant-based proxy signature for delegation signing rights to provide authentication to the proxies
Simple public-key infrastructure to provide secure access and authentication.

Implementation of cloud computing in the field of IT:

Cloud computing provides an appropriate security for the IT field. It avoids the unwanted users who want to access the software without any authority. By implementing this technology every service can able to operate only based on pay-per-use. This technology also provides a big data storing facility for the users who want to store their data. By using this storing facility users can able to store their data with huge convenience. Also there is a huge security for this data with direct hardware management. Here is an example for the establishment of cloud computing vendors, Amazon Elastic Compute Cloud (EC2) and Amazon Simple Storage Service (S3). They analyzed the owners in various approaches to encourage them to store the data. For that they providing assurance such as integrity, confidentiality and access control of the outsourced data. To gain all services users will prefer for the cloud computing. But the user gets vendor lock-in and has to use all the service by this particular cloud service provider.

In some cases users want to access another cloud service for low price and more effective. They want to confirm to a specific service provider in this way. For that user has to use multi-service provider on individual basis and pay separately for the service to each provider. The scenario of multi-cloud presents a model called collaboration of multi-cloud where the user vendor lock-in can be abolished with an agreement between the various cloud service provider that an authorized user of a particular cloud service provider can gain access to different service provider as per his requirement and cost management. To avoid the vendor lock-in syndrome, SaaS must be portable on top of various cloud PaaS and IaaS providers. This portability allows the migration from one provider to another in order to take advantage of cheaper prices or better qualities of services (QoS).

Appirio Cloud Storage, IBM's Mashup Center and Force.com for the Google App engine are examples of cloud mashup centre. These anxieties over the institution of such collaboration are that the architecture, protocols and other platform are on the research level. Another aspect is that it might be difficult that the various cloud service provider can get into collaboration so that a user can gain access to different service provider while he/she is an authenticated user of a single cloud service provider. In a multi-provider hosting scenario, the Service Provider is responsible for the multi-cloud provisioning of the services.

Thus, the Service provider contacts the possible Infrastructural Providers, negotiates terms of use, deploys services, monitors their operation, and potentially migrates services (or parts thereof) from misbehaving Infrastructural Providers.

Infrastructural Providers are managed independently and placement on different providers is treated as multiple instances of deployment. However, Apart from this issue the main role has to been played by the researchers to develop a mechanism to bring this collaboration or mashup centre into a real world for the standardized and cost effective of use cloud computing. The issue of security will also get generated as soon these mashup centre starts working which also must be look around as the service provider should not get it as a threat while implementing these centre.

DISCUSSION

As the challenges pertaining to security issues have been discussed in the earlier section, case studies corresponding to same issue are discussed in this section.

Here is a discussion for the multiple real-world cases where cloud computing were negotiation. The ways the company moderate the all incidents. For every case various attacks will be briefly described. Here also discussed about the information of the case which will be prevention and presented methods.

Malware Injection:

In a malware-injection attack an opponent attempts to inject malicious code into a system. In the form of scripts, active content, code and other software this attack can appear. Valid user is always ready to run in the cloud server. The personal service accepts the occurrence for computation in the cloud. The only verification is made to decide if the case matches a valid existing service. However, the integrity of the instance is not checked.

It is a valid service by penetrating the case and replacement, if the malware activity succeeds in the cloud. In May 2009, United States Department of Treasury stimulated four public websites offline for the Bureau of Engraving. After printing and discovering malicious code was integrated to the parent side. Cloud service supplier hosting the company's website was victim to an intrusion attack. As a result numerous websites were affected. Roger Thompson, chief research officer for Anti-Virus Guard (AVG) Technologies discovered malicious code was injected into the damages pages. Hackers added a tiny clip of a practically unnoticeable iFrame HTML code that readdressed visitors to a Ukrainian website. IFrame (Inline Frame) is an HTML document embedded within another HTML document on a website. From there, a variety of web-based attacks were commenced by means of an easy-to-purchase malicious toolkit called the Eleanor Exploit Pack.

Prevention measure:

Server workers require verifying for and exploiting iFrame code to prevent such type of attack. Firefox users have to fix No Script and set “Plugins Forbid iFrame” option. Window users must make sure that they have installed every security updates and have a dynamic anti-malware guard running.

Social Engineering Attack

This social engineering attack frequently happens in cloud computing. It disrupts that relies strongly on human communication and often recreating other people to break normal security measures.

To entirely destroy the technical developer, hackers used a social engineering attack in August 2012. This story explains regarding the dangerous blind spot among the identity verification systems utilized by Apple and Amazon. The hackers found the victim's @me.com address online which communicated them that there was a relate Apple ID account. To add a credit card number to the victim's account hacker called Amazon customer service. The agent asked the hacker for the billing associated email address, address and name (all information the hacker found on the internet) on the victim's account. Once the hacker answered these questions successfully the representative added the new credit card onto the account. Once ending the call, the hacker called Amazon customer service back and explained to the representative that he had lost access to his account. The Amazon representative asked the hacker for his billing address and a credit card associated with the account; the hacker used the new credit card information he provided from the previous phone call. Once the hacker gave the representative the information they added a new email address to the victim's account. Upon logging onto Amazon's website the hacker requested a password reset the email address he just created. The hacker now had access to the victim's Amazon account and credit card information on file. The hacker then called Apple technical support and requested a password reset on the victim's @me.com email account. The hacker could not answer any of the victim's account security questions, but Apple offered him another option. The Apple delegate only desired a billing address and the last four digits of the victim's credit card and gave the hacker a temporary password. Once the hacker had entranced into the victim's Apple account each and every information from the victim's iPod account, Mac Book and iPad was remotely wipe out.

Preventive measure:

Apple confirmed its temporarily disabled customers' capability to reset an Apple ID password by using phone. As an alternative, customers need to use Apple's online “iForgot” system. In the course of action they will work on a much stronger authentication method. That proves customers are who they say they are. Amazon customer service agent will no longer change account settings like credit card or email addresses by phone

Account Hijacking:

In July 2012 one more issue was happened. The cloud storage service declared that to access third-party sites hackers used usernames and passwords stolen from Drop box users' accounts. It was modified after consumers protested about Spam. They are getting to email address valid only for the Drop box accounts. With the help of stolen password, the hackers are able to access an employee account that includes a file in which user email addressed is shown. The company supposed customers who ever apply the similar password on various websites create an opportunity for hackers to access their accounts on some other websites.

Preventive measure:

With the intention to control a frequent attack, Drop box has applied two-factor authentication into the company's security controls. Two-factor authentication is described as a client entering in two of the subsequent three properties to establish his/her identity: something the user knows (e.g, password, PIN), something the user has (e.g., ATM card) and/or something the user is (e.g., biometric characteristic, such as a fingerprint). The company commenced latest automated mechanisms to recognize suspicious activities and a new page to demonstrate the entire logins.

Wireless Local Area Network Attack

In a wireless local area network attack a hacker fall into a certified user's wireless local area network to make attacks there are likely network injection attacks, identify theft, denial of service, accidental association and man-in-the-middle etc.

In January 2011, German security researcher Thomas Roth utilized cloud computing to break wireless networks that trusted on pre-shared passphrases, likely seen in homes and small businesses. The outcome of the approach exposed that wireless computing that depend on the pre-shared key (WPA-PSK) system for safety is fundamentally unconfident.

Roth's program was run on Amazon's Elastic Cloud Computing (EC2) system. Utilizing the huge power of Amazon's cloud the program was capable to work out through 400,000 likely passwords per second. It would general cost tens of thousands of dollars to buy the computers to execute the program, but Roth maintains that a typical password can be guessed by EC2 and his software in about six minutes. The type of EC2 computers utilized in the attack costs $.28 cents per minute, so $1.68 is all it took to hack into a wireless network.

Preventive measure:

WPA-PSK is measured to be secure because the measuring power desired to run through all the promises of passphrases is huge. Even though cloud computing make available this kind computing power today, and is low-cost. It is optional that maximum of 20 characters are sufficient to create a passphrase which cannot be cracked, however the additional characters integrated, the stronger the passphrase will be. A Best selection of numbers, letters and symbols should be integrated in the passphrase and it must be altered regularly. Dictionary letters and words replacement (i.e "n1c3" instead of "nice") must be prevented.

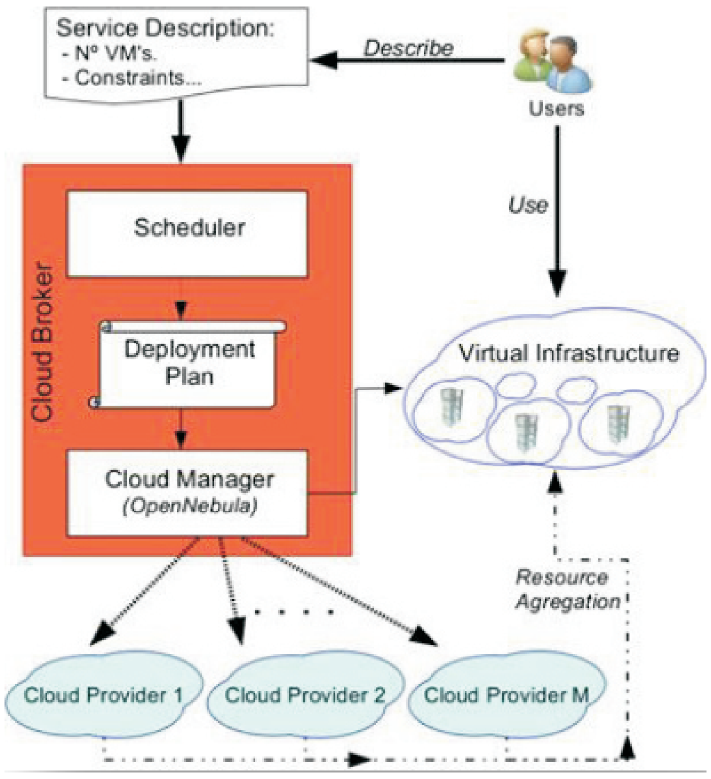

Figure - Cloud brokering architecture overview

In cloud computing, subscribers have to pay the service providers for the storage service. This service does not only provides flexibility and scalability for the data storage, it also provide customers with the benefit of paying only for the amount of data they need to store for a particular period of time, without any concerns for efficient storage mechanisms and maintainability issues with large amounts of data storage [8]. The cost effectiveness of deployment of cloud depends upon the deployment of virtual infrastructure it also affects whether it is static or dynamic deployment.

Many researchers focus only on static deployment where the user of service providers' condition does not change but in some cases the deployment has to be changed according to the time factor so as to be cost effective. Cloud computing can be classified as a new paradigm for the dynamic provisioning of computing services supported by state-of-the-art data centers that usually employ Virtual Machine (VM) technologies for consolidation and environment isolation purposes [9].

The optimal deployment of VM is an important factor for cost effectiveness of cloud service provider. The challenge is for determining the provisioning of virtual infrastructure as it should not be over\under provision. The system architecture given in fig. 1 gives an improved model of dynamic scheduler of multi-cloud brokering algorithm. This broker consist of service description, cloud broker and cloud service provider. The user can request the service descriptor template for virtual infrastructure which consists of number of VM to be deployed among available cloud.

The cloud broker which is an intermediate between service descriptor and cloud service provider has to perform two major tasks i.e. placement of virtual resources and management of these resources. The scheduler is responsible for the allotment of virtual infrastructure in available clouds. This situation is been implemented in static and dynamic environment. In the static approach, the placement decision is made once, according to the current user and pricing conditions. The dynamic approach is suitable for variable conditions (e.g., variable resource prices, required virtual resources, or cloud provider resources availability), so a new placement decision can be made when conditions change.

CONCLUSION:

A brief idea about cloud computing which states that cloud computing is about processing on various resources over the network. The cloud has three models called Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) in which 'Saas' is the most important. The three different types of cloud environment are public, private and hybrid clouds.

Multi cloud environment can be defined as 'cloud of clouds' in which multiple clouds are formed as a single cloud. Among the multi cloud model 'Depsky' is the major one.

Switching to cloud computing from traditional computing involves certain aspects such as Removal / Reduction of Capital Expenditure, reduced administration costs, improved resource utilization, economies of sales etc. There are various characteristics pertaining to cloud computing. Few of them are high scalability, agility, multi sharing, shared infrastructure, network access etc. Considering the challenges, security issues concerned to cloud computing is the most important aspect. The case studies describe the real time implementation of cloud computing in IT organizations.

RECOMMENDATIONS:

Recommendations for Platform as a Service (Paas)

The associated NIST standards, Federal Information Security management Act and special publications such as FIPS 200, FIPS 199, SP 800-53, etc, publications will administrate to paas systems for the cause of federal information systems and for those who will function on the benefit of US Government.

Section 9 provides generic recommendations for cloud computing services. For general recommendations we can search in appendix A also on the allocation of roles and responsibilities between cloud providers and customers.

Paas systems have some additional suggestion and are as follows.

Generic Interfaces: It is suggested to check out whether the application infrastructure interfaces such as queue, hash table, file which are available in the platform are suitable to hold interoperability and portability of the application ,before taking a decision to develop new application on a public Paas cloud platform. It support generic interfaces are preferable.

Standard Languages and Tools: Select a paas system that function with regulated tools and languages until it reaches that the only useful options are paas system and it is defined to help tools and languages.

Data Access: Select a Paas system that function with an ordinary data access protocols such as SQL.

Data Protection: Data protection will examine the paas providers data protection mechanisms, data location configuration, and data base transaction processing technologies and it will estimate weather the paas will reach the compliance, confidentiality, integrity needs of the organization that uses the subscribe paas application.

Application Frameworks: If there is a chance select a paas system which presents an application development framework and consists of architecture and tools for reducing security susceptibility.

Component Testing: In order to take any decision to install any new application on a public paas cloud transform ,first it is crucial to make sure that the software libraries which comprise of execution phase or compilation phase will act as deliberated in terms of both functionality and performance.

Security: Enterprise security policies can be prescribed by making sure that the paas application can be arranged to function in a protected manner and like identification and authorization paas application must be included with present existing enterprise security frameworks.

Secure Data Deletion: Secure data deletion requires a cloud providing a mechanism for dependably removing data on a consumer's demand

Recommendations for Infrastructure as a Service (Iaas)

The associated NIST standards, Federal Information Security management Act and special such as FIPS 200, FIPS 199, SP 800-53, etc, publications will administrate to paas systems for the cause of federal information systems and for those who will function on the benefit of US Government. Section 9 provides generic recommendations for cloud computing services. For general recommendations we can search in appendix A also on the allocation of roles and responsibilities between cloud providers and customers Paas systems have some additional suggestion and are as follows.

Multi-tenancy: In the form of virtual machines paas cloud provider will provides computing resources and in order to protect VMS from attacks make sure that the provider has machinery. (a)on the same physical host form other VMs (b) from the network initiate attacks(c) and as well as from the physical hosts .prevention mechanisms and typical attack detection comprise of virtual private networks, virtual firewalls, and virtual IDS/IPs .

Data Protection: Data protection will examine the paas providers data protection mechanisms, data location configuration, and data base transaction processing technologies and it will estimate weather the paas will reach the compliance, confidentiality, integrity needs of the organization that uses the subscribe paas application.

Secure Data Deletion: Secure data deletion requires a cloud providing a mechanism for dependably removing data on a consumer's demand

Administrative Access: Make sure that the limited set of trained users can supply administrative access to those resources when they are charging computing resources from a paas cloud contribute in the structure of physical servers and virtual machines.

VM Migration: VM migration will create an approach for future movement of virtual machines and related storage among vary cloud providers.

Virtualization Best Practices: For the administration of networks, conventional systems and for the use of virtualization paas will follow best practices that are NIST Guide to protect for full virtualization knowledge.

Certain recommendations are specified in this section, in order to further improvise the concept of cloud computing and also help in better implementation of the system. These recommendations specified are corresponding to Software as a Service (Saas), Platform as a Service (Paas) and Infrastructure as a Service (Iaas). They are as follows:

Recommendations for Software as a Service (Saas)

For Federal information systems and those functioned on side of the US Government, the Federal Information Security Management Act of 2002 and the related NIST standards and special publications (e.g. FIPS 199, FIPS 200, SP 800-53, etc.)Will implies on SaaS systems. The following are additional recommendations for SaaS systems:

Data Protection: Analyze the SaaS supplier's data protection mechanisms, data location configuration and database organization/transaction processing technologies, and evaluate whether they will collect the confidentiality, availability needs, integrity and compliance of the organization that will be utilizing the subscribed SaaS application.

Client Device/Application Protection: Steady with the FIPS 199 impact level of the data being computed, safeguard the cloud consumer's client device (e.g., a computer running a Web browser) as result to manage the exposure to attacks.

Encryption: Require that strong encryption using a robust algorithm with keys of required strength be used for Web sessions whenever the subscribed SaaS application requires the confidentiality of application interaction and data transfers. Also necessitate that the similar effort need to imply on stored data. Federal agencies must employ government-approved cryptographic algorithms for digital signature and encryption, and the execution required to be FIPS 140-2 authorized. Knowing about how cryptographic keys are controlled and who has access to them. Make sure that cryptographic keys are sufficiently sheltered.

Secure Data Deletion: Require that cloud providers offer a mechanism for reliably deleting data on a consumer's request.

Administrative Access: Make sure that the limited set of trained users can supply administrative access to those resources when they are charging computing resources from a paas cloud contribute in the structure of physical servers and virtual machines.

VM Migration: VM migration will create an approach for future migration of virtual machines and their related storage among vary cloud providers.

Virtualization Best Practices: For the administration of conventional systems and networks and for the use of virtualization paas will follow best practices that are NIST Guide to protect for full virtualization knowledge.

BIBLIOGRAPHY

1.Gens, F. (2008). "Defining “Cloud Services” and “Cloud Computing”." IDC exchange. Retrieved September 1, 2010, from http://blogs.idc.com/ie/?p=190
2.Leyden, T. (2009). Sys-con Media. Retrieved March 5, 2010, from http://tleyden.sys-con.com/node/1150011
3.Myerson, J. M. (Composer). (2009). "Cloud computing versus grid computing.". IBM developer works. IBM.
4.NIST. (2009). "Computer Security Resource Centre". Retrieved april 29, 2010, from http://csrc.nist.gov/groups/SNS/cloudcomputing/
5.TED. (2010). Bill Gates on energy: Innovating to zero! Retrieved March 12, 2010, from http://www.ted.com/talks/bill_gates.html
6.Vaquero, L. M.-M. (2009). "A Break in the Clouds: Towards a Cloud Definition.". ACM SIGCOMM Computer Communication Review , 50-55.
7.Varia, J. (2010). Cloud Architectures. Retrieved June 14, 2010,from http://jineshvaria.s3.amazonaws.com/public/cloudarchitectures-varia.pdf