International Refereed Journal of Engineering and Science (IRJES)
ISSN (Online) 2319-183X, (Print) 2319-1821
Volume 2, Issue 2(February 2013), PP.01-13
www.irjes.com

Cloud Computing Security Issues And Challenges

Pranita P. Khairnar,
Electronics Department, Amrutvahini College of Engineering, Sangamner
Prof. V.S. Ubale
Asst. Prof. Electronics Department, Amrutvahini College of Engineering, Sangamner

Abstract- *Cloud computing has generated a lot of interest and competition in the industry and it is recognize as one of the top 10 technologies of 2010. It is an internet based service delivery model which provides internet based services, computing and storage for users in all market including financial, health care & government. Cloud security is becoming a key differentiator and competitive edge between cloud providers. From the providers point of view a Cloud is a very large distributed system which poses many challenges. Cloud computing is clearly one of today's most enticing technology areas to its cost-efficiency and flexibility. There is a growing trend of using cloud services for ever growing storage and data processing needs.*

I. INTRODUCTION

Cloud computing is one of today's most exciting technologies due to its ability to reduce costs associated with computing while increasing flexibility and scalability for computer processes. During the past few years, cloud computing has grown from being a promising business idea to one of the fastest growing parts of the IT industry. IT organizations have expresses concern about critical issues (such as security) that exist with the widespread implementation of cloud computing. These types of concerns originate from the fact that data is stored remotely from the customer's location; in fact, it can be stored at any location.

Cloud computing received significant attention recently as it changes the way computation and services to customers, For example, it changes the way of providing and managing computing resources, such as CPUs, databases, and storage systems. Today, leading players, such as Amazon, Google, IBM, Microsoft, and Salesforce.com offer their cloud infrastructure for services.

Cloud computing is the next stage of the Internet evolution. A typical cloud must have several distinct properties: elasticity and scalability, multi-tenancy, self-managed function capabilities, service billing and metering functions, connectivity interfaces and technologies. In addition, a cloud supports large scale user accesses at distributed locations over the Internet, offers on-demand application services at anytime, and provides both virtual and/or physical appliances for customers. There are three types of clouds: a) private clouds, which are internal clouds based on a private network behind a firewall; b) public clouds, which are the clouds with public accessible services over the Internet; and c) hybrid clouds, which are made of different types of clouds, including public and private clouds.(1)

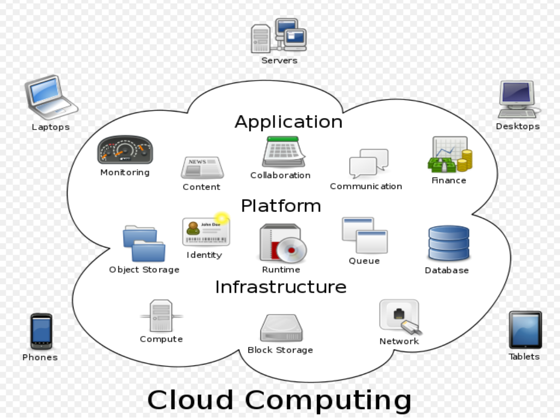


Fig:Cloud architecture

- General Definition - The term cloud is used as a metaphor for the Internet, based on the cloud drawing used in the past to represent the telephone network, and later to depict the Internet in computer network diagrams as an abstraction of the underlying infrastructure it represents and computing reflects the ability of performing computing tasks.

- Wikipedia defines it as “ An Internet-based computing, whereby shared resources, software and information are provided to computers and other devices on-demand, like a public utility.”
- A technical definition is “ A computing capability that provides an abstraction between the computing resource and its underlying technical architecture(e.g., servers, storage, networks), enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction.”(2)

II. NEED OF CLOUD COMPUTING

Cloud computing enables users to store and process all their data on the web via the Internet, with no doubts security is one of main significant concerns. A more fundamental reason preventing companies from moving to cloud computing is that the cloud computing platform is inherently less secure than the traditional network infrastructure. Security must be integrated into every aspect of cloud computing platforms to make users trust that their data is secure.

Security, in particular, is one of the most argued-about issues in the cloud computing field; several enterprises look at cloud computing warily due to projected security risks. The risks of compromised security and privacy may be lower overall, however, with cloud computing than they would be if the data were to be stored on individual machines instead of in a so - called "cloud" (the network of computers used for remote storage and maintenance). Comparison of the benefits and risks of cloud computing with those of the status quo are necessary for a full evaluation of the viability of cloud computing. Consequently, some issues arise that clients need to consider as they contemplate moving to cloud computing for their businesses.

III. SECURITY ISSUES AND IN CLOUD COMPUTING

A. Cloud Deployments Models:

In the cloud deployment model, networking, platform, storage, and software infrastructure are provided as services that scale up or down depending on the demand. These fundamental elements of the cloud require security which depends and varies with respect to
-the deployment model that is used
-the way by which it is delivered
The Cloud Computing model has three main deployment models which are:
1. Private cloud
2. Public cloud
3. Hybrid cloud
4. Community cloud

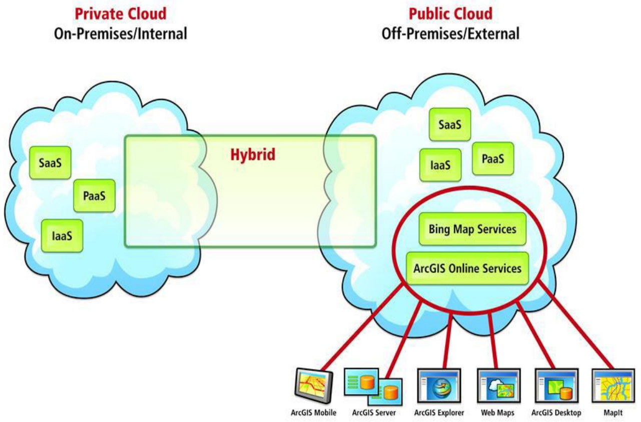


Fig:Cloud deployement models(3)

1. Private cloud

Private cloud is a new term that some vendors have recently used to describe offerings that emulate cloud computing on private networks. It is set up within an organization’s internal enterprise data centre. In the private cloud, scalable resources and virtual applications provided by the cloud vendor are pooled together and available for cloud users to share and use. It differs from the public cloud in that all the cloud resources and applications are managed by the organization itself, similar to Intranet functionality. Utilization on the private cloud can be much more secure than that of the public cloud because of its specified internal exposure. Only the organization and designated stakeholders may have access to operate on a specific Private cloud.

2. Public cloud

Public cloud describes cloud computing in the traditional mainstream sense, whereby resources are dynamically provisioned on a fine-grained, self-service basis over the Internet, via web applications/web services, from an off-site third-party provider who shares resources and bills on a fine-grained utility computing basis. It is typically based on a pay-per-use model, similar to a prepaid electricity metering system which is flexible enough to cater for spikes in demand for cloud optimization. Public clouds are less secure than the other cloud models because it places an additional burden of ensuring all applications and data accessed on the public cloud are not subjected to malicious attacks.

3. Hybrid cloud

Hybrid cloud is a private cloud linked to one or more external cloud services, centrally managed, provisioned as a single unit, and circumscribed by a secure network. It provides virtual IT solutions through a mix of both public and private clouds. Hybrid Cloud provides more secure control of the data and applications and allows various parties to access information over the Internet. It also has an open architecture that allows interfaces with other management systems. Hybrid cloud can describe configuration combining a local device, such as a Plug computer with cloud services. It can also describe configurations combining virtual and physical, collocated assets -for example, a mostly virtualized environment that requires physical servers, routers, or other hardware such as a network appliance acting as a firewall or spam filter.

4. Community cloud

The cloud infrastructure is shared among a number of organizations with similar interests and requirements. This may help limit the capital expenditure costs for its establishment as the costs are shared among the organizations. The operation may be in-house or with a third party on the premises.

Public cloud benefits:
o Low investment hurdle: pay for what you use
o Good test/development environment for applications that scale to many servers

Public cloud risks:
o Security concerns: multi-tenancy and transfers over the Internet
o IT organization may react negatively to loss of control over data center function

Private cloud benefits:
o Fewer security concerns as existing data center security stays in place
o IT organization retains control over data center

Private cloud risks:
o High investment hurdle in private cloud implementation, along with purchases of new hardware and software
o New operational processes are required; old processes not all suitable for private cloud

Hybrid cloud benefits
o Operational flexibility: run mission critical on private cloud, dev/test on public cloud
o Scalability: run peak and bursty workloads on the public cloud

Hybrid cloud risks:
o Hybrid clouds are still being developed; not many in real use
o Control of security between private and public clouds; some of same concerns as in public cloud (4)

B. Cloud Computing Service Delivery Models:

Following on the cloud deployment models, the next security consideration relates to the various cloud computing service delivery models. The three main cloud service delivery models are:
1. Infrastructure as a Service (IAAS)
2. Platform As a Service (PAAS)
3. Software As A Service (SAAS)

Combining the three types of clouds with the delivery models we get a holistic cloud illustration as seen in Figure, surrounded by connectivity devices coupled with information security themes. Virtualized physical resources, virtualized infrastructure, as well as virtualized middleware platforms and business applications are being provided and consumed as services in the Cloud. Cloud vendors and clients need to maintain Cloud computing security at all interfaces. The next section of the paper introduces challenges faced in the Cloud computing domain.

A. Cloud Infrastructure as a Service (IaaS)

A model in which an organization outsources the equipment used to support operations including storage, hardware, virtual servers, databases, and networking components. The service provider owns the equipment and is responsible for housing, running, and maintaining it. (5)

Characteristics of IaaS

As with the two previous sections, SaaS and PaaS, IaaS is a rapidly developing field. That said there are some core characteristics which describe what IaaS is. IaaS is generally accepted to comply with the following:

- Resources are distributed as a service
- Allows for dynamic scaling
- Has a variable cost, utility pricing model
- Generally includes multiple users on a single piece of hardware (6)

Cloud Software as a Service (SaaS)

The capability offered to the consumer is to use the provider’s commercially available applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a Web browserOne of the most common uses for SaaS is for Web-based email services. SaaS enables enterprises to obtain the use of such commercially available software on demand without the need to invest in IT resources knowledgeable in its support. (5)

Characteristics of SaaS

Like other forms of Cloud Computing, it is important to ensure that solutions sold as SaaS in fact comply with generally accepted definitions of Cloud Computing. Some defining characteristics of SaaS include:

- Web access to commercial software.
- Software is managed from a central location.
- Software delivered in a “one to many” model. (6)

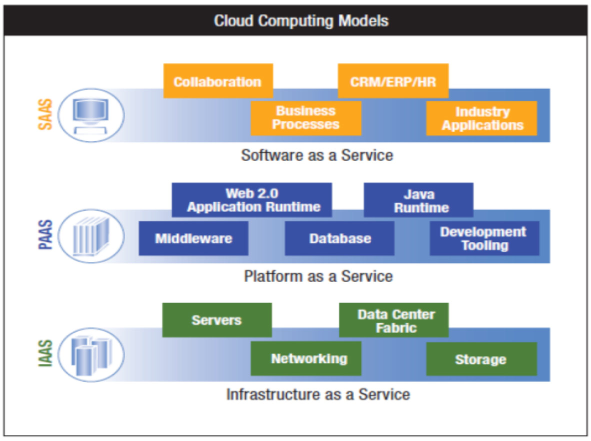
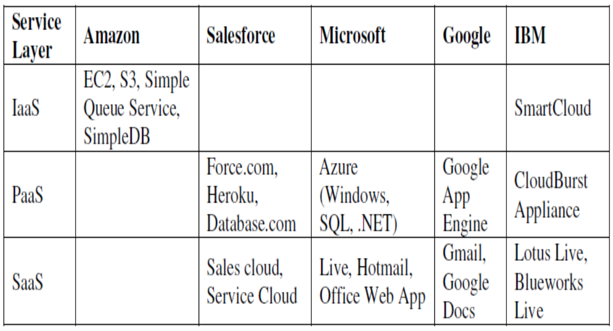


Fig 2.4: Cloud computing service delivery models (7)



Service Layer	Amazon	Salesforce	Microsoft	Google	IBM
IaaS	EC2, S3, Simple Queue Service, SimpleDB				SmartCloud
PaaS		Force.com, Heroku, Database.com	Azure (Windows, SQL, .NET)	Google App Engine	CloudBurst Appliance
SaaS		Sales cloud, Service Cloud	Live, Hotmail, Office Web App	Gmail, Google Docs	Lotus Live, Blueworks Live

Table2.1. Cloud platform offers for different cloud service layers (8)

Cloud Platform as a Service (PaaS)

The two components of PaaS are the place on which software can be launched (platform), and the services being provided (solution stack). Resources being delivered via PaaS typically include infrastructure and applications. In many cases the data being used is also stored in the cloud and the end user's terminal may contain only an operating system and Web browser. In addition, end users can write their own code and the PaaS provider then uploads that code and presents it on the Web. SalesForce.com's Force.com is an example. The PaaS model enables resources to be increased easily with demand since end users share the same cloud. This is often called multi-tenant cloud computing.(5)

Characteristics of PaaS

There are a number of different takes on what constitutes PaaS but some basic characteristics include,

•Services to develop, test, deploy, host and maintain applications in the same integrated development environment. All the varying services needed to fulfill the application development process.

•Multi-tenant architecture where multiple concurrent users utilize the same development application.

•Built in scalability of deployed software including load balancing and failover. (6)

IV. SOME OTHER SECURITY ISSUES IN CLOUD COMPUTING

1. Data security: The enterprise data is stored outside the enterprise boundary

- Security vulnerabilities in the application
- Malicious employees

2. Network security

- All data flow over the network needs to be secured in order to prevent leakage of sensitive information.
- This involves the use of strong network traffic encryption techniques
- Malicious users can exploit weaknesses in network security configuration to sniff network packets

3. Data locality

- The customer does not know where the data is getting stored
- Certain types of data cannot leave the country because of potentially sensitive information

4. Data integrity

- In a distributed system, there are multiple databases and multiple applications

-One of the biggest challenges with web services is transaction management

-At the protocol level, HTTP (Hyper Text Transfer Protocol) does not support transactions or guaranteed delivery

5. Data segregation

- Data of various users will reside at the same location

→Intrusion of data of one user by another becomes possible in this environment

-This intrusion can be done either by hacking through the loop holes in the application by injecting client code into the SaaS system

6. Data access

- A company will have its own security policies based on which each employee can have access to a particular set of data
- These security policies must be adhered by the cloud to avoid intrusion of data by unauthorized users

7. Authentication and authorization

8. Data confidentiality issue

Cloud computing services exist in many variations, including

-data storage sites

-video sites

-tax preparation sites

-personal health record websites

The entire contents of a user's storage device may be stored with single/many cloud provider(s)

9. Data breaches

Since data from various users and business organizations lie together in a cloud environment breaching into the cloud environment will potentially attack the data of all the users (9)

V. Challenges for the cloud computing

The following are some of the notable challenges associated with cloud computing, and although some of these may cause a slowdown when delivering more services in the cloud, most also can provide opportunities, if resolved with due care and attention in the planning stages.

- Security and Privacy — Perhaps two of the more "hot button" issues surrounding cloud computing relate to storing and securing data, and monitoring the use of the cloud by the service providers. These issues are generally attributed to slowing the deployment of cloud services. These challenges can be addressed, for example, by storing the information internal to the organization, but allowing it to be used in the cloud. For this to occur, though, the security mechanisms between organization and the cloud need to be robust and a Hybrid cloud could support such a deployment.

• Lack of Standards — Clouds have documented interfaces; however, no standards are associated with these, and thus it is unlikely that most clouds will be interoperable. The Open Grid Forum is developing an Open Cloud Computing Interface to resolve this issue and the Open Cloud Consortium is working on cloud computing standards and practices. The findings of these groups will need to mature, but it is not known whether they will address the needs of the people deploying the services and the specific interfaces these services need. However, keeping up to date on the latest standards as they evolve will allow them to be leveraged, if applicable.

• Continuously Evolving — User requirements are continuously evolving, as are the requirements for interfaces, networking, and storage. This means that a "cloud," especially a public one, does not remain static and is also continuously evolving.

• Compliance Concerns — The Sarbanes-Oxley Act in the US and Data Protection directives in the EU are just two among many compliance issues affecting cloud computing, based on the type of data and application for which the cloud is being used. The EU has a legislative backing for data protection across all member states, but in the US data protection is different and can vary from state to state. As with security and privacy mentioned previously, these typically result in Hybrid cloud deployment with one cloud storing the data internal to the organization.(10)

Issues of security, reliability, and performance should be addressed to meet specific requirement of different organizations, infrastructures, and functions.

•**Security**

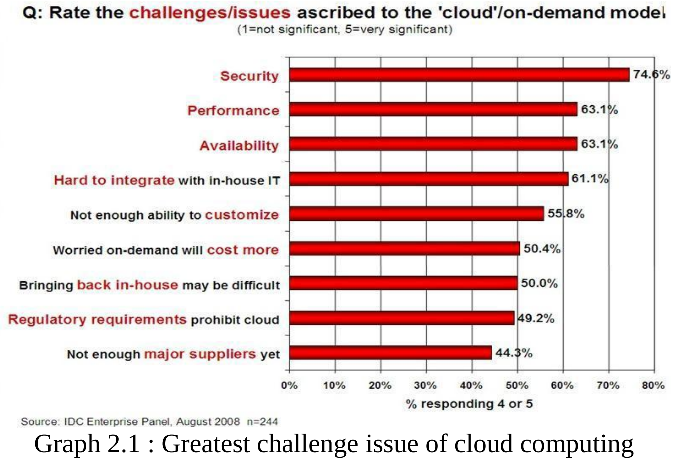
As different users store more of their own data in a cloud, being able to ensure that one users' private data is not accessible to other users who are not authorized to see it becomes more important. While virtualization technology offers one approach for improving security, a more fine – grained would be useful for many applications.

•**Reliability**

As more users come to depend on the services offered by a cloud, reliability becomes increasingly important, especially for long-running or missioncritical applications. A cloud should be able to continue to run in the presence of hardware and software faults. Google has developed an approach that works well using commodity hardware and their own software. Other applications might require more stringent reliability that would be better served by a combination of more robust hardware and/or software-based fault-tolerance techniques.

•**Vulnerability to Attacks**

If a cloud is providing compute and storage services over the Internet such as the Amazon approach, security and reliability capabilities must be extended to deal with malicious attempts to access other users' files and /or to deny service to legitimate users. Being able to prevent, detect, and recover from such attacks will become increasingly important as more people and organizations use cloud computing for critical applications.(11)



Source: IDC Enterprise Panel, August 2008 n=244

Graph 2.1 : Greatest challenge issue of cloud computing

From one point of view, security could improve due to centralization of data and increased security-focused resources. On the other hand concerns persist about loss of control over certain sensitive data, and the lack of security for stored kernels entrusted to cloud providers. If those providers have not done good jobs securing their own environments, the consumers could be in trouble. Measuring the quality of cloud providers' approach to security is difficult because many cloud providers will not expose their infrastructure to customers.

This work is a survey more specific to the different security issues and the associated challenges that has emanated in the cloud computing system.(3).

VI. SYSTEM OVERVIEW

The earlier version of the Cloud Security Alliance's guidance featured definitions that were written prior to the published work of the scientists at the U.S. National Institute of Standards and Technology (NIST) and their efforts around defining cloud computing.

NIST's publication is generally well accepted, and we have chosen to align with the NIST Working Definition of cloud computing (version 15 as of this writing) to bring coherence and consensus around a common language so we can focus on use cases rather than semantic nuance.

It is important to note that this guide is intended to be broadly usable and applicable to organizations globally. While NIST is a U.S. government organization, the selection of this reference model should not be interpreted to suggest the exclusion of other points of view or geographies.

NIST defines cloud computing by describing five essential characteristics, three cloud service models, and four cloud deployment models. They are summarized in visual form in figure.

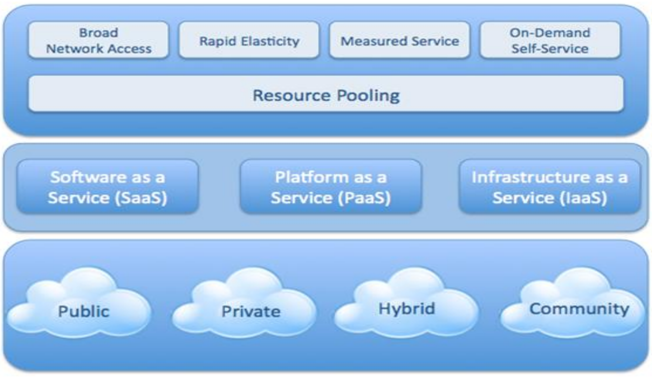


Fig 3.1: Visual model of NIST working definition of cloud

• On-demand self service: Allows for the provision of services based on current demand requirements. This is done automatically using software automation, enabling the expansion and contraction of service capability, as needed. This dynamic scaling needs to be done while maintaining high levels of reliability and security.

•Broad network access: computing capabilities can be accessed through the network by (thin or thick) client platforms using standard mechanisms;

•Elasticity: capabilities can be provisioned dynamically in order to enable a customer application to scale out quickly, and can be dynamically released in order to enable it to scale in (in general, the customer perceives unlimited capabilities that can be purchased in any quantity at any time);

•Measured service: Cloud resource and service usages are optimized through a pay-per-use business model, and are to be monitored, controlled and reported transparently to both their customer and provider.

•resource pooling: virtual and physical resources can be pooled and assigned dynamically to consumers, according to their demand, using a multi-tenant model.(12)

3 Solutions for Against Cloud Security Problems

There are several traditional solutions to mitigate security problems that exist in the Internet environment, as a cloud infrastructure, but nature of cloud causes some security problem that they are especially exist in cloud environment.

Access Control

1. Control access to information.
2. Manage user access rights.
3. Encourage good access practices.
4. Control access to network services.
5. Control access to operating systems.
6. Control access to applications and systems.

Data privacy protection in cloud computing

Following are the main types of security mechanism:

1.Encryption transforms data or information into something that an attacker or adversary cannot understand. Encryption provides a means to implementation of data confidentiality.

2.Authentication is used to verify the claimed identity of an information owner or user or other entity. Authentication proves "who you are". Authorization follows authentication. Authorization defines or deals with what are actions allowed to be performed by an information owner or user once she is authenticated.

In more advanced authentication systems, the system side will generate a random number to send the user a challenge message, requesting the user to transmit an encrypted response message in reply to the challenge message, thus authenticating that the user has the correct encryption key. Without this key, the user will not be allowed the access. In the process of challenge and response the client□ s encrypted key uses the client□ s password to convert a derived value and in this program, each communication between the client and server is unique, and a hacker using an old message would fail to access the system. In addition, the One-Time Password (OTP) authentication system differs from most person to another person for a password.. Most people understand a password to be a password chosen by the user to be meaningful, and can be used again and again. The emphasis of OTP however is the single-use nature of the password. By this means the security can be fulfilled conceptually which can be hacked by hackers who can then use the data in the message to log into the service as the user or to misuse.

3.Use of filters

Companies like vontu, wedsense and vercept and many other have proposal of a system which designed to handle our network from the data, so that automatically it blocks the sensitive data.

4.The use reputable service

Even if file is encrypted, some online activities which involves online processing of documents wants to save the file but it is difficult to protect. This means that user need to carefully consider services from which they will not get to risk from their own brand name and will not allow data leakage, it would not share data with marketers. (13)

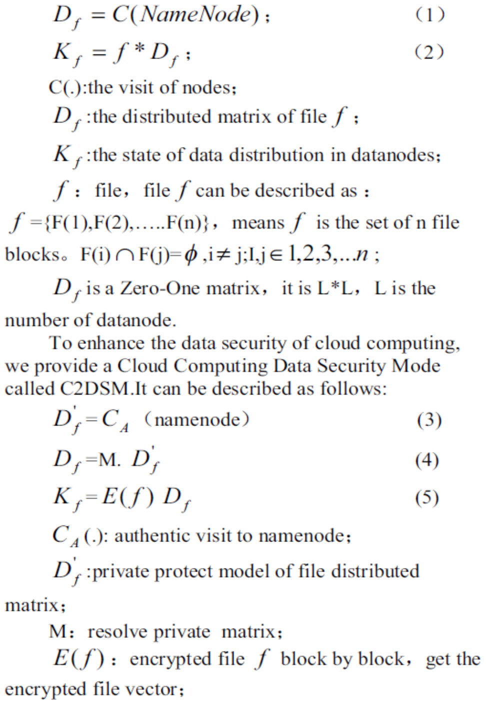
3.4 Data Security Model for Cloud Computing

A.Principle of Data Security

All the data security technic is built on confidentiality, integrity and availability of these three basic principles. Confidentiality refers to the so-called hidden the actual data or information, especially in the military and other sensitive areas, the confidentiality of data on the more stringent requirements. For cloud computing, the data are stored in "data center", the security and confidentiality of user data is even more important. The so-called integrity of data in any state is not subject to the need to guarantee unauthorized deletion, modification or damage. The availability of data means that users can have the expectations of the use of data by the use of capacity.

B.Data Security Model

Data model of cloud computing can be described in math as follows:



$$D_f = C(NameNode)\text{；} \qquad (1)$$

$$K_f = f * D_f\text{；} \qquad (2)$$

C(.):the visit of nodes；

D_f :the distributed matrix of file f ；

K_f :the state of data distribution in datanodes；

f ： file，file f can be described as ：

f ={F(1),F(2),…..F(n)}， means f is the set of n file blocks。F(i) $\cap$ F(j)= ϕ ,i $\neq$ j;I,j $\in$ 1,2,3,...n ;

D_f is a Zero-One matrix，it is L*L，L is the number of datanode.

To enhance the data security of cloud computing, we provide a Cloud Computing Data Security Mode called C2DSM.It can be described as follows:

$$D'_f = C_A \text{（namenode）} \qquad (3)$$

$$D_f = \text{M. } D'_f \qquad (4)$$

$$K_f = E(f)\ D_f \qquad (5)$$

C_A (.): authentic visit to namenode；

D'_f :private protect model of file distributed matrix；

M：resolve private matrix；

$E(f)$ ：encrypted file f block by block，get the encrypted file vector；

This model can be show by Figure(14)

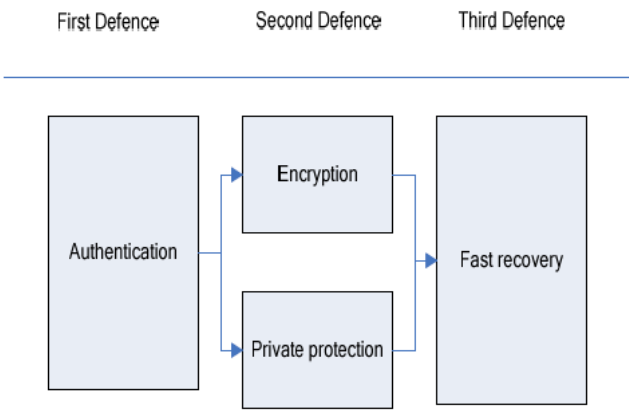


Fig 3.3: Data Security Model for Cloud Computing

VII. ANALYSIS

Example 1: Mogulus

□ Mogulus is a live broadcast platform on the internet.*(cloud customer)*

• Producers can use the Mogulus browser-based Studio application to create LIVE, scheduled and on-demand internet television to broadcast anywhere on the web through a single player widget.

□ Mogulus is entirely hosted on cloud *(cloud provider)*

□ On Election night Mogulus ramped to:

• 87000 videos @500kbps = 43.5 Gbps

• http://www.mogulus.com

Example 2: Animoto

□ Animoto is a video rendering & production house with service available over the Internet *(cloud customer)*

• With their patent-pending technology and high-end motion design, each video is a fully customized orchestration of user-selected images and music in several formats, including DVD.

□ Animoto is entirely hosted on cloud *(cloud provider)*

□ Released Facebook App: users were able to easily render their photos into MTV like videos

• Ramped from 25,000 users to 250,000 users in three days

• Signing up 20,000 new users per hour at peak

• Went from 50 to 3500 servers in 5 days

• Two weeks later scaled back to 100 servers

• http://www.animoto.com

Example 3: New York Times

□ Timesmachine is a news archive of the NY Times available in pdf over the Internet to newspaper subscribers *(cloud customer)*

□ Timesmachine is entirely hosted on cloud *(cloud provider)*

□ Timesmachine needed infrastructure to host several terabits of data

• Internal IT rejected due to cost

• Business owners got the data up on cloud for $50 over one weekend

• http://timesmachine.nytimes.com

Some other users:

□ Startups & Small businesses

• Can use clouds for everything

• SaaS, IaaS, collaboration services, online presence

□ Mid-Size Enterprises

• Can use clouds for many things

• Compute cycles for R&D projects, online collaboration, partner integration, social networking, new business tools

□ Large Enterprises

• More likely to have hybrid models where they keep some things in house

• On premises data for legal and risk management reasons Streamlined Security Analysis Process

Security Analysis

□ Identify Assets

• Which assets are we trying to protect?

• What properties of these assets must be maintained?

 Identify Threats

• What attacks can be mounted?

• What other threats are there (natural disasters, etc.)?

 Identify Countermeasures

• How can we counter those attacks?

 Appropriate for Organization-Independent Analysis

• We have no organizational context or policies

Identify Threats

 Failures in Provider Security

 Attacks by Other Customers

 Availability and Reliability Issues

 Legal and Regulatory Issues

 Perimeter Security Model Broken

 Integrating Provider and Customer Security Systems(15)

4.2 Approach to Cloud Computing

1. Amazon

Amazon is best known for selling books online, but they are also actively investing in services that allow developers to take advantage of their computing technology. Amazon Web Services provide developers use of open APIs to access Amazon's vast infrastructure in a manner vaguely reminiscent of timeshared computing. By using these APIs, developers can create interfaces and access the computing infrastructure provided by Amazon on a fee-based schedule, with the ability to grow as needed. Software developers, start-up companies, and established companies in need of reliable computing power are members of a large and growing crowd using Amazon services.

One of these services is the beta launch of Amazon Elastic Compute Cloud or EC2. The Amazon Elastic Compute Cloud provides virtualization for developers to load Amazon-managed machines with their preferred software environments and execute custom applications. This is accomplish by first creating an Amazon Machine Instance(AMI) with the operating system, custom configuration setting libraries, and all needed applications. Once created, the AMI is loaded into the Amazon Simple Storage service(AS3) and receives an unique identifier. The unique identifier can then be used to run as many instances of the AMI as needed using Amazons APIs. Additionally, Amazon provides a set of prebuilt AMIs that can be used by developers. Amazon is also now claiming location transparency for a globally distributed cloud. They are building out their computational footprint to be more geographically distributed. Additionally, they are improving fault tolerance by creating Availability Zones that will allow users to create instances of their applications in distributed regions.

2. Microsoft

Microsoft announced its Azure Services Platform In October,2008. Similar to the amazon approach, Microsoft is developing a cloud-based, hosted-services platform. In addition to providing compute and storage resources for consumers to develop and host applications, Microsoft is also offering cloud applications that are already developed and ready for consumption. The Azure Service Platform is built on the Windows Azure cloud operating system, which provides a development, hosting, and management environment for cloud applications. Numerous services are available on top of the Azure operating system including Live Services and .NET Services. During the Community Technology Preview, Azure is offered for free to allow users and consumers to test and evaluate it.

Once Azure is launched for commercial use it will be priced using a consumption-based model. Consumption will be measured in compute time, bandwidth, and storage and transactions (put and gets). Microsoft is using a combination of Microsoft .NET framework and the Microsoft Visual Studio development tools to provide a base for developers to easily launch new solutions in the cloud. It is noted that both applications running in the cloud and outside of the cloud can use the Azure cloud platform. For the initial offering, only applications built with .NET can be hosted, but Microsoft claims that this constraint will be relaxed for Azure in 2009. Windows Azure divides application instances into virtual machines (VMs) similar to the Amazon AMIs described earlier. Unlike the Amazon AMIs, a Windows Azure developer cannot supply his/her own VM image. Developers create Web role and Worker role instances, where a Web role accept incoming HTTP requests and Worker roles are triggered by Web roles via a queue. Any work performed by a Worker role instance can then be stored in the Azure storage or sent outside of the cloud network. Web role instances are stateless. To expand the performance of an application, multiple Worker role instances can be run across dedicated processor cores. If a Worker role or Web role fails, the Azure fabric restarts it.(11)

3. Other Cloud Computing Approaches and Applications

Amazon, Google, and Microsoft are not alone investing in computing as a service. Other organizations to test the waters include Dell, IBM, Oracle, and some universities. IBM is providing a variety of cloud-based services by using existing functionality and capabilities of the IBM Tivoli Portfolio . Tivoli is a collection of products and software services that can be used as building blocks to support IBM Service Management software. IBM.s cloud-based services, which target independent software vendors , offer design of cloud infrastructures, use of worldwide cloud computing centers, and integration of cloud services.

Many companies are delivering services from the cloud. Some notable examples as of 2010 include the following:

• **Google** — Has a private cloud that it uses for delivering many different services to its users, including email access, document applications, text translations, maps, web analytics, and much more.

• **Microsoft —** Has Microsoft® Sharepoint® online service that allows for content and business intelligence tools to be moved into the cloud, and Microsoft currently makes its office applications available in a cloud.

• **Salesforce.com** — Runs its application set for its customers in a cloud, and its Force.com and Vmforce.com products provide developers with platforms to build customized cloud services.(10)

Photograph4.1: Different cloud service providers

VIII. CONCLUSION AND FUTURE

To summarize, the cloud provides many options for the everyday computer user as well as large and small businesses. It opens up the world of computing to a broader range of uses and increases the ease of use by giving access through any internet connection. However, with this increased ease also come drawbacks. You have less control over who has access to your information and little to no knowledge of where it is stored. You also must be aware of the security risks of having data stored on the cloud. The cloud is a big target for malicious individuals and may have disadvantages because it can be accessed through an unsecured internet connection.

If you are considering using the cloud, be certain that you identify what information you will be putting out in the cloud, who will have access to that information, and what you will need to make sure it is protected. Additionally, know your options in terms of what type of cloud will be best for your needs, what type of provider will be most useful to you, and what the reputation and responsibilities of the providers you are considering are before you sign up.(16)

The three different service models for the delivery of cloud computing, IaaS, Saas, and PaaS, provide enterprises with the ability to mix and match the best service model to the business needs of their organization based upon requirements and payment options.(17)

Cloud Computing is a term that doesn't describe a single thing – rather it is a general term that sits over a variety of services from Infrastructure as a Service at the base, through Platform as a Service as a development tool and through to Software as a Service replacing on-premise applications. For organizations looking to move to Cloud Computing, it is important to understand the different aspects of Cloud Computing and to assess their own situation and decide which types of solutions are appropriate for their unique needs.(6)

FUTURE -

What Will Cloud Computing Be in Ten Years?

Customers do not care much about the technical details of computing. They only wish to receive answers every time and fast. Requested information must be available regardless of the computing device they use. Responses must be secure. There should be no restrictions as to the place from where they communicate. Information must be available for people authorized to make use of what they receive. The sources of information must include information received from people, from sensors or from public web sites. Information must be available to and from ground locations, ships, submarines airplanes and satellites. A user must be able to connect with every commercial enterprise on the Internet. (18)

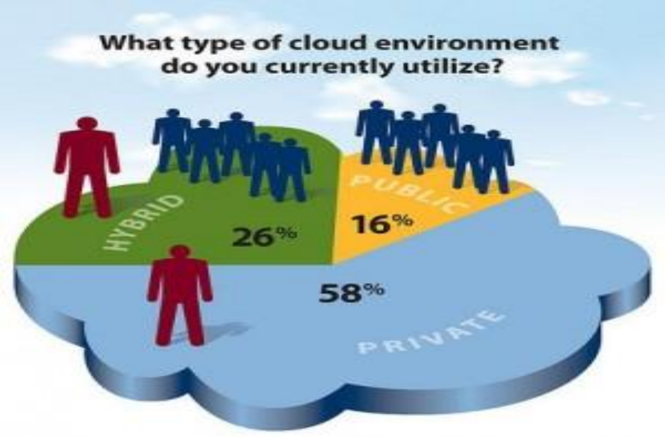


Fig 5.1: Current use of cloud (19)

So, what does the future hold for cloud computing? There are several likely trends we'll see in the next few years:

• **Cloud solutions beyond email and online storage will reach consumers.** While enterprises and larger businesses are already using cloud solutions for many different types of applications, at this point the two areas that have hit the consumer world have been storage and email. Those two areas will doubtlessly grow, but we'll also see increasing popularity for other applications.

• **Smartphone will become consumers' hubs for cloud applications.** The beauty of cloud applications is that they can be run on many different types of devices and from anywhere with an Internet connection. For most users, that means access via smartphones. Users always have smartphones on hand, and smartphones bring Internet capability right along with them.

• **Home users will dabble in "thin" clients.** The thin client will never take over the home consumer space, largely because the capability to provide intense graphics for gaming and other uses requires beefy hardware. That said, for users who operate primarily in the cloud, low-end "disposable" appliance-type computers will continue to gain ground. The $100 off-the-shelf PC isn't that far away, and cloud computing will only serve to push the market further in that direction.

• **The Fermium model will continue to grow and dominate the cloud.** The most widely used cloud application – Gmail – is free to end users. Most consumer cloud applications offer a free basic version, but charge a premium for advanced features or more resources. Freemium and subscription models will continue to duke it out, with most vendors going for a hybrid of the two.

Cloud computing will add to the Apple/Google feud. Cloud solutions are just fuel on the fire. In some ways, the competition is good for the marketplace. For consumers stuck in the middle, though, it will be frustrating, especially as the major players offer fewer and fewer options for using or connecting to the competitor's product. Accessing iCloud on an Android, for example, is a non-starter. This may lead to dominance for one or the other, or it may mean opportunity for plenty of third parties who are able to provide truly cross-platform cloud solutions. In the end, that's probably the best scenario, as cross-platform functionality should be at the heart of any cloud computing solution.(19)

REFERNCES

[1] http://www. .princeton.edu/~ddix/risks-benefits.html 1
[2] http://en.wikipedia.org/wiki/Cloud_computing 2
[3] IEEE paper on The Security Issues of Cloud Computing Over Normal & IT Sector, International Journal of Advanced Research in Computer Science and Software Engineering. 3
[4] http://docs.media.bitpipe.com/io_10x/io_100433/item_419065/HPIntel_sCloudComputing_SO%23034437_E-Guide_052611.pdf 10
[5] http://www.keane.com/resources/pdf/WhitePapers/Cloud-Computing-Risks-and-Benefits.pdf 6
[6] http://broadcast.rackspace.com/hosting_knowledge/whitepapers/Understanding-the-Cloud-Computing-Stack.pdf 7
[7] http://cscjournals.org/csc/manuscript/Journals/IJCN/volume3/Issue5/IJCN-176.pdf 8
[8] http://mygreatname.com/set-up-linux-apache-server/how-to-set-up-linux-apache-server-08.htm 11
[9] PPT_A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications 5
[10] White Paper on Introduction to Cloud Computing, www.dialogic.com.21
[11] http://www.nsa.gov/research/_files/publications/cloud_computing_overview.pdf20

[12] https://wiki.cloudsecurityalliance.org/guidance/index.php/Cloud_Computing_Architectural_FrameworkWhat Comprises Cloud Computing? 13

[13] http://www.nsa.gov/research/_files/publications/cloud_computing_overview.pdf17

[14] IEEE paper on Data Security Model for Cloud Computing, Proceedings of the 2009 International Workshop on Information Security and Application (IWISA 2009)18

[15] Cloud Computing: Finding the Silver Lining, Steve Hanna, Juniper Networks19

[16] The Basics of Cloud Computing,pdf.US-CERT15

[17] http://www.keane.com/resources/pdf/WhitePapers/Cloud-Computing-Risks-and-Benefits.pdf22

[18] http://pstrassmann.blogspot.in/2011/05/what-will-cloud-computing-be-in-ten.html23

[19] http://www.techcrates.com/the-probable-future-of-cloud-computing/24

Ms. Pranita P. Khairnar has completed her B.E(Electronics) & currently appear to M.E(Electronics) at Amrutvahini College of Engineering, Sangamner. Dist.- Ahmednagar, Maharashtra, India.

Prof. V. S. Ubale, has completed her M.E.(Electronics) & B.E. (E& TC). He is working as a Assistant Professor in Electronics Department, Amrutvahini College Of Engineering, Sangamner, Dist. Ahmednagar, Maharashtra, India. Prof Ubale has teaching experience of 11 years to Undergraduate, Graduate & Post Graduate Students. Prof V. S Ubale has Published 02 papers in International Journal,& presented 04 papers in International Conference & 03 papers in National Conferences